

Pepwave Surf SOHO

User Manual

Pepwave Product:

Surf SOHO

Pepwave Firmware 8.1.2 May 2021

COPYRIGHT & TRADEMARKS

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

Table of Contents

Introduction and Scope	5
Glossary	6
Product Features LAN VPN Firewall Outbound Policy QoS Other Supported Features	8 8 9 9 9 9
Pepwave Surf SOHO Router Overview	10
Panel Appearance	10
LED Indicators	13
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	14 14 15 15 15 15
Installation	17
Preparation	17
Constructing the Network	17
Connecting to the Web Admin Interface	17
SpeedFusion Cloud	21
Activate SpeedFusion Cloud Service	21
Enable SpeedFusion Cloud	23
Connect Clients to Cloud	31
Link Wi-Fi to Cloud	32
Optimize Cloud Application	34
Configuring the LAN Interface(s)	35
Network Settings	35
Port Settings	42
Configuring the WAN interface	43
WAN > Quality Monitoring	43
WAN > Ethernet WAN	44
WAN > Physical Interface Settings	45

WAN > Health Check Settings	46
WAN > Bandwidth Allowance Monitor	141
WAN > Additional IP Address Settings	49
WAN > Dynamic DNS Settings	49
Wi-Fi WAN and USB WiFi Network connection	50
WAN > WiFi Connection Profiles	141
WAN > Signal threshold settings	54
Indication of WiFi strength values:	54
PepVPN	55
PepVPN > Send ALL traffic	59
Outbound Policy Management	60
Port Forwarding	63
UPnP / NAT-PMP Settings	65
NAT Mappings	66
QoS	68
Bandwidth Control	68
Application Prioritization	68
Firewall	70
Outbound and Inbound Firewall Rules	71
Intrusion Detection and DoS Prevention	75
Content Blocking	76
Routing Protocols	77
OSPF & RIPv2	77
BGP	80
Remote User Access	83
L2TP with IPsec	83
OpenVPN	83
PPTP	84
Authentication Methods	84
Miscellaneous Settings	86
RADIUS Server	86
Certificate Manager	88
Service Forwarding	88
Service Passthrough	90
Grouped Networks	91
SIM Toolkit	92
AP	95
Wireless SSID	95
Settings	100

System Settings	102
Admin Security	102
Firmware	106
Time	107
Schedule	108
Email Notification	109
Event Log	112
SNMP	113
InControl	115
Configuration	115
Feature Add-ons	116
Reboot	116
Tools	117
Ping	117
Traceroute Test	118
Wake-on-LAN	118
WAN Analysis	119
Status	123
Device	123
Active Sessions	125
Client List	127
OSPF & RIPv2	128
BGP	128
PepVPN Status	128
Event Log	131
WAN Quality	132
Usage Reports	133
Appendix A: Restoration of Factory Defaults	137
Appendix B: Declaration	138

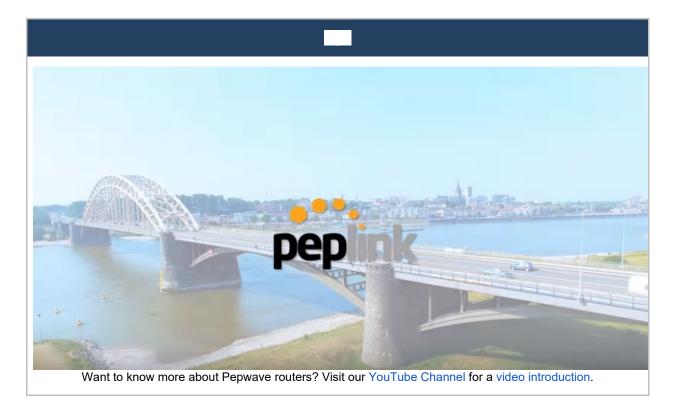


Introduction and Scope

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:

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
ТСР	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

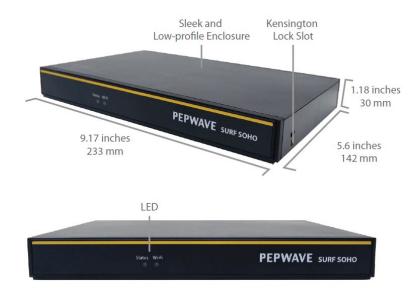
- Quality of service for different applications and custom protocols
- User group classification for different service levels
- Bandwidth usage control and monitoring on group- and user-level
- Application prioritization for custom protocols and DSL/cable optimization

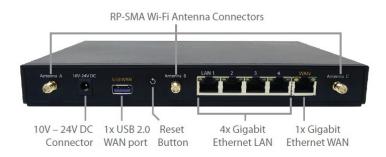
Other Supported Features

- 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





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

LED Indicators

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

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

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

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</u> <u>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-know-about-it/29658

Wi-Fi Air Monitoring

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

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

```
    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).



Installation

The following section details connecting Pepwave routers to your network.

Preparation

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

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

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

Constructing the Network

Construct the network according to the following steps:

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

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

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

Connecting to the Web Admin Interface

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

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

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

PEPWAVE	
Copygni 6 Papuna, Ali ngita nasrwal.	Login Username: Password: Login

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	АР	System	Status		Apply Changes
	You mu	st change your default	naceword n		4				
				ow to procee	u				
	Change Current P	Password assword							
	New Pass	word			0				
	Confirm I	New Password	Require at	least 10 chara	cters,	lower and u	upper case	, with numbe	ers.
				Save and	d appl	Y			

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

PEPWAVE	Dashboard Spe	edFusion Cloud Net	vork Advanced	AP System	Status	Apply Changes
	WAN Connect					?
	Priority 1 (High		ected to 🔆 📖	·	Wireles	s Networks Details
	Priority 2	No Ci	ble Detected			Details
	Priority 3 Disabled		rag desired (Priority	y 3) connections h	ere	
	Wi-Fi WAI	N on 2.4 📋 Disat	led			Details
	LAN Interface					
	Router IP Addr	ess: 192.168.50.1				🗧 ON 🗸 Details
	PepVPN					Status
			🧧 Esta	blished		
	Device Inform Model: Firmware: Uptime: CPU Load: Throughput:	Pepwave Surf 8.1.1 build 49 0 days 10 hot 92.0 kbps	94 Irs 6 minutes 39%			
		tance Status: 📒 Turn				
			opyright © Pepwav	e. All rights reserv	ed.	

The **Dashboard** shows current WAN, LAN, and Wi-Fi AP statuses. Here, you can change WAN connection priority and switch on/off the Wi-Fi AP.



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

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



SpeedFusion Cloud

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



*SpeedFusion Cloud is supported in firmware version 8.1.0 and above. SpeedFusion Cloud is a subscription basis. SpeedFusion Cloud license can be purchased at <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.

peplink	Dashboard	Setup Wizard	SpeedFusion Cloud	Network	AP System	Status	Apply Changes
	a S	peedFus	ion Cloud				
	Aggregate y	our bandwidth, conn	ect you to different geo-location	on, and more.			
	<u>ب</u>		ivation key now licious features powered by S	SpeedFusion.			
		Choose Clou Which cloud yo	d Location u'd like to connect?				
		Connect Clie Select a cloud f	nts to Cloud or your laptops, phones, or o	ther devices.			
Logout	((t-	Link Wi-Fi to Create a Wi-Fi	Cloud SSID that is dedicated for the	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 Fr	ee 30-Day Trial			
Please select the devices to activate. On	ly eligible devices will be displayed.			
Y FILTER				
Groups All	Model V All	Device Name ✓ Please Enter	Serial Number Please Enter	
Total: 2 eligible device(s)				Grid 📕 List
☑ ▼				l device(s) selected
	MAX Hotspot LTE (Europe/Int'l GSM) MAX			
Devices Per Page 25 💙				ACTIVATE

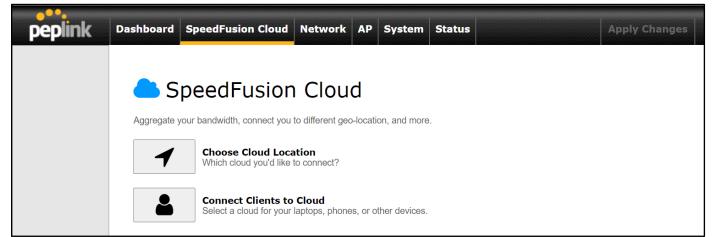


From **System > Features Add-ons**, paste the license key into the window and click on **Activate** once you have received the license key.

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	АР	System	Status	Apply Changes
System								
 Admin Security 	Feature	Activation						
 Firmware 	Activation	і Кеу						a6199b23e54fe148f876e75
 Time 								249c5af05ef747c958e346e 56afa46e34db668f55dff5ff
 Schedule 			75dff46f80	9dd4cef09be1	8a619	9d16bbfa96	5c3083b48a7d33	37ade187a5ce2e4e1
Email Notification								
Event Log				Activ	ate			
SNMP								
 SMS Control 								
 InControl 								
 Configuration 								
 Feature Add-ons 								
 Reboot 								
Tools								
Ping								
 Traceroute 								
Wake-on-LAN								
WAN Analysis								

Enable SpeedFusion Cloud

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

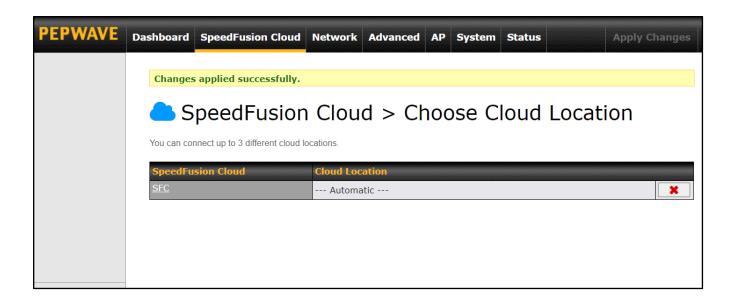


Choose Automatic > Click on the green tick button to confirm the change.

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System	Status		Apply Cl	hanges
				d > Cł	າວດ	ose C	loud	Locat	ion	
	SpeedFu	sion Cloud	United Sta	atic atic (SYD) (FRA) O)					~	

Click on Apply Changes to save the change.

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP S	System	Status	Apply Changes	
	less s	Changes will be effectiv peedFusion	ı Clou		-	-		ocation	/
	SpeedFu SFC	sion Cloud	Cloud Loc Automa					*	



PEPWAVE	Dashboard SpeedFusion (Cloud Network	Advanced	AP System	Status	Apply Changes
	WAN Connection Status Priority 1 (Highest)		hannannan			?
	Priority 2	Drag de	esired (Priority 1	.) connections h	ere	
	Cellular 1	II 📒 Connected t	to MY MAXIS 🛄	-A		Details
	2 Cellular 2	📶 🦲 Connected t	to MY MAXIS 🛄	A		Details
	Priority 3	Drag d	esired (Priority 3) connections h	ere	
	Disabled			.,		
	1 WAN 1	Disabled				Details
	2 WAN 2	Disabled				Details
	诸 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: 192.168	3.50.1				
	Wi-Fi AP					ON 🗸 Details
	SpeedFusion Cloud SFC Data usage allowance: 98.4	0 CR (Expipy data:	Establi	shed		
	Data usage anowance: 98.4	o de (Expiry date:	5ep 01, 2020)			

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



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	າວດ	ose C	loud	Locat	ion
	SpeedFu SFC	sion Cloud	Cloud Loc Automa						*

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 Cl	nanges
										×
		sion Cloud Profile								
	Enable Cloud Loo	ation	Automa	tic 🗸						_
			·							
	1 - De	efault +								
	Tunn	el Options							hin	
	Local	/ Remote Tunnel ID	1 (default	tunnel)						
	Tunne	l Name	Default							
	Data	Port 🤅	🔍 🔍 Auto	Custom						
	Bandy	vidthLimit 🤇 🤅								
	WAN	Smoothing 🤅	Overall Red	lundancy Level				Off 🗸		
			Maximum L	evel on the Sam	e Link			Off 🗸		
	Forwa	rd Error Correction	Off	~						
	Receiv	ve Buffer 🤶	0	ms						

PEPWAVE	Dashboard SpeedFusion Cloud Network Advanced AP System Status App	ly Changes
		×
	SpeedFusion Cloud Profile	
	Enable 🗹	
	Cloud Location Automatic 🗸	
	1 - Default 2 - WAN Smoo * +	
	Tunnel Options	
	Local / Remote Tunnel ID 2	
	Tunnel Name WAN Smoothing	
	Data Port 🕐 🔍 Auto 🔿 Custom	
	Bandwidth Limit 🕐 🗌	
	WAN Smoothing 🕐 Overall Redundancy Level Normal 🗸	
	Maximum Level on the Same Link Normal V	
	Forward Error Correction 🕐 Off 🗸	
	Receive Buffer 🕐 🛛 ms	



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

WAA Connection Status (*) Priority 1 (Highest) Drag desired (Priority 1) connections have Priority 2 (*) (*) Cellular 1 (*) (*) Cellular 2 (*) (*) Connected to MY MAXIS (*) Details (*) Disabled Details (*) Orag desired (Priority 3) connections here Disabled (*) VAN 1 Disabled Details (*) VAN 2 Disabled Details (*) Cellular 3 Disabled Details (*) Wi-H MAN Disabled Details (*) LAN 1 as WAN Disabled Details <t< th=""><th>PEPWAVE</th><th>Dashboard SpeedFusion (</th><th>Cloud Network</th><th>Advanced AP</th><th>System Status</th><th>Apply Changes</th></t<>	PEPWAVE	Dashboard SpeedFusion (Cloud Network	Advanced AP	System Status	Apply Changes
Priority 2 If Cellular 1 and Connected to MY MAXIS INTEA If Cellular 2 and Connected to MY MAXIS INTEA Priority 3 Drag desired (Priority 3) connections here Disabled If WAN 1 Disabled If Cellular 3 Disabled If Cellular 3 Disabled If Cellular 3 Disabled If Cellular 4 Disabled If LAN 1 as WAN Disabled If LAN 2 as WAN Disabled Details If LAN 3 as WAN Disabled If AN 1 interface Router IP Address: 192.168.50.1 Wi + If AP ON v Details If PEPWAVE_EBB4			Drag do	sired (Drigrity 1) of	apportions berg	0
Image: Connected to MY MAXIS [112] Details Image: Connected to MY MAXIS [112] Details Priority 3 Drag desired (Priority 3) connections here Disabled Details Image: WAN 1 Disabled Image: WAN 2 Disabled Image: WAN 3 Disabled Image: WAN 4		Driority 2	Diag de	siled (Phoney 1) ce	Sinections nere	
Priority 3 Disabled 1 WAN 1 Disabled 2 WAN 2 Disabled 1 Cellular 3 Disabled 1 Cellular 3 Disabled 1 Cellular 3 Disabled 1 Cellular 4 Disabled 1 Cellular 4 Disabled 1 Cellular 4 Disabled 1 LAN 1 as WAN Disabled 1 LAN 2 as WAN Disabled 1 LAN 2 as WAN Disabled 1 LAN 2 as WAN Disabled 1 LAN 3 as WAN Disabled 1 Details 1 LAN 1 Interface Router IP Address: 192.168.50.1 Wi-Fi AP 0 N ∨ Details ▼ PEPWAVE_EBB4		62	Connected to	MY MAXIS LTEA		Details
Drag desired (Priority 3) connections here Disabled ① WAN 1 Disabled ② WAN 2 Disabled ③ Cellular 3 Disabled ③ Cellular 3 Disabled ④ Cellular 4 Disabled ④ Wi-Fi WAN Disabled ④ Wi-Fi WAN Disabled ● LAN 1 as WAN Disabled ● LAN 2 as WAN Disabled ● LAN 3 as WAN Disabled ● LAN 3 as WAN Disabled ● PEPWAVE_EBB4 ON ▼ Details		-3	Connected to	MY MAXIS LTEA		Details
Disabled Details 1 WAN 1 Disabled Details 2 WAN 2 Disabled Details 1 Cellular 3 Disabled Details 1 Cellular 4 Disabled Details 1 Cellular 4 Disabled Details 1 Cellular 4 Disabled Details 2 UAN 1 Disabled Details 2 LAN 1 Disabled Details 2 LAN 2 Disabled Details 2 LAN 3 Disabled Details 2 LAN 3 Disabled Details 2 LAN 3 Disabled Details 3 LAN 3 Disabled Details 3 LAN 1 Disabled Details 3 LAN 1 Disabled Details 3 N Disabled Details 3 N Disabled Details 3 N Disabled Details 3 PEPWAVE_EBB4 ON < Details		Priority 3	Drag de	sired (Priority 3) of	onnections here	
I WAN 1 Disabled Details 2 WAN 2 Disabled Details I Cellular 3 Disabled Details I Cellular 4 Disabled Details I LAN 1 as WAN Disabled Details I LAN 2 as WAN Disabled Details I LAN 3 as WAN Disabled Details I LAN 1 Interface Mirit AP ON ✓ Details I PEPWAVE_EBB4 ON ✓ Details ON ✓ Details		Disabled	brag de	since (Friding 5) co		
Image: SpeedFusion Cloud		1	Disabled			Details
Image: Cellular 4 Disabled Image: Cellular 4<		2 WAN 2	Disabled			Details
Image: SpeedFusion Cloud						
3 LAN 1 as WAN Disabled Details 4 LAN 2 as WAN Disabled Details 5 LAN 3 as WAN Disabled Details LAN Interface Router IP Address: 192.168.50.1 Wi-Fi AP ON ✓ Details SpeedFusion Cloud		14 Cellular 4	Disabled			Details
 4 LAN 2 as WAN Disabled Details 5 LAN 3 as WAN Disabled Details LAN Interface Router IP Address: 192.168.50.1 Wi-Fi AP ON ✓ Details SpeedFusion Cloud		🗟 Wi-Fi WAN	Disabled			Details
5 LAN 3 as WAN Disabled Details LAN Interface Router IP Address: 192.168.50.1 Wi-Fi AP ON ✓ Details Image: Contract of the image of the im		3 LAN 1 as WAN	Disabled			Details
LAN Interface Router IP Address: 192.168.50.1 Wi-Fi AP ■ ON ▼ Details © ● PEPWAVE_EBB4 SpeedFusion Cloud		4 LAN 2 as WAN	Disabled			Details
Router IP Address: 192.168.50.1 Wi-Fi AP ♥ ● PEPWAVE_EBB4 SpeedFusion Cloud		5 LAN 3 as WAN	Disabled			Details
Wi-Fi AP ON ∨ Details Image: SpeedFusion Cloud Image: SpeedFusion Cloud		LAN Interface				
		Router IP Address: 192.168	8.50.1			
SpeedFusion Cloud		Wi-Fi AP				ON 🗸 Details
SFC (1 - Default) Established		SpeedFusion Cloud				
		SFC (1 - Default)		📒 Establishe	d	
SFC (2 - WAN Smoothing) Established		SFC (2 - WAN Smoothing)		📒 Establishe	d	
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)		Data usage allowance: 98.4	10 GB (Expiry date: S	ep 01, 2020)		



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

PEPWAVE	Dasl	hboard	SpeedFusion	Cloud	Network	Advanced	АР	System	Status			Changes
Advanced												
 SpeedFusion 		Outboun	d Policy									?
IPsec VPN	(Custom										
GRE Tunnel												
 Outbound Policy 		Add a l	New Custom R	tule							×	?
Port Forwarding												
NAT Mappings		Service	Name		to_internet		ļ					
QoS		Enable			Z							
User Groups		Source		?	IP Address	✔ 192.16	8.50.1	.0				×
 Bandwidth Control 		Destina	tion	<u> </u>	Any	~						
 Application 		Protoco		?	Any 🗙 🗲 ::	Protocol Selec	tion ::	~				
Firewall		Algorith	m	?	Priority	~						
 Access Rules 		Priority	Order	?	Hiahest Priori	tv		Not In U	Jse			<u>(?)</u>
Content Blocking						(1 - Defau						
				Ļ	Cloud: SFC	(2 - WAN		┛				
Routing Protocols					WAN: WAN			-				
OSPF & RIPv2					WAN: Cellu							
BGP					WAN: Cellu							
Remote User Access					WAN: Cellu WAN: Cellu							
Misc. Settings					WAN: USB			_				
 High Availability 					WAN: Wi-F			-				
RADIUS Server					WAN: LAN							
 Certificate Manager 					WAN: LAN Lowest Priorit							
 Service Forwarding 		When N Availabl	o Connections ar e	re ?	Drop the Traf	fic 🗸]					
 Service Passthrough 			te Sessions on ion Recovery	?	🗌 Enable							
GPS Forwarding												
NTP Server									Save	Cance		
 Grouped Networks 									Curre			

Outbound Policy Custom					?
Rules (^W Drag and drop Service	rows by the left to chan Algorithm	ge rule order) Source	Destination	Protocol / Port	?
		SPF / BGP / RIPv2 F Fusion Cloud Routes		, Fore	
<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					() ()

Connect Clients to Cloud

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

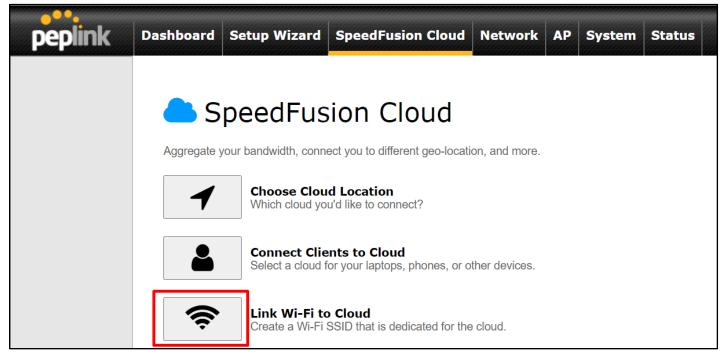
peplink	Dashboard	SpeedFusion Cloud	Network	AP	System	Status		Apply Changes
	i Sp	peedFusion	Cloud	d				
	Aggregate yo	ur bandwidth, connect you t	to different geo	locatio	on, and more			
	4	Choose Cloud Loca Which cloud you'd like t						
		Connect Clients to Select a cloud for your I		s, or ot	her devices.			

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

peplink	Dashboard	SpeedFusion Cloud	Network	AP	System	Status			Apply C	hanges
	Saved! C	Changes will be effectiv	e after click	ting t	he 'Apply (Changes'	button.			
	a S	peedFusion	Cloud	d >	> Cor	nnect	t Cli	ents to C	Cloud	
		the selected clients will be re	directed to the	assign	ed cloud.					
	Automatic		Client					IP Address		
			MY-Room-/	A-Dell	PC (40:23:	43:26:F7:	93)	192.168.52.179		×
							~			+
					Save					

Link Wi-Fi to Cloud

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





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

peplink	Dashboard	Setup Wizard	SpeedFusion Cloud	Network	АР	System	Status		Apply Change	es
	a S	peedFus	sion Cloud >	> Link	W	'i-Fi t	o Clo	bud		
	The new SS	BID will inherit all setti	ings from the existing SSID ir	cluding the Se	curity F	Policy.				
	SpeedFu	sion Cloud		hindhidd	iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	hindhid		hhhhh		
	Automatio		Reference SSID		SSID	for Cloud				
			Home		Hom	ne_SFC			×	
				~					+	
				Save						

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

LAN Interface						
Router IP Address: 192.168.54.1						
Wi-Fi AP				ON ✓ Details		
穼 🔒 HomeBunker	奈 🔒 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**.

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	АР	System	Status	Apply Changes
	a S	peedFusion	l Clou	d				
	Aggregate	your bandwidth, connect you	to different geo	o-location, and m	ore.			
	<u> </u>	Get your activation Enjoy all the delicious f		ed by SpeedFusi	ion.			
	4	Choose Cloud Loca Which cloud you'd like						
	-	Connect Clients to Select a cloud for your		es, or other devic	es.			
	(î;	Link Wi-Fi to Cloud Create a Wi-Fi SSID th		for the cloud.				
		Optimize Cloud Ap Connect to Google, Mic		and others using	the Ck	oud.		

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 wi	Il be redirected to the assigned cloud.					
Singapore (SIN)						
SFC-SIN	Cloud Application					
	Zoom	×				
	[v]	+				
	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	
VLAN1	1	2.2.2.2/24	×
VLAN2	2	3.3.3.3/24	×
New LAN			

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

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

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

IP Settings IP Address	255.255.0 (/24)
IP Address	The IP address and subnet mask of the Pepwave router on the LAN.

Network Settings		?	
Name		Help	<u>Close</u>
VLAN ID		To define a layer-2 bridging bas PepVPN, please click <u>here</u> .	sed
Inter-VLAN routing			

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 Bridg	ing		?
PepVPN Profiles to Bridg	e ?	No profile is available	Help <u>Close</u>
Spanning Tree Protocol			If you want to enable DHCP Option 82 Injection, please click <u>here</u> .
Override IP Address when ? bridge connected		${ullet}$ Do not override ${ullet}$ Static ${ullet}$ By DHCP ${ullet}$ As None	This allow the device to inject Option 82 with Router Name information before forwarding the DHCP Request
DHCP Server			packet to PepVPN peer, such that the DHCP Server can identify where does this request come from.
PepVPN Profiles to Bridge	Layer 2 P	ote network of the selected PepVPN profiles will be brid epVPN, they will be connected and operate like a single l vill be sent over the VPN.	

Remote Network Isolation	Enable this option if you want to block network traffic between the remote networks, this will not affect the connectivity between them and this local LAN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
Override IP Address when	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.
bridge connected	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.
	Click on the question Mark if you want to enable DHCP Option 82.
DHCP Option 82	This allows the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to a PepVPN peer, such that the DHCP Server can identify where the request originates from.

DHCP Server						
DHCP Server	?	Enable				
DHCP Server Logging	Help					
IP Range	built-	k the Enable box to enable the in DHCP server which serves			255.255.255.0 (/24)	T
Lease Time	If yo	P requests on the LAN. u want to enable DHCP relay er, click <u>here</u> .	i O Mir	าร		
DNS Servers		Assign DNS server aut	tomatically			
BOOTP						
Extended DHCP Option		Option		Value		
		No Extended DHCP Option				
				Add		
DHCP Reservation	?	Name	MAC Addres	S	Static IP	
			00:00:00:0	0:00:00		+

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.
Enable logging of DHCP events in the eventlog by selecting the checkbox.
These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
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.
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.
Check this box to enable BOOTP on older networks that still require it.
In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the Add button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
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



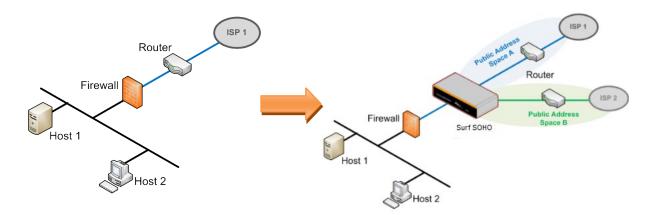
remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3**.

DHCP Relay Settings	
DHCP Relay) 🗹 Enable
DHCP Server IP Address	DHCP Server 1: DHCP Server 2:
DHCP Option 82	
DHCP Relay Logging	

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

Drop-In Mode

Drop-in mode (or transparent bridging mode) eases the installation of the Surf SOHO on a live network between the firewall and router, such that changes to the settings of existing equipment are not required. The following diagram illustrates drop-in mode setup:





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

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

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

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

Drop-In Mod	e Settings	
Enable		
WAN for Drop-	In Mode ?	WAN Apply NAT on VLAN networks outgoing Internet traffic VLAN network(s) may route their outgoing Internet traffic to this unit. When this checkbox is checked their traffic will be NAT'd before forwarding out of this WAN. Leave this checkbox checked if you are not sure.
Share Drop-In	IP ?	
Shared IP Add	ress ?	255.255.255.0 (/24) 🗸
Static Route		Destination Network Subnet Mask
		255.255.255.0 (/24) 🗸 🕂
WAN Default G	iateway 🕐	I have other host(s) on WAN segment IP Address
		▲
WAN DNS Serv	vers ?	DNS server 1: DNS server 2:
NOTE: The DH	CP Server Settings w	/ill be overwritten.
The following \ Dynamic DNS		overwritten: Connection Method, MTU, Health Check, Additional Public IP, and
The PPTP Serv	er will be disabled.	
Tip: please rev	view the DNS Forward	ding setting under the Service Forwarding section.
Enable		es the installation of the Surf SOHO on a live network between the existing firev nat no configuration changes are required on existing equipment. Check the box mode feature.
l for Drop-In Mode	Select the WAN po be disabled automa	ort to be used for drop-in mode. If WAN is selected, the high availability feature atically.
red Drop-In IP ^A	notification, remote	s enabled, the passthrough IP address will be used to connect to WAN hosts (en e syslog, etc.). The SOHO will listen for this IP address when WAN hosts accur by the SOHO (web admin access from the WAN, DNS server requests, 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.
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.)
	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.).

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

Static Route Settings				?
Static Route	Destination Network	Subnet Mask	Gateway	
	192.168.113.0	255.255.255.0 (/24) 🔻	192.168.112.10	×
		255.255.255.0 (/24) 🔻		+

Static Route	This table is for defining static routing rules for the LAN segment. A static route consists of th network address, subnet mask, and gateway address. The address and subnet mask values are <i>w.x.y.z</i> format.
	The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote route sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnet 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 interfac Any traffic destined for a network/mask pair will be directed to the corresponding gateway instead routed through WANs.

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

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

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

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

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

DNS Proxy Settings			?
Enable			
DNS Caching			
Include Google Public DNS ? Servers			
Local DNS Records	Host Name	IP Address	
			+
Domain Lookup Policy 🔗 ?	Domain	Connection	
			• +
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 shown with		

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 . 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.		
DNS Resolvers ^A	Check the box to enable the WINS server. A list of WINS clients will be displayed at Network>LAN>DNS Proxy Settings>DNS Resolvers . This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion [™] peer is selected, you may enter the VPN peer's DNS resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.		

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

Port Settings

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

Port	Port Settings			
	Name	Enable	Speed	Advertise Speed
1	LAN Port 1			
2	LAN Port 2		Auto	
3	LAN Port 3		Auto 🔻	
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.

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.

WAN Connection Status			?
Priority 1 (Highest)			
0	Connected		Details
Priority 2			
	📶 🦲 Standby	Wireless Networks	Details
Priority 3			
💿 ==== = ====	Cold Standby	Wireless Networks	Details
Priority 4 (Lowest)			
	Drag desired (Priority 4) connections here		
Disabled			
	Drag desired (Disabled) connections here		
WAN Quality 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.

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.





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 •		
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 ○ Disconnect		
Reply to ICMP Ping	● Yes ○ No		
Upload Bandwidth	10 Mbps •		
Download Bandwidth	110 Mbps •		

WAN Connection Name	Enter a name to represent this WAN connection.
Hume	
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
	L2TPGRE
	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 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 it when this WAN connection is no longer in the highest priority and has entered the standby state.	
Reply to ICMP PingIf No is selected, this option is disabled and the system will not reply to any ICMP ping echo require to the WAN IP addresses of this WAN connection(Default option is "Yes")		
Upload Bandwidth	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.	
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.	

WAN > Physical Interface Settings

Port Speed	This setting specifies port speed and duplex configurations of the WAN port. By default, Auto is selected and the appropriate data speed is automatically detected by the Pepwave router. In the event of negotiation issues, the port speed can be manually specified. You can also choose whether or not to advertise the speed to the peer by selecting the Advertise Speed checkbox.
ΜΤυ	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 rur each time the WAN connection establishes.



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

MAC Address Clone	Some service providers (e.g., cable providers) identify the client's MAC address and require the client to always use the same MAC address to connect to the network. In such cases, change the WAN interface's MAC address to the original client PC's MAC address via this field. The defau MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient Clicking Default restores the MAC address to the default value.
VLAN	Click the square if you wish to enable VLAN functionality for the WAN connection and enable multiple broadcast domains. Once you enable VLAN, you will be able to enter a name for 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: Vise first two DNS servers as PING Hosts	
Timeout ?	5 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 your to keep track of network usage. To enable this function, connect to the Web Admin Interface and go to Network WAN. Check the box Enable next to Bandwidth Allowance Monitor and you can see the following:

Bandwidth Allowance Monitor		
Bandwidth Allowance Monitor	?	✓ 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.

peplink PEPWAVE



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 Setting	is menerican and a second s
Additional IP Address (IP Address Subnet Mask 255.255.255 (/32)

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 the list pressina the Delete after them in the list. from bv button selectina 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 no-ip.org	
Confirm Password	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	O Auto O Custom Edit Channels:				
Output Power	Max 🔻 🗖 Boost				
Data Rate	• Auto O 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				

Channel Width	choose between the av	choose between the available options 20 Mhz, 20/40Mhz, 20/40/80 Mhz				
Channel Selection	Determine whether the following table will appe	ear:	utomatic	ally selecte	d. If you se	
	Edit auto channels	Clear 2.4 GHz:	All	₹3 ₹8	✔ 4 ✔ 9	 ✓ 5 ✓ 10
					ОК	Cancel
Output Power	Low, Medium, High, Ma	ax (boost options	for tickb	ox).		

	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 \fbox 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	
	WPA/WPA2-Personal	×
	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 V				
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: 				

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

OK

Cancel

	Security	Open •		
	• WEP			
	Security	WEP		
	Encryption Key			
		✓ Hide Characters		
	• WPA/WPA2 –			
	Security	WPA/WPA2-Personal		
	Shared Key 🤗	Image: Second secon		
	• WPA/WPA2 – I			
	Security	WPA/WPA2-Enterprise V		
	Login ID	WPA/WPA2-Enterprise •		
	Password			
	Confirm Password			
	EAP Method	PEAP T		
	EAP Phase 2 Method	EAP/CHAP T		
	EAP outer	Anonymous		
	authentication identity	User Credentials		
	WPA3 – Perso			
	WPA3 – Perso			
	Security	WPA3-Personal V		
	Shared Key	✓ Hide Characters		
	• WPA2/WPA3			
	Security	WPA2/WPA3-Personal		
	Shared Key			
		Hide Characters		
	• 802.1x with c	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	ion O Anonymous		
	identity	O User Credentials O Other:		
eferred BSSID	Configure the BSSIE	D; the BSSID is the MAC address of the wireless access point (WAP)		
Connection Method	Choose DHCP or Sta	tatic IP		
ONS servers	Configure the DNS servers that this WAN connection should use			

WAN > Signal threshold settings

Signal Threshold Settings				h			· · · · · · · · · · · · · · · · · · ·
Acceptable Level	•	•	a	at.,	att.	all	

If signal threshold is defined, this connection will be treated as down when a weaker than threshold signal is determined. The signal threshold can also be configured using values (this option can be enabled after selecting the question mark)

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

Indication of WiFi strength values:

-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 Peplink site-to-site VPN core engine of technology. establishing WAN It is ideal for а secure tunnel over any 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 Speed	Fusion Cloud	Network Ad	vanced AP S	System Status	Apply	Changes
Advanced							
PepVPN							
 GRE Tunnel 	PepVPN					AE	
Port Forwarding							
NAT Mappings	🗿 InControl man	agement enabled	d. Settings can no	v be configured o	n <u>InControl</u> .		
QoS	Profile	Remote 1	ID Ren	note Address(es	1		0
 Bandwidth Control 	Frome	Kennote		N Connection De			
 Application 				New Profile			
Firewall							
 Access Rules 	Send All Traffic	To					
 Content Blocking 	No PepVPN profile	selected					
Routing Protocols							
OSPF & RIPv2	Rules (Urag a	nd drop rows b	by the left to cha	nge rule order)			?
BGP	Service	Alor	orithm	Source	Destination	Protocol	
						/ Port	
Remote User Access	Service			(Auto)		7 Port	•
				(Auto) Add Rule		7 - 512	
Access						// Port	
Access Misc. Settings	PepVPN Local II)	SURF SOHO 8	Add Rule		// Port	
Access Misc. Settings RADIUS Server Certificate	PepVPN Local II		SURF_SOHO_8	Add Rule		77012	
Access Misc. Settings RADIUS Server Certificate Manager Service	PepVPN Local II Local ID PepVPN Setting) (Add Rule	ars)		Second
Access Misc. Settings RADIUS Server Certificate Manager Service Forwarding Service	PepVPN Local II Local ID)		Add Rule	ecs)		2
Access Misc. Settings RADIUS Server Certificate Manager Service Forwarding Service Passthrough Grouped	PepVPN Local II Local ID PepVPN Setting) (Recomment Fast (Appro Faster (App Extreme (U) 	Add Rule Add Rule	·	d higher bandwidth ov	erhead

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

PepVPN Profile		?
Name ?	4	
Active		
Encryption ?	● 🔒 256-bit AES ○ 🗗 OFF	
Authentication	Remote ID / Pre-shared Key	
Remote ID / Pre-shared Key	Remote ID	Pre-shared Key
		5
NAT Mode 📀		
Remote IP Address / Host ? Names (Optional)	If this field is empty, this field on the remote ur	it must be filled
Cast		
Cost ?	10	

1 2 3 * +

Local / Remote Tunnel ID	?	1 (default tunnel)
Tunnel Name		
Data Port	?	UDP 🔹 🖲 Auto 🔾 Custom
Bandwidth Limit	?	✓ Download: kbps ▼ (0: Unlimited) Upload: kbps ▼ (0: Unlimited)
Receive Buffer	?	0 ms
Use IP ToS		 Image: A state of the state of
Latency Difference Cutoff	?	500 ms
		Save Cancel

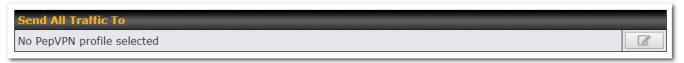
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, 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.



Multiple PepVPN profiles between the same 2 sites

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

PepVPN > Send ALL traffic



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

Send All Traffic	
Send All Traffic To	ONS Server 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	Intersection In	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 overheal 	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.

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**

Rules (\#Drag and drop rows by the left to change rule order)								
Service	Algorithm	Source	Destination	Protocol / Port				
	PepVPN	I / OSPF / BGP / F	IPv2 Routes					
HTTPS Persistence Enforced WAN: WAN Any Any TCP 443								
		Add Rule		·				

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

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

peplink PEPWAVE



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 R	ule	
Service Name		
Enable		
Source		Any 🔻
Destination	?	IP Network Mask: 255.255.255.0 (/24)
Protocol	?	Any Any Any
Algorithm	?	Enforced •
Enforced Connection	?	
		Save Cancel

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	 This field allows you to configure the default action when all the selected Connections are not available. Drop the Traffic - Traffic will be discarded.
Available	 Use Any Available Connections - Traffic will be routed to any available Connection, even it is no 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 thi 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	hinnin tinnin			
No Services Defined							
Add Service							

To define a new service, click Add Service.

Port Forward	ling	×			
Enable		8			
Service Name					
Protocol		TCP • + :: Protocol Selection :: •			
Port		Any Port			
Inbound IP Add (Require at leas address)		Connection / IP Address(es) All Clear Image: Connection / IP Address(es) Image: Clear Image: Clear Image: Clear Image: Clear Ima			
Server IP Addre	ess 🥐				
		Save Cancel			
Enable	This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.				
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore "_" characters.				
Protocol	The Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the Servers setting. Please see below for details on the Port and Servers settings. Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remain manually				



ort	the following ma	g specifies the port(s) that correspond to the service, and can be configured to behave in one anners: Ile Port, Port Range, Port Map, and Range Mapping
	Port	Image: Any Port Image: Any Port
	specified by the	affic that is received by the Pepwave router via the specified protocol is forwarded to the serve e Servers setting. For example, with IP Protocol set to TCP , and Port set to Any Port , all TC ded to the configured servers.
	Port	Single Port Service Port: 80
	forwarded via th	affic that is received by the Pepwave router via the specified protocol at the specified port ne same port to the servers specified by the Servers setting. For example, with IP Protocol s ort set to Single Port and Service Port 80, TCP traffic received on port 80 is forwarded to t
	configured serv	ers via port 80.
	configured serv	Port Range Service Ports: 80 - 88
	Port Port Range: tra is forwarded via IP Protocol set	Port Range Service Ports: 80 - 88 affic that is received by the Pepwave router via the specified protocol at the specified port ran the same respective ports to the LAN hosts specified by the Servers setting. For example, w
	Port Port Range: tra is forwarded via IP Protocol set	Port Range Service Ports: 80 - 88 affic that is received by the Pepwave router via the specified protocol at the specified port ran the same respective ports to the LAN hosts specified by the Servers setting. For example, w t to TCP , and Port set to Port Range and Service Ports 80-88, TCP traffic received on po
	Port Port Range: tra is forwarded via IP Protocol set 80 through 88 is Port Port Port Mapping:	Port Range Service Ports: 80 - 88 affic that is received by the Pepwave router via the specified protocol at the specified port range to the LAN hosts specified by the Servers setting. For example, we to TCP, and Port set to Port Range and Service Ports 80-88, TCP traffic received on points forwarded to the configured servers via the respective ports. Port Mapping Service Port: 80 Map to Port: 88
	Port Port Range: tra is forwarded via IP Protocol set 80 through 88 is Port Port Port Mapping: forwarded via a For example, w	Port Range Service Ports: 80 - 88 affic that is received by the Pepwave router via the specified protocol at the specified port ran to the same respective ports to the LAN hosts specified by the Servers setting. For example, we to TCP, and Port set to Port Range and Service Ports 80-88, TCP traffic received on ports forwarded to the configured servers via the respective ports. Port Mapping Service Port: 80 Map to Port: 88 traffic that is received by Pepwave router via the specified protocol at the specified port
	Port Port Range: tra is forwarded via IP Protocol set 80 through 88 is Port Port Port Mapping: forwarded via a For example, w 88, TCP traffic of	Port Range Service Ports: 80 - 88 affic that is received by the Pepwave router via the specified protocol at the specified port range to the LAN hosts specified by the Servers setting. For example, we to TCP, and Port set to Port Range and Service Ports 80-88, TCP traffic received on points forwarded to the configured servers via the respective ports. Port Mapping Service Port: 80 Map to Port: 88 traffic that is received by Pepwave router via the specified protocol at the specified port different port to the servers specified by the Servers setting. traffic that is received by Pepwave router via the specified protocol at the specified port different port to the servers specified by the Servers setting. trith IP Protocol set to TCP, and Port set to Port Mapping, Service Port 80, and Map to Port

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 W	izard	Network	AP	System	Status		Apply Changes
tatus									
 Device 	Forward	ed Ports							
 Ethernet Ports 	External 🔺	Internal	Intern	al Address	UPnP	/ NAT-PMP	Protocol	Description	
 Active Sessions 	8080	8080	192.10	68.1.10	UPnP		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)	
	G 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

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



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

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

Inbound firewall rules override the Inbound Mappings settings.



QoS

Bandwidth Control

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

Individual Bandwidth Limit	
Enable	
User Bandwidth Limit	Download Upload 0 Mbps ▼ 0 Mbps ▼ (0: Unlimited)

Application Prioritization

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

Application	Priority	?
-	Thigh ▼	*
	Thigh ▼	×
Sec. 24	↑ High ▼	×
	Thigh ▼	×
	Add	

https://www.peplink.com

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.

Туре	Supported Application	ns 🔍 Custom Applications
Category	Audio Video Streaming	
Application	Audio Video Streaming Database Email File Sharing / Transfer IM Miscellaneous Remote Access Security / Tunneling VoIP	Applications OK Cancel

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	\checkmark

PepVPN Traffic Optimization

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

PepVPN Traffic Optimization	
Enable	\checkmark



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 S	peedFusion Cloud N	etwork	Advanced	AP Syst	tem Status	Apply Cl	ianges
Advanced								
PepVPN	Outbound F	irewall Rules (\UDrag a	nd drop ro	ws by the left i	to change r	rule order)		?
 GRE Tunnel 	Rule	Protoco		•		Destination	Action	
Port Forwarding	<u>Default</u>	Any	Any			Any	O	i
NAT Mappings				Add Ru	ıle			
QoS	7 - 1 - 1 - 1	ewall Rules (Urag an	d drop rou	r hu tha laft ta	change au	le order)		
 Bandwidth 	Rule	ewall Rules (Corag an Protoco		Source	change ru	Destination	Action	?
Control	Default	Any	Any	Any		Any	Action	
 Application 	<u>.</u>	7.0.7	7.1.19	Add Ru	ule	7.1.19		
Firewall								
 Access Rules 	Internal Ne	twork Firewall Rules (Drag and	drop rows by	the left to	change rule order)		?
 Content Blocking 	Rule	Protoco				Destination	Action	
Routing Protocols	<u>Default</u>	Any	Any			Any	S	
 OSPF & RIPv2 				Add Ru	ule			
BGP								
Remote User Access		etection and DoS Preve	ention					?
Misc. Settings	Disabled							
RADIUS Server		ce Firewall Rules (\"Dra						
 Certificate 			ig and dro					?
Manager	Rule Default	Any		An	AN	Any	Action	
 Service Forwarding 	Delaute	007		Add Ru	<u></u>	OUY		<u> </u>
 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 drop rows by the left to change rule order)							
Rule	Protocol	Source	Destination	Action			
<u>test</u>	Any	Any	Any	0	×		
<u>Default</u>	Any	Any	Any	0			

Click Add Rule to display the following screen:

New Firewall Rule		
Rule Name		
Enable		Always on V
Protocol	?	Any ✔ ← :: Protocol Selection :: ✔
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	6	×	
<u>Default</u>	Any	Any	Any	Any	0		
			Add Rule				

x

Click Add Rule to display the following screen:

Add	a	New	In	bound	Fire	wall	Rul	e

New Firewall Rule		
Rule Name		
Enable		Always on V
WAN Connection	?	Any 🗸
Protocol	?	Any V CIProtocol Selection :: V
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 (\UDrag 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			

x

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

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 I	Firewall R	tules (*	Dr	ag and drop rows to change	rul	le order)			?
Rule		rotocol	So	ource IP		Destination IP Port		olicy	
No web ad	<u>ccess</u> T	СР	An An		An 80		C	eny	×
No FTP	access	к "р		Any Any		Any 21		Den	у 💌
<u>Default</u>	A	ny	An	ιγ	Ar	ıy	4	llow	
				Add Rule					

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

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

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

will be required.

Intrusion Detection and DoS Prevention

Intrusion Detection and DoS Prevention	
Disabled	

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

feature, click . , check the **Enable** check box, and press the **Save** button.

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

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

Content Blocking

Application Blocking Please Select Applicat				?
Web Blocking				?
Preset Category High Moderate Low Custom	 Adware P2P/File sharing 	 Audio-Video Pornography 	 File Hosting Update Sites 	
Content Filtering Data Update Customized Domains	base Auto (🦳 🗌	_	_	?
Exempted Domains fro	om Web Blocking			+
Exempted Subnets			Subnet Mask	•
URL Logging			255.255.255.0 (/24)	• +
Enable Log Server Host		<u></u> 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 advertised v	vhen no network advertising is chosen.	+	
Static Route Advertising	?	Enable	C Enable		
-	\sim	Excluded Networks Subnet Mask			
			255.255.255.0 (/24) 💙	+	
Save					

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

OSPF settings	
Area ID	
Link Type	Image: Broadcast Oppoint-to-Point
Authentication	None T
Interfaces	Help Close Click here to customize interface cost
	Save Cancel

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

None T	
	Save Cancel
	None •

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						

PepVPN Route Isolation	Enable this option if you want to isolate PepVPN peers from each other. Received PepVPN routes wi not be forwarded to other PepVPN peers to reduce bandwidth consumption.
	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 Advertising	Selected networks will be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAI networks will be advertised by default.
J	All the networks belonging to interfaces that have OSPF or RIPv2 enabled will be advertised even if the are not selected in this table.
Static Route Advertising	Enable this option to advertise LAN static routes over OSPF & RIPv2. Static routes that match th 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

B	GP Profile											
P	rofile Name											
E	nable		2									
Ir	nterface		Untagged LA	N	~							
R	outer ID		LAN IP Ad O Custom:	ddres	s							
A	utonomous System											
N	eighbor	?	IP Address		Autonom System	ous	Multihop / TTL	Passv	vord	AS-Pat Preper		
							disable					+
H	old Time	?	240									
N	ext Hop Self	?										
iB	GP Local Preference	?	100									
в	FD	?	🗌 Enable									
	Name	This field is	for specifying a	a nam	e to represe	ent th	is profile.					
	Enable		his box t will be disable	is d.	checked	9	this	BGP	profile	will	be	enabled
	Interface	the interface where BGP neighbor is located										
	Autonomous System	The Autonomous System Number (ASN) of this profile										
	Neighbor	BGP Neighbor's details										
	IP address	Neighbor's I	P address									
	Autonomous System	Neighbor's A	ASN									

Multihop/TTL	Time-to-live(TTL)ofBGPpacket.Leave it blank if BGP neighbor is directly connected, otherwise you must specify a TTL value. Accurately, this option should be used if the configured neighbor IP address does not match the selected Interface's network subnets. TTL value must be between 2 to 255.								
Password	Optional password for MD5 authentication of BGP sessions.								
AS-Path Prepending:	AS path to be prepended to the routes received from this neighbor. The value must be a comma separated ASN. For example "64530,64531" will prepend "64530, 64531" to received routes.								
Hold Time	Time in seconds to wait for a keepalive message from the neighbor before considering the BGP connection is staled. This value must be either 0 (infinite hold time) or between 3 and 65535 inclusively.								
Next Hop Self	Enable this option to advertise own source address as next hop when propagate routes.								
iBGP Local Preference	Metric advertised to iBGP neighbors to indicate the preference for external routes. Value must between 0 to 4294967295 inclusively. Default: 100								
BFD	Enable this option to add Bidirectional Forwarding Detection for path failure detection. All direct connected neighbors use the same physical interface share same BFD settings. All multi hop neighbors share same Multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.								

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

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

	Assign Community to matched prefixes.
Set Community	Community: Two numbers in new-format. e.g. 65000:21344 Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284

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

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

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

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



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

Remote User Access

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

L2TP with IPsec

Remote User Access Settings		
Enable	\checkmark	
VPN Type	● L2TP with IPsec ○ PPTP ○ OpenVPN	
Preshared Key		
	✓ Hide Characters	

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

Continue to configure the authentication method.

OpenVPN

Remote User Access Settings		
Enable		
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 🔻	
Authentication		Local User Accounts 🔻	
User Accounts	?	Username	Password
Connect to Network	Select the VL	AN network for remote users to enable remote	e user access on.
Authentication	uthentication Determine the method of authenticating remote users		

User accounts:

This setting allows define the Remote User Accounts. you to 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 V
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 Serv	ver	*
Name		
Host		
Port	1812	
Secret		
	Hide Characters	

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

Accounting Server	×
Name	
Host	
Port	1813
Secret	Hide Characters
	Save Cancel

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			
Aud 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	✓ Enable			
Settings	Source Network	TCP Port	Server IP Address	Server Port



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	C Enable		
Connection		Enable Forwarding?	SMTP Server	SMTP Por
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 Settings				
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 Setup					
Custom Service Forwarding	Enable				
Settings	Source Network	TCP Port	Server IP Address	Server Port	
	T				+

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

Service Passthrough

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

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

Some Internet services need to be specially handled in a multi-WAN environment. Pepwave routers can handle these



services such that Internet applications do not notice being behind a multi-WAN router. Settings for service passthrough support are available here.

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

Grouped Networks

Grouped Networks					
Name	Networks				
Add Group					

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

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

In	this	example	we'll	create	а	group	"accounting"
Click s	ave when you h	ave finished adding	the required n	etworks.			

Grouped Networks				
Name	Accounting	Accounting		
Networks	Network	Subnet Mask		
	192.168.50.192	255.255.255.224 (/27) 🔻 🗶		
		255.255.255 (/32) 🔹 🔶		

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

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System
Advanced						
PepVPN	Add a I	New Outbound Firew	all Rule			
GRE Tunnel						
Port Forwarding	New Fi	rewall Rule				
NAT Mappings	Rule Na					
QoS	Enable					
 Bandwidth Control 	Protocol		Any 🗸	+ :: Protocol S	Selecti	on :: 💙
 Application 	Source	(Grouped I	Network 🗸 🗛	ccount	ing 🗸
Firewall	Destinat	tion 🤇	Any Addre	255 🗸		
Access Rules	Action	(Allow	O Deny		

SIM Toolkit

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

SIM Status
No SIM information

USSD

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

Cellular
1
254287583888888
USSD •
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	2342073025425Mt
ТооІ	SMS T

SMS		Refresh
Jun 21, 2017 18:00	PM Transfergers, your well processes the Withelite - you can always this when you first high at them as also Tableat	×
May 06, 2017 12:23	(Abov) where is 'Non-new with is ready to view. On to your Phylic summittee your desition, or or a realistic phase which have https://www.doi.org/abov/2010/01/10/10/01/01/01/01/01/01/01/01/01/	×
Mar 15, 2017 10:03	From Herry Sector There is placed interconnect a the behavior time Riccards Thermody, 7 year services (Parket, year out principalities intercipi.);y (Pin-Dis)	×
Mar 06, 2017 14:50	(MAX) (Process): Your years with its manipular views. On its years PhyS manuachters years should up an an a maining phasemetric it. Survey https://www.its.com/actional/actional/action/acti	×
Dec 28, 2016 09:53	From Three its, an improvation appropriate to mentio half-press offer that to control you, the offer september your from to take, that mention meaning-charge wit result to futures on-your next (etc.) Three	×
Dec 06, 2016 13:09	Material -Protection 1. Your report shall in moder to come. On his pour Physics compose sharkings or or is mainted phones class here a help of mainted strengt council, second or	×
Nov 08, 2016 11:29	Proper Standar revels. There is placented real-structures in the fluctures that MAC annumber same. If your sensitivity effected, you can part-spheric fluctures a structure and	×
Sep 07, 2016 17:05	Press literar head more detailer temportubing your modes of determining balancement "the car bus a bats wathor to meet your result from the system of the press graph."	×



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
AP									
 Wireless SSID 	InControl management enabled. Wireless SSID can now be configured on <u>InControl</u> .								
 Settings 	SSID			Security Poli	icy				
Status	CONTRACTOR OF			WPA2 - Persor	nal				×
 Access Point 					New SSID				
 Wireless SSID 									
 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	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 (<u>https://forum.peplink.com/t/lan-isolation-with-balance30-and-ap-one-ac-mini-help-needed/3914/4</u>) 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.
	Default: Disable

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

Енстурион	AES.COMP
802.1X Version	● V1 ○ V2
Management Frame Protection	Default (Disabled) 🗸
Fast Transition 🤶	

Security Policy	 This setting configures the wireless authentication and encryption methods. Available options: : Open (No Encryption) WPA3 -Personal (AES:CCMP) WPA2/WPA3 -Personal (AES:CCMP) WPA2 -Personal (AES:CCMP) WPA2 - Enterprise WPA/WPA2 - Personal (TKIP/AES: CCMP) WPA/WPA2 - Enterprise
	When WPA/WPA2 - Enterprise is selected, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the Shared Key option does not apply and is therefore hidden. When using this method, select the appropriate version using the V1/V2 controls. The security level of this method is known to be very high.
	When WPA/WPA2 - Personal is selected, a shared key is used for data encryption and authentication. When using this configuration, the Shared Key option should be enabled. Key length must be between eight and 63 characters (inclusive). The security level of this method is known to be high.
	NOTE: When WPA2/WPA3- Personal is configured, if a managed AP which is NOT WPA3 PSK capable, the AP Controller will not push those WPA3 and WPA2/WPA3 SSID to that AP.
Management Frame Protection	This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action.
Fast Transition	When WPA2/WPA3 - (Personal / Enterprise) is selected, the Fast Transition option is the standard defined for 801.11r to reduce the association process when it roams from one Access Point to another Access Point.

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

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 🗸		

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



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

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

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



Settings

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

Wi-Fi Radio Settings		
Operating Country	United States	
SSID	2.4GHz 5GHz	
Wi-Fi AP Settings		(?)
Protocol	802.11ng • 802.11ac •	
Channel Width	20/40 MHz • 80 MHz •	
Channel	Auto Edit Auto Edit Channels: 1 2 3 4 5 6 7 8 9 10 11 Channels: 36 40 44 48 149 153 157 1	.61
Auto Channel Update	Daily at Clear All Daily at Clear All 00:00 01:00 02:00 03:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 16:00 17:00 22:00 23:00 20:00 21:00 22:00 23:00 Wait until no active client associated Wait until no active client associated	:00 :00 :00 :00 :00
Output Power	Max Boost Max Boost 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		

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

Protocol	This option allows you to specify which client association requests will be accepted. By default, 802.11ng is selected.
Channel Width	Settingsfor2.4GHzAPand5GHzAPcanbeconfiguredhere:2.4GHz:40MHz, 20/40MHzand20MHzare available. The default setting is20/40MHz, which allowsbothwidthstobeusedsimultaneously.80MHz, 40Mhz, 20Mhz, and (20/40MH) are available. The default setting is80MHz.Note:802.11ngand802.11ngare not part of the802.11standard. It is simply a notation for indicating802.11nuse on the2.4-GHzband (11ng) or802.11nuse on the5-GHzband (11na).
Channel	This option allows you to select which 802.11 RF channel will be used.
Auto Channel Update	Indicate the time of day for updating the automatic channel selection.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – Max , High , Mid , and Low . The actual output power will be bound by the regulatory limits of the selected country.
Client Signal Strength Threshold ^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is dBm.
Maximum number of clients	Enter the maximum number of clients that can simultaneously connect to the wireless network or enter 0 to allow an unlimited number of connections.
Beacon Rate ^A	This option is for setting the transmit bit rate for sending a beacon. By default, 1Mbps is selected.
Beacon Interval ^A	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM ^A	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to 1 ms .
RTS Threshold	Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.



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

System Settings

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

PEPWAVE	Dashboard SpeedFusion Cloud	Network Advanced AP System Status Apply Changes
System		
 Admin Security 	Admin Settings	?
Firmware	Device Name	hostname: surf-soho-
Time	Admin User Name	admin
Schedule	Admin Password	
Email Notification	Confirm Admin Password	
Event Log	Read-only User Name	user
SNMP	User Password	
 InControl 	Confirm User Password	
 Configuration 		
Feature Add-ons		
Reboot	Authentication Method	Local Account RADIUS TACACS+
Tools	CLI SSH & Console	C Enable
Ping	Security	HTTPS V
 Traceroute 	Web Admin Access	LAN Only V
Wake-on-LAN	Web Admin Port	443
 WAN Analysis 		
Logout		Save

Admin Security

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



Device NameXXXX, wheAdmin User NameAdmin UserAdmin PasswordThis field alConfirm Admin PasswordThis field alRead-only User NameRead-onlyUser PasswordThis field alConfirm User PasswordThis field alWeb Session TimeoutThis field sp router terminaWeb Session TimeoutWith this exp server. Autionly access communica set to Local Available op • Local AuthenticatiaAuthentication MethodAuthenticatia AuthenticatiaAuthentication MethodAuthenticatia Accounting F Accounting F	re XXX refer er Name is set lows you to sp lows you to ve User Name is lows you to ve blod. lows you to ve blod. lows you to ve becifies the nu inates its acce s. Local admi te with the ext l Account. ptions: cal Account ADIUS	define a name for this Pepwave router. By default, Router Name is set as surf-sol fers to the last 4 digits of the unit's serial number. et as <i>admin</i> by default, but can be changed, if desired. specify a new administrator password. verify and confirm the new administrator password. is set as <i>user</i> by default, but can be changed, if desired. specify a new user password. Once the user password is set, the read-only user feature verify and confirm the new user password. number of hours and minutes that a web session can remain idle before the Pepwa cess to the web admin interface. By default, it is set to 4 hours .
Admin PasswordThis field alConfirm Admin PasswordThis field alRead-only User NameRead-onlyUser PasswordThis field al will be enathConfirm User PasswordThis field al will be enathWeb Session TimeoutThis field sp router terminationWeb Session TimeoutWith this exp server. Autionly access communica set to Local Available op • Local AuthenticatiaAuthentication MethodAuthenticatia AuthenticatiaAuthentication Accounting F Accounting FAccounting F Accounting F	lows you to sp lows you to ve User Name is lows you to sp oled. lows you to ve pecifies the nu inates its acce s. Local authent henticated use s. Local admi te with the ext l Account. ptions: cal Account ADIUS	specify a new administrator password. verify and confirm the new administrator password. is set as <i>user</i> by default, but can be changed, if desired. specify a new user password. Once the user password is set, the read-only user feature verify and confirm the new user password. number of hours and minutes that a web session can remain idle before the Pepwa cess to the web admin interface. By default, it is set to 4 hours . entication is selected, the web admin will authenticate using the corresponding exter isers are treated as either "admin" with full read-write permission or "user" with rea- min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, i
Confirm Admin PasswordThis field alRead-only User NameRead-onlyUser PasswordThis field al will be enabledConfirm User PasswordThis field al router terminalWeb Session TimeoutThis field sp router terminalWeb Session TimeoutWith this exp server. Autionly access communical set to Local Available op Authentication Authentication Authentication Authentication Authentication Authentication Accounting F Accounting F	lows you to ve User Name is lows you to spoled. lows you to ve pecifies the nu inates its acce ternal authent henticated use s. Local admi te with the ext l Account. ptions: cal Account ADIUS	verify and confirm the new administrator password. is set as <i>user</i> by default, but can be changed, if desired. specify a new user password. Once the user password is set, the read-only user feature verify and confirm the new user password. number of hours and minutes that a web session can remain idle before the Pepwa cess to the web admin interface. By default, it is set to 4 hours . entication is selected, the web admin will authenticate using the corresponding externation is selected, the web admin with full read-write permission or "user" with read- min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, it
PasswordThis field allRead-only User NameRead-onlyUser PasswordThis field all will be enableConfirm User PasswordThis field allWeb Session TimeoutThis field sp router terminalWeb Session TimeoutWith this exp server. Autionly access communica set to Local Available op • Lo • R/Authentication MethodAuthenticatii Authenticatii Authenticatii Authenticatii	User Name is lows you to spoled. lows you to ve pecifies the nu inates its acce s. Local admi te with the ext l Account. ptions: cal Account ADIUS	is set as <i>user</i> by default, but can be changed, if desired. specify a new user password. Once the user password is set, the read-only user feature verify and confirm the new user password. number of hours and minutes that a web session can remain idle before the Pepwa cess to the web admin interface. By default, it is set to 4 hours . entication is selected, the web admin will authenticate using the corresponding exter isers are treated as either "admin" with full read-write permission or "user" with rea- min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, i
NameRead-onlyUser PasswordThis field al will be enabledConfirm User PasswordThis field alWeb Session TimeoutThis field sp router terminalWeb Session TimeoutWith this exp server. Autionly access communical set to Local Available of • Local • RAAuthentication MethodAuthenticatii Authenticatii Authenticatii	lows you to spoled. lows you to ve pecifies the nu inates its acce ternal authent henticated use s. Local admi te with the ext l Account. ptions: cal Account ADIUS	specify a new user password. Once the user password is set, the read-only user feature verify and confirm the new user password. number of hours and minutes that a web session can remain idle before the Pepwa cess to the web admin interface. By default, it is set to 4 hours . entication is selected, the web admin will authenticate using the corresponding exter isers are treated as either "admin" with full read-write permission or "user" with rea min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, i
Oser Passwordwill be enabledConfirm User PasswordThis field alWeb Session TimeoutThis field sp router terminalWith this experience server. Autionly access communicaset to Local Available op • Lo • R/Authentication MethodAuthenticatii Accounting F Accounting F	lows you to ve becifies the nu inates its acce tternal authent henticated use s. Local admi te with the ext l Account. ptions: cal Account ADIUS	verify and confirm the new user password. number of hours and minutes that a web session can remain idle before the Pepwa cess to the web admin interface. By default, it is set to 4 hours . entication is selected, the web admin will authenticate using the corresponding exter isers are treated as either "admin" with full read-write permission or "user" with rea min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, i
PasswordThis field alWeb Session TimeoutThis field s router termWith this ex- server. Autionly access communica- set to Local Available op • Lo • R/Authentication MethodAuthentication Method	ternal authent thenticated use s. Local admi te with the ext Account. ptions: cal Account	number of hours and minutes that a web session can remain idle before the Pepwa cess to the web admin interface. By default, it is set to 4 hours . entication is selected, the web admin will authenticate using the corresponding exter isers are treated as either "admin" with full read-write permission or "user" with rea min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, i
Timeout router termination of router termination of router termination of the second seco	inates its acce sternal authent henticated use s. Local admi te with the ext Account. ptions: cal Account ADIUS	cess to the web admin interface. By default, it is set to 4 hours . entication is selected, the web admin will authenticate using the corresponding exter isers are treated as either "admin" with full read-write permission or "user" with rea min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, i
Authentication Method	henticated use s. Local admi ite with the ext l Account. ptions: cal Account ADIUS	isers are treated as either "admin" with full read-write permission or "user" with rea min and user accounts will be disabled. However, when the device is not able external server, local accounts are enabled to allow emergency access. By default, i
Authentication Authentication Method Accounting F		
Authentication Method Accounting F	on Protocol	MS-CHAP v2 V
Authentication Method Accounting F		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 Method Accounting F	on Host	or you may go to <u>KADIOS Server</u> page to define multiple profiles
Method Accounting R Accounting R		1812
Accounting P Accounting P	on Secret	
Accounting F		V Hide Characters
Accounting F		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
	lost	
	Port	1813
Accounting S	Secret	Hide Characters
Authenticatio	on Timeout	3 seconds
Authenti Protocol		

	Authentication Port	This setting specifies the UDP destination port for authentication requests.
	Authentication Secret	This field is for entering the secret key for accessing the RADIUS server.
	Accounting Host	This specifies the IP address or hostname of the RADIUS server host.
	Accounting Port	This setting specifies the UDP destination port for accounting requests.
	Accounting Secret	This field is for entering the secret key for accessing the accounting server.
	Authentication Timeout	This option specifies the time value for authentication timeout
	TACACS+	
	Authentication Method TACACS+ Server	O Local Account O RADIUS TACACS+
	TACACS+ Server Secret	✓ Hide Characters
	TACACS+ Server Timeout	3 seconds
	TACACS+ Server	This specifies the access address of the external TACACS+ server.
	TACACS+ Server Secret	This field is for entering the secret key for accessing the RADIUS server.
	TACACS+ Server Timeout	This option specifies the time value for TACACS+ timeout
CLI SSH & Console	The CLI (command line inter information regarding CLI, pla	face) can be accessed via SSH. This field enables CLI support. For addition ease refer to Section 30.5.
CLI SSH Access	This menu allows you to choo	ose between granting access to LAN and WAN clients, or to LAN clients only.
CLI SSH Port	This field determines the port	on which clients can access CLI SSH.
Security	HTTPHTTPSHTTP/HTTPS	ne protocol(s) through which the web admin interface can be accessed: s enabled by default to force HTTPS access to the web admin interface.
Web Admin Access	LAN onlyLAN/WAN	ne network interfaces through which the web admin interface can be accessed: /AN 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**.

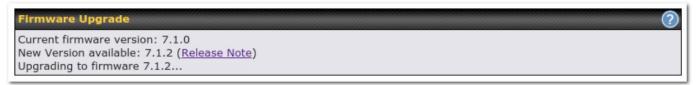
Firmware Upgrade	(2)
Current firmware version: 8.0.0 Firmware check pending	
	Check for Firmware

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 New Version available: 7.1.2 (Release Note)
 Time 	New Version available. 7.1.2 (<u>helease 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.

9%

Validation success...

*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	v				
				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**.

Time Settings					
Time Zone	(GMT) Greenwich Mean Time : Dublin, I	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▼			
Time Server	0.pepwave.pool.ntp.org	Default			
Save					

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

Schedule

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

Name	Time	Used by		
No schedule profile defined				
New Schedule				

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

Edit schedule profile					
Schedule Settings					
Enable		The schedule function of those associated features will be lost if profile is disabled.		disabled.	
Name					
Schedule		Always on 🔻			
Used by					
Schedule Map					
Sunday	Midnight	4am	8am Noon	4pm	8pm
Monday					
Tuesday	· · · · · · · · · ·	· · · · · · · ·		· · · · · · · · · · · · · · · ·	
Wednesday	· · · · · · · · · ·	· · · · · · · ·		· · · · · · · · · · · · · · ·	
Thursday	· · · · · · · · · ·	~ ~ ~ ~ ~ ~ ~ ~		· · · · · · · · · · · · · · ·	
Friday	· · · · · · · · ·	· · · · · · · ·		· · · · · · · · · · · · · ·	
Saturday	· · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·	
				Sav	e Cancel

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

Email Notification

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

Email Notification Setup		
Email Notification	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	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 addresses 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	0
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	
[<-] 250-smtp.gmail.com at your service, [14.192.209.255]	_
[<-] 250-SIZE 35882577	
[<-] 250-8BITMIME	
[<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH	
[<-] 250-ENHANCEDSTATUSCODES	
[<-] 250-PIPELINING	
[<-] 250-CHUNKING	
[<-] 250 SMTPUTF8	
-> AUTH PLAIN 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		
Push Events		
	Save	

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



SNMP

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

SNMP Settings		
SNMP Device Name		
Location ?		
SNMP Port	161 Default	
SNMPv1	Enable	
SNMPv2c	Enable	
SNMPv3	Enable	
SNMP Trap	Enable	
	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 Device Name	This field shows the router name defined at System>Admin Security.
SNMP Port	This option specifies the port which SNMP will use. The default port is 161 .
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.
SNMP Trap	This option allows you to enable SNMP Trap

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

SNMP Community	×	
Community Name		I
Allowed Network	/ 255.255.0 (/24) ▼	I
	Save Cancel	
Community Name This setting spe	ifies the SNMP community name.	

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

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

SHA V	
DES V	

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 box beside the "Privately Host InControl" open, and enter the IP Address of your InControl Host.

You can sign up for an InControl account at <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	
BUILT BUILT		
Download Active Configurations		
	Download	
Upload Configurations		?
Configuration File	Choose File No file chosen	
	Upload	

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:				
Irmware 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 SpeedFusion[™] VPN connection. You can specify the number of pings in the field **Number of times**, to a maximum number of 10 times. **Packet Size** can be set to a maximum of 1472 bytes. The ping utility is located at **System>Tools>Ping**, illustrated below:

Ping				
Connection	WAN 1 •			
Destination	8.8.8.8			
Packet Size	56			
Number of times	Times 5			
	Start Stop			
Results	Clear Log			
PING 8.8.8.8 (8.8.8.8) from 10.22.1.182 5	6(84) bytes of data.			
64 bytes from 8.8.8.8: icmp_req=1 ttl=12:	1 time=11.8 ms			
64 bytes from 8.8.8.8: icmp_req=2 ttl=12:	1 time=11.7 ms			
64 bytes from 8.8.8.8: icmp_req=3 ttl=12:	1 time=11.6 ms			
64 bytes from 8.8.8.8: icmp_req=4 ttl=121 time=11.6 ms				
64 bytes from 8.8.8.8: icmp_req=5 ttl=12:	1 time=11.4 ms			
8.8.8.8 ping statistics				
5 packets transmitted, 5 received, 0% pack	xet loss, time 4006ms			
rtt min/avg/max/mdev = 11.427/11.680/1				

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	Clear Log
Transmission In: IN. 2722.2008-000	DA.223.289.895, 32 hops max, 82 hyte packate
1 10.41.137.254 (10.41.137	(54) 3.708 ma-4.472 ma-9.287 ma
2 10.00.00.254 (10.00.00.25	C 8.809 ma 1.290 ma 1.446 ma
3 10-88-88-1 (10-88-98-1) L-	75 mg 1.525 mg 1.868 mg
* 18.88.3.2 (18.88.3.2) % 18	mg 0.202 mg 0.106 mg
1 118-142-88-254 (118-142-4	8.254) 3.384 ma 138.175.240.22 (138.175.240.22) 5.707 ma 118.383.88.254 (118.383.88.254) 3.472 ma
1 181 75 46 129 CHL 75 46	200 5.488 mg 188.85.225.46 (148.85.225.46) 5.201 mg 5.201 mg
7 220 128 1 18 (220 128 1	(80) 4.301 mg 7.498 mg 7.498 mg
8 108-175-88-184 (108-175-8	8.0940 4.811 mg 205.128.8.1 (205.128.8.1) 4.872 mg 180.72.085.118 (180.75.085.108) 4.341 mg
\$ 100.108.8.209 (200.108.8.	100) 3.300 mg 73.54.584.346 (73.54.584.346) 4.401 mg 230.538.8.305 (230.538.8.300) 4.678 mg
10 75 14 203 20 (75 14 203	10 9-842 mg 74.125.48.158 (74.125.48.158) 4.877 mg 75.14.255.30 (75.14.255.30) 9.884 mg
11 79-14-209-30 (79-14-209-	101 & 584 mg 208,46,202,141 (208,46,202,141) 7 315 mg 208,46,245,36 (208,46,245,30) 4,484 mg
12 208-88 202 212 (208-86.2	\$2.2121 4.872 mg 205.85.242 162 (205.85.242 162) 4.809 mg 6.589 mg
13 214.238.82.47 (214.238.1	
	1.001 0.175 mg 0.164 mg 0.002 mg

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 ▼ 00:00:00:00:00:00	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	АР	System	Status
System							
 Admin Security 	WAN	l Performar	nce An	alvsis			
Firmware		point-to-point WAN performa					
Time							
 Schedule 		As a server	ublia ID addres				
Email Notification		For the peer who has p	oublic IP addres	ses to accept co	onnecti	on.	
Event Log							
SNMP	>>	As a client For the peer to initiate	connection.				
 InControl 							
 Configuration 							
Feature Add-ons							
 Reboot 							
Tools							
Ping							
 Traceroute 							
Wake-on-LAN							
WAN Analysis							
The default port is 60	00 and can be	changed if required. The	IP address o	f the WAN inte	erface	will be sho	wn in the W

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



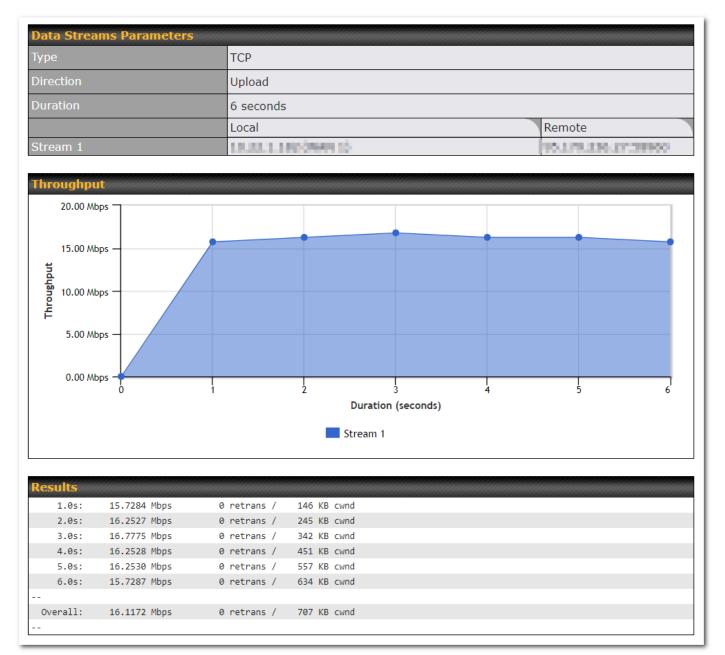
PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System	Status	Apply Changes
System								
Admin Security	WAN	l Performar	ice An	alvsis				
Firmware		point-to-point WAN performa						
Time								
 Schedule 	Server S	ettings			-			
Email Notification	Status		Listenin	ig (Control Port	t: 600	0)		
Event Log	Control Pe	ort	6000					
SNMP				Apply	Stop	p		
 InControl 								
 Configuration 	WAN Co	nnection Status			iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii			
Feature Add-ons	📳 WAN			1				
Reboot	🔮 USB		No Devi	ce Detected				
Tools	💿 Wi-Fi 🗤	WAN on 2.4 GHz	🔲 Disabled	9				
Ping	💿 Wi-Fi 🗤	VAN on 5 GHz	🗌 Disabled	Н				
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 Status	Apply Changes
System			
Admin Security	WAN Performar	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	▼	×
Wake-on-LAN	3 Not Used	~	× ×
WAN Analysis	4 Not Used	~	×
Logout	5 Not Used	✓	× (
	6 Not Used	♥	×
	7 Not Used	v	×
	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	The second se
Model	Pepwave Surf SOHO MK3
Product Code	SUS-SOHO
Hardware Revision	1
Serial Number	1000 - 0000 - 000
Firmware	La car access
PepVPN Version	8.0.0
Modem Support Version	1023 (<u>Modem Support List</u>)
InControl Managed Configurations	Firmware, Scheduled Reboot
Host Name	LAN GROUPS THE
Uptime	6 days 3 hours 30 minutes
System Time	Fri Sep 06 03:00:20 MST 2019
Diagnostic Report	Download
Remote Assistance	Turn On

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**

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



Active Sessions

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

Overview Search		
ession data captured within on	e minute. <u>Refresh</u>	
Service	Inbound Sessions	Outbound Sessions
Amazon	0	1
<u>DNS</u>	0	55
Facebook	0	2
Google	0	19
Google Play Store	0	1
HTTP	0	2
Psec	0	2
Office 365	0	42
SIP	0	46
<u>SSH</u>	0	1
SSL	3	170
STUN	0	2
Skype	0	5
XMPP	0	1
Interface	Inbound Sessions	Outbound Sessions
	0	308
	2	155
	0	0
	0	0
and a second	0	42
and the second se	0	0
	Top Clients	
Client IP Address	Total Sessions	
172.16.150.10	174	
10.22.1.253	151	
10.22.1.166	91	
172.16.150.12	75	
10.22.1.157	60	

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

You can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to **Status>Active Sessions>Search**.

Overview	Search					
Session dat	ta capture	d within one minute. <u>Re</u>	<u>efresh</u>			
IP / Subnet		Source or Destination 🔻	/ 255.255.255 (/32) 🔻			
Port		Source or Destination 🔻				
Protocol / S	ervice	ТСР	•			
Interface		 WAN 1 J Cellular 1 VPN 	2 WAN T2 Cellu		🗆 察 Wi-Fi WA 🗆 🔮 USB	N
Search						
Outbound						
Protocol	Source IP	Destination IP	Service No sessions	Interface		Idle Time
Total searc	hed result	s: 0	110 363310113			
Inbound	hindhidd		i i i i i i i i i i i i i i i i i i i			
Protocol	Source IP	Destination IP	Service	Interface		Idle Time
Total searc	hed result	rs: 0	No sessions			
Transit	hininin					
Protocol	Source IP	Destination IP	Service No sessions	Interface		Idle Time
Total searc	hed result	rs: 0				

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



Client List

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

lter		Online Clients Only DHCP Clients Only				
lient List						
IP Address 🔺	Name	Download Uploa (kbps) (kbps		Network Name (SSID)	Signal (dBm)	Impor
10.		1	6 10:00104-03/07-08.			•
10.	NOTES TRADE		4 (\$100-\$0)\$404046			
10.			4 3HEROLEUM			۲
10.	situria.		6 IO40038/04/08/38			۲
10.	Contraction of the		1.1011-0.0010-0.0010			
10.	ap and 1963		6 IO1A004918A38			۲
10.	N2010-104		H REPORTED			
10.			A PRACE PRICE			۲
10.	ANTE 100	1	6 IO1A00.040043			
10.	COLUMN TWO IS NOT	20	14 HOUSEDONESE			۲
10.	min the		I DESCRIPTION OF REAL			•
10.	James Sealing		N IN CONTRACTO			۲
10.	min 141a		8 10 1A 00 (A 40 0)			•
10.			E RECENCIÓN DA CO			۲
10.	0.000		6. (A. 97 (2) (2) (2) (3)	PER. 244_1	 -62	•
10.			I DESCRIPTION OF			•
10.	discuss 62		4 10 20 M (0.40 a)	PER-205_1	 -46	۲
10.	Store Section	10.00	8 10 10 10 10 10 10			•
10.	0400-01-00C		4 1000/00/01/00/00			•
10.	NEWSCON-MARKING		4 NUMBER OF STREET	PER. (%)_1		•
10.	dana da		1 10-0039-01-08-08			
10.			1 (0.00 N 0.00 D			۲
10.			I DEMONSTRATIONS			•
10.	(P-0603)		4 KOR000000			
10.	in completes		ALC: NUMBER OF STREET			۲
10.10.10.10.10	60° 1207	1 A A A A A A A A A A A A A A A A A A A	A REPORT AND A			•
10.00			4 10 10 10 10 10 10 10			•
172			ALC: UNDER STREET, SALES			
17:	100-100 C		4.00000303404.00.00			
17:	and a		0.000000000000000			•



UCDE & DID''

OSPF & RIPv2		
Area	Remote Networks	
▼0.0.0.0		
PedVPN	192.168 /24	

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

BGP

BGP			
	Profile	Neighbor	
		No information	

Information on BGP can be found in this section.

PepVPN Status

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

Show disconnected profiles

Remote Peer 🔺	Profile	Information	
ADA0-FFFC-11F8	FH	192.168.77.0/24	
🔒 🕨 3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24	

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

PepVPN with SpeedFusion - Rem	Show all profiles	
Search	SFC	

	Remote Peer 🔺	Profile			Informatio	n			
۵	 SFC-SIN-001 (SFC-SIN-001) 	SFC			SpeedFusi	on Cloud			>
	WAN1				Not availa	ble - WAN disable	d		
	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 availa	ble - WAN disable	d		
	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

connection.

ш

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

Local WAN Remote WAN All WAN-to-WAN **Overall Statistics** WAN2 WAN3 WAN5 400.00 Mbps 400.00 Mbps 400.00 Mbps 200.00 Mbp 200.00 Mbps 200.00 Mbps Throughput M J 200.00 Mbp 200.00 Mbps 200.00 Mbp: 400.00 Mbps 500 400.00 400.00 Mbps 500 Mbps 500 Latency (ms) M 250 250 250 N. 1 h h. m-0 10k 0 10k 0 10k Downlink Quality (pkt/s) 4 5k 5k 5k M A . n ž 🎍 🏨 ۵. 4 A 0k 5k 0k 5k 0k 5k Uplink Quality (pkt/s) * 2.5k 2.5k 2.5k 0k 5k Ok 5k Link Quality ▲ Packet loss △ Packet out-of-order Downlink Stats (pkt/s) 2 Downlink Stats (pkt/s) Å Ok 10k Ok 10k Uplink Stats (pkt/s) 9 Uplink Stats (pkt/s) 92 Ī. ÷. X Uplink Stats • Packet fragmentation • Redundant packet generated by FEC • Redundant packet generated by WAN Smoothing 4 Þ

When pressing the

>

^J button the following menu will appear:

PepVPN Details More information Connection Information More information Profile SFC Remote ID SFC-SIN-001 Device Name SFC-SIN-001 Serial Number 1197-A047-2E3D

WAN Statistics					<u>III.</u>			
Remote Connections	🗌 Sh	Show remote connections						
WAN Label	💿 wa	AN Name 🔿 IP Add	fress and Port					
WAN1	•		Not available - WAN disal	bled				
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 disal	bled				
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 🗸	Ghart
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

tatus										
Device			T							
Active Sessions	- I	Device Event	Log	Firewal	Event Lo	og				
Client List		Device Even							🗹 Auto I	Jofrach
OSPF & RIPv2		1111111111111111111111							Auto	terresn
BGP		Sep 30 09:23:2						;)		-
		Sep 30 09:17:0		m:						
Event Log		Sep 30 09:10:3 Sep 30 09:10:1								
AN Quality		Sep 30 09:09:0								
sage Reports		Sep 30 09:08:2								
		Sep 30 09:07:5								
Real-Time		Sep 30 09:07:3								
Hourly		Sep 30 08:56:3	3 WAN:							
Daily		Sep 30 08:56:0	5 WAN							
Monthly		Sep 30 08:55:5	2 WAN:							
monuny		Sep 30 08:55:1	5 WAN:							
Logout		Sep 30 08:55:1	1 WAN:							
		Sep 30 08:54:4	2 WAN							
		Sep 30 08:54:0	4 WAN							
		Sep 30 08:53:4								
		Sep 30 08:52:5								
		Sep 30 08:52:1								
		Sep 30 08:35:5								
		Sep 30 08:35:3								
		Sep 30 07:24:0	5 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.





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.

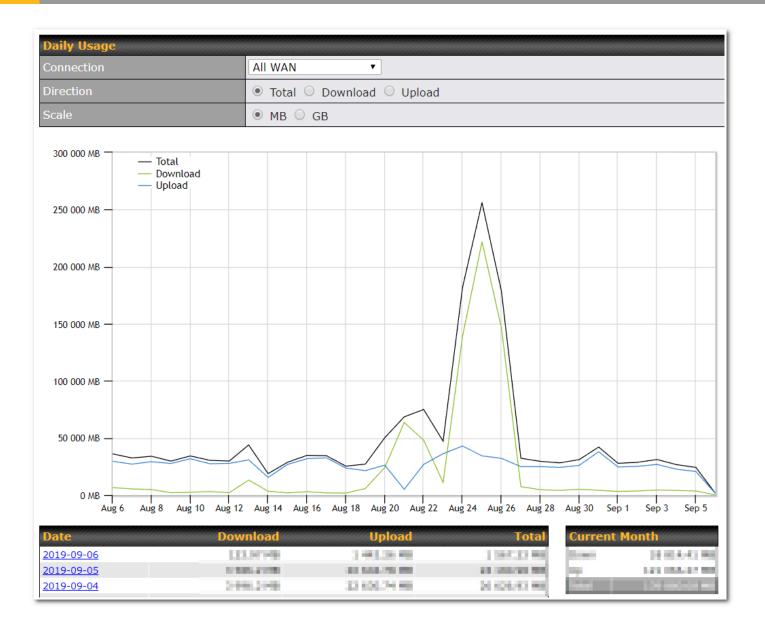
Hourly Usage		ana	mmmmmmmm			
Connection	All WAN	•				
Direction	💿 Total 🔘 Download	🖲 Total 🔘 Download 🔍 Upload				
Scale	● MB ○ GB					
3 500 MB						
— Total — Download						
— Upload		Λ				
3 000 MB						
2 500 MB -						
2 000 115						
2 000 MB -						
1 500 MB						
1 000 MB -	\land					
	\sim					
		/				
500 MB	\wedge			\sim		
0 MB - 06:00 09	:00 12:00	15:00 18:00	21:00 Sep 6	03:00		
	.00 12.00	15.00 18.00	21.00 560 0	05.00		
Date		Download	Upload	Total		
03:00		8.3 MB	241.64 MB	249.94 MB		
02:00		13.42 MB	400.42 MB	413.85 MB		
01:00		65.46 MB	401.72 MB	467.17 MB		
00:00		36.59 MB	392.84 MB	429.44 MB		
Yesterday		21.12.140	400.01 MD	421.14.145		
<u>23:00</u> 22:00		21.13 MB 85 95 MB	400.01 MB	421.14 MB 673 64 MB		

Daily

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

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

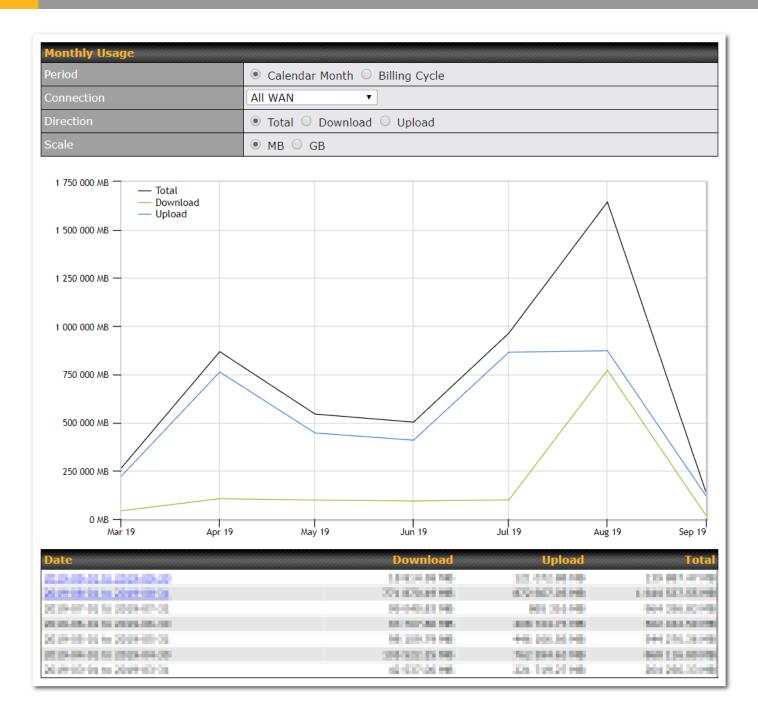
Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).



Monthly

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

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



Appendix A: Restoration of Factory Defaults

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

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

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

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

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

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

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

Appendix B: Declaration

The device supports time division technology

Federal Communication Commission Interference Statement

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

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

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

peplink PEPWAVE



<u>CE Statement for Pepwave Routers</u>

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

EN 60950-1: 2006 + A11 : 2009+A1 : 2010+ A12: 2011

Safety of Information Technology Equipment

EN50385 : 2002 / Article 3(1)(a)

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

EN 300 328 V1.7.1: 2006

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

□ EN 301 908-1 V5.2.1: 2011

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

EN 301 511 V9.0.2: 2003

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

EN 301 489-1 V1.9.2: 2008

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-7 V1.3.1: 2005

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

EN 301 489-17 V2.2.1: 2012

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

EN 301 489-24 V1.5.1: 2010

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

		$\mathbf{\Phi}$
C	E 0081	U

•

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



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