Pepwave MAX

User Manual

Pepwave Products:

MAX Transit Pro E , MAX Transit LTEA

Pepwave Firmware 8.1.1

March 2021

Copyright & Trademarks

Table of Contents

Introduction and Scope 7

Glossary 8

Product Features 9

Supported Network Features 9

WAN 9

LAN 10

VPN 10

Firewall 10

Captive Portal 10

Outbound Policy 10

AP Controller 11

QoS 11

Other Supported Features 12

Pepwave MAX Mobile Router Overview 13

MAX Transit Pro E 13

MAX Transit LTEA 14

Advanced Feature Summary 15

Drop-in Mode and LAN Bypass: Transparent Deployment 15

QoS: Clearer VoIP 16

Per-User Bandwidth Control 16

High Availability via VRRP 17

USB Modem and Android Tethering 17

Built-In Remote User VPN Support 18

SIM-card USSD support 18

DPI Engine 19

NetFlow 19

Wi-Fi Air Monitoring 19

Installation 20

Preparation 20

Constructing the Network 20

Configuring the Network Environment 21

Mounting the Unit 22

Wall Mount 22

Car Mount 22

Connecting to the Web Admin Interface 23

SpeedFusion Cloud 25
Activate SpeedFusion Cloud Service 25
Enable SpeedFusion Cloud 28
Connect Clients to Cloud 35
Link Wi-Fi to Cloud 36
Optimize Cloud Application 38

Configuring the LAN Interface(s) 39
Basic Settings 39
Port Settings 50
Captive Portal 51

Configuring the WAN Interface(s) 54
Ethernet WAN 54
DHCP Connection 57
Static IP Connection 58
PPPoE Connection 58
L2TP Connection 60
Cellular WAN 62
Wi-Fi WAN 67
Creating Wi-Fi Connection Profiles 73
WAN Health Check 74
Dynamic DNS Settings 77

Advanced Wi-Fi Settings 79

ContentHub Configuration 83
ContentHub 83
Configuring the ContentHub 83
Configure a website to be published from the ContentHub 83
Configure an application to be published from the ContentHub 86

MediaFast Configuration 88
Setting Up MediaFast Content Caching 88
Scheduling Content Prefetching 89
Viewing MediaFast Statistics 91

Bandwidth Bonding SpeedFusionTM / PepVPN 93
PepVPN 93

The Pepwave Router Behind a NAT Router 99

IPsec VPN 102

IPsec VPN Settings 102

Outbound Policy 107

Outbound Policy 107

Adding Rules for Outbound Policy 109

Algorithm: Weighted Balance 113

Algorithm: Persistence 114

Algorithm: Enforced 115

Algorithm: Priority 115

Algorithm: Overflow 116

Algorithm: Least Used 117

Algorithm: Lowest Latency 117

Expert Mode 117

Port Forwarding 119

UPnP / NAT-PMP Settings 120

NAT Mappings 122

QoS 124

User Groups 124

Bandwidth Control 124

Application 125

Application Prioritization 125

Prioritization for Custom Applications 125

DSL/Cable Optimization 126

Firewall 127

Outbound and Inbound Firewall Rules 128

Access Rules 128

Apply Firewall Rules to PepVpn Traffic 132

Intrusion Detection and DoS Prevention 132

Content Blocking 133

Application Blocking 133

Web Blocking 133

Customized Domains 134

Exempted User Groups 134

Exempted Subnets 134

URL Logging 134

Routing Protocols 135
OSPF & RIPv2 135
BGP 137

Remote User Access 141
L2TP with IPsec 141
OpenVPN 141
PPTP 142
Authentication Methods 142

Miscellaneous Settings 144
High Availability 144
Certificate Manager 147
Service Forwarding 148
SMTP Forwarding 148
Web Proxy Forwarding 149
DNS Forwarding 150
Custom Service Forwarding 150
Service Passthrough 150
UART 152
GPS Forwarding 154
Ignition Sensing 154
Ignition Sensing installation 155
GPIO Menu 157
NTP Server 157
Grouped Networks 158
SIM Toolkit 158

AP 161
AP Controller 161
Wireless SSID 161
Wireless Mesh 165
Settings 166

AP Controller Status 172
Info 172
Access Point (Usage) 174
Wireless SSID 176
Mesh / WDS 177
Wireless Client 178
Nearby Device 179

Event Log 180

Toolbox 181

System Settings 182
Admin Security 182
Firmware 185
Web admin interface : automatically check for updates 185
Web admin interface : install updates manually 186
The InControl method 187
Time 188
Schedule 188
Email Notification 189
Event Log 192
SNMP 193
SMS Control 196
InControl 197
Configuration 197
Feature Add-ons 198
Reboot 199

Tools 200
Ping 200
Traceroute Test 201
PepVPN Test 201
Wake-on-LAN 202
CLI (Command Line Interface Support) 202

Status 203
Device 203
GPS Data 205
Active Sessions 205
Client List 207
WINS Client 208
UPnP / NAT-PMP 208
OSPF & RIPv2 209
BGP 209
SpeedFusion Status 210
Event Log 212

WAN Quality 214

Usage Reports 215
Real-Time 215
Hourly 216
Daily 216
Monthly 217

Appendix A: Restoration of Factory Defaults 220

Appendix B: Declaration 221

Introduction and Scope

Pepwave routers provide link aggregation and load balancing across multiple WAN connections, allowing a combination of technologies like 3G HSDPA, EVDO, 4G LTE, Wi-Fi, external WiMAX dongle, and satellite to be utilized to connect to the Internet.

The MAX wireless SD-WAN router series has a wide range of products suitable for many different deployments and markets. Entry level SD-WAN models such as the MAX BR1 are suitable for SMEs or branch offices. High-capacity SD-WAN routers such as the MAX HD2 are suitable for larger organizations and head offices.

This manual covers setting up Pepwave routers and provides an introduction to their features and usage.

Tips
Want to know more about Pepwave routers? Visit our YouTube Channel for a video introduction!   SMART CITIES CITY OF THE FUTURE DATA-TRANSFER INCOMING CALL https://youtu.be/13M-JHRAICA

Glossary

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

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

WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network

1 Product Features

Pepwave routers enable all LAN users to share broadband Internet connections, and they provide advanced features to enhance Internet access. Our Max BR wireless routers support multiple SIM cards. They can be configured to switch from using one SIM card to another SIM card according to different criteria, including wireless network reliability and data usage.

Our MAX HD series wireless routers are embedded with multiple 4G LTE modems, and allow simultaneous wireless Internet connections through multiple wireless networks. The wireless Internet connections can be bonded together using our SpeedFusion technology. This allows better reliability, larger bandwidth, and increased wireless coverage compared to use only one 4G LTE modem.

Below is a list of supported features on Pepwave routers. Features vary by model. For more information, please see peplink.com/products.

1.1 Supported Network Features

1.1.1 WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- Built-in cellular modems
- USB mobile connection(s)
- Wi-Fi WAN connection
- Network address translation (NAT)/port address translation (PAT)
- Inbound and outbound NAT mapping
- IPsec NAT-T and PPTP packet passthrough
- MAC address clone and passthrough
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS (supported service providers: changeip.com, dyndns.org, no-ip.org, tzo.com and DNS-O-Matic)
- Ping, DNS lookup, and HTTP-based health check

1.1.2 LAN

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

1.1.3 VPN

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

1.1.4 Firewall

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

1.1.5 Captive Portal

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

1.1.6 Outbound Policy

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

service

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

1.1.7 AP Controller

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

1.1.8 QoS

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

1.2 Other Supported Features

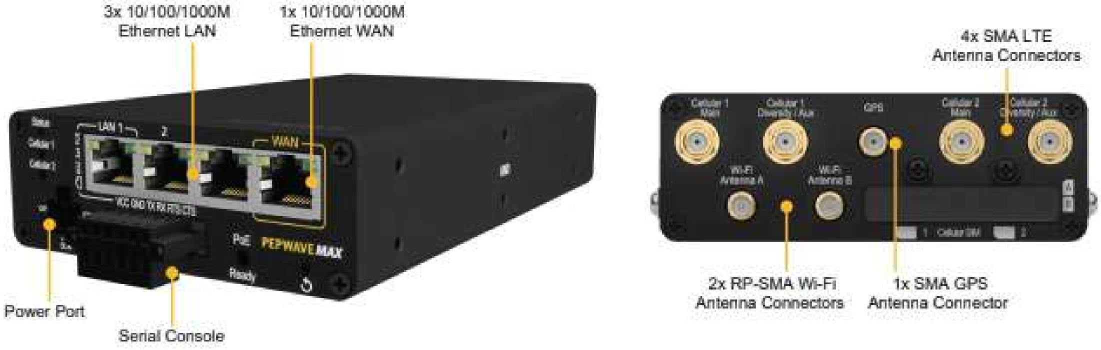
- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface (default redirection to HTTPS)
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Time server synchronization
- SNMP
- Email notification
- Read-only user for web admin
- Shared IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Built-in WINS servers*
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Event log
- Active sessions
- Client list
- WINS client list *
- UPnP / NAT-PMP
- Real-time, hourly, daily, and monthly bandwidth usage reports and charts
- IPv6 support
- Support USB tethering on Android 2.2+ phones

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

2 Pepwave MAX Mobile Router Overview

2.1 MAX Transit Pro E

2.1.1 Panel Appearance



3x 10/100/1000M Ethernet LAN
1x 10/100/1000M Ethernet WAN
4x SMA LTE Antenna Connectors
Status
Cellular 1
Cellular 2
LAN 1
2
WAN
VCC GND TX RX RTS CTS
PoE
PEPWAVE MAX
Ready
Cellular 1 Main
Cellular 1 Diversity / Aux
GPS
Cellular 2 Main
Cellular 2 Diversity / Aux
Wi-Fi Antenna A
Wi-Fi Antenna B
1 Cellular SIM 2
Power Port
Serial Console
2x RP-SMA Wi-Fi Antenna Connectors
1x SMA GPS Antenna Connector

2.1.2 LED Indicators

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

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

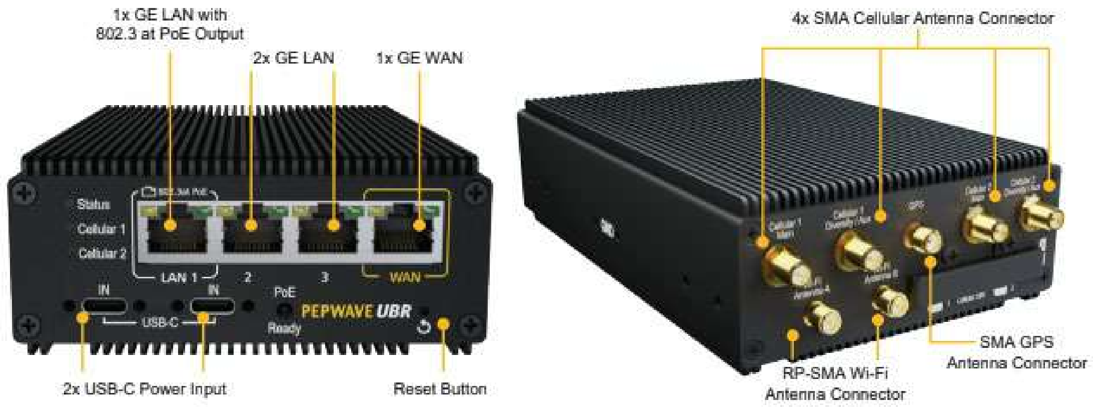
Cellular Indicators		
Cellular 1 / Cellular 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic

	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.2 MAX Transit Pro E

2.2.1 Panel Appearance



2.2.2 LED Indicators

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

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

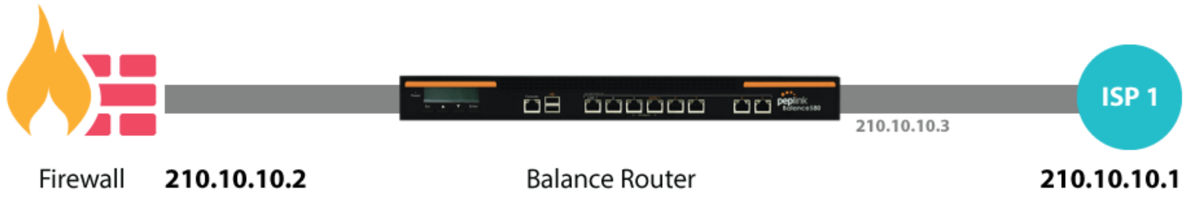
Cellular Indicators		
Cellular 1 / Cellular 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)

	Green	Connected to network(s)

LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

3 Advanced Feature Summary

3.1 Drop-in Mode and LAN Bypass: Transparent Deployment



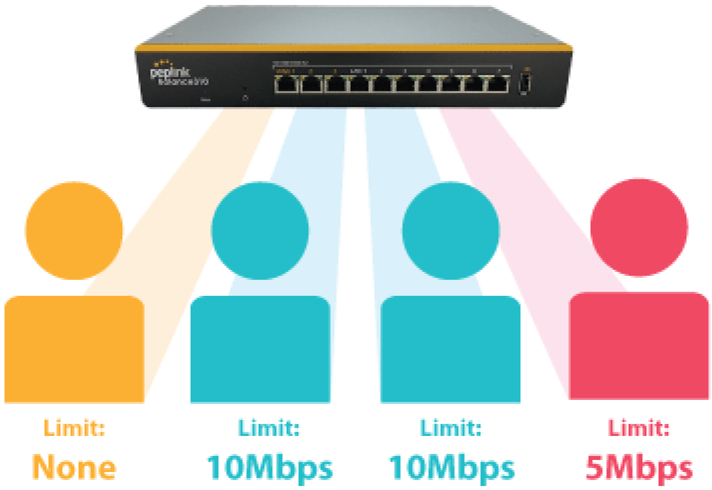
As your organization grows, it may require more bandwidth, but modifying your network can be tedious. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. For any reason your Peplink router looses power, the **LAN Bypass** will safely and automatically bypass the Peplink router to resume your original network connection.

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

3.2 QoS: Clearer VoIP

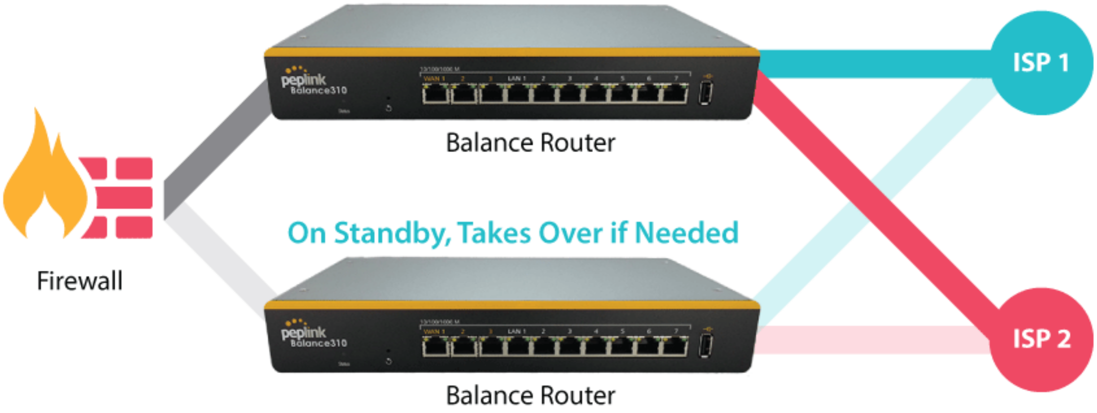
VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.

3.3 Per-User Bandwidth Control



With per-user bandwidth control, you can define bandwidth control policies for up to 3 groups of users to prevent network congestion. Define groups by IP address and subnet, and set bandwidth limits for every user in the group.

3.4 High Availability via VRRP



When your organization has a corporate requirement demanding the highest availability with no single point of failure, you can deploy two Peplink routers in High Availability mode. With High Availability mode, the second device will take over when needed.

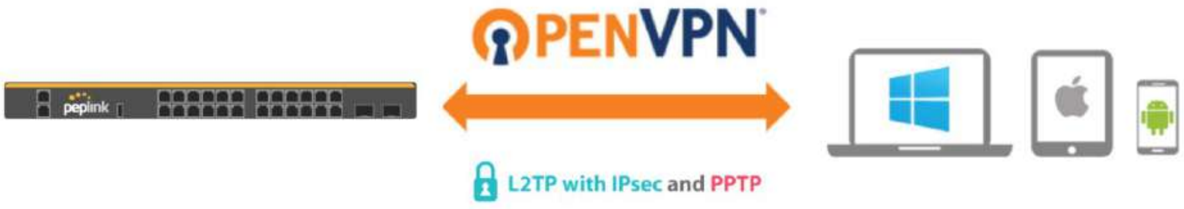
Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

3.5 USB Modem and Android Tethering

For increased WAN diversity, plug in a USB LTE modem as a backup. Peplink routers are compatible with over 200 modem types. You can also tether to smartphones running Android 4.1.X and above.

Compatible with: MAX 700, HD2 (all variants except IP67), HD4 (All variants)

3.6 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

3.7 SIM-card USSD support

Cellular-enabled routers can now use USSD to check their SIM card’s balance, process pre-paid cards, and configure carrier-specific services.

Click here for full instructions on using USSD

3.8 DPI Engine

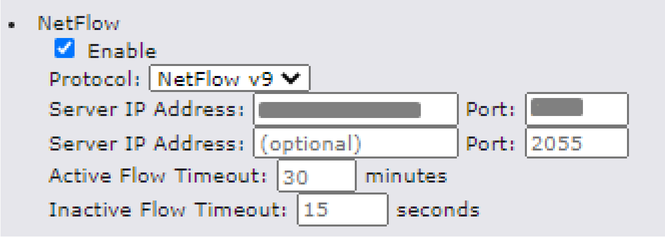
The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.

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

3.9 NetFlow

NetFlow protocol is used to track network traffic. Tracking information from NetFlow can be sent to the NetFlow collector, which analyzes data and generates reports for review.

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



- NetFlow

☑ Enable

Protocol: NetFlow v9

Server IP Address: [redacted] Port: [redacted]

Server IP Address: (optional) Port: 2055

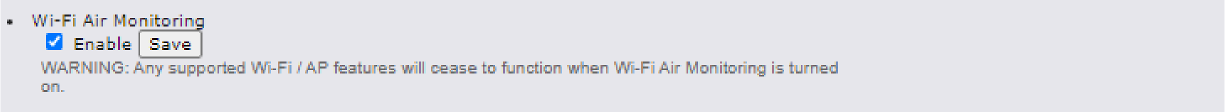
Active Flow Timeout: 30 minutes

Inactive Flow Timeout: 15 seconds

3.10 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.

4 Installation

The following section details connecting Pepwave routers to your network.

4.1 Preparation

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

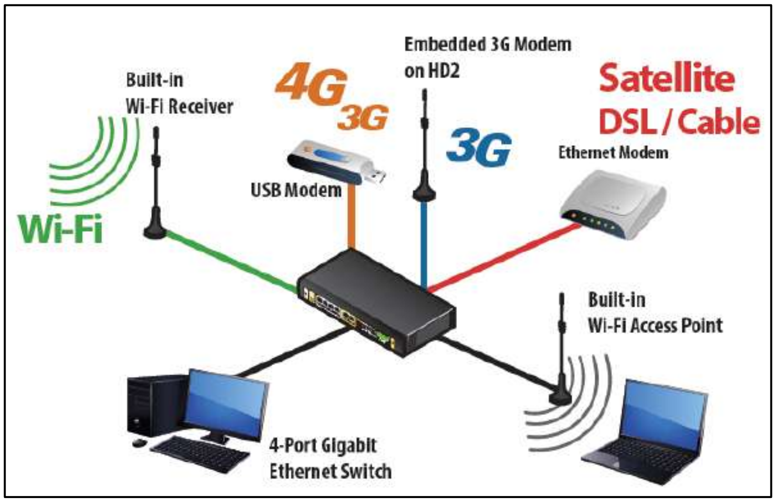
- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
  - **Ethernet WAN**: A 10/100/1000BaseT UTP cable with RJ45 connector
  - **USB**: A USB modem
  - **Embedded modem**: A SIM card for GSM/HSPA service
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

4.2 Constructing the Network

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

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

The following figure schematically illustrates the resulting configuration:



4.3 Configuring the Network Environment

To ensure that the Pepwave router works properly in the LAN environment and can access the Internet via WAN connections, please refer to the following setup procedures:

- LAN configuration

  For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.

  For advanced configuration, go to **Section 9, Configuring the LAN Interface(s)**.

- WAN configuration

  For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.

  For advanced configuration, go to **Section 9.2, Captive Portal**.

5 Mounting the Unit

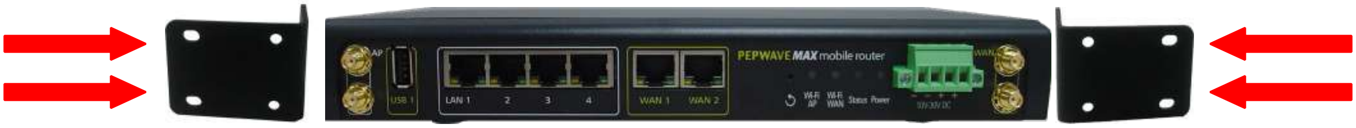
5.1 Wall Mount

The Pepwave MAX 700/HD2/On-The-Go can be wall mounted using screws. After adding the screw on the wall, slide the MAX in the screw hole socket as indicated below. Recommended screw specification: M3.5 x 20mm, head diameter 6mm, head thickness 2.4mm.

The Pepwave MAX BR1 requires four screws for wall mounting.

5.2 Car Mount

The Pepwave MAX700/HD2 can be mounted in a vehicle using the included mounting brackets. Place the mounting brackets by the two sides and screw them onto the device.



6 Connecting to the Web Admin Interface

1. Start a web browser on a computer that is connected with the Pepwave router through the LAN.
2. To connect to the router's web admin interface, enter the following LAN IP address in the address field of the web browser:

   http://192.168.50.1

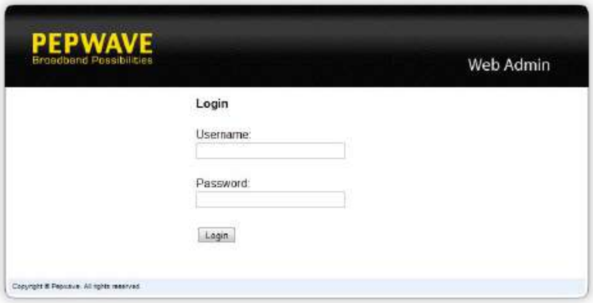
   (This is the default LAN IP address for Pepwave routers.)

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

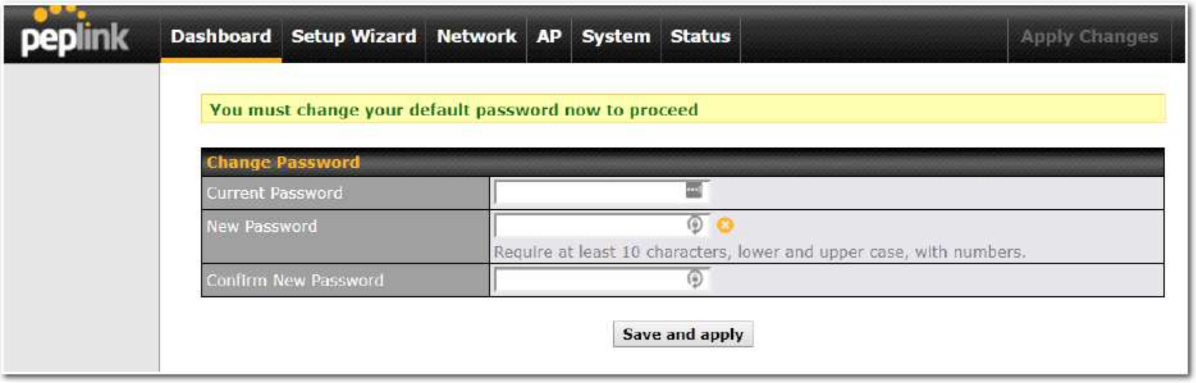
   Username: admin

   Password: admin

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



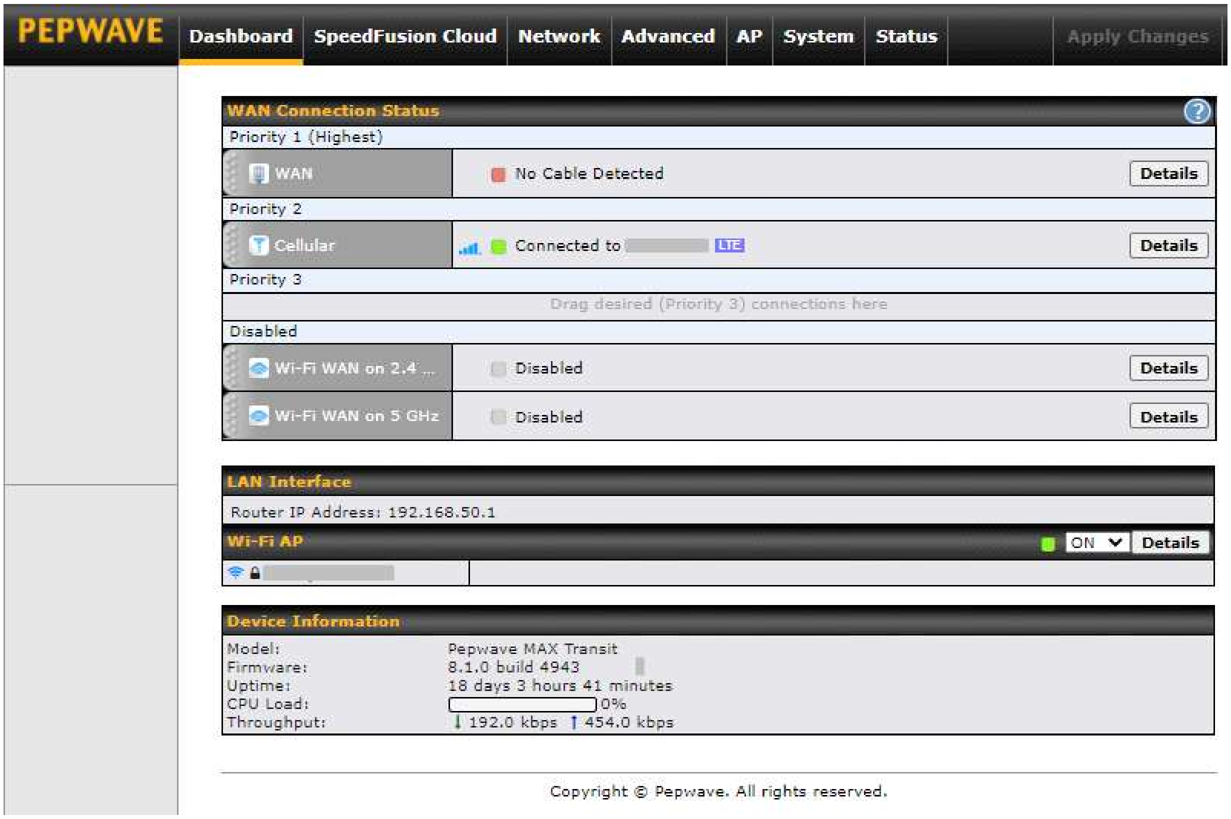
- You must change the default password on the first successful logon.
- Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.
- When HTTP is selected, the URL will be redirected to HTTPS by default.



You must change your default password now to proceed

Change Password	
Current Password	
New Password	Require at least 10 characters, lower and upper case, with numbers.
Confirm New Password	

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



WAN Connection Status

Priority 1 (Highest)

WAN — No Cable Detected

Priority 2

Cellular — Connected to [redacted] LTE

Priority 3

Drag desired (Priority 3) connections here

Disabled

Wi-Fi WAN on 2.4 ... — Disabled

Wi-Fi WAN on 5 GHz — Disabled

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP

[redacted]

Device Information

Model:	Pepwave MAX Transit
Firmware:	8.1.0 build 4943 [redacted]
Uptime:	18 days 3 hours 41 minutes
CPU Load:	0%
Throughput:	↓ 192.0 kbps ↑ 454.0 kbps

Copyright © Pepwave. All rights reserved.

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

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

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

7 SpeedFusion Cloud

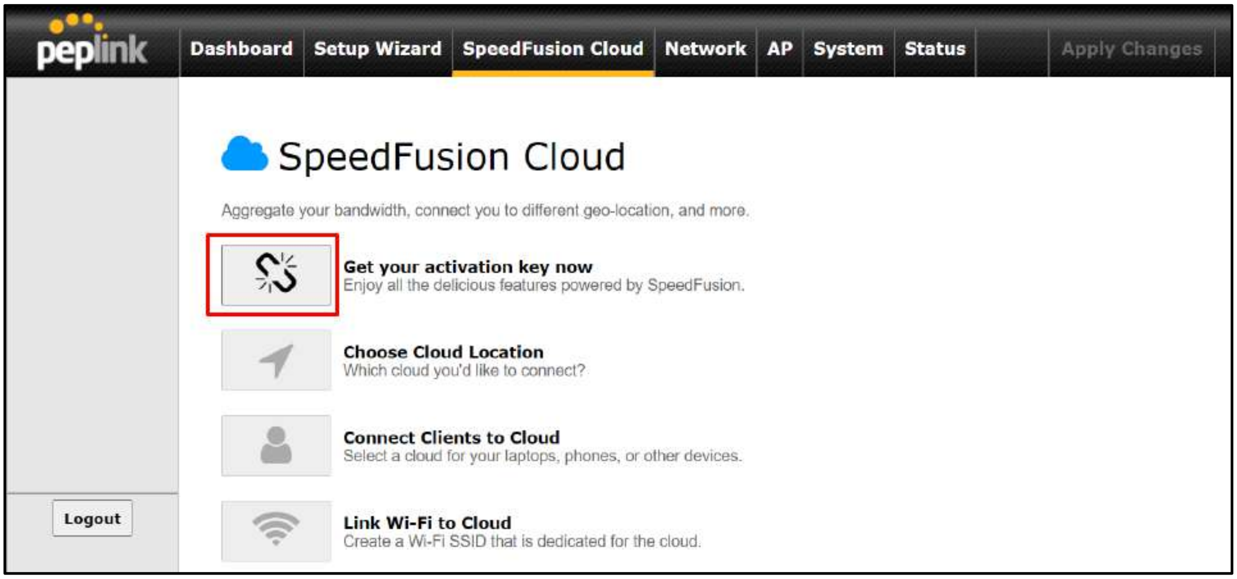
With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*

Hosted by peplink
SpeedFusion
Cloud
peplink

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

7.1 Activate SpeedFusion Cloud Service

You are entitled to a 30-day 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.



SpeedFusion Cloud

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

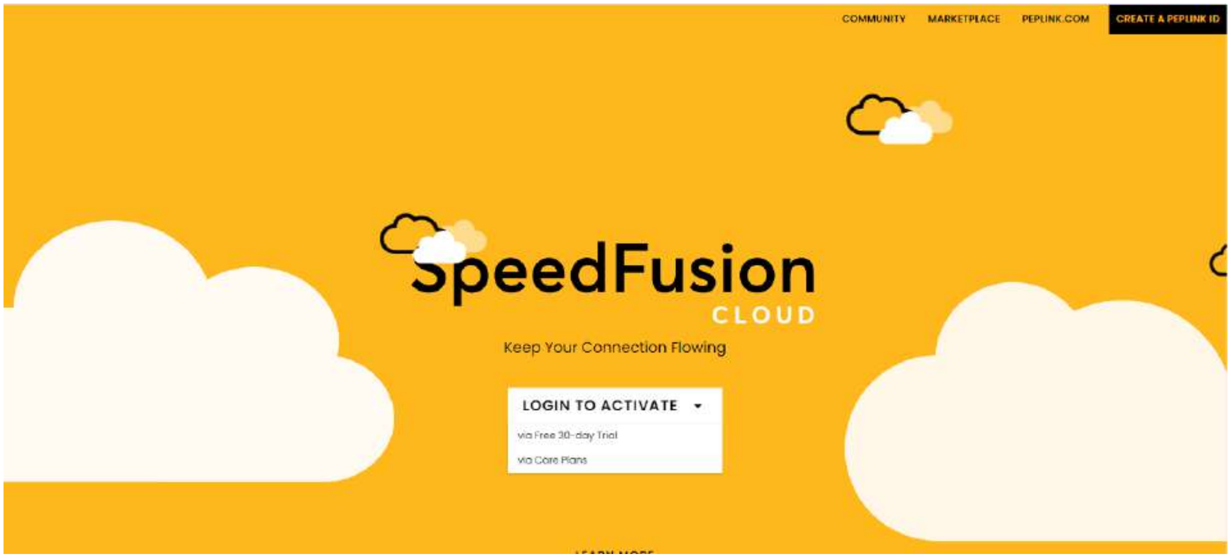
Get your activation key now
Enjoy all the delicious features powered by SpeedFusion.

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

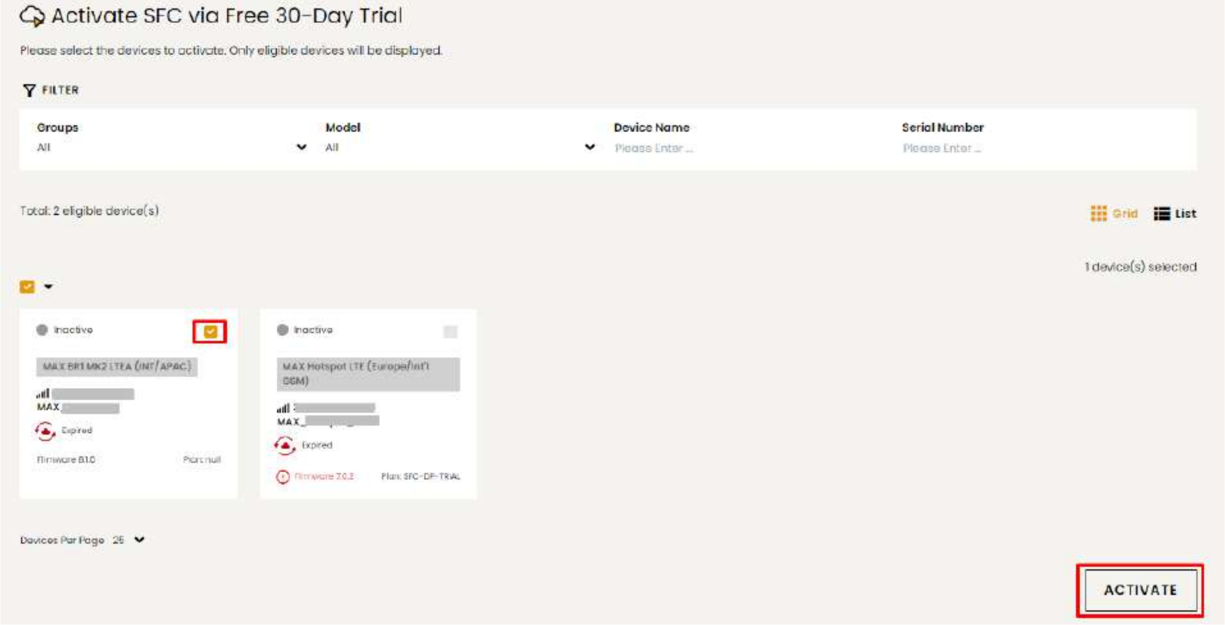
Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

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

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



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



Activate SFC via Free 30-Day Trial

Please select the devices to activate. Only eligible devices will be displayed.

FILTER

Groups: All
Model: All
Device Name: Please Enter ...
Serial Number: Please Enter ...

Total: 2 eligible device(s)

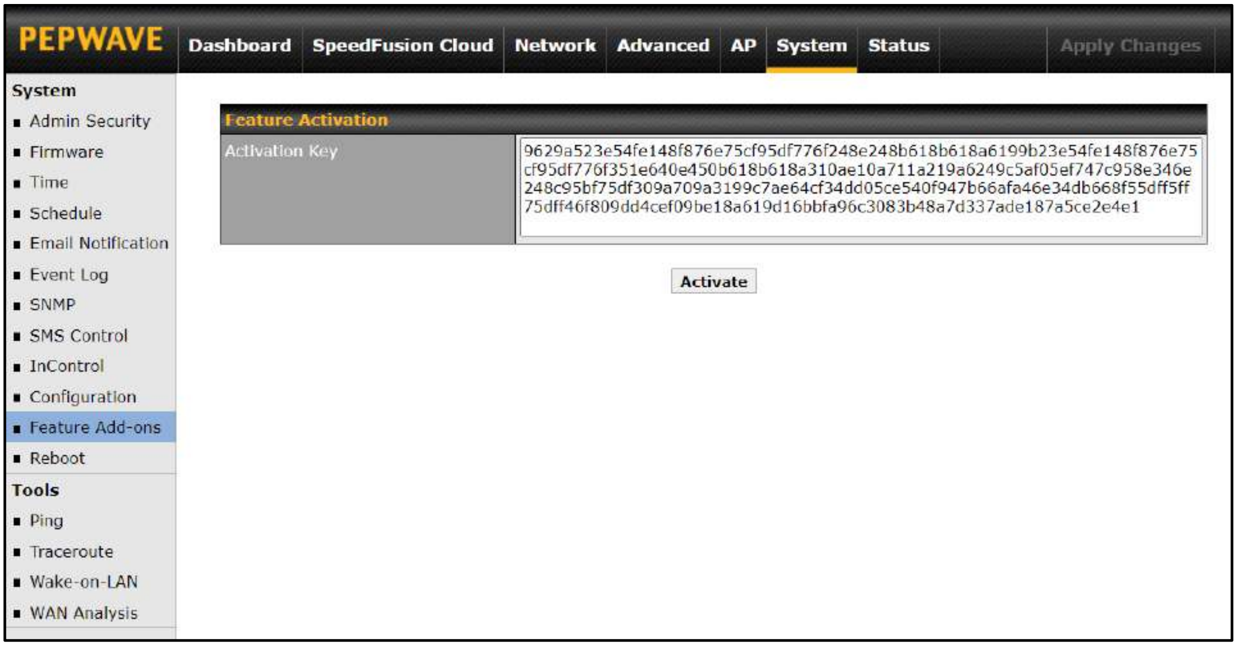
1 device(s) selected

☑ Inactive
MAX BR1 MK2 LTEA (INT/APAC)
[redacted]
MAX [redacted]
Expired
Firmware 8.1.0   Plan: null

□ Inactive
MAX Hotspot LTE (Europe/Int'l GSM)
[redacted]
MAX_[redacted]
Expired
Firmware 7.0.2   Plan: SFC-DF-TRIAL

Devices Per Page 25

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



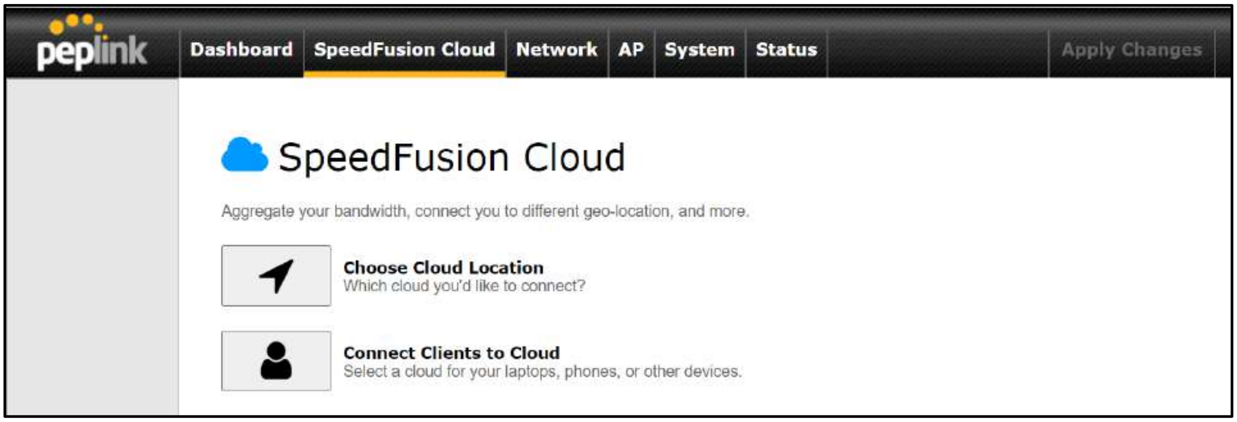
Feature Activation

Activation Key

```
9629a523e54fe148f876e75cf95df776f248e248b618b618a6199b23e54fe148f876e75
cf95df776f351e640e450b618b618a310ae10a711a219a6249c5af05ef747c958e346e
248c95bf75df309a709a3199c7ae64cf34dd05ce540f947b66afa46e34db668f55dff5ff
75dff46f809dd4cef09be18a619d16bbfa96c3083b48a7d337ade187a5ce2e4e1
```

7.2 Enable SpeedFusion Cloud

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



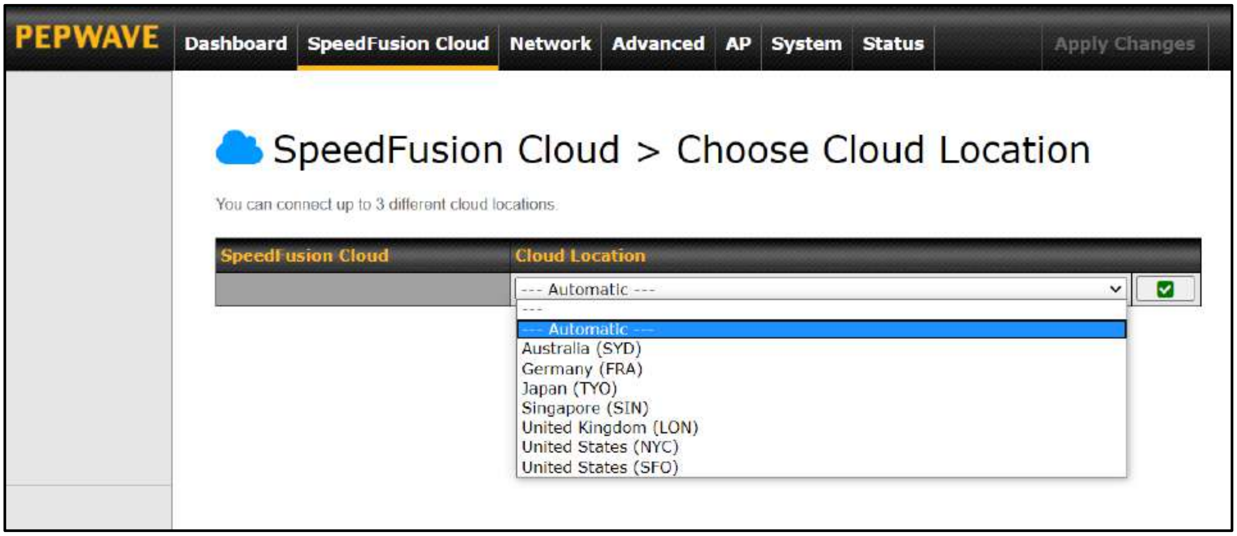
SpeedFusion Cloud

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

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

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

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

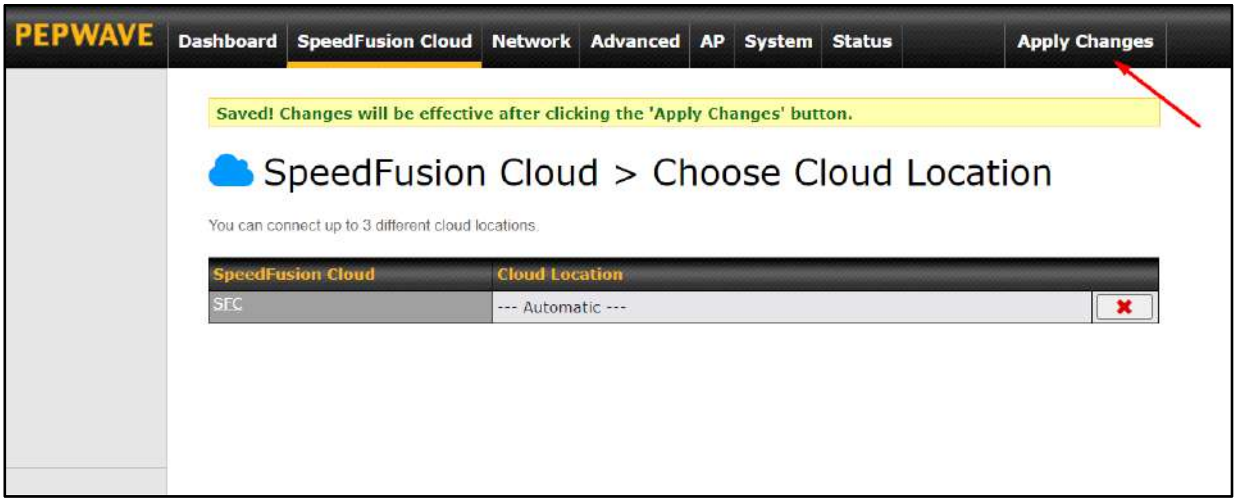


SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location
	--- Automatic --- ☑

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

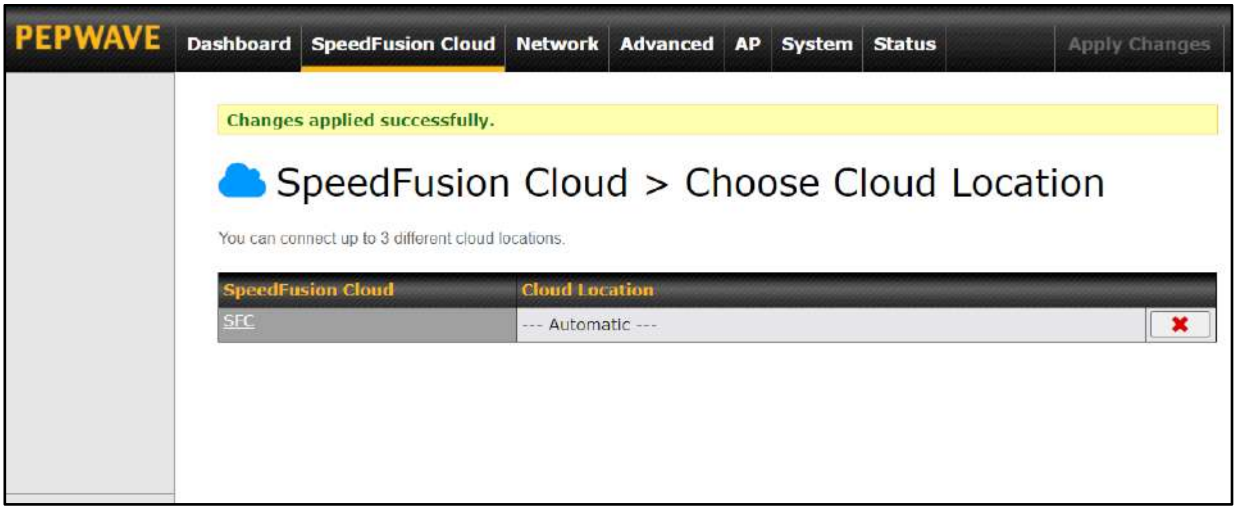


Saved! Changes will be effective after clicking the 'Apply Changes' button.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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



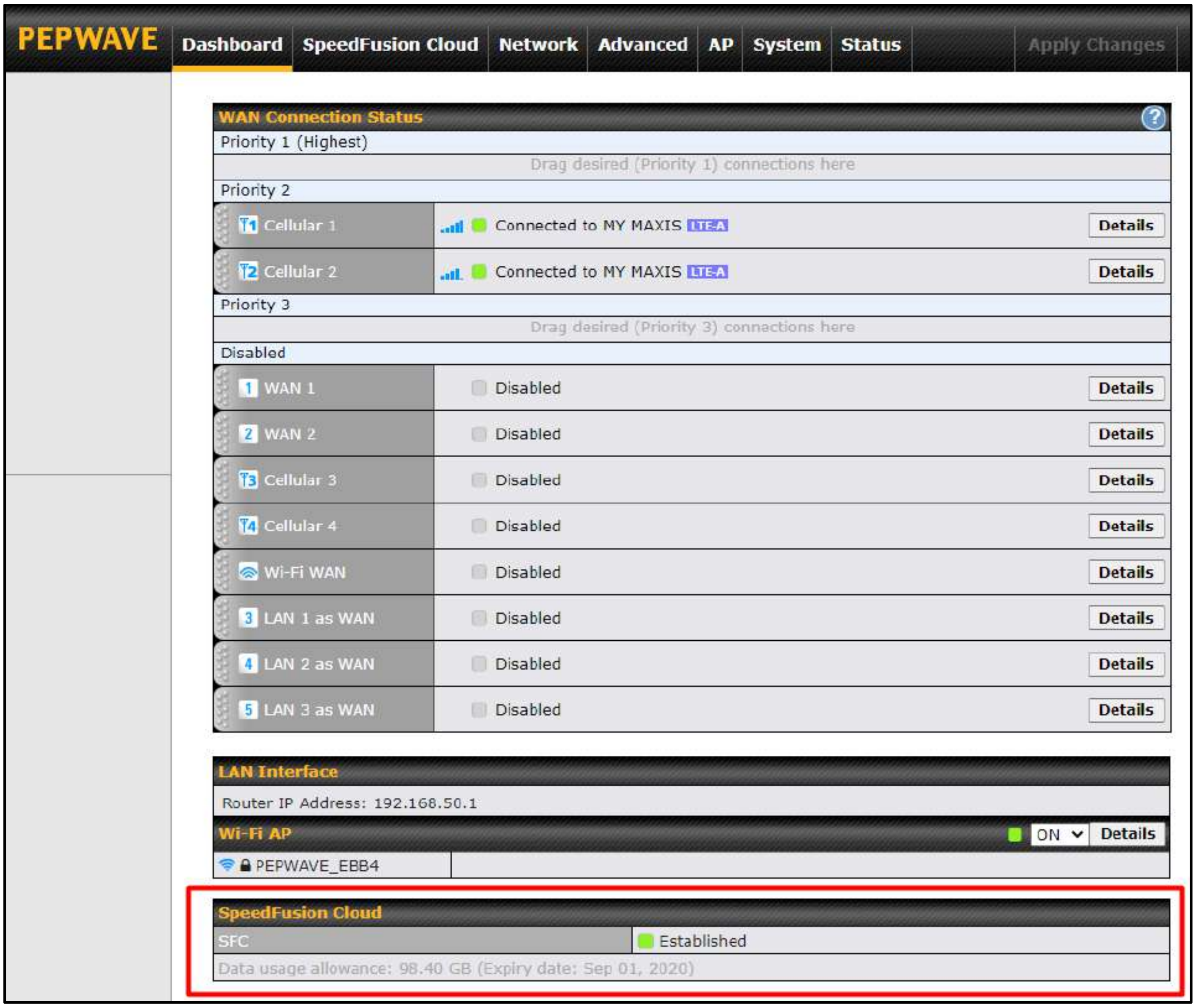
Changes applied successfully.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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

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



WAN Connection Status

Priority 1 (Highest)	
	Drag desired (Priority 1) connections here
Priority 2	
T1 Cellular 1	🟩 Connected to MY MAXIS LTE-A — Details
T2 Cellular 2	🟩 Connected to MY MAXIS LTE-A — Details
Priority 3	
	Drag desired (Priority 3) connections here
Disabled	
1 WAN 1	Disabled — Details
2 WAN 2	Disabled — Details
T3 Cellular 3	Disabled — Details
T4 Cellular 4	Disabled — Details
Wi-Fi WAN	Disabled — Details
3 LAN 1 as WAN	Disabled — Details
4 LAN 2 as WAN	Disabled — Details
5 LAN 3 as WAN	Disabled — Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP 🟩 ON Details

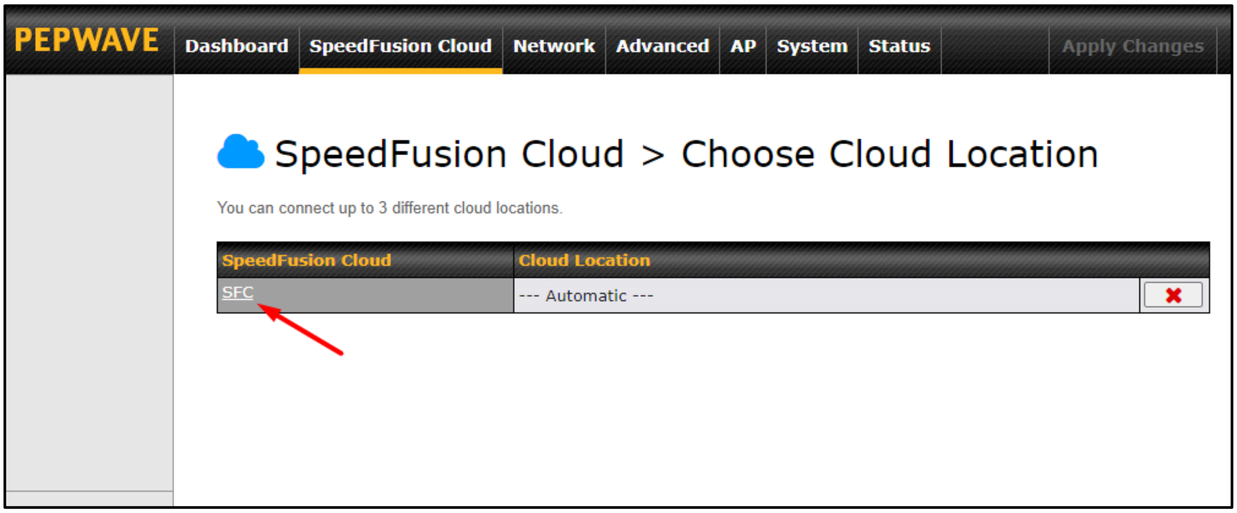
PEPWAVE_EBB4

SpeedFusion Cloud

SFC 🟩 Established

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

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

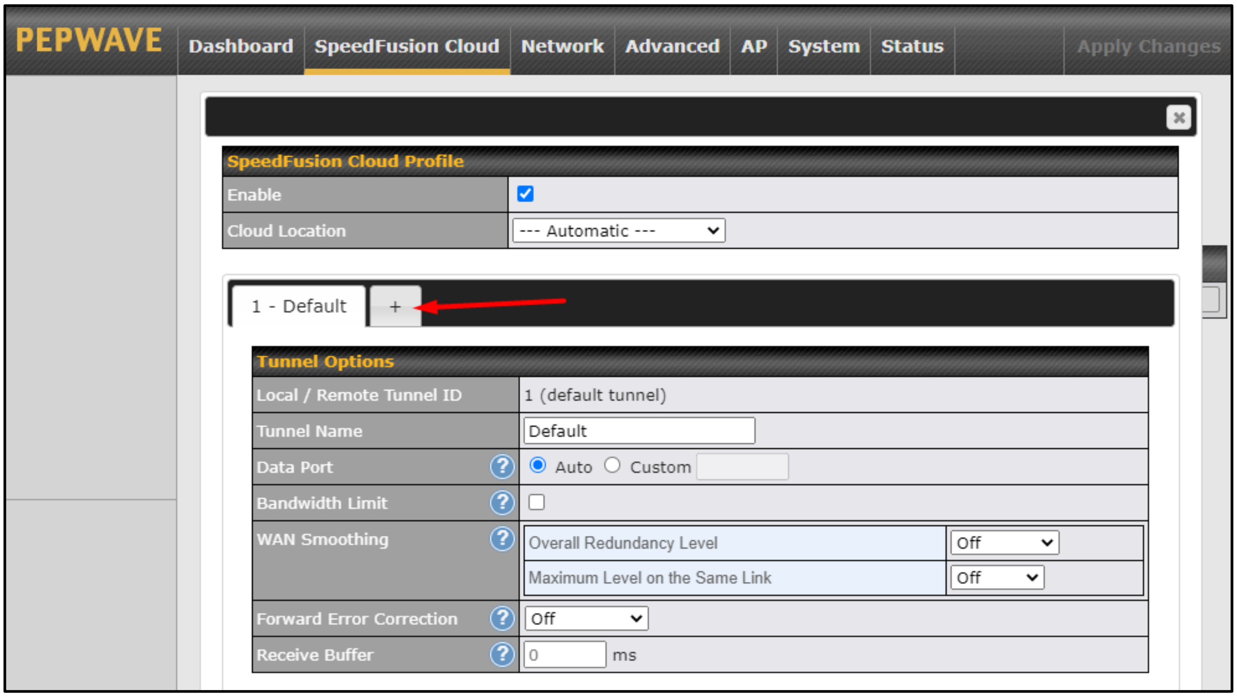


SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

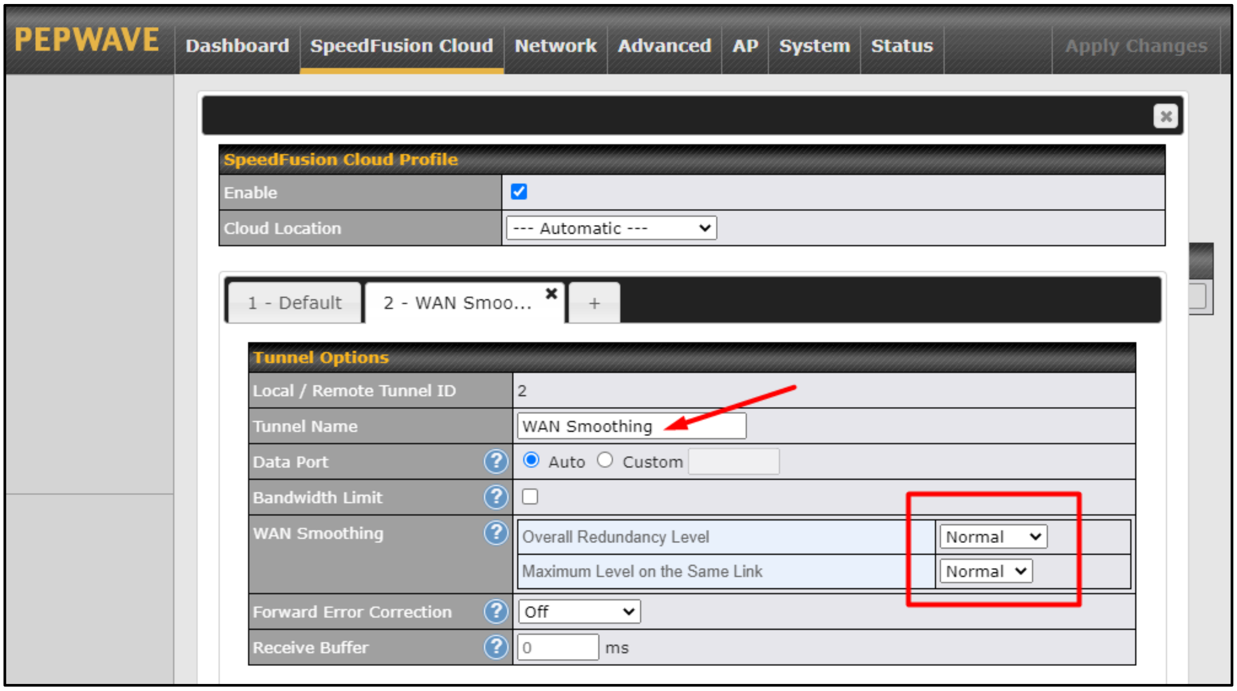
SpeedFusion Cloud	Cloud Location	
SFC	--- Automatic ---	✖

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



SpeedFusion Cloud Profile	
Enable	☑
Cloud Location	--- Automatic ---

Tunnel Options		
Local / Remote Tunnel ID	1 (default tunnel)	
Tunnel Name	Default	
Data Port	● Auto ○ Custom	
Bandwidth Limit	□	
WAN Smoothing	Overall Redundancy Level	Off
	Maximum Level on the Same Link	Off
Forward Error Correction	Off	
Receive Buffer	0 ms	



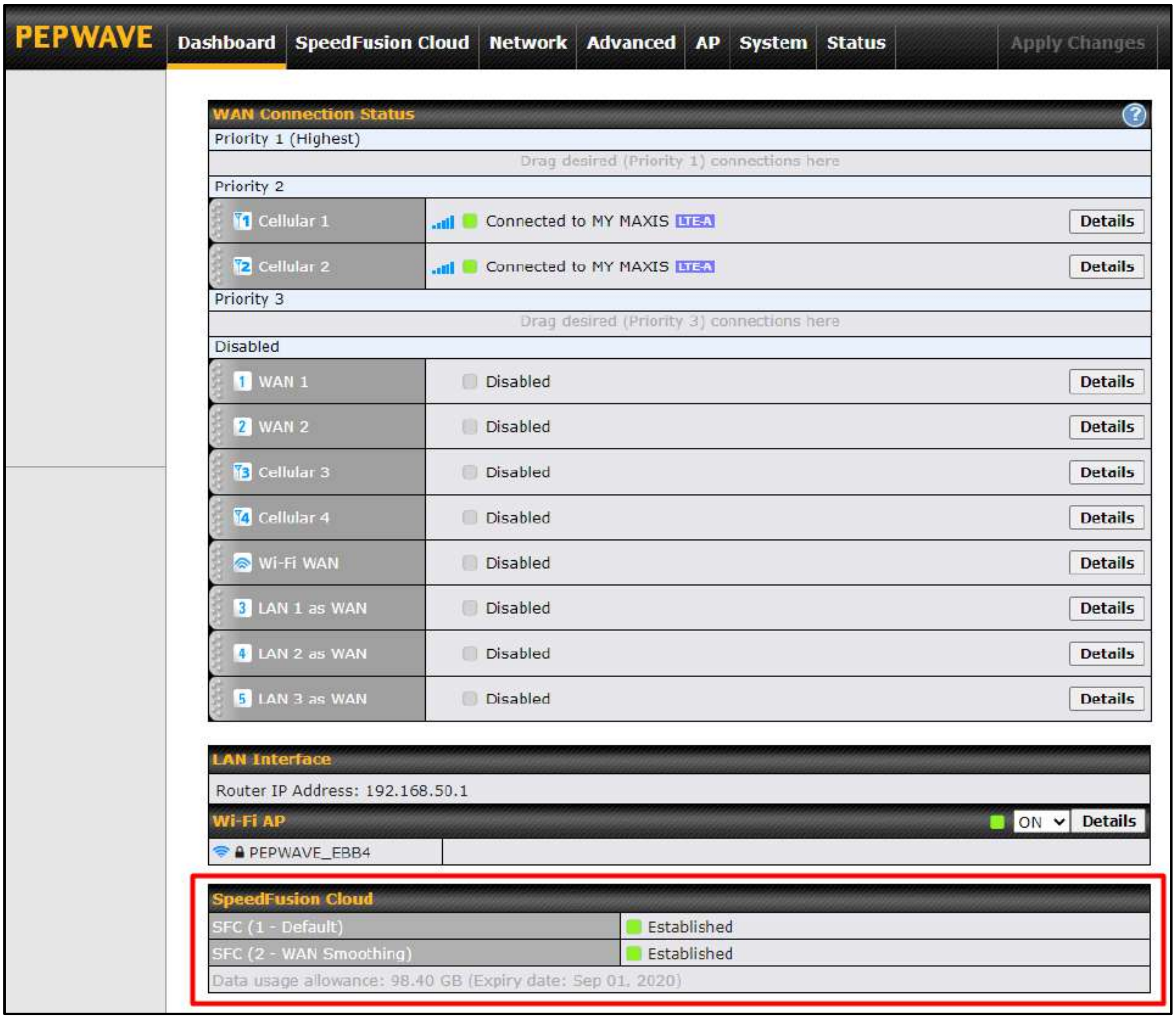
SpeedFusion Cloud Profile

Enable	☑
Cloud Location	--- Automatic ---

Tunnel Options

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

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



WAN Connection Status

Priority 1 (Highest)		
	Drag desired (Priority 1) connections here	
Priority 2		
Cellular 1	🟩 Connected to MY MAXIS LTE-A	Details
Cellular 2	🟩 Connected to MY MAXIS LTE-A	Details
Priority 3		
	Drag desired (Priority 3) connections here	
Disabled		
WAN 1	Disabled	Details
WAN 2	Disabled	Details
Cellular 3	Disabled	Details
Cellular 4	Disabled	Details
Wi-Fi WAN	Disabled	Details
LAN 1 as WAN	Disabled	Details
LAN 2 as WAN	Disabled	Details
LAN 3 as WAN	Disabled	Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP 🟩 ON Details

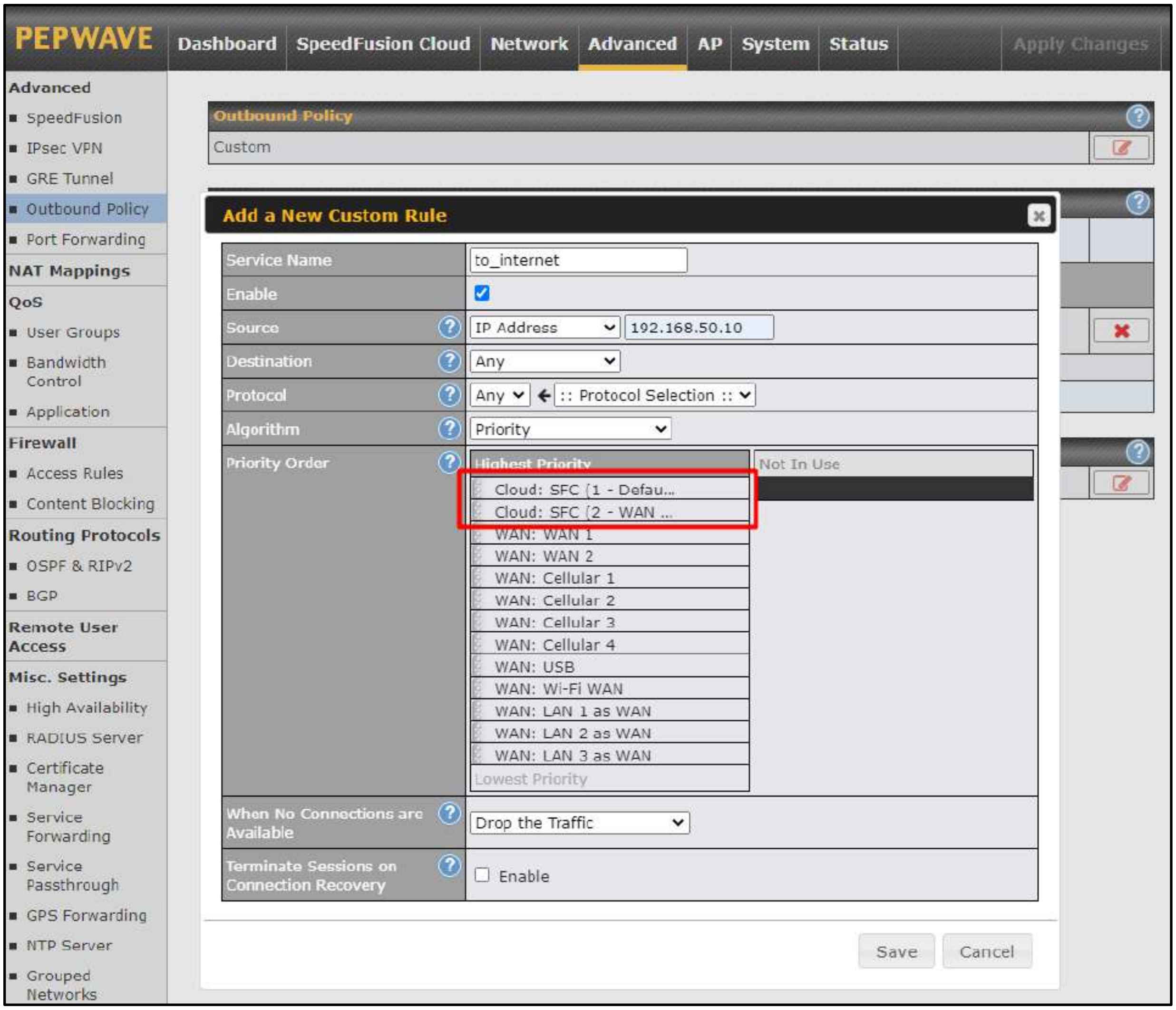
PEPWAVE_EBB4

SpeedFusion Cloud

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

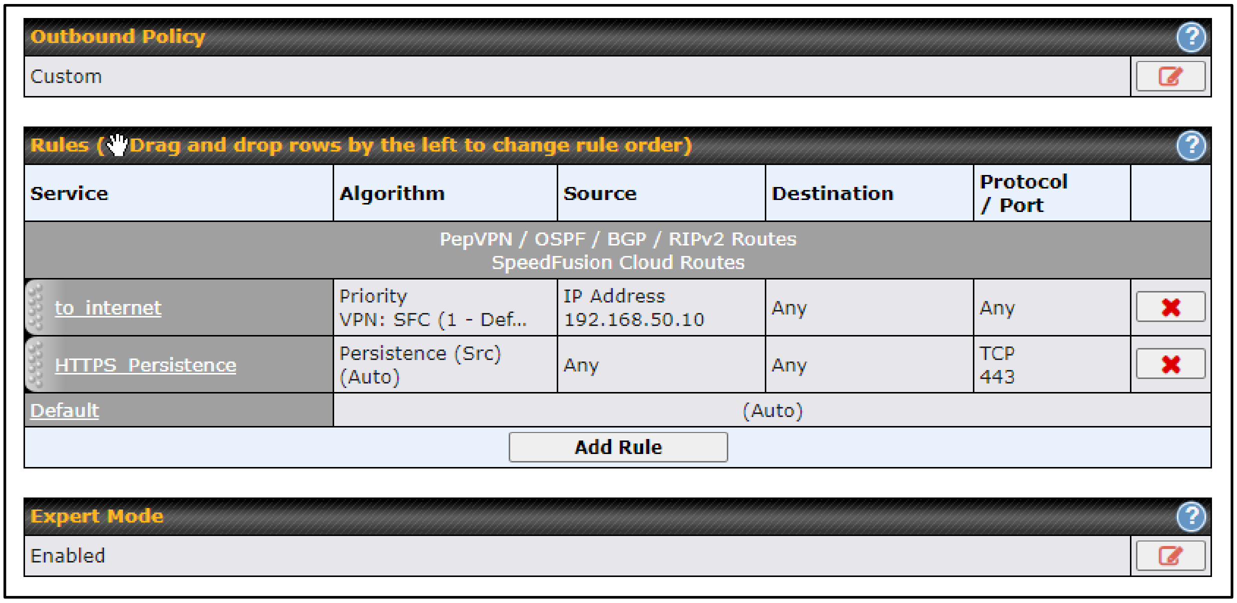
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)

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



Add a New Custom Rule

Service Name	to_internet
Enable	☑
Source	IP Address 192.168.50.10
Destination	Any
Protocol	Any ← :: Protocol Selection ::
Algorithm	Priority
Priority Order	Highest Priority Cloud: SFC (1 - Defau... Cloud: SFC (2 - WAN ... WAN: WAN 1 WAN: WAN 2 WAN: Cellular 1 WAN: Cellular 2 WAN: Cellular 3 WAN: Cellular 4 WAN: USB WAN: Wi-Fi WAN WAN: LAN 1 as WAN WAN: LAN 2 as WAN WAN: LAN 3 as WAN Lowest Priority Not In Use
When No Connections are Available	Drop the Traffic
Terminate Sessions on Connection Recovery	□ Enable



Outbound Policy

Custom

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

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

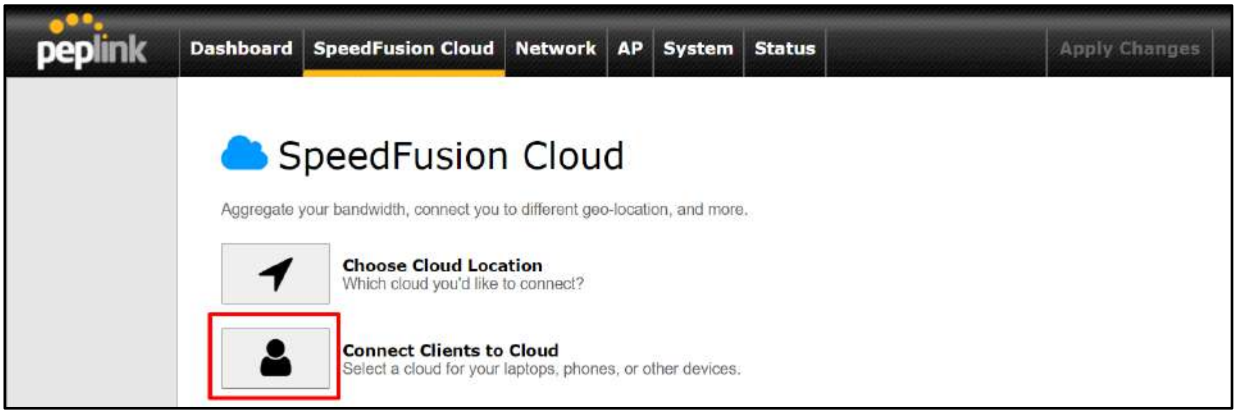
Add Rule

Expert Mode

Enabled

7.3 Connect Clients to Cloud

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



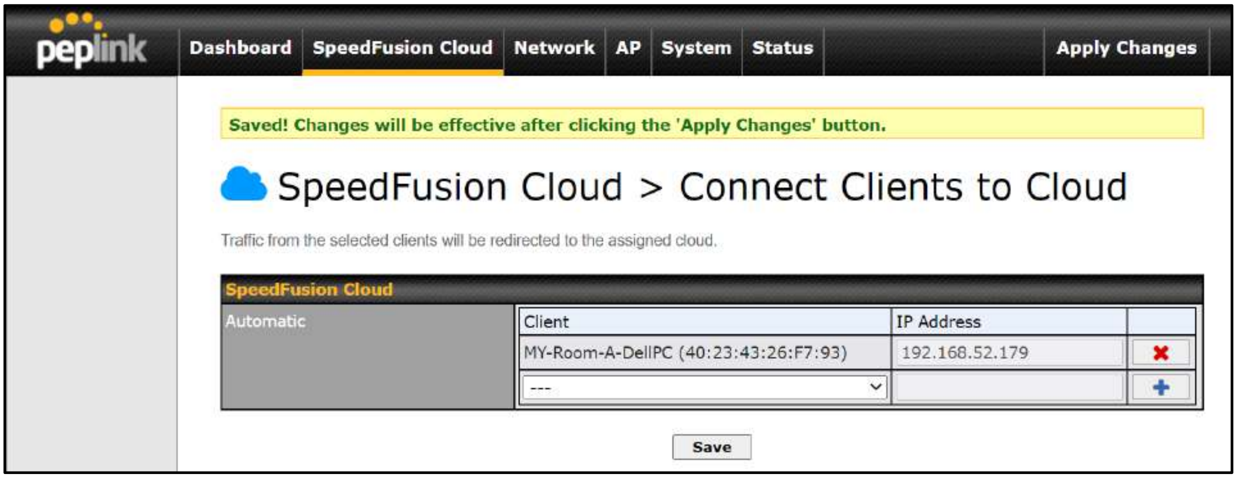
SpeedFusion Cloud

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

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

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

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



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

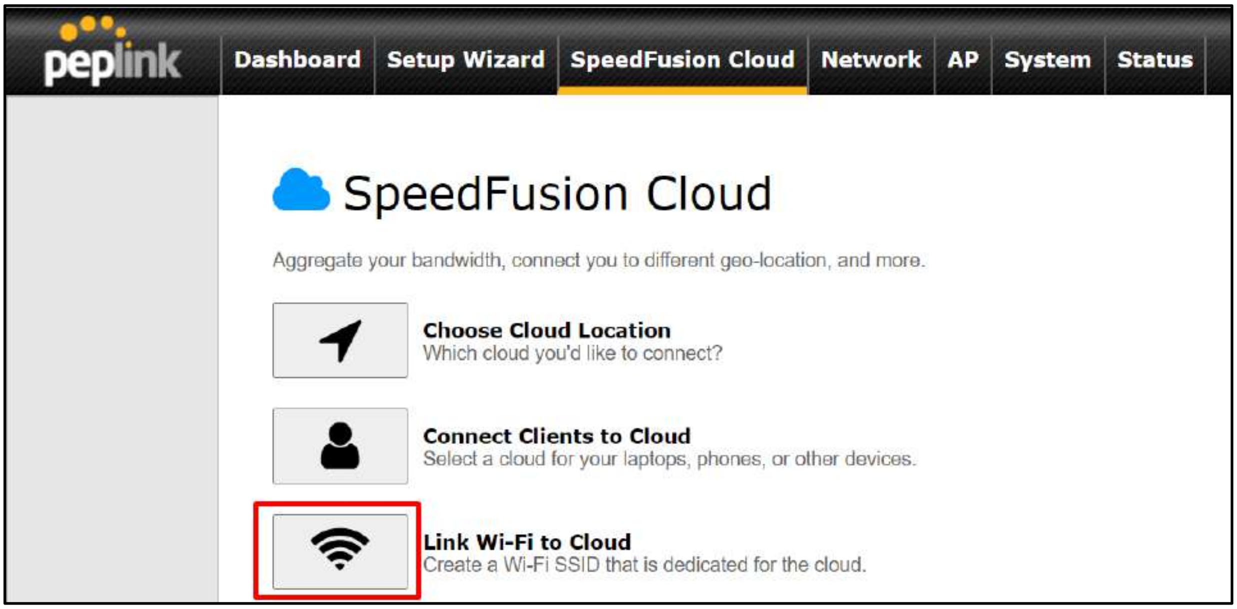
SpeedFusion Cloud > Connect Clients to Cloud

Traffic from the selected clients will be redirected to the assigned cloud.

SpeedFusion Cloud	Client	IP Address	
Automatic	MY-Room-A-DellPC (40:23:43:26:F7:93)	192.168.52.179	✖
	---		+

7.4 Link Wi -Fi to Cloud

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



SpeedFusion Cloud

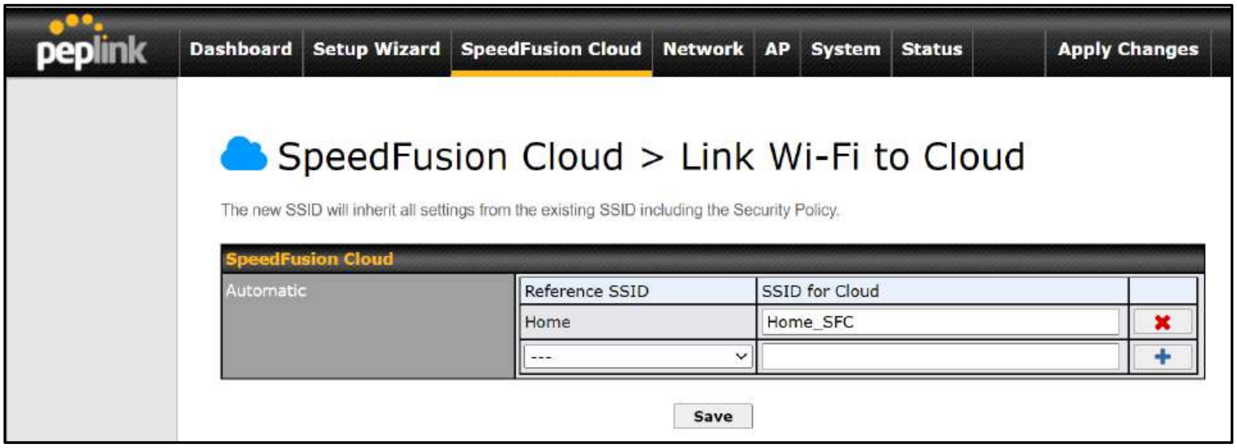
Aggregate your bandwidth, connect you to different geo-location, and more.

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

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

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

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



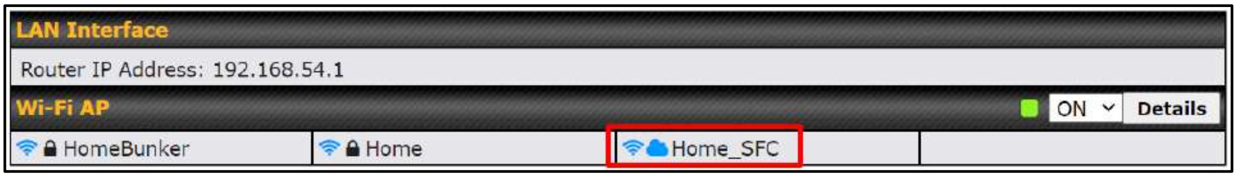
SpeedFusion Cloud > Link Wi-Fi to Cloud

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

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

Save

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



LAN Interface

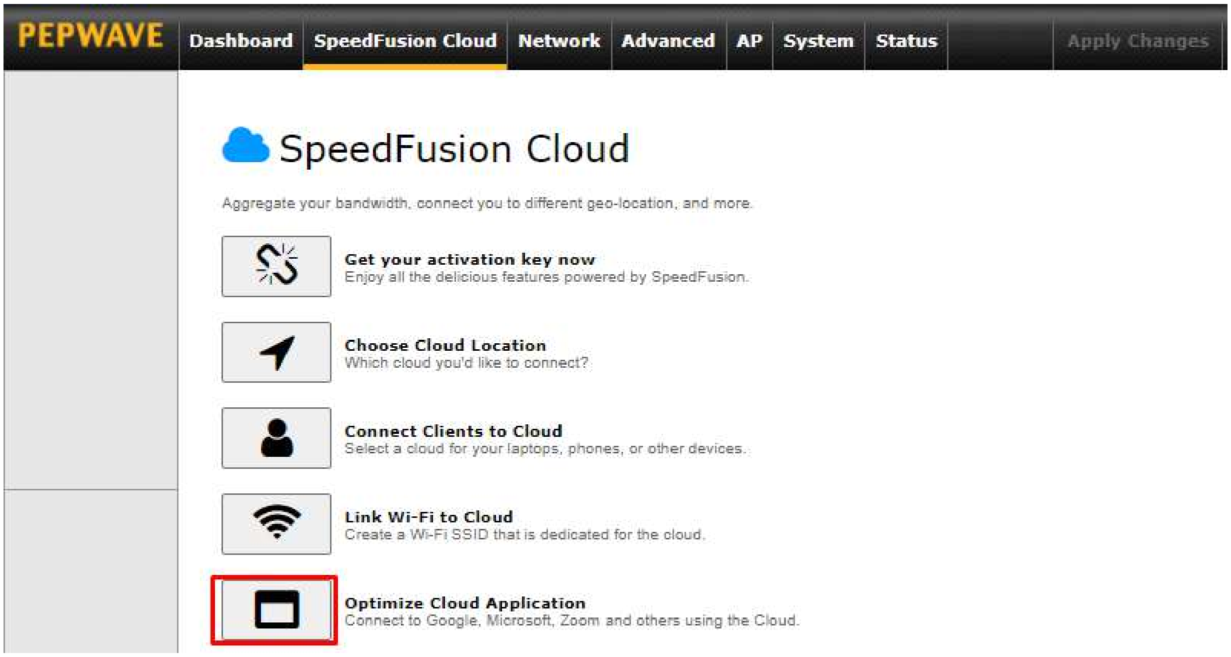
Router IP Address: 192.168.54.1

Wi-Fi AP 🟩 ON Details

HomeBunker	Home	Home_SFC	

7.5 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**.



SpeedFusion Cloud

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

Get your activation key now
Enjoy all the delicious features powered by SpeedFusion.

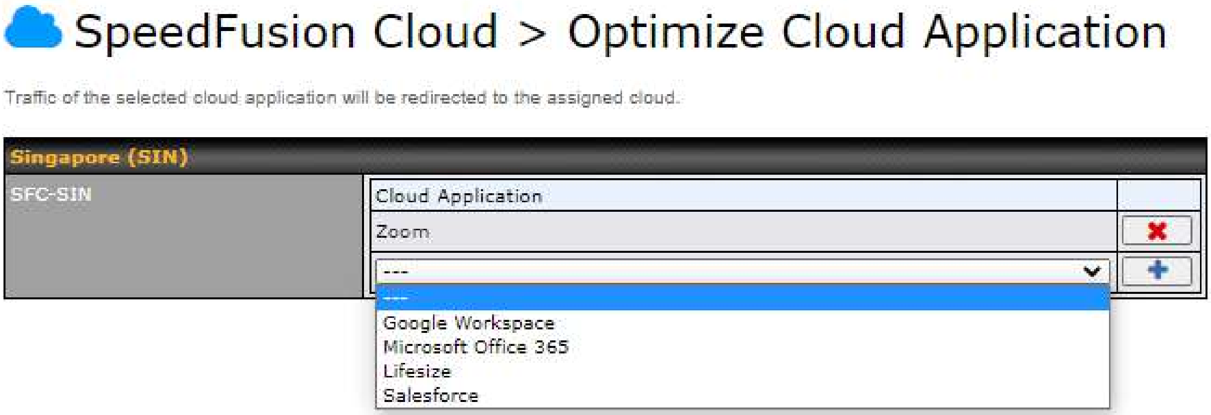
Choose Cloud Location
Which cloud you'd like to connect?

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

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

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

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



SpeedFusion Cloud > Optimize Cloud Application

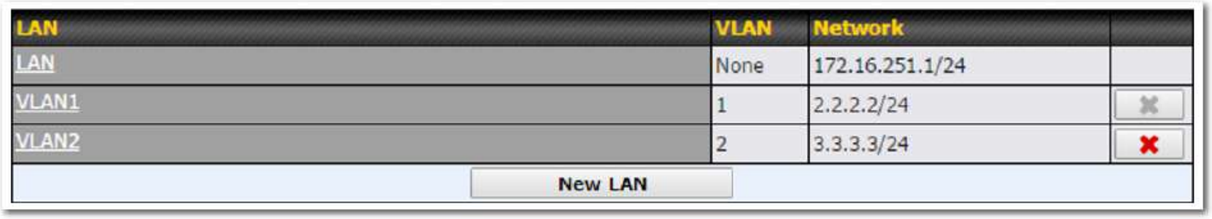
Traffic of the selected cloud application will be redirected to the assigned cloud.

Singapore (SIN)		
SFC-SIN	Cloud Application	
	Zoom	✖
	---	✚

8 Configuring the LAN Interface(s)

8.1 Basic Settings

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

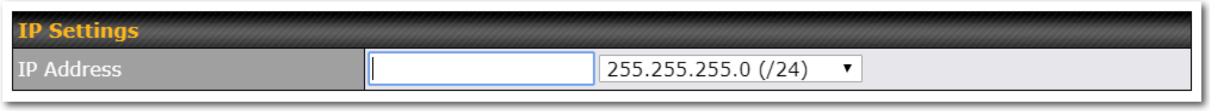


LAN	VLAN	Network	
LAN	None	172.16.251.1/24	
VLAN1	1	2.2.2.2/24	✖
VLAN2	2	3.3.3.3/24	✖

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

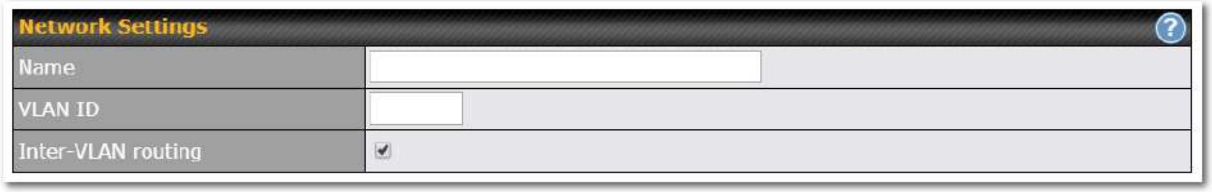
Alternatively, a red “X” means that there are no settings using the VLAN. You can delete that VLAN by clicking the red “X”

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



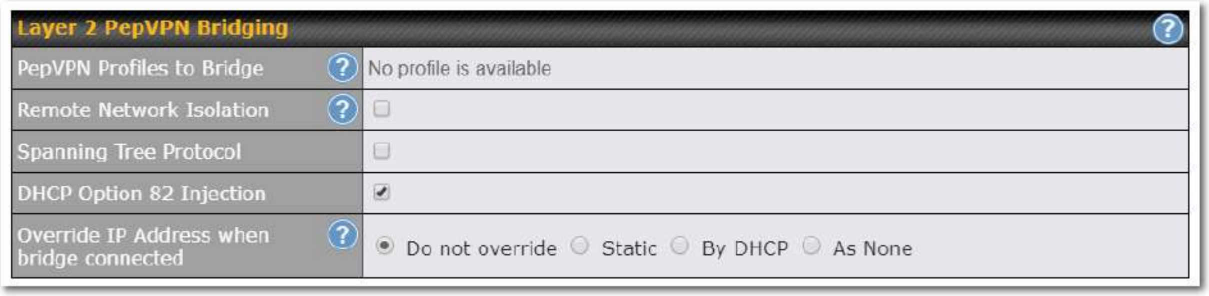
IP Settings		
IP Address		255.255.255.0 (/24) ▾

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



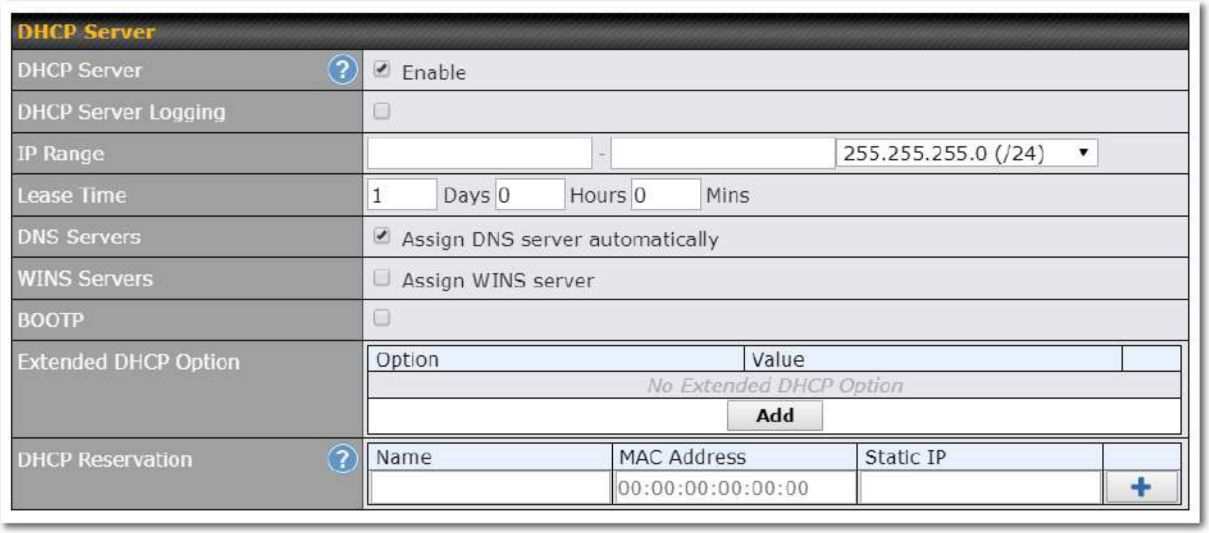
Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☑

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



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

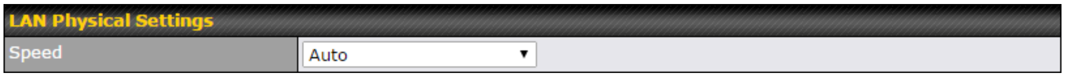
Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Remote Network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



DHCP Server	
DHCP Server	☑ Enable
DHCP Server Logging	□
IP Range	- 255.255.255.0 (/24) ▾
Lease Time	1 Days 0 Hours 0 Mins
DNS Servers	☑ Assign DNS server automatically
WINS Servers	□ Assign WINS server
BOOTP	□
Extended DHCP Option	Option / Value No Extended DHCP Option Add
DHCP Reservation	Name / MAC Address / Static IP 00:00:00:00:00:00 +

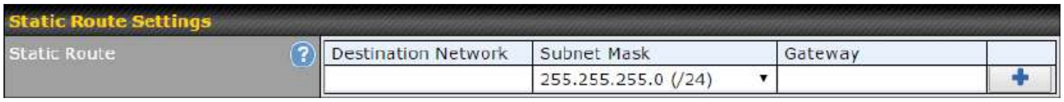
DHCP Server Settings	
DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.
DHCP Server Logging	Enable logging of DHCP events in the eventlog by selecting the checkbox.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Servers	This option allows you to optionally specify a Windows Internet Name Service (WINS) server. You may choose to use the **built-in WINS server** or **external WINS servers**. When this unit is connected using SpeedFusion^{TM}, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP **WINS Server** setting. Afterward, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.

	To define an extended DHCP option, click the **Add** button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press ✚ to create a new record. Press ✖ to remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.**



LAN Physical Settings	
Speed	Auto ▾

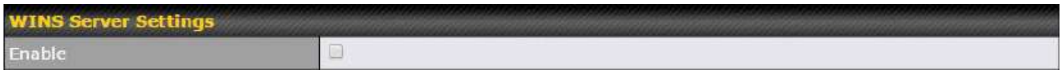
LAN Physical Settings	
Speed	This is the port speed of the LAN interface. It should be set to the same speed as the connected device to avoid port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device. **Auto** is selected by default. You can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



Static Route Settings

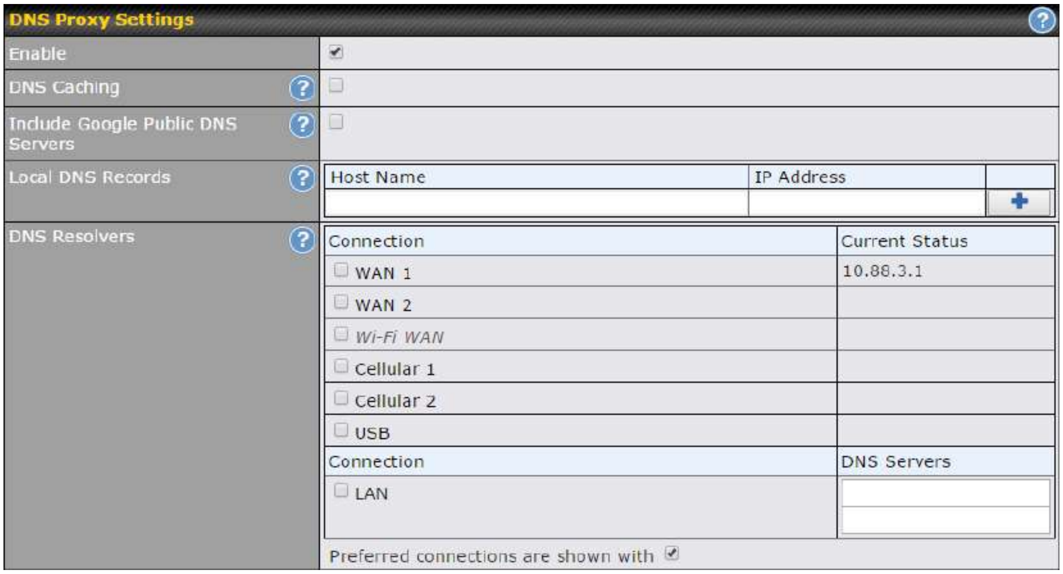
Static Route ?	Destination Network	Subnet Mask	Gateway	
		255.255.255.0 (/24) ▾		✚

Static Route Settings	
Static Route	This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in *w.x.y.z* format. The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press ✚ to create a new route. Press ✖ to remove a route.



WINS Server Settings	
Enable	□

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



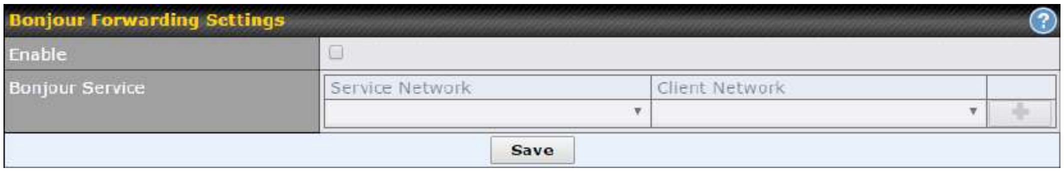
DNS Proxy Settings	
Enable	☑
DNS Caching	□
Include Google Public DNS Servers	□
Local DNS Records	Host Name / IP Address ✚
DNS Resolvers	Connection / Current Status □ WAN 1 — 10.88.3.1 □ WAN 2 □ Wi-Fi WAN □ Cellular 1 □ Cellular 2 □ USB Connection / DNS Servers □ LAN Preferred connections are shown with ☑

DNS Proxy Settings	
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion^{TM} peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN connection.
DNS Caching	This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can help improve DNS lookup time. However, it cannot return the most up-to-date result for those frequently updated DNS records. By default, **DNS Caching** is disabled.
Include Google Public DNS Servers	When this option is **enabled**, the DNS proxy server will also forward DNS requests to Google's Public DNS Servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Pepwave router, the corresponding IP address will be returned. Press ✚ to create a new record. Press ✖ to remove a record.

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

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

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



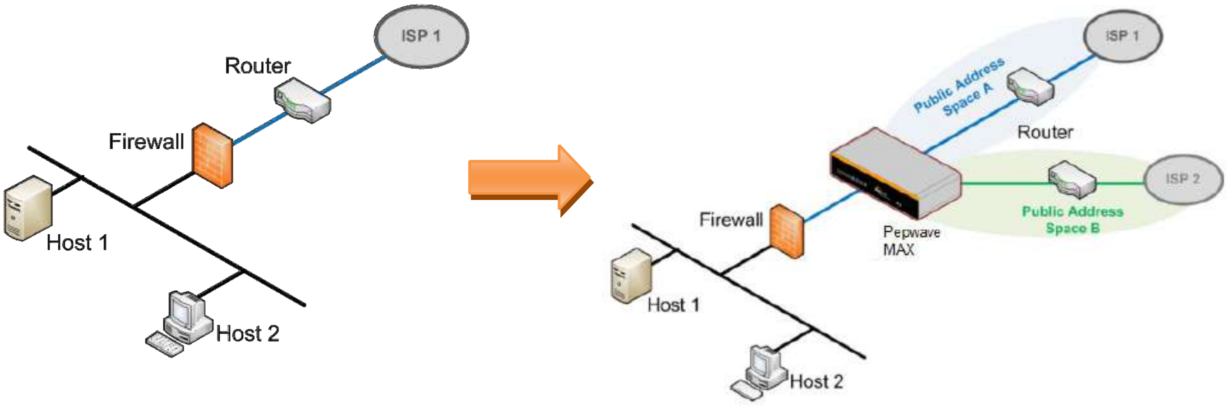
Bonjour Forwarding Settings		
Enable	□	
Bonjour Service	Service Network	Client Network
	▾	▾

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

Drop -In Mode

Drop-in mode (or transparent bridging mode) eases the installation of the Pepwave MAX on a live network between the firewall and router, such that changes to the settings of existing equipment are not required.

The following diagram illustrates drop-in mode setup:

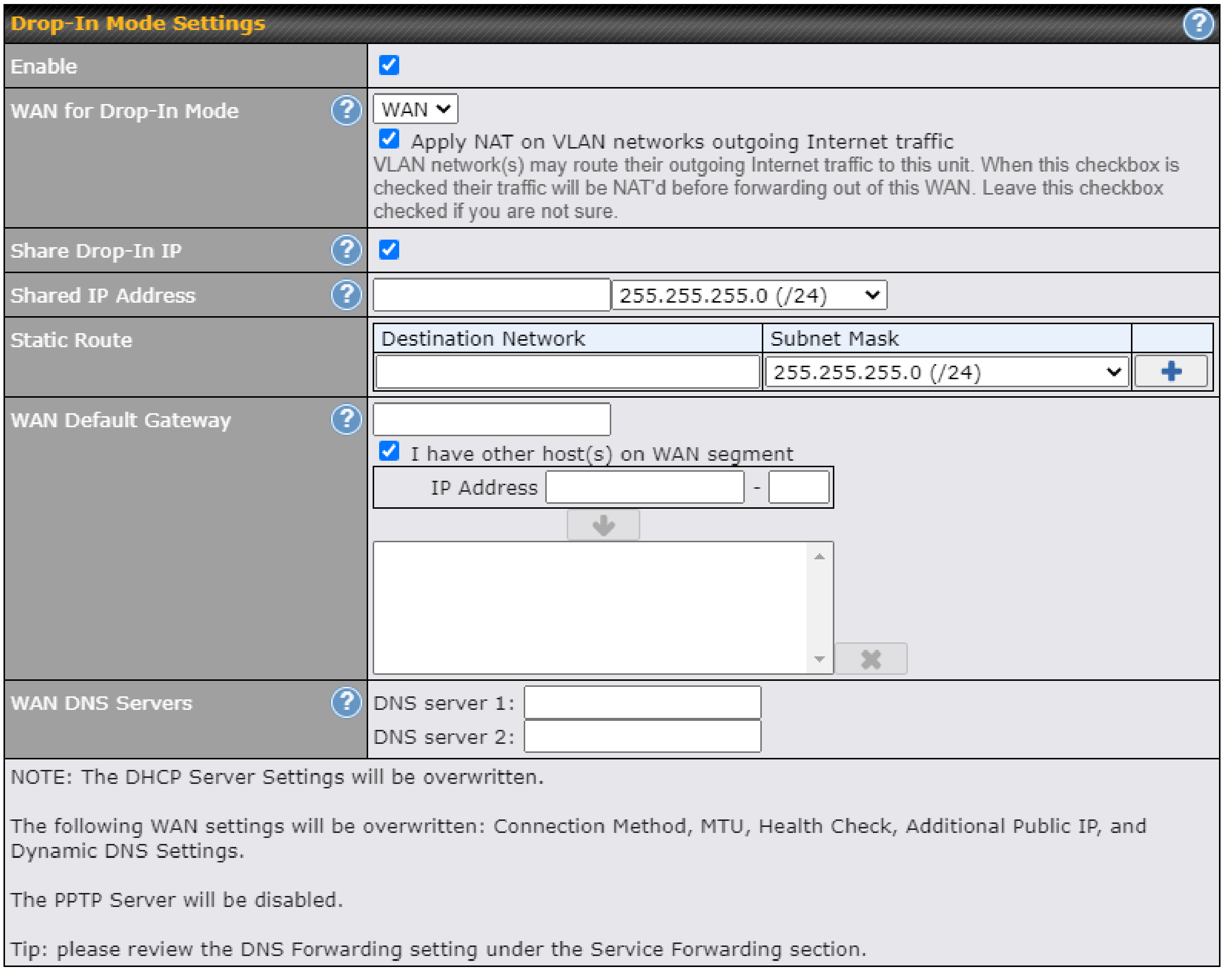


Check the box Enable to enable the Drop-in Mode. After enabling this feature and selecting the WAN for Drop-in mode, various settings including the WAN's connection method and IP address will be automatically updated.

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

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

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



Drop-In Mode Settings

Enable	☑
WAN for Drop-In Mode	WAN ☑ Apply NAT on VLAN networks outgoing Internet traffic VLAN network(s) may route their outgoing Internet traffic to this unit. When this checkbox is checked their traffic will be NAT'd before forwarding out of this WAN. Leave this checkbox checked if you are not sure.
Share Drop-In IP	☑
Shared IP Address	255.255.255.0 (/24)
Static Route	Destination Network · Subnet Mask: 255.255.255.0 (/24) +
WAN Default Gateway	☑ I have other host(s) on WAN segment IP Address -
WAN DNS Servers	DNS server 1: DNS server 2:

NOTE: The DHCP Server Settings will be overwritten.

The following WAN settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.

The PPTP Server will be disabled.

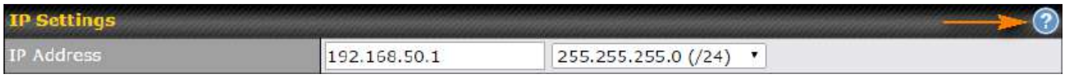
Tip: please review the DNS Forwarding setting under the Service Forwarding section.

Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of the Pepwave MAX on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If **WAN** is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^A	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The MAX will listen for this IP address when WAN hosts access services provided by the MAX (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The MAX will listen for this IP address when LAN hosts access services provided by the MAX (web admin access from the WAN, DNS proxy, etc.).
Shared IP	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

Address[A]	connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the ? button next to "WAN Default Gateway" and check the other **host(s) on the WAN segment** box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

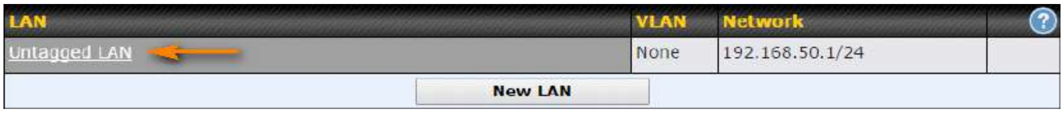
[A] - Advanced feature, please click the ? button on the top right-hand corner to activate.

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



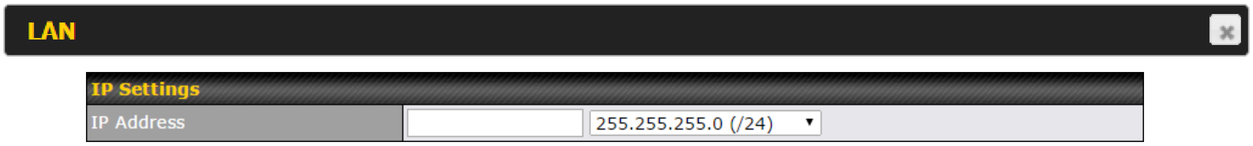
IP Settings		
IP Address	192.168.50.1	255.255.255.0 (/24)

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



LAN	VLAN	Network
Untagged LAN	None	192.168.50.1/24

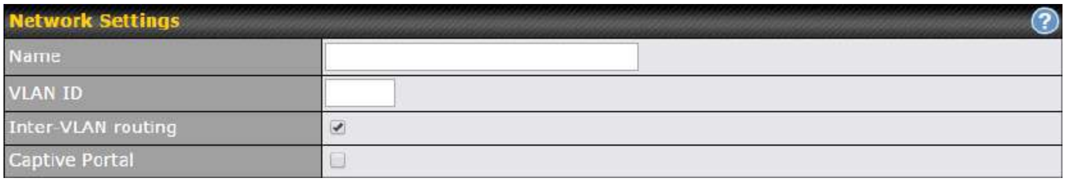
The following settings are displayed when creating a new LAN or editing an existing LAN.



LAN

IP Settings		
IP Address		255.255.255.0 (/24)

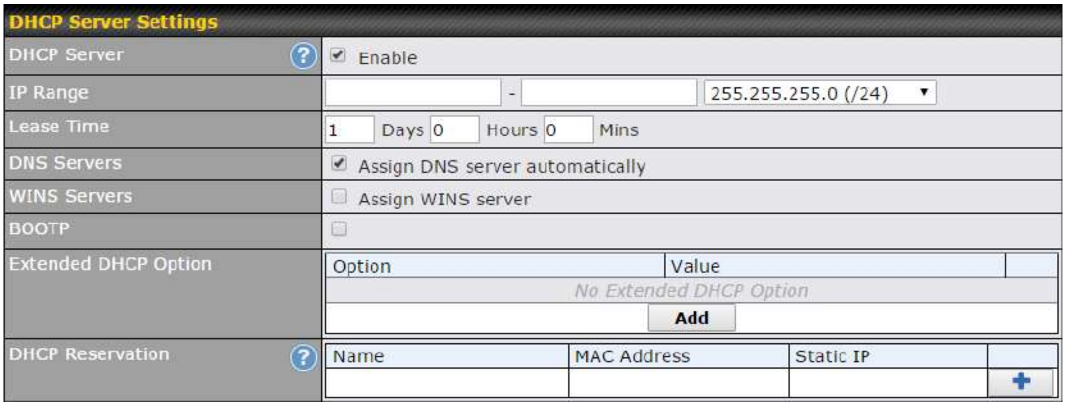
IP Settings	
IP Address & Subnet Mask	Enter the Pepwave router's IP address and subnet mask values to be used on the LAN.



Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☑
Captive Portal	□

Network Settings

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



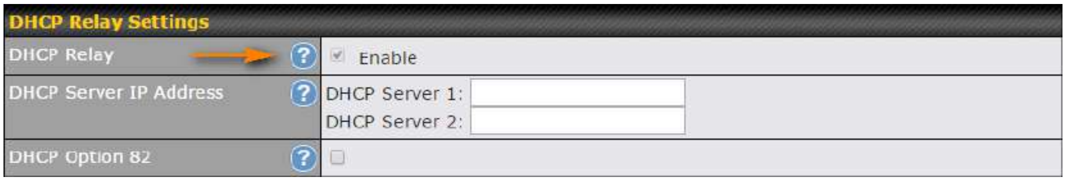
DHCP Server Settings

DHCP Server ?	☑ Enable
IP Range	- 255.255.255.0 (/24) ▾
Lease Time	1 Days 0 Hours 0 Mins
DNS Servers	☑ Assign DNS server automatically
WINS Servers	□ Assign WINS server
BOOTP	□
Extended DHCP Option	Option / Value *No Extended DHCP Option* Add
DHCP Reservation ?	Name / MAC Address / Static IP / +

DHCP Server Settings	
DHCP Server	When this setting is enabled, the Pepwave router's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collisions on the LAN. To enable DHCP bridge relay, please click the ? icon on this menu item.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of **Lease Time**, the assigned IP address will no longer be valid and the IP address assignment must be renewed.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Servers	This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion^{TM}, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their **DHCP WINS Servers** setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS

	clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press + to create a new record. Press ✖ to remove a record. Reserved clients information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.**

To configure DHCP relay, first click the ? button found next to the **DHCP Server** option to display the settings.



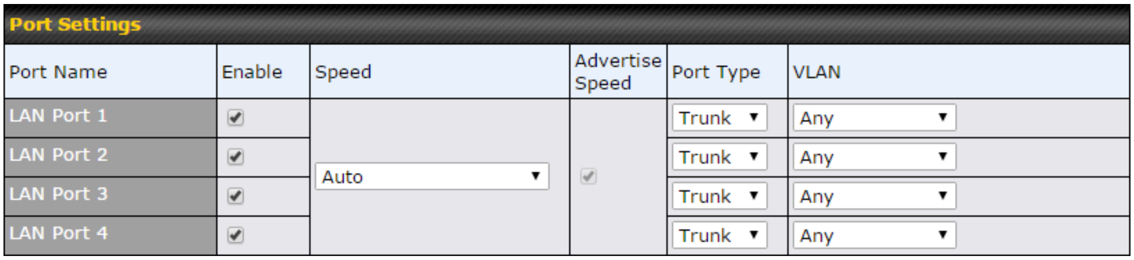
DHCP Relay Settings	
DHCP Relay ?	☑ Enable
DHCP Server IP Address ?	DHCP Server 1: DHCP Server 2:
DHCP Option 82 ?	□

DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the ? icon to disable DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in **DHCP Server 1** and **DHCP Server 2.**
DHCP Option 82	DHCP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device's MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.

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

8.2 Port Settings

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



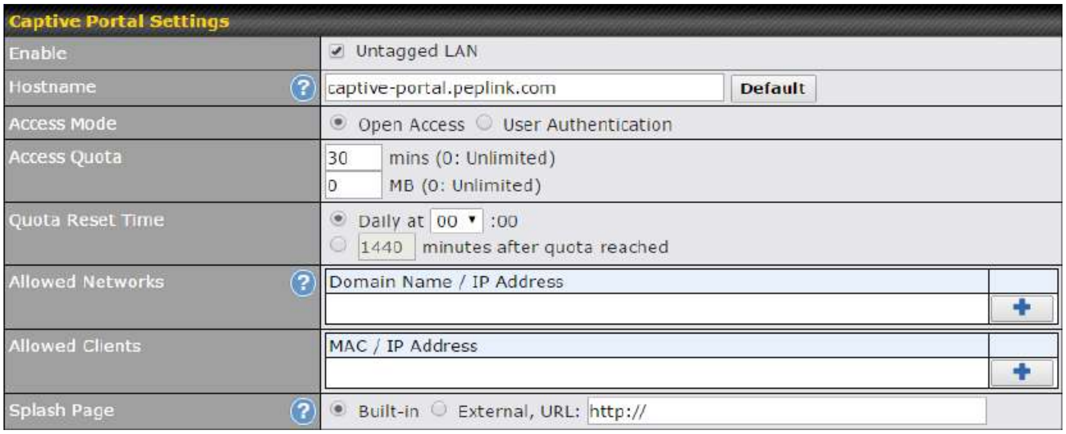
Port Settings

Port Name	Enable	Speed	Advertise Speed	Port Type	VLAN
LAN Port 1	☑	Auto ▾	☑	Trunk ▾	Any ▾
LAN Port 2	☑			Trunk ▾	Any ▾
LAN Port 3	☑			Trunk ▾	Any ▾
LAN Port 4	☑			Trunk ▾	Any ▾

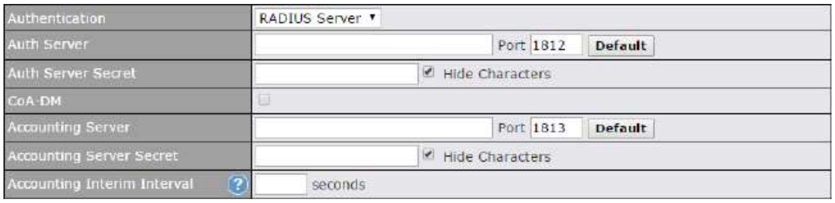
On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

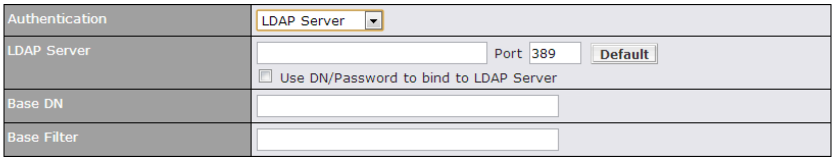
8.3 Captive Portal

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

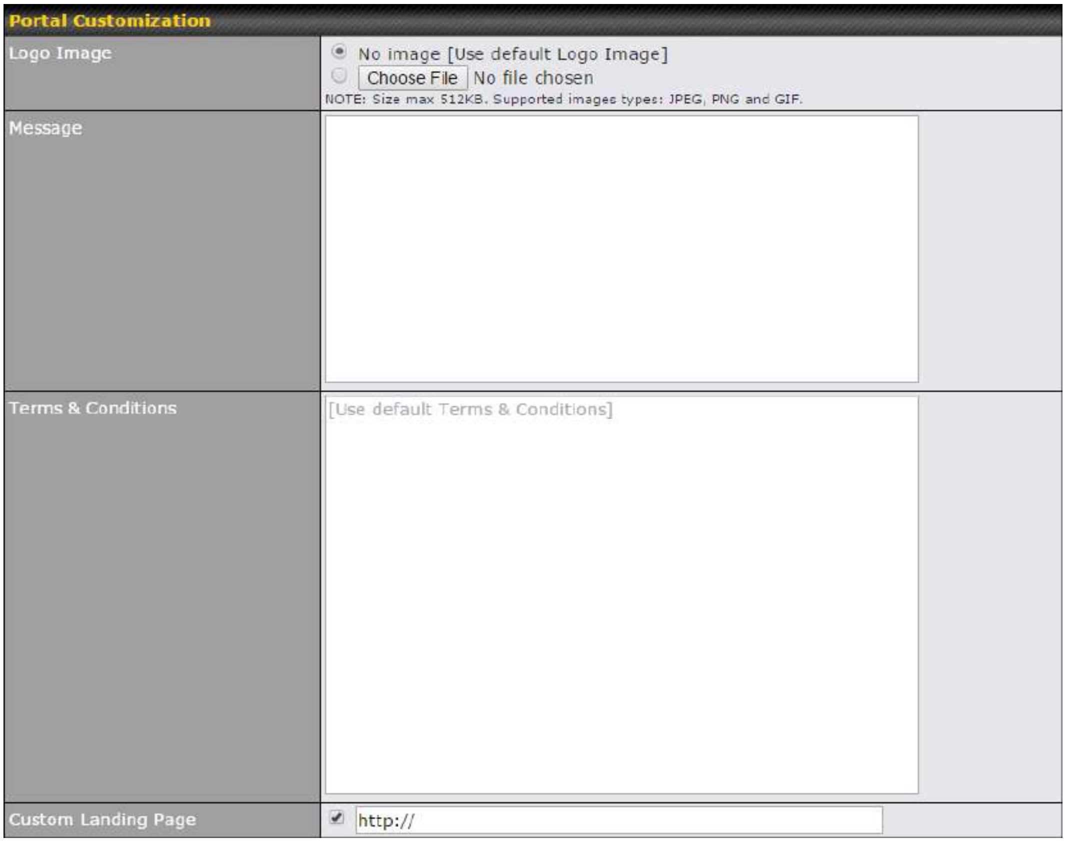


Captive Portal Settings	
Enable	☑ Untagged LAN
Hostname ?	captive-portal.peplink.com [Default]
Access Mode	● Open Access ○ User Authentication
Access Quota	30 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	● Daily at 00 ▾ :00 ○ 1440 minutes after quota reached
Allowed Networks ?	Domain Name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

Captive Portal Settings	
Enable	Check **Enable** and then, optionally, select the LANs/VLANs that will use the captive portal.
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click **Default**.
Access Mode	Click **Open Access** to allow clients to freely access your router. Click **User Authentication** to force your clients to authenticate before accessing your router.
RADIUS Server	This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:  Authentication: RADIUS Server ▾ Auth Server: Port 1812 [Default] Auth Server Secret: ☑ Hide Characters CoA-DM: □ Accounting Server: Port 1813 [Default] Accounting Server Secret: ☑ Hide Characters Accounting Interim Interval ?: seconds Fill in the necessary information to complete your connection to the server and enable authentication.
LDAP Server	This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:

	 Authentication: LDAP Server LDAP Server: Port 389 Default □ Use DN/Password to bind to LDAP Server Base DN Base Filter Fill in the necessary information to complete your connection to the server and enable authentication.
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.
Allowed Networks	Add networks that can bypass the captive Portal in this field. To whitelist a network, enter the domain name / IP address here and click ✚. To delete an existing network from the list of allowed networks, click the ✖ button next to the listing.
Allowed Clients	Add MAC address and /or IP addresses for client devices that are allowed to bypass the Captive Portal. Clients accessing these domains and IP addresses will not be redirected to the splash page.
Splash Page	Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define.

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



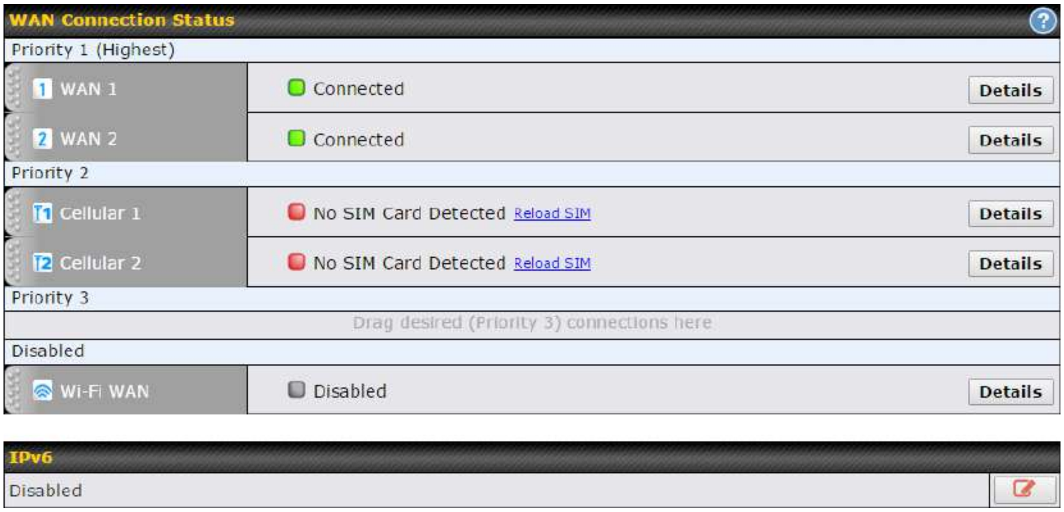
Portal Customization

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

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

9 Configuring the WAN Interface(s)

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



WAN Connection Status

Priority 1 (Highest)		
1 WAN 1	🟩 Connected	Details
2 WAN 2	🟩 Connected	Details
Priority 2		
T1 Cellular 1	🟥 No SIM Card Detected Reload SIM	Details
T2 Cellular 2	🟥 No SIM Card Detected Reload SIM	Details
Priority 3		
Drag desired (Priority 3) connections here		
Disabled		
Wi-Fi WAN	■ Disabled	Details

IPv6

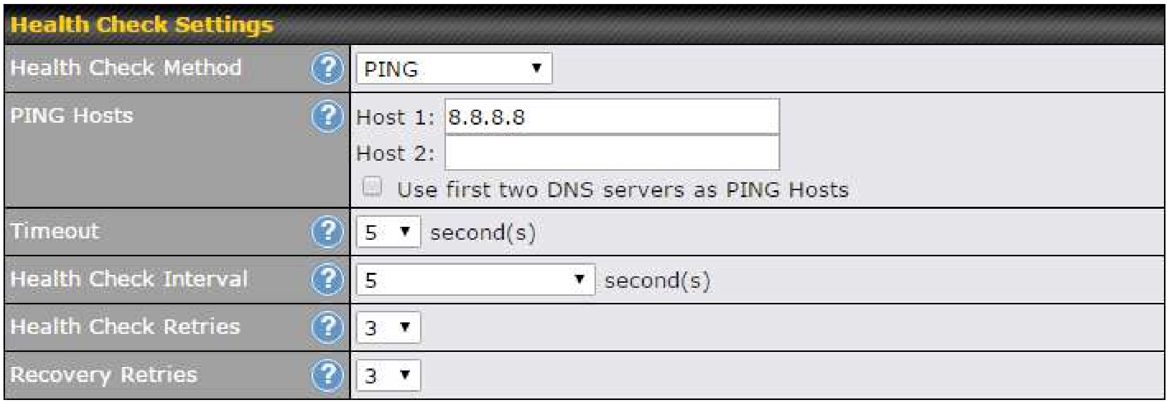
Disabled

To able 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.

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

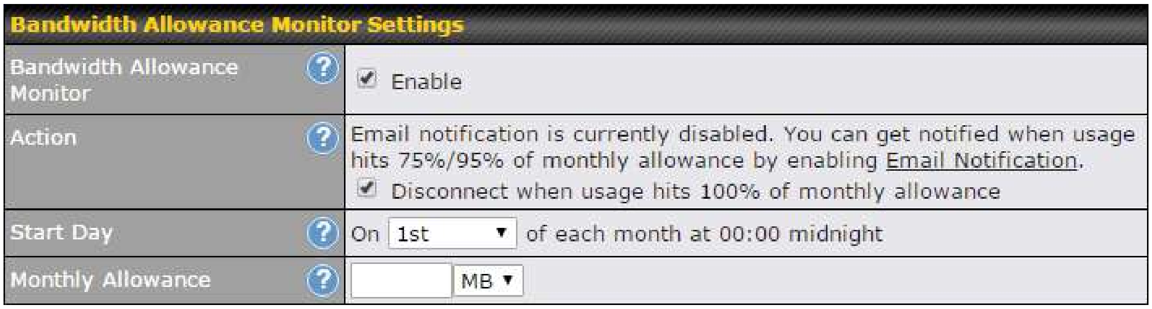
9.1 Ethernet WAN



Health Check Settings

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

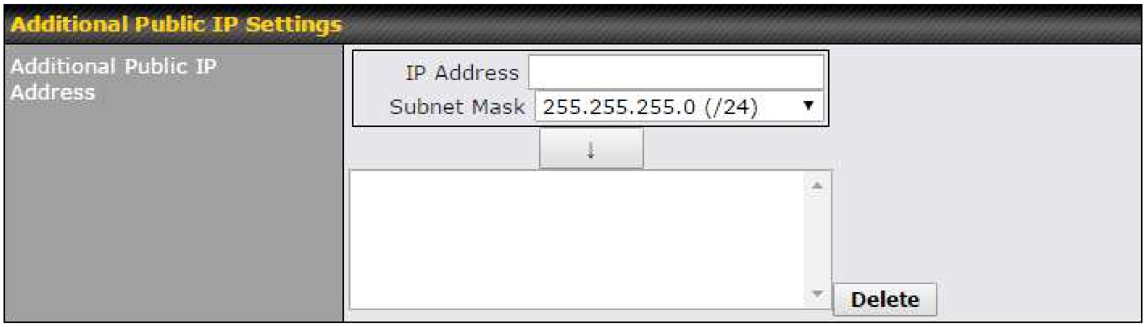
Health Check Settings	
Health Check Method	This field specifies the Health Check method to be used for this WAN connection. ● Disabled - The WAN connection is always considered to be up and will not be treated as down for any IP routing errors. ● PING - ICMP PING packets will be issued to test connectivity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



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

Bandwidth Allowance Monitor Settings

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



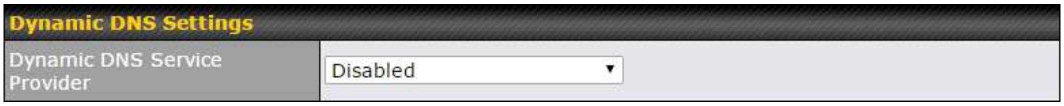
Additional Public IP Settings

Additional Public IP Address

IP Address

Subnet Mask 255.255.255.0 (/24)

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



Dynamic DNS Settings

Dynamic DNS Service Provider: Disabled

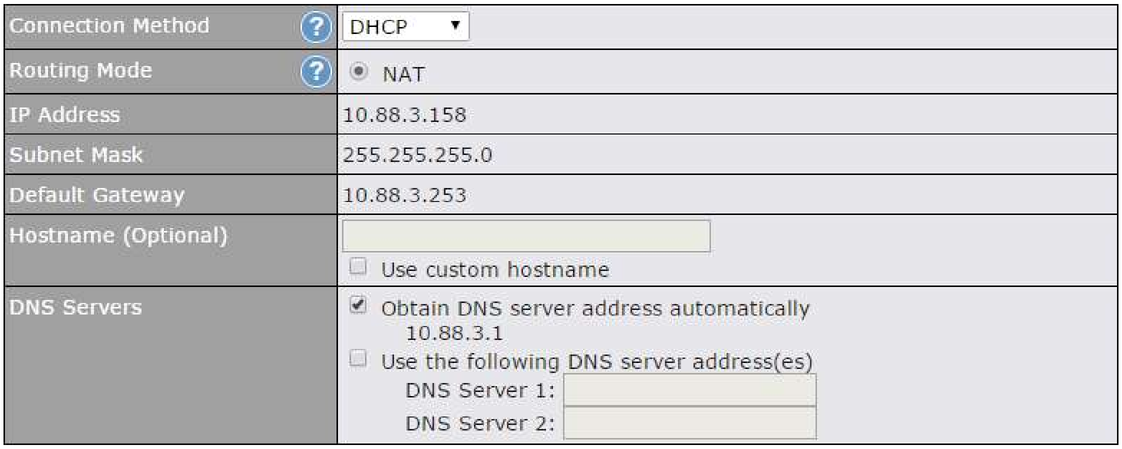
Dynamic DNS Settings	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: ● changeip.com ● dyndns.org ● no-ip.org ● tzo.com ● DNS-O-Matic Select **Disabled** to disable this feature. See **Section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

9.1.1 DHCP Connection

There are four possible connection methods:

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

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

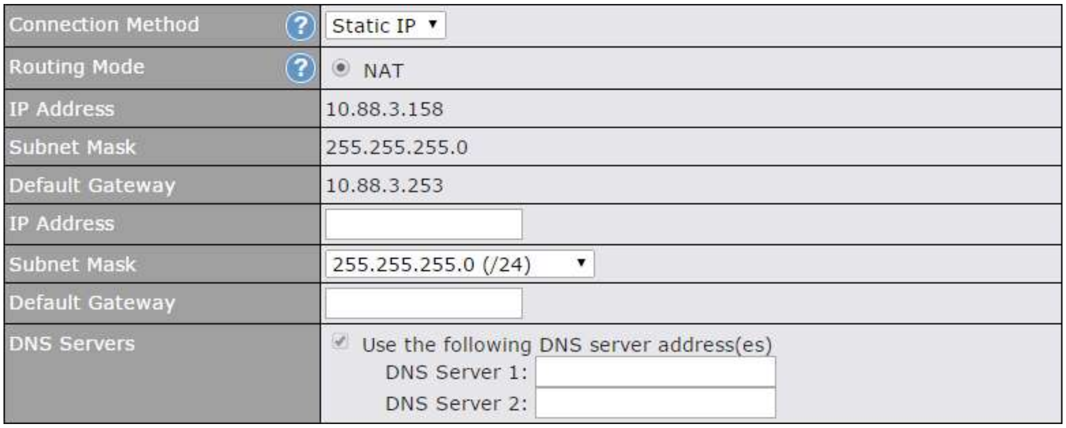


Connection Method	DHCP ▾
Routing Mode	● NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
Hostname (Optional)	□ Use custom hostname
DNS Servers	☑ Obtain DNS server address automatically 10.88.3.1 □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

DHCP Connection Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address/ Subnet Mask/ Default Gateway	This information is obtained from the ISP automatically.
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

9.1.2 Static IP Connection

The static IP connection method is suitable if your ISP provides a static IP address to connect directly.

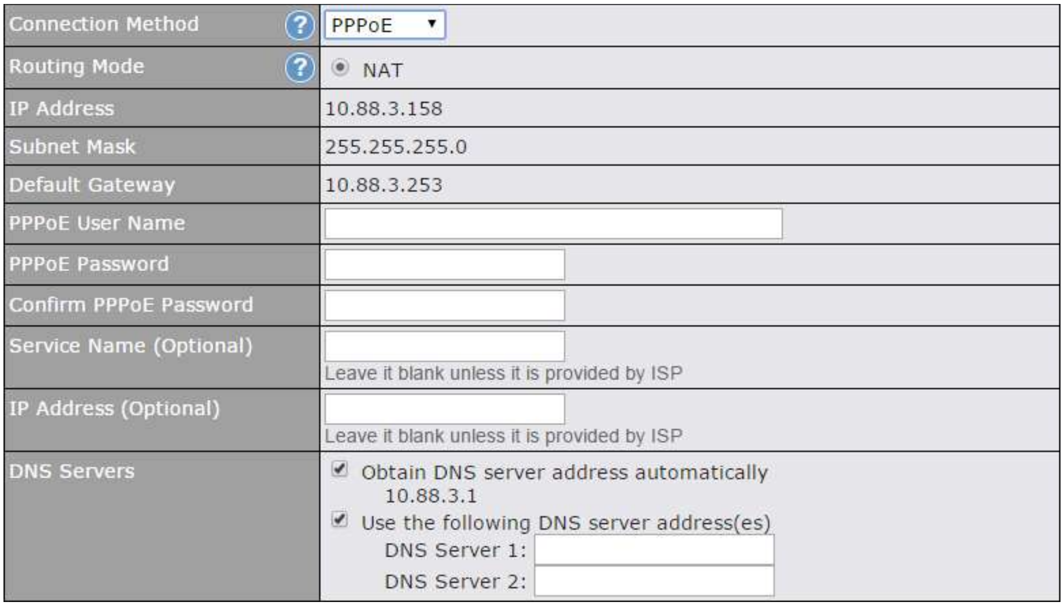


Connection Method ?	Static IP ▾
Routing Mode ?	● NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
IP Address	
Subnet Mask	255.255.255.0 (/24) ▾
Default Gateway	
DNS Servers	☑ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

Static IP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

9.1.3 PPPoE Connection

This connection method is suitable if your ISP provides a login ID/password to connect via PPPoE.

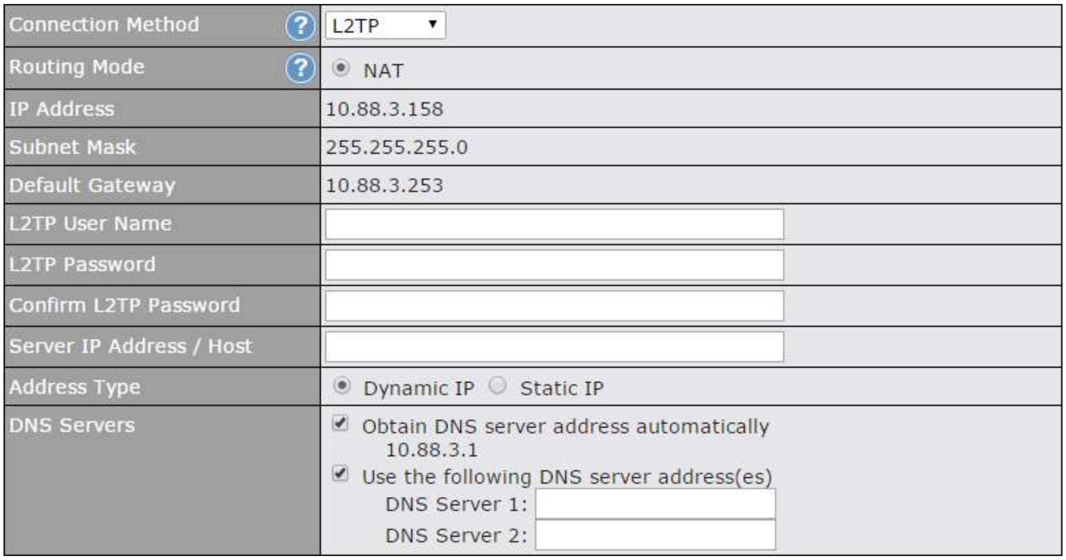


Connection Method	PPPoE ▾
Routing Mode	● NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	Leave it blank unless it is provided by ISP
IP Address (Optional)	Leave it blank unless it is provided by ISP
DNS Servers	☑ Obtain DNS server address automatically 10.88.3.1 ☑ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	This information is obtained from the ISP automatically.
PPPoE Username / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service name is provided by the ISP. **Note: Leave this field blank unless it is provided by your ISP.**
IP Address (Optional)	If your ISP provides a PPPoE IP address, enter it here. **Note: Leave this field blank unless it is provided by your ISP.**
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

9.1.4 L2TP Connection

L2TP has all the compatibility and convenience of PPTP with greater security. Combine this with IPsec for a good balance between ease of use and security.

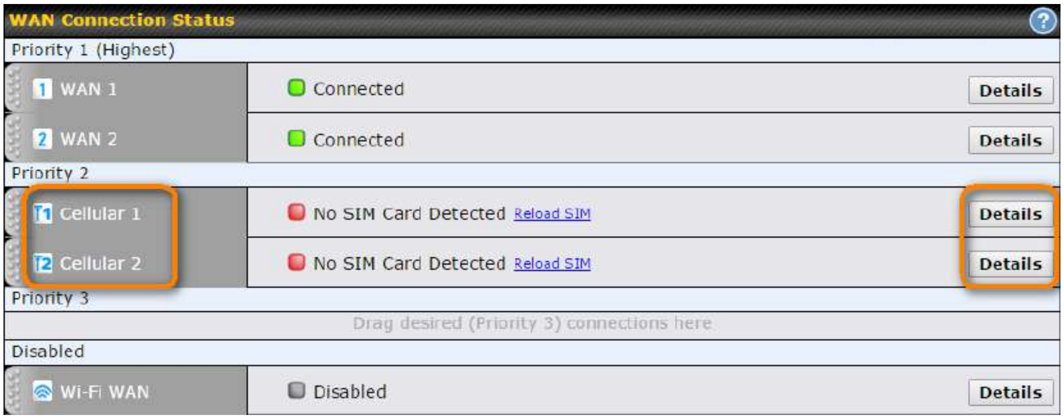


Connection Method	L2TP ▾
Routing Mode	● NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
L2TP User Name	
L2TP Password	
Confirm L2TP Password	
Server IP Address / Host	
Address Type	● Dynamic IP ○ Static IP
DNS Servers	☑ Obtain DNS server address automatically 10.88.3.1 ☑ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

L2TP Settings	
L2TP Username / Password	Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.
Confirm L2TP Password	Verify your password by entering it again in this field.
Server IP Address / Host	L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
Address Type	Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)

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

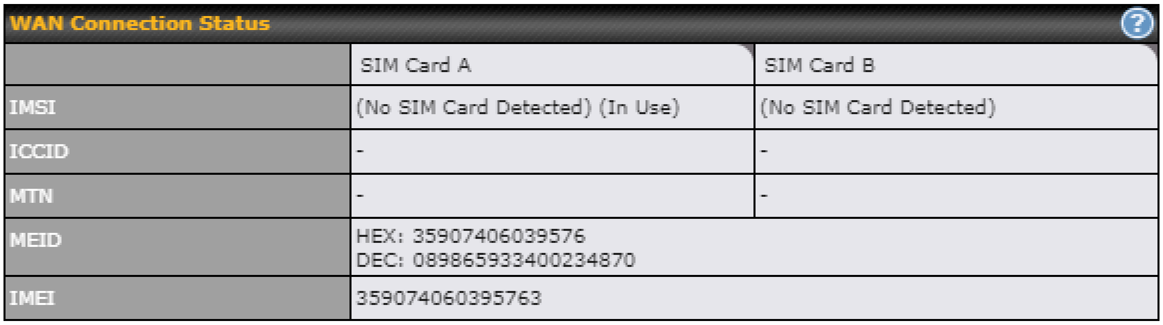
9.2 Cellular WAN



WAN Connection Status

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

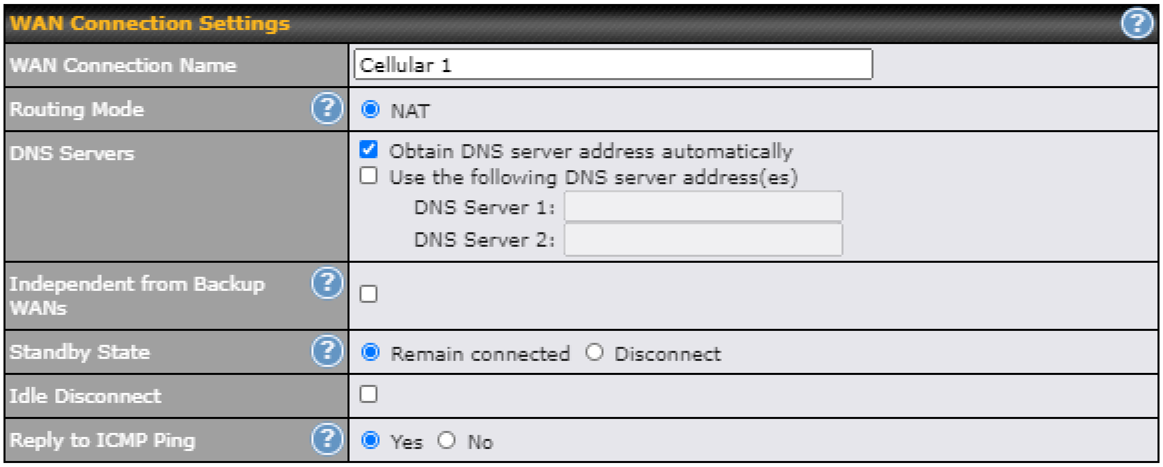
To access cellular WAN settings, click **Network>WAN>Details**.



WAN Connection Status

	SIM Card A	SIM Card B
IMSI	(No SIM Card Detected) (In Use)	(No SIM Card Detected)
ICCID	-	-
MTN	-	-
MEID	HEX: 35907406039576 DEC: 089865933400234870	
IMEI	359074060395763	

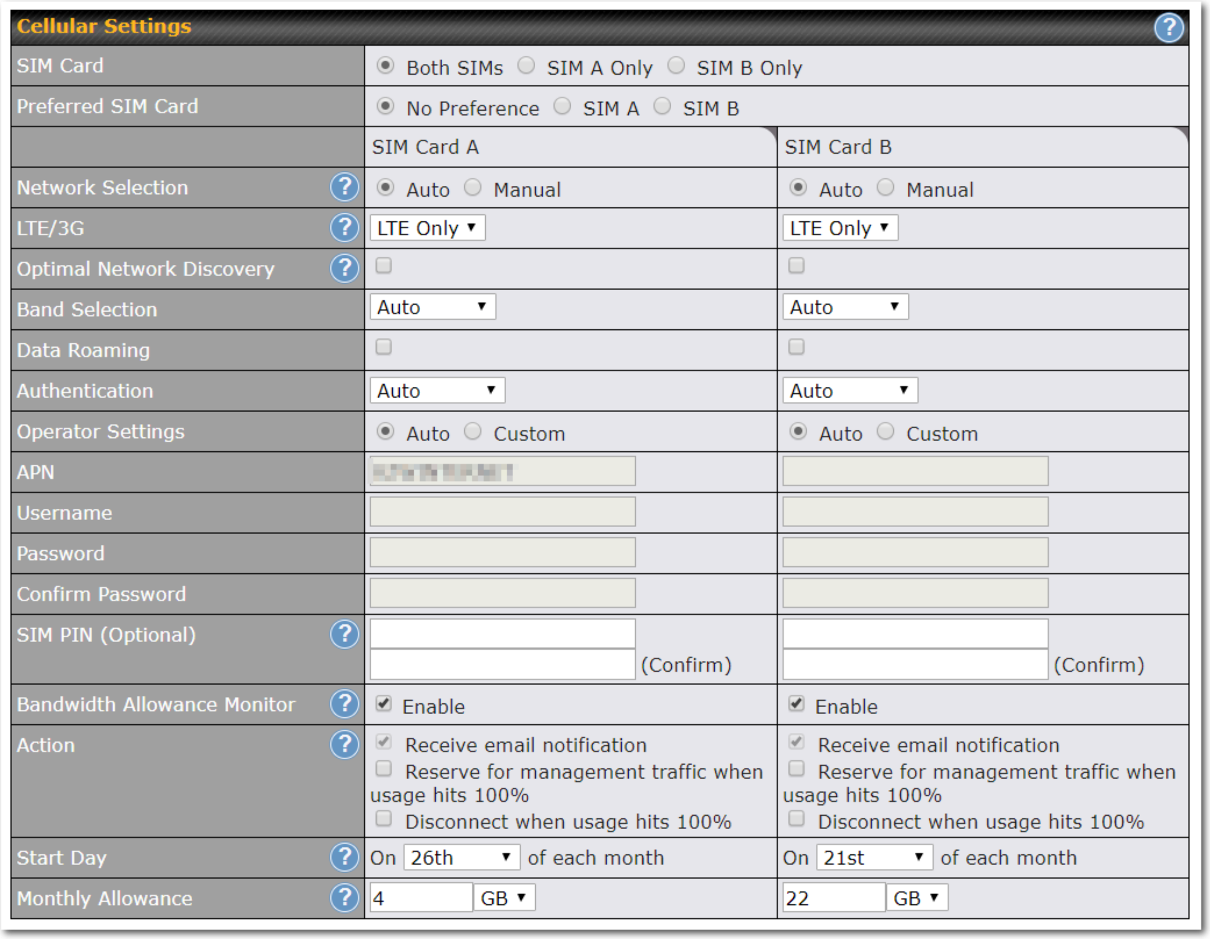
WAN Connection Status	
IMSI	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
ICCID	This is a unique number assigned to a SIM card used in a cellular device.
MEID	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.



WAN Connection Settings	
WAN Connection Name	Cellular 1
Routing Mode	● NAT
DNS Servers	☑ Obtain DNS server address automatically □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Independent from Backup WANs	□
Standby State	● Remain connected ○ Disconnect
Idle Disconnect	□
Reply to ICMP Ping	● Yes ○ No

Connection Settings	
WAN Connection Name	Indicate a name you wish to give this WAN connection
Routing Mode	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding. In the case if you need to choose IP Forwarding for your scenario. Click the ? button to enable IP Forwarding.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Standby State	This option allows you to choose whether to remain connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, bringing up this WAN connection to active makes it immediately available for use.

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

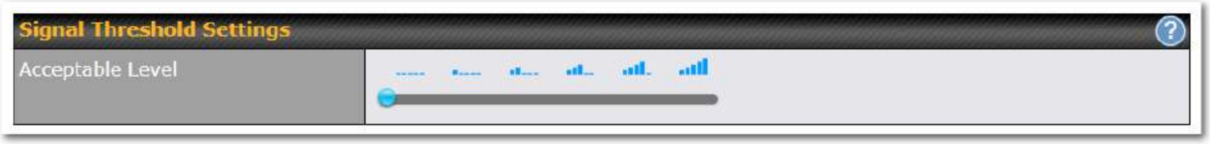


Cellular Settings		
SIM Card	● Both SIMs ○ SIM A Only ○ SIM B Only	
Preferred SIM Card	● No Preference ○ SIM A ○ SIM B	
	SIM Card A	SIM Card B
Network Selection	● Auto ○ Manual	● Auto ○ Manual
LTE/3G	LTE Only ▾	LTE Only ▾
Optimal Network Discovery	□	□
Band Selection	Auto ▾	Auto ▾
Data Roaming	□	□
Authentication	Auto ▾	Auto ▾
Operator Settings	● Auto ○ Custom	● Auto ○ Custom
APN	[redacted]	
Username		
Password		
Confirm Password		
SIM PIN (Optional)	(Confirm)	(Confirm)
Bandwidth Allowance Monitor	☑ Enable	☑ Enable
Action	☑ Receive email notification □ Reserve for management traffic when usage hits 100% □ Disconnect when usage hits 100%	☑ Receive email notification □ Reserve for management traffic when usage hits 100% □ Disconnect when usage hits 100%
Start Day	On 26th ▾ of each month	On 21st ▾ of each month
Monthly Allowance	4 GB ▾	22 GB ▾

Cellular Settings	
SIM Card	Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards.
Preferred SIM Card	If both cards were enabled on the above field, then you can designate the priority of the SIM card slots here.
LTE/3G	This drop-down menu allows restricting cellular to particular band. Click the ? button to enable the selection of specific bands.
Optimal	Cellular WAsN by default will only handover from 3G to LTE network when there is no active

Network Discovery	data traffic, enable this option will make it run the handover procedures after fallback to 3G for a defined effective period, even this may interrupt the connectivity for a short while.
Band Selection	When set to **Auto,** band selection allows for automatically connecting to available, supported bands (frequencies) . When set to Manual, you can manually select the bands (frequencies) the SIM will connect to.
Data Roaming	This checkbox enables data roaming on this particular SIM card. When data roaming is enabled this option allows you to select in which countries the SIM has a data connection. The option is configured by using MMC (country) codes.Please check your service provider's data roaming policy before proceeding.
Authentication	Choose from **PAP Only** or **CHAP Only** to use those authentication methods exclusively. Select **Auto** to automatically choose an authentication method.
Operator Settings	This setting alloes allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select **Custom** to enter your carrier's **APN**, **Login**, **Password**, and **Dial Number** settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**.
APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Signal Threshold Settings



Signal Threshold Settings

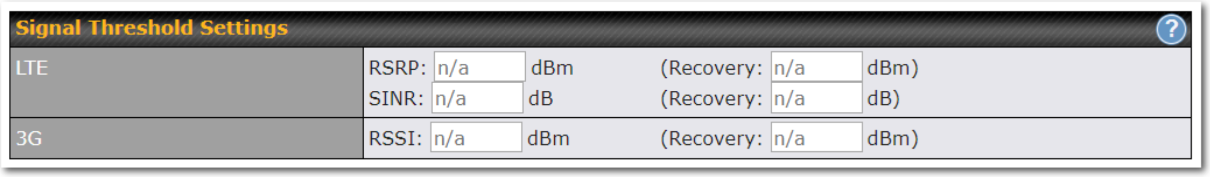
Acceptable Level

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

The following values are used by the threshold scale:

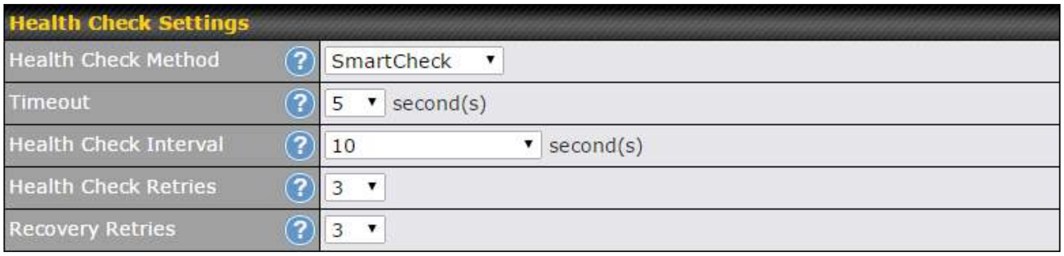
	0 bars	1 bar	2 bars	3 bars	4 bars	5 bars
LTE / RSSRP	-140	-128	-121	-114	-108	-98
3G / RSSI	-120	-100	-95	-90	-85	-75

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



Signal Threshold Settings

LTE	RSRP: n/a dBm SINR: n/a dB	(Recovery: n/a dBm) (Recovery: n/a dB)
3G	RSSI: n/a dBm	(Recovery: n/a dBm)

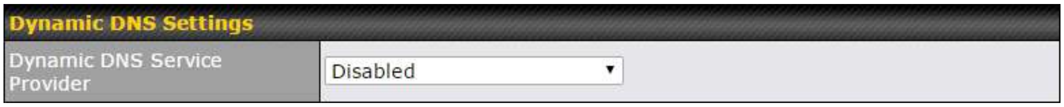


Health Check Settings

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

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

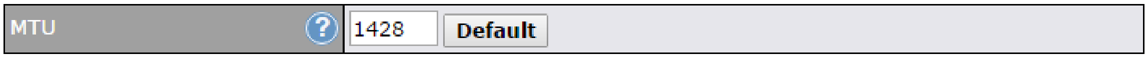
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



Dynamic DNS Settings

Dynamic DNS Service Provider: Disabled ▾

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

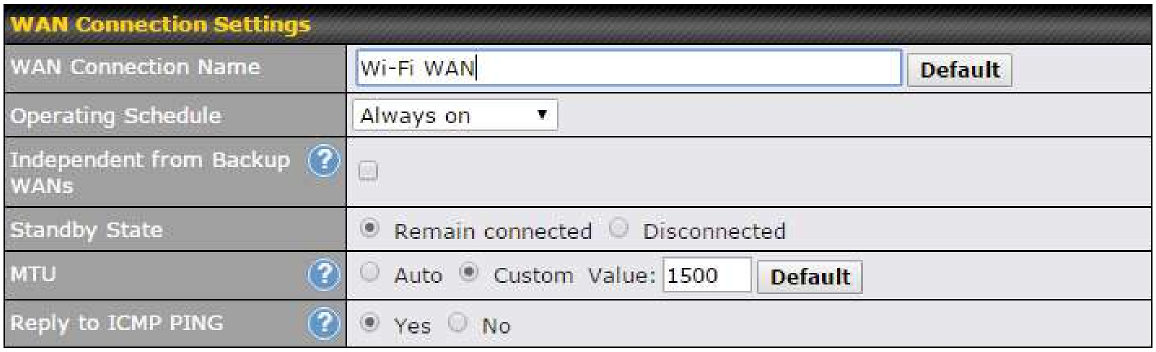


MTU ? 1428 Default

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

9.3 Wi-Fi WAN

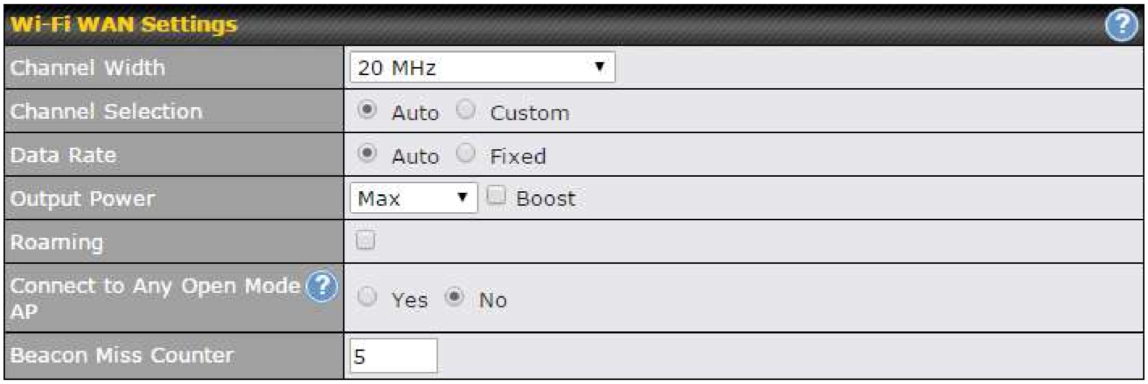
To access Wi-Fi WAN settings, click **Network>WAN>Details**.



WAN Connection Settings

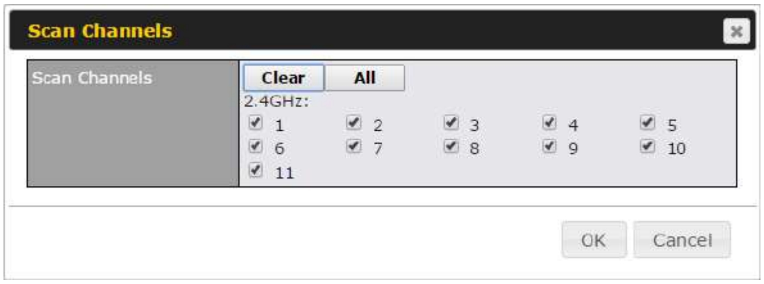
WAN Connection Name	Wi-Fi WAN Default
Operating Schedule	Always on ▾
Independent from Backup WANs ?	□
Standby State	● Remain connected ○ Disconnected
MTU ?	○ Auto ● Custom Value: 1500 Default
Reply to ICMP PING ?	● Yes ○ No

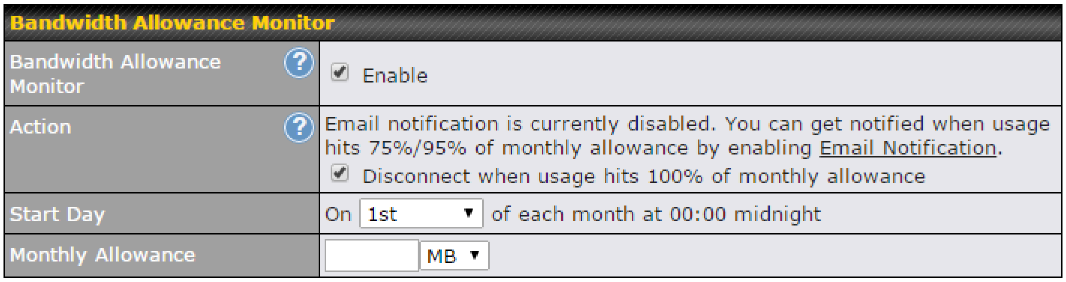
WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Operating Schedule	Click the drop-down menu to apply a time schedule to this interface.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections.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



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

Wi-Fi WAN Settings	
Channel Width	Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz
Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:

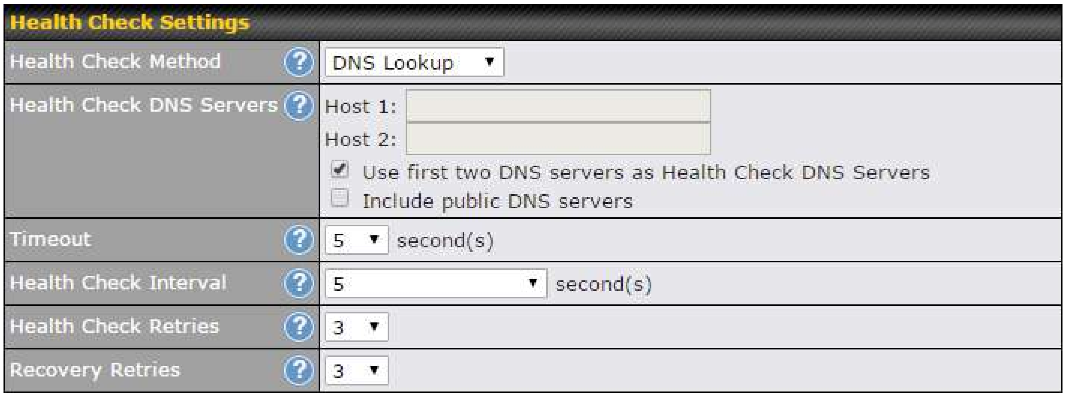
	 **Scan Channels** Scan Channels: Clear / All 2.4GHz: ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 OK Cancel
Data Rate	Selecting Auto will enable the router to automatically determine the best data rate, while manually selecting a rate will force devices to connect using the fixed rate.
Output Power	If you are setting up a network with many Wi-Fi devices in close proximity, then you can configure the output power here. Click the “boost” button for additional power. However, with that option ticked, output power may exceed local regulatory limits.
Roaming	Checking this box will enable Wi-Fi roaming. Click the ? icon for additional options.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.
Beacon Miss Counter	This sets the threshold for the number of missed beacons.



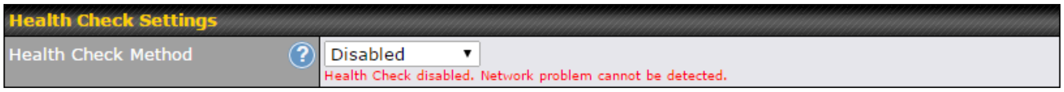
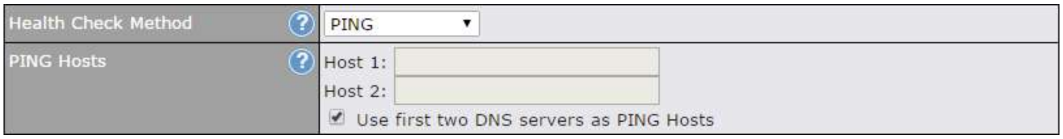
Bandwidth Allowance Monitor

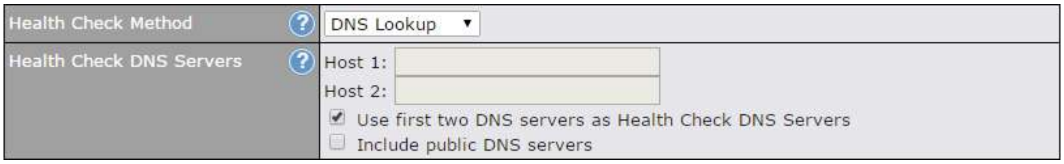
Bandwidth Allowance Monitor ?	☑ Enable
Action ?	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st ▾ of each month at 00:00 midnight
Monthly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

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



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

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

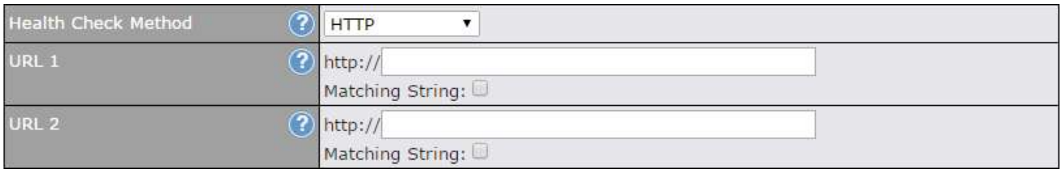


Health Check Method	DNS Lookup ▾
Health Check DNS Servers	Host 1: Host 2: ☑ Use first two DNS servers as Health Check DNS Servers ☐ Include public DNS servers

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

Health Check DNS Servers	This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS Lookup. If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional. If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also n response received from the public DNS servers. Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

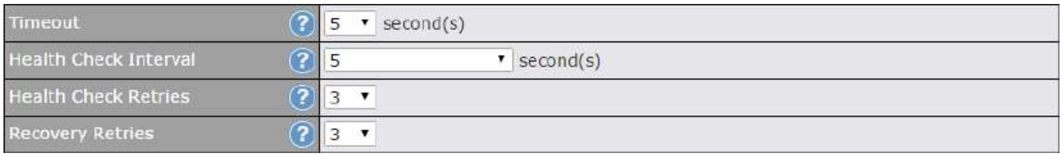


Health Check Method	HTTP ▾
URL 1	http:// Matching String: ☐
URL 2	http:// Matching String: ☐

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

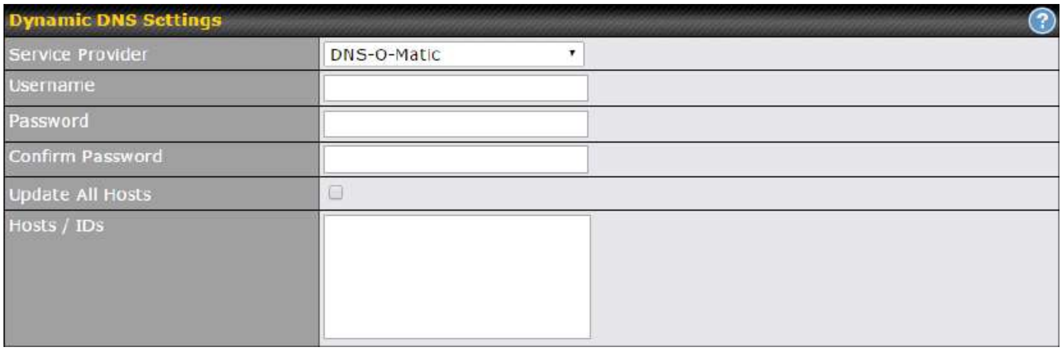
URL1	**WAN Settings>WAN Edit>Health Check Settings>URL1** The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.
URL 2	**WAN Settings>WAN Edit>Health Check Settings>URL2** If **URL2** is also provided, a health check will pass if either one of the tests passed.

Other Health Check Settings



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

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



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

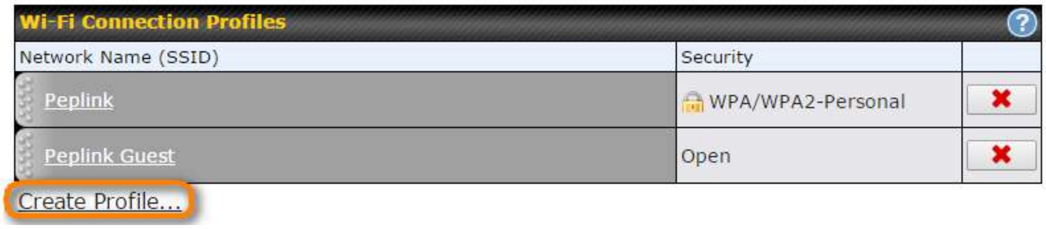
Dynamic DNS Settings	
Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are: ● changeip.com ● dyndns.org ● no-ip.org ● tzo.com ● DNS-O-Matic Select **Disabled** to disable this feature.
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.

Password / Pass / TZO Key	This setting specifies the password for the dynamic DNS service.
Update All Hosts	Check this box to automatically update all hosts.
Hosts / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

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

9.3.1 Creating Wi-Fi Connection Profiles

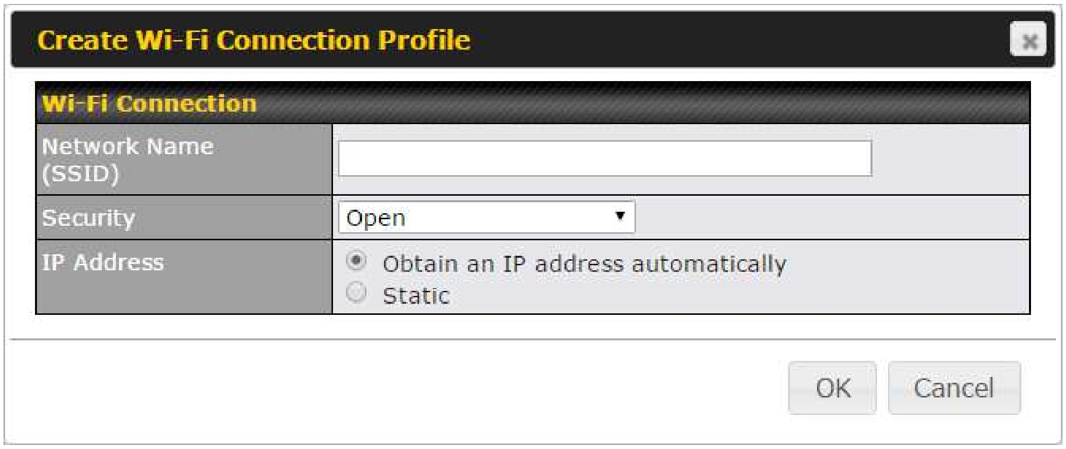
You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden-SSID access points. Click **Network>WAN>Details>Create Profile…** to get started.



Wi-Fi Connection Profiles

Network Name (SSID)	Security	
Peplink	WPA/WPA2-Personal	✖
Peplink Guest	Open	✖

This will open a window similar to the one shown below



Create Wi-Fi Connection Profile

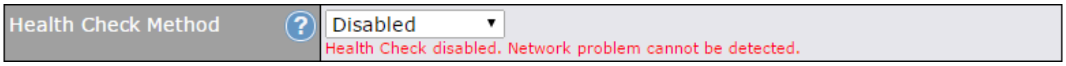
Wi-Fi Connection	
Network Name (SSID)	
Security	Open
IP Address	● Obtain an IP address automatically ○ Static

Wi-Fi Connection Profile Settings	
Type	Select whether the network will connect automatically or manually.
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network. Available options: • **Open** • **WPA3 -Personal (AES:CCMP)** • **WPA2/WPA3 -Personal (AES:CCMP)** • **WPA2 – Personal: AES:CCMP** • **WPA2 – Enterprise: AES: CCMP** • **WPA/ WPA2 – Personal: TKIP/AES:CCMP** • **WPA/ WPA2 – ENterprise: TKIP/AES:CCMP**

9.4 WAN Health Check

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

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

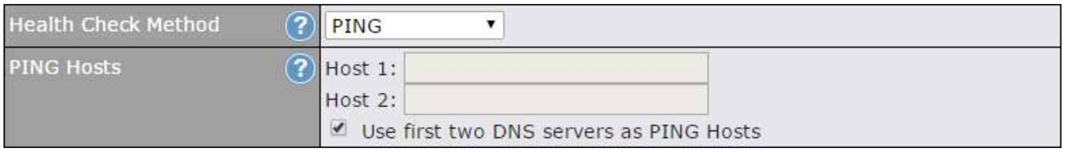


Health Check Method: Disabled

Health Check disabled. Network problem cannot be detected.

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

Health Check Method: PING



Health Check Method: PING

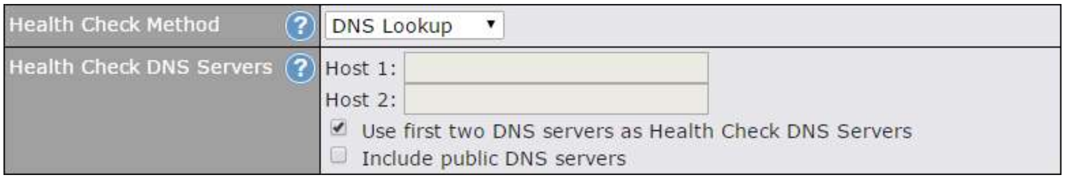
PING Hosts: Host 1: Host 2:

☑ Use first two DNS servers as PING Hosts

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

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

Health Check Method: DNS Lookup



Health Check Method: DNS Lookup

Health Check DNS Servers: Host 1: Host 2:

☑ Use first two DNS servers as Health Check DNS Servers

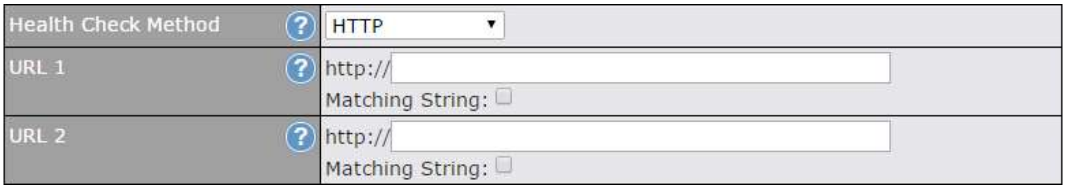
☐ Include public DNS servers

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

Health Check DNS Servers	This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS lookup. If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional. If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers. Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

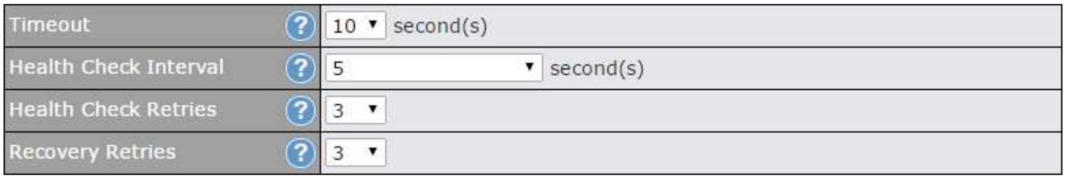
Health Check Method: HTTP

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



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

URL1	**WAN Settings>WAN Edit>Health Check Settings>URL1** The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.
URL 2	**WAN Settings>WAN Edit>Health Check Settings>URL2** If **URL2** is also provided, a health check will pass if either one of the tests passed.

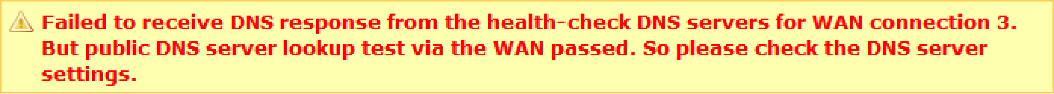


Timeout	10 ▾ second(s)
Health Check Interval	5 ▾ second(s)
Health Check Retries	3 ▾
Recovery Retries	3 ▾

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

Automatic Public DNS Server Check on DNS Test Failure
When the health check method is set to **DNS Lookup** and health checks fail, the Pepwave router will

automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:



⚠ **Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.**

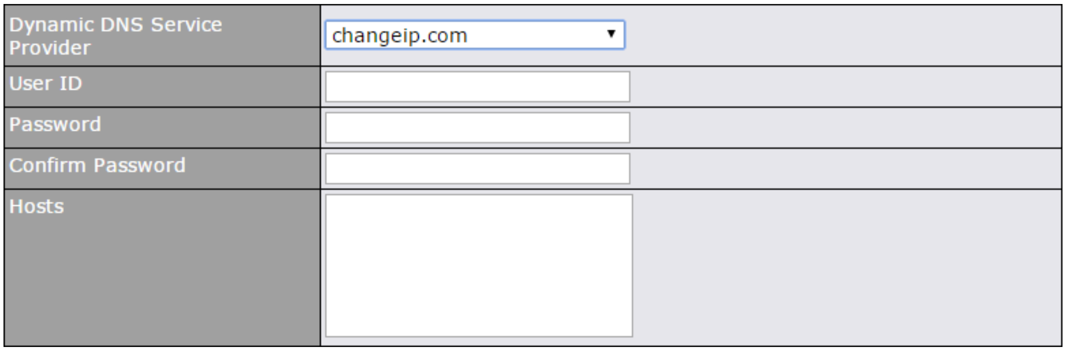
9.5 Dynamic DNS Settings

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

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

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

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



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

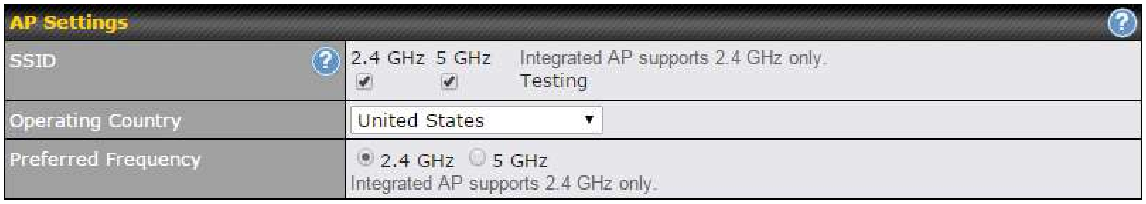
Dynamic DNS Settings	
Dynamic DNS	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: ● changeip.com ● dyndns.org

	● no-ip.org ● tzo.com ● DNS-O-Matic ● Others… Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API. Select **Disabled** to disable this feature.
Account Name / Email Address	This setting specifies the registered user name for the dynamic DNS service.
Password / TZO Key	This setting specifies the password for the dynamic DNS service.
Hosts / Domain	This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

Important Note
In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN's IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service providers' policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long time. Therefore the Pepwave router performs an update every 23 days, even if a WAN's IP address has not changed.

10 Advanced Wi-Fi Settings

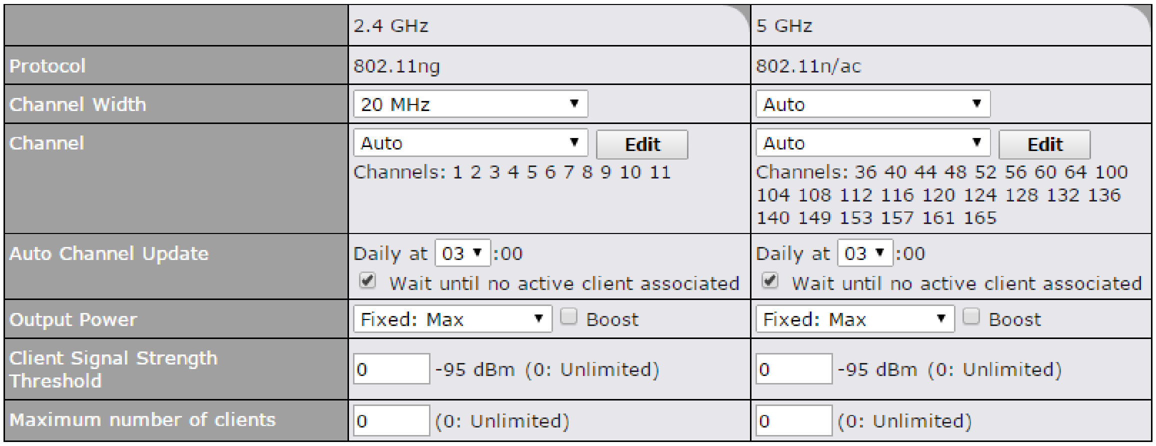
Wi-Fi settings can be configured at **Advanced>Wi-Fi Settings** (or **AP>Settings** on some models). Note that menus displayed can vary by model.



AP Settings	
SSID	2.4 GHz 5 GHz Integrated AP supports 2.4 GHz only. ☑ ☑ Testing
Operating Country	United States ▾
Preferred Frequency	● 2.4 GHz ○ 5 GHz Integrated AP supports 2.4 GHz only.

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

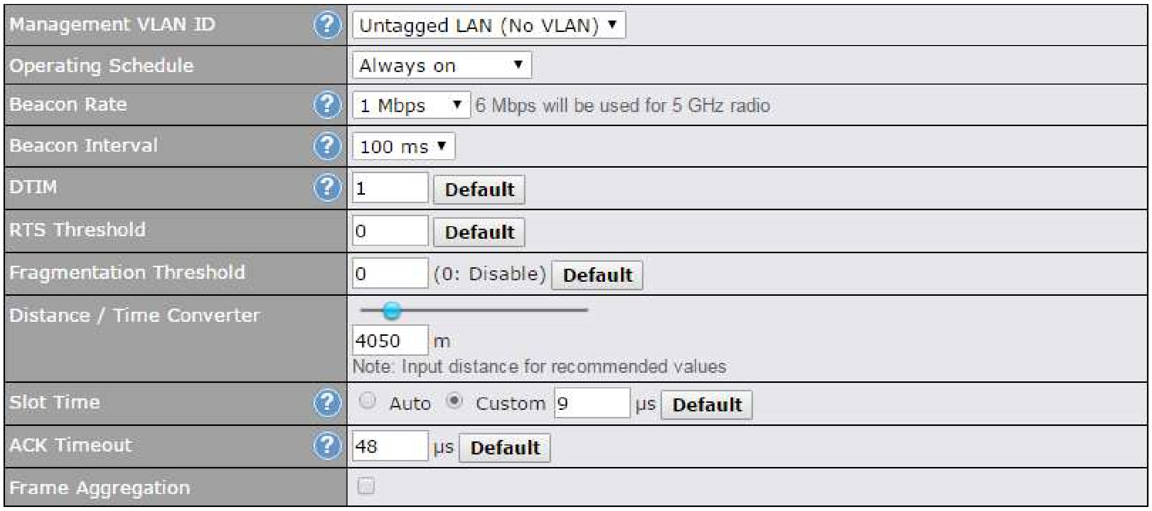
Important Note
Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.



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

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

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

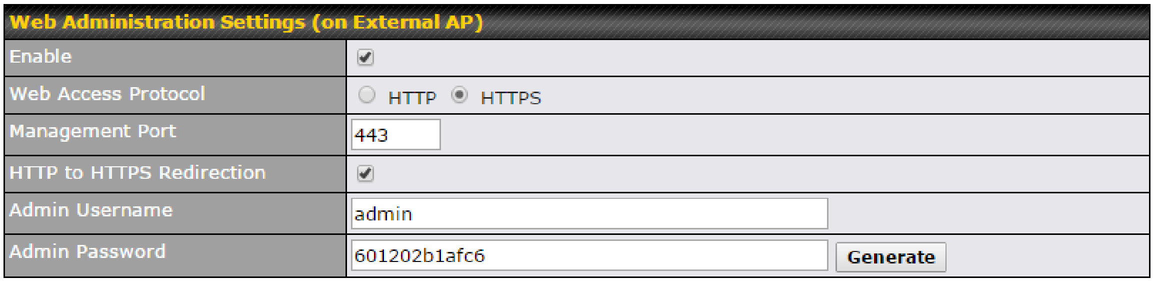


Management VLAN ID	Untagged LAN (No VLAN) ▾
Operating Schedule	Always on ▾
Beacon Rate	1 Mbps ▾ 6 Mbps will be used for 5 GHz radio
Beacon Interval	100 ms ▾
DTIM	1 Default
RTS Threshold	0 Default
Fragmentation Threshold	0 (0: Disable) Default
Distance / Time Converter	4050 m Note: Input distance for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

Advanced AP Settings	
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as communication traffic between the AP and the AP Controller. The value is zero by default, which means that no VLAN tagging will be applied. NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller.
Operating Schedule	Choose from the schedules that you have defined in System>Schedule. Select the schedule for the integrated AP to follow from the drop-down menu.
Beacon Rate [A]	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.
Beacon Interval [A]	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DTIM [A]	This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to **1 ms**.
RTS Threshold [A]	The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500.
Fragmentation Threshold [A]	This setting determines the maximum size of a packet before it gets fragmented into multiple pieces.
Distance / Time Convertor	Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout.
Slot Time [A]	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to **9 μs**.

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

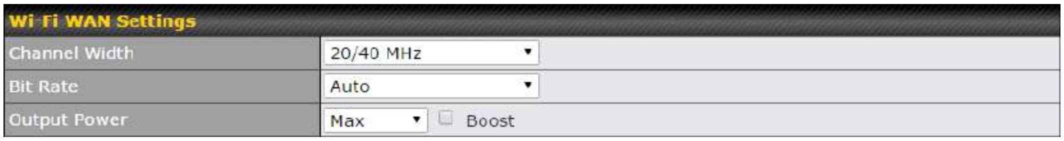
A - Advanced feature, please click the ? button on the top right-hand corner to activate.



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

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

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



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

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

11 ContentHub Configuration

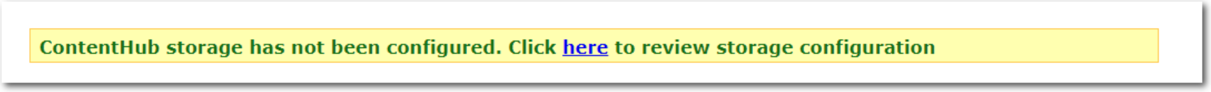
11.1 ContentHub

ContentHub allows you to deliver webpages and applications to users connected to the SSID using the local storage on your router like the Max HD2/HD4 with Mediafast, which can store up to 8GB of media. Users will be able to access news, articles, videos, and access your web app, without the need for internet access.

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

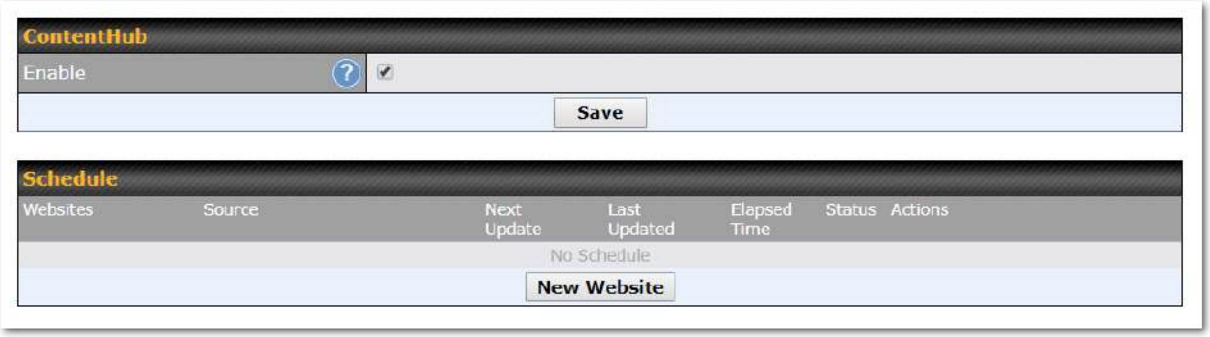
11.2 Configuring the ContentHub

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



ContentHub storage has not been configured. Click here to review storage configuration

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



ContentHub

Enable	☑

Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
No Schedule						

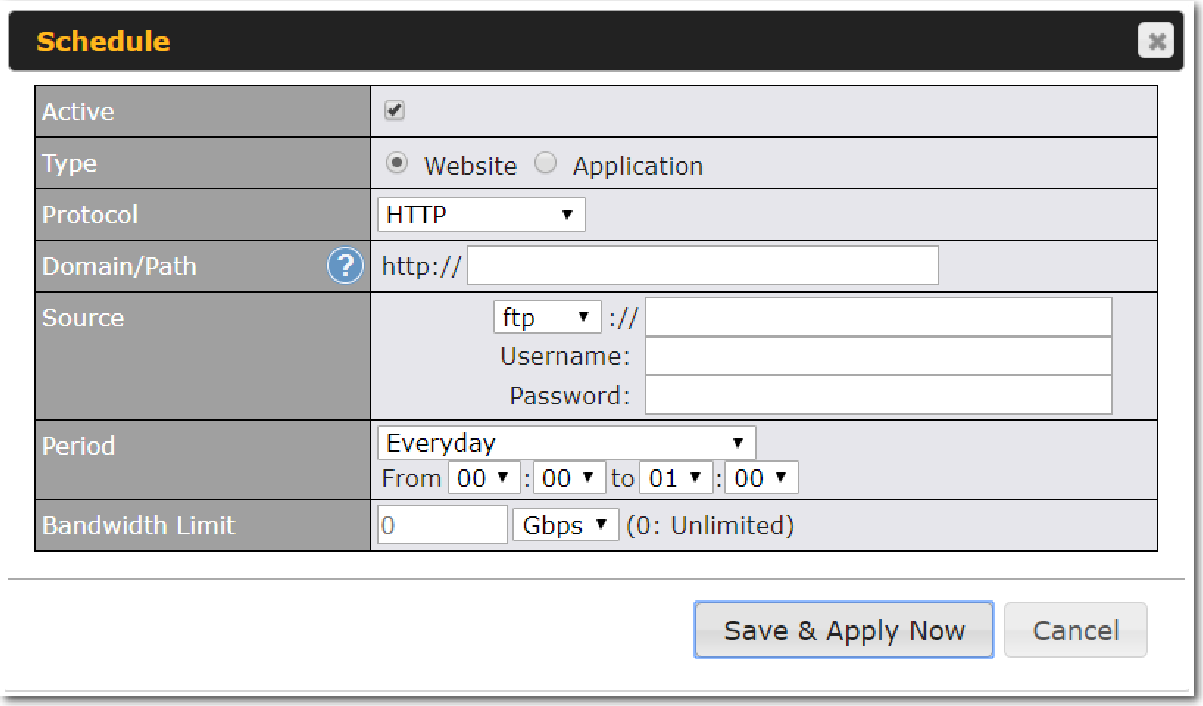
On an external server configure content (a website or application) that will be synced to the ContentHub; for example a html5 website.

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

11.3 Configure a website to be published from the ContentHub

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

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

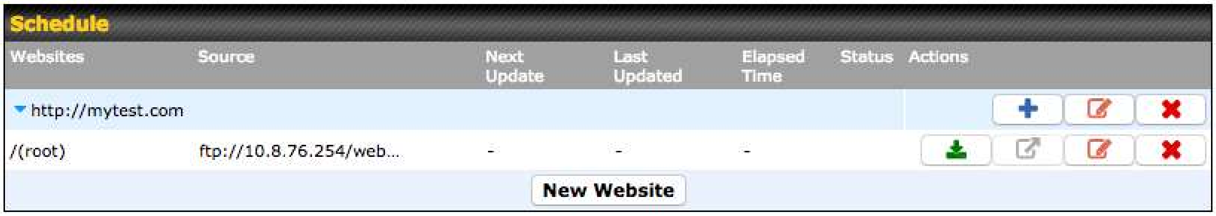


Schedule

Active	☑
Type	● Website ○ Application
Protocol	HTTP ▾
Domain/Path	http://
Source	ftp ▾ :// Username: Password:
Period	Everyday ▾ From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾
Bandwidth Limit	0 Gbps ▾ (0: Unlimited)

Schedule	
Active	Checkbox toggles the activation of the content
Type	This option allows you to select Website or Application
Protocol	HTTP,HTTPS or both
Domain/Path	The contenhub uses this as the domain name for client access (such as http://mytest.com).
Method	Only applicable for **Application** type: Choose between sync or file upload
Source	Enter the server details that the content will be downloaded from. Enter your credentials under **Username** and **Password**.
Period	This field determines how often the Router will search for updates to the source content.
Bandwidth Limit	Used to limit the bandwidth for each client to access the web server.

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

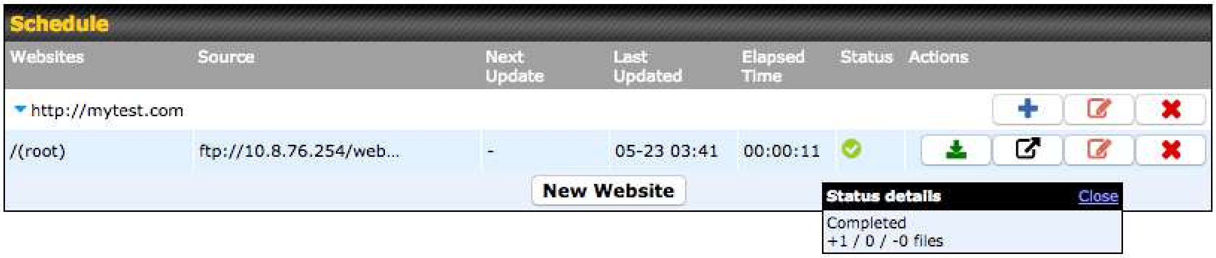


Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						✚ ✎ ✖
/(root)	ftp://10.8.76.254/web...	-	-	-		⬇ ↗ ✎ ✖

New Website

The content will be sync based on the **Period** that is configured before. If you want to trigger the sync manually, you can click “⬇”. The “Status” column shows the sync progress. When the sync complete, there is a summary as shown in the screenshot below:



Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						✚ ✎ ✖
/(root)	ftp://10.8.76.254/web...	-	05-23 03:41	00:00:11	✓	⬇ ↗ ✎ ✖

New Website

Status details Close

Completed
+1 / 0 / -0 files

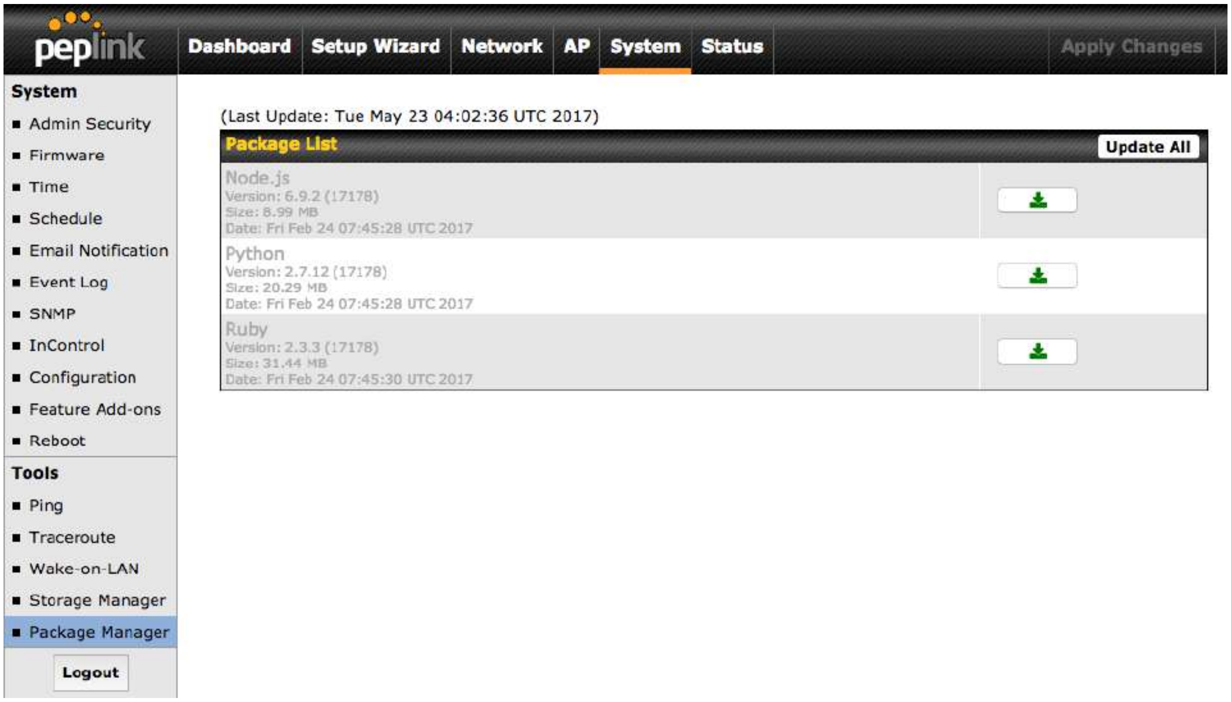
To access the content, open a browser in MFA’s client and enter the domain configured before (such as http://mytest.com).

11.4 Configure an application to be published from the ContentHub

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

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

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



(Last Update: Tue May 23 04:02:36 UTC 2017)

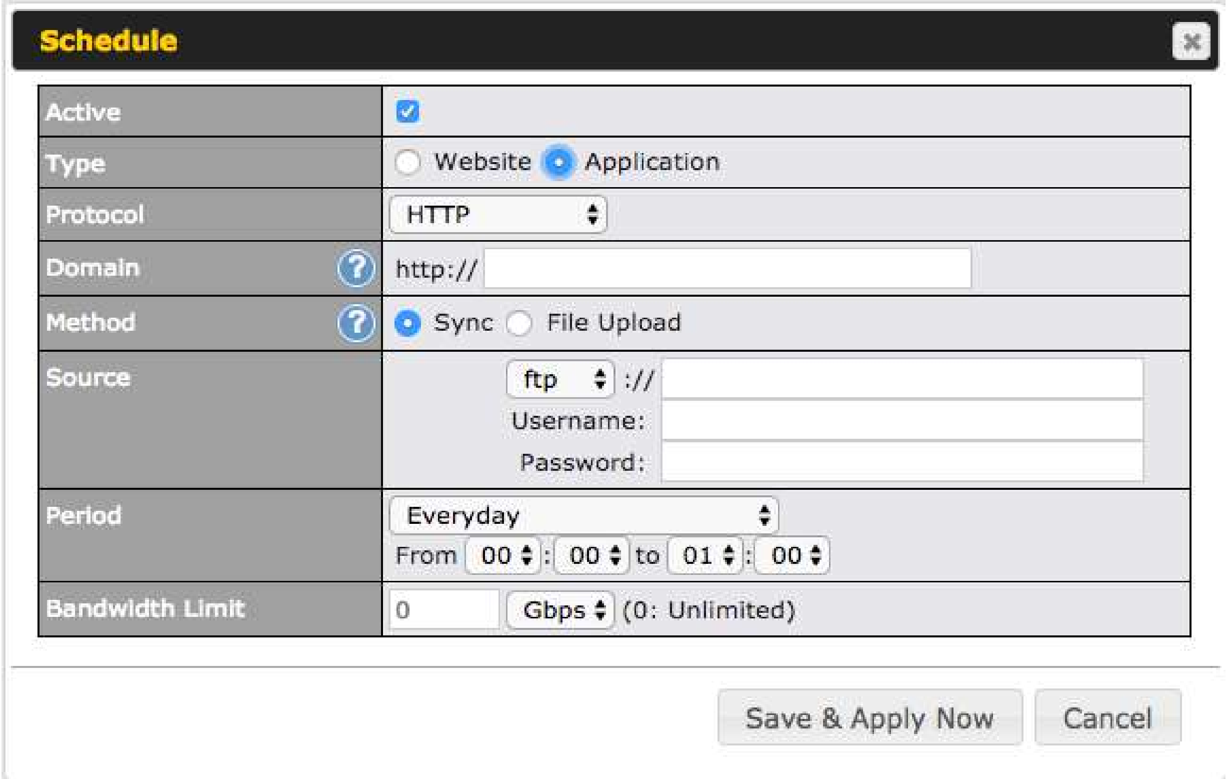
Package List

Node.js
Version: 6.9.2 (17178)
Size: 8.99 MB
Date: Fri Feb 24 07:45:28 UTC 2017

Python
Version: 2.7.12 (17178)
Size: 20.29 MB
Date: Fri Feb 24 07:45:28 UTC 2017

Ruby
Version: 2.3.3 (17178)
Size: 31.44 MB
Date: Fri Feb 24 07:45:30 UTC 2017

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



Schedule

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

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

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

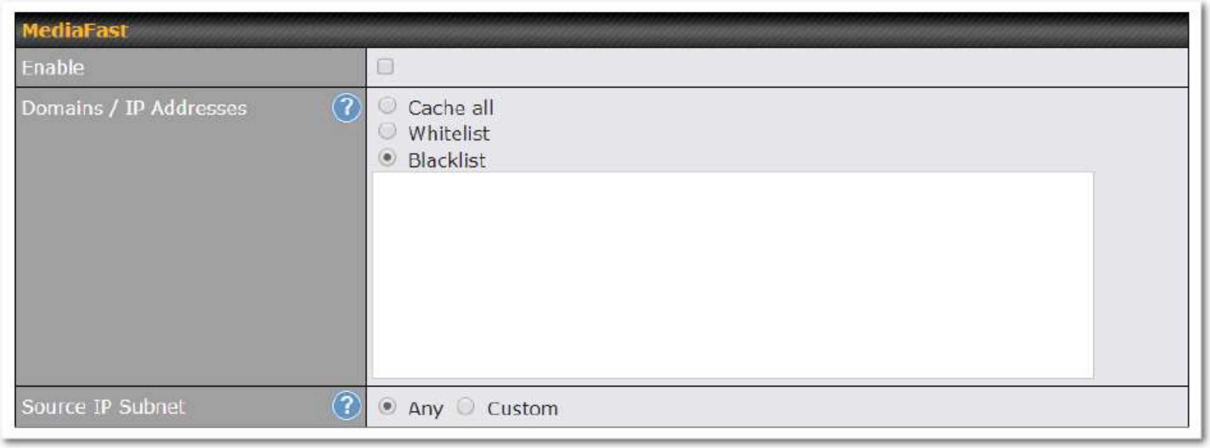
1. Implement two bash script files, start.sh and stop.sh in root folder, to start and stop your application. the Mediafast router will only execute start.sh and stop.sh when the corresponding website is enabled and disabled respectively.
2. Compress your application files and the bash script to .tar.gz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

12 MediaFast Configuration

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

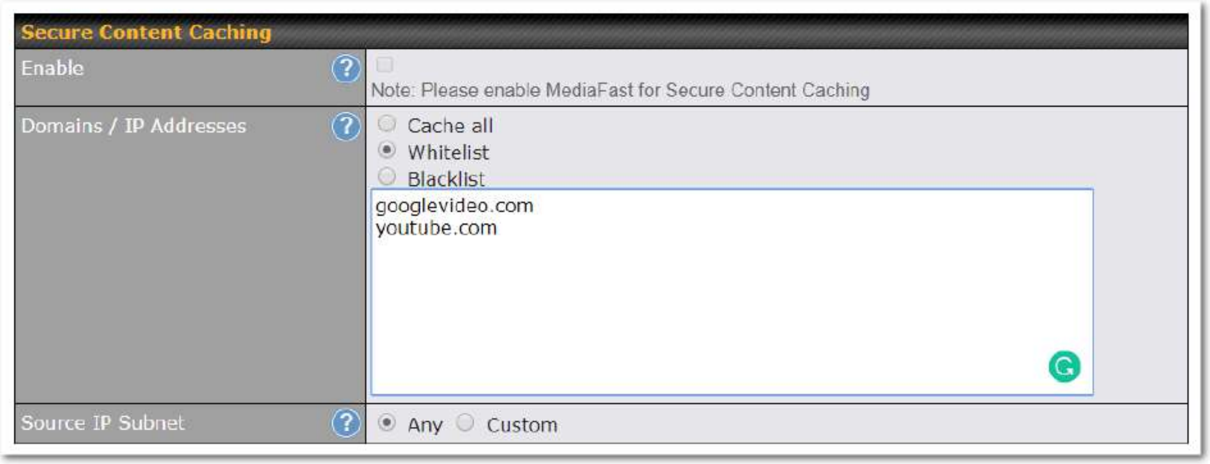
12.1 Setting Up MediaFast Content Caching

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



MediaFast	
Enable	□
Domains / IP Addresses	○ Cache all ○ Whitelist ● Blacklist
Source IP Subnet	● Any ○ Custom

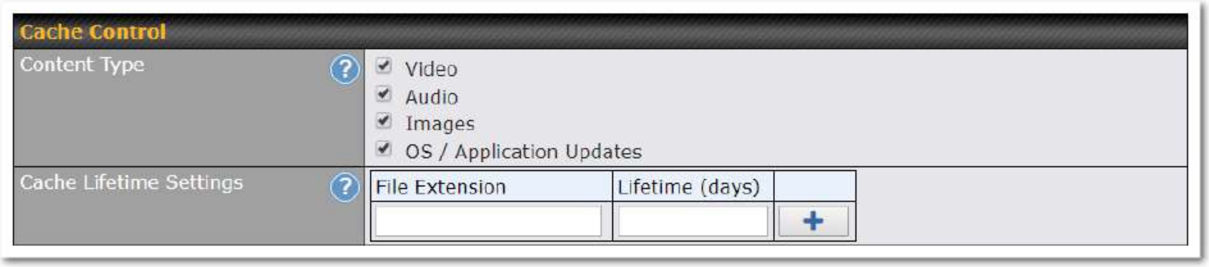
MediaFast	
Enable	Click the checkbox to enable MediaFast content caching.
Domains / IP Addresses	Choose to **Cache on all domains**, or enter domain names and then choose either **Whitelist** (cache the specified domains only) or **Blacklist** (do not cache the specified domains).
Source IP Subnet	This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



Secure Content Caching	
Enable	□ Note: Please enable MediaFast for Secure Content Caching
Domains / IP Addresses	○ Cache all ● Whitelist ○ Blacklist googlevideo.com youtube.com
Source IP Subnet	● Any ○ Custom

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

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

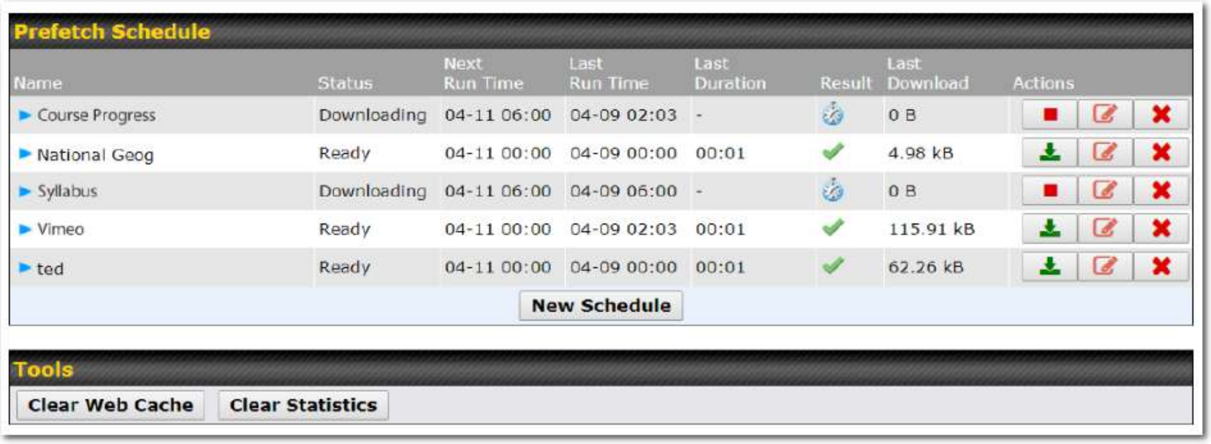


Cache Control	
Content Type	☑ Video ☑ Audio ☑ Images ☑ OS / Application Updates
Cache Lifetime Settings	File Extension | Lifetime (days) | +

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

12.2 Scheduling Content Prefetching

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



Prefetch Schedule

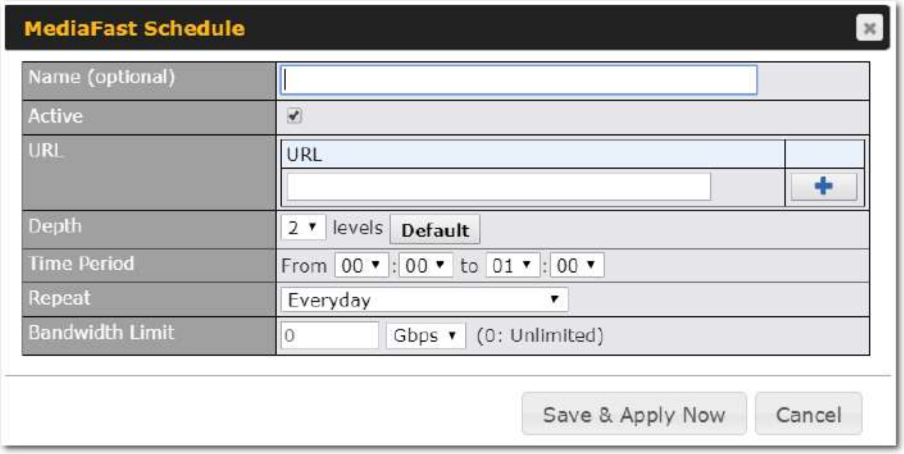
Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
► Course Progress	Downloading	04-11 06:00	04-09 02:03	-	⏲	0 B	■ ✎ ✖
► National Geog	Ready	04-11 00:00	04-09 00:00	00:01	✓	4.98 kB	⬇ ✎ ✖
► Syllabus	Downloading	04-11 06:00	04-09 06:00	-	⏲	0 B	■ ✎ ✖
► Vimeo	Ready	04-11 00:00	04-09 02:03	00:01	✓	115.91 kB	⬇ ✎ ✖
► ted	Ready	04-11 00:00	04-09 00:00	00:01	✓	62.26 kB	⬇ ✎ ✖

New Schedule

Tools

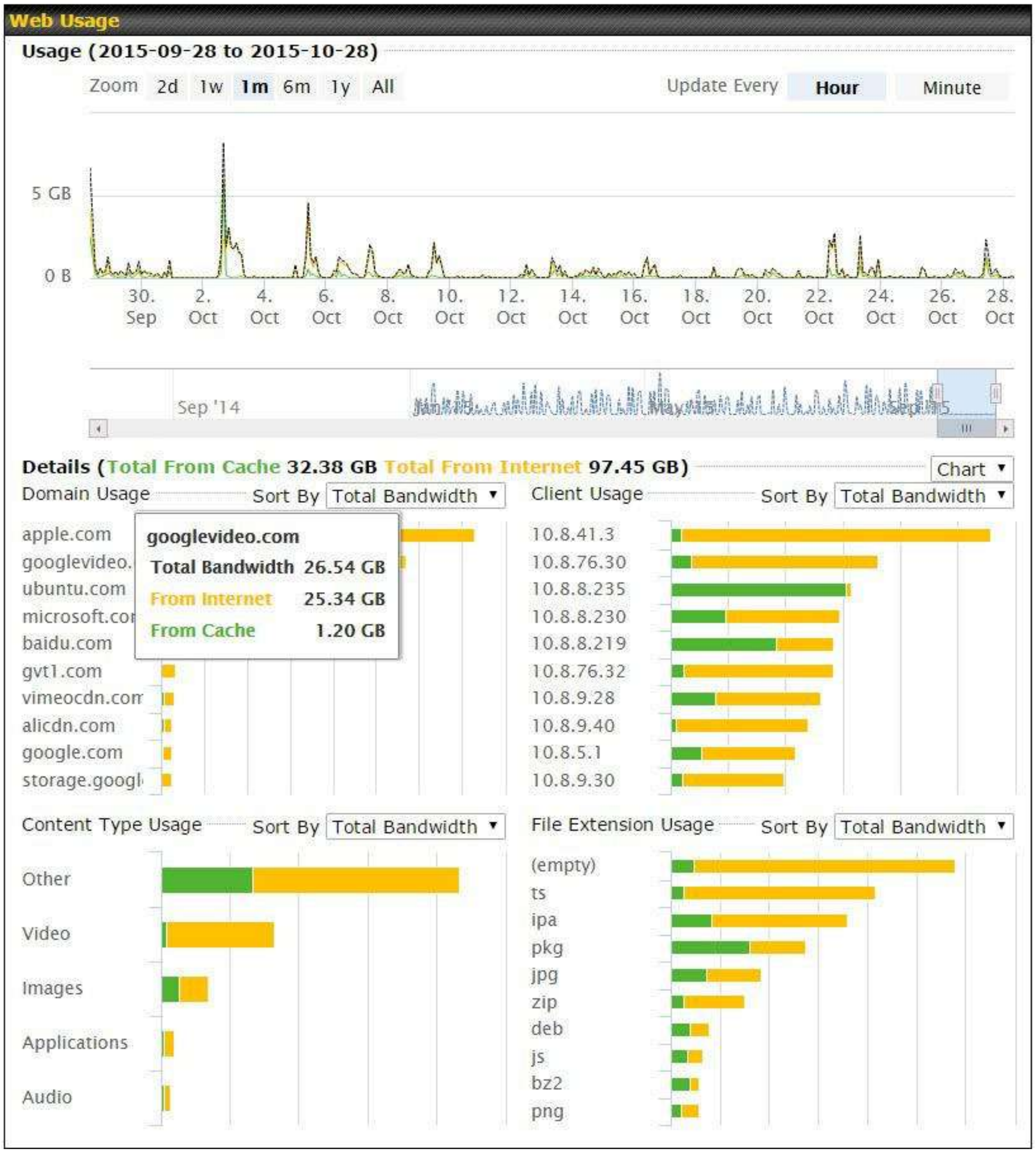
Clear Web Cache | Clear Statistics

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

	 MediaFast Schedule Name (optional): Active: ☑ URL: URL ✚ Depth: 2 levels Default Time Period: From 00 : 00 to 01 : 00 Repeat: Everyday Bandwidth Limit: 0 Gbps (0: Unlimited) Save & Apply Now Cancel Simply provide the requested information to create your schedule.
Clear Web Cache	To clear all cached content, click this button. Note that this action cannot be undone.
Clear Statistics	To clear all prefetch and status page statistics, click this button.

12.3 Viewing MediaFast Statistics

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



Web Usage

Usage (2015-09-28 to 2015-10-28)

Zoom 2d 1w 1m 6m 1y All

Update Every: Hour

Details (Total From Cache 32.38 GB Total From Internet 97.45 GB)

Domain Usage — Sort By: Total Bandwidth

googlevideo.com

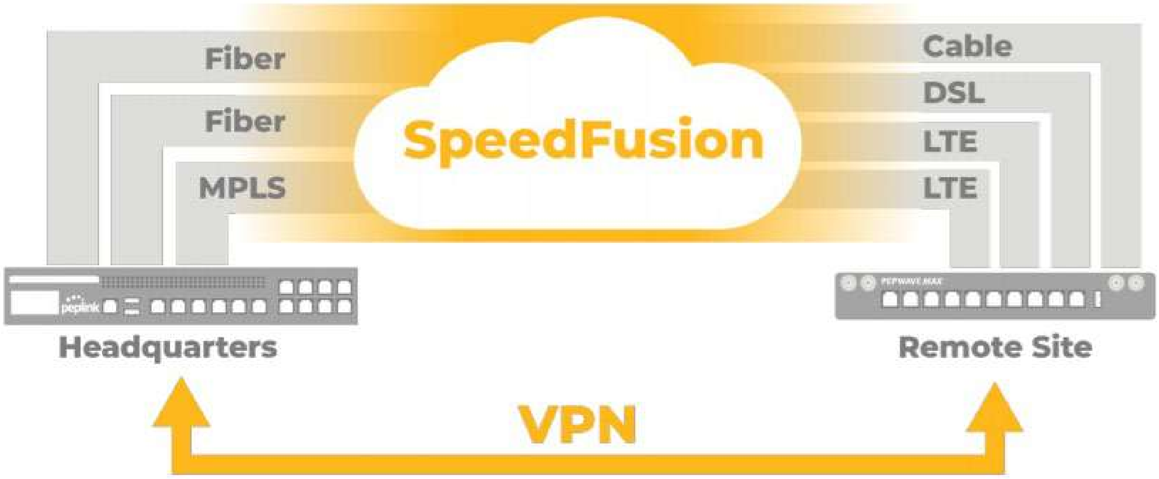
Total Bandwidth	26.54 GB
From Internet	25.34 GB
From Cache	1.20 GB

Client Usage — Sort By: Total Bandwidth

Content Type Usage — Sort By: Total Bandwidth

File Extension Usage — Sort By: Total Bandwidth

13 Bandwidth Bonding SpeedFusion™ / PepVPN



Pepwave bandwidth bonding SpeedFusion™ is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion functionality securely connects your Pepwave router to another Pepwave or Peplink device (Peplink Balance 210/310/380/580/710/1350 only). Data, voice, or video communications between these locations are kept confidential across the public Internet.

Bandwidth bonding SpeedFusion™ is specifically designed for multi-WAN environments. In case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic.

Different models of our SD-WAN routers have different numbers of site-to-site connections allowed. End-users who need to have more site-to-site connections can purchase a SpeedFusion license to increase the number of site-to-site connections allowed.

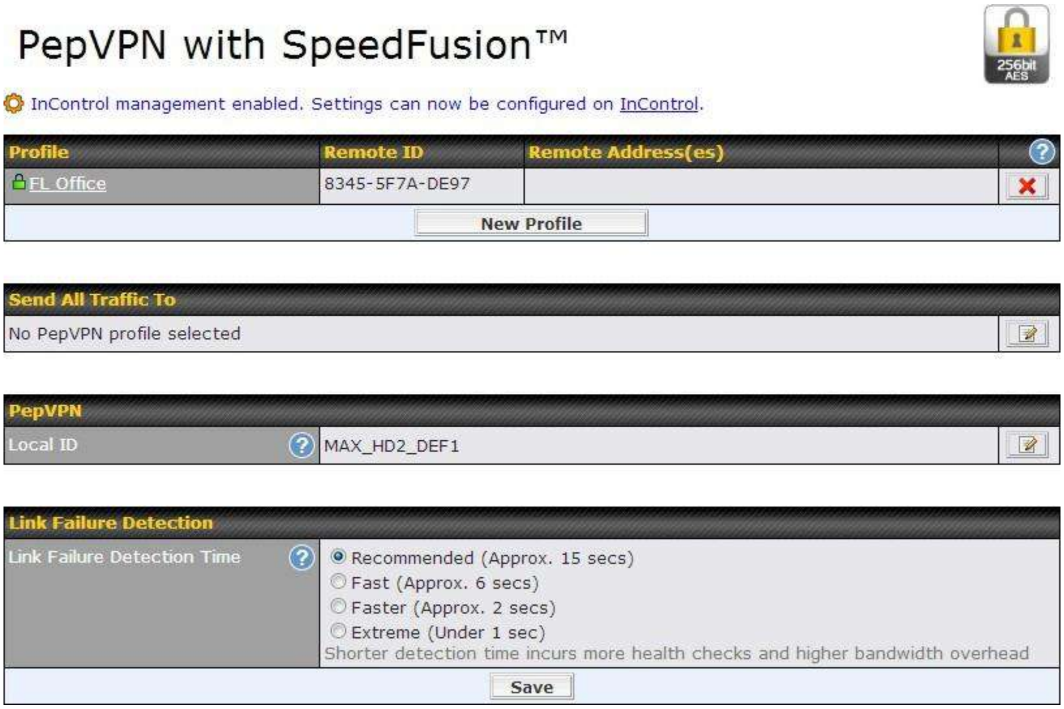
Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.

VPN bandwidth bonding is supported in Firmware 5.1 or above. All available bandwidth will be utilized to establish the VPN tunnel, and all traffic will be load balanced at packet level across all links. VPN bandwidth bonding is enabled by default.

13.1 PepVPN

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

Advanced>PepVPN.



PepVPN with SpeedFusion™

InControl management enabled. Settings can now be configured on InControl.

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

Send All Traffic To	
No PepVPN profile selected	

PepVPN	
Local ID	MAX_HD2_DEF1

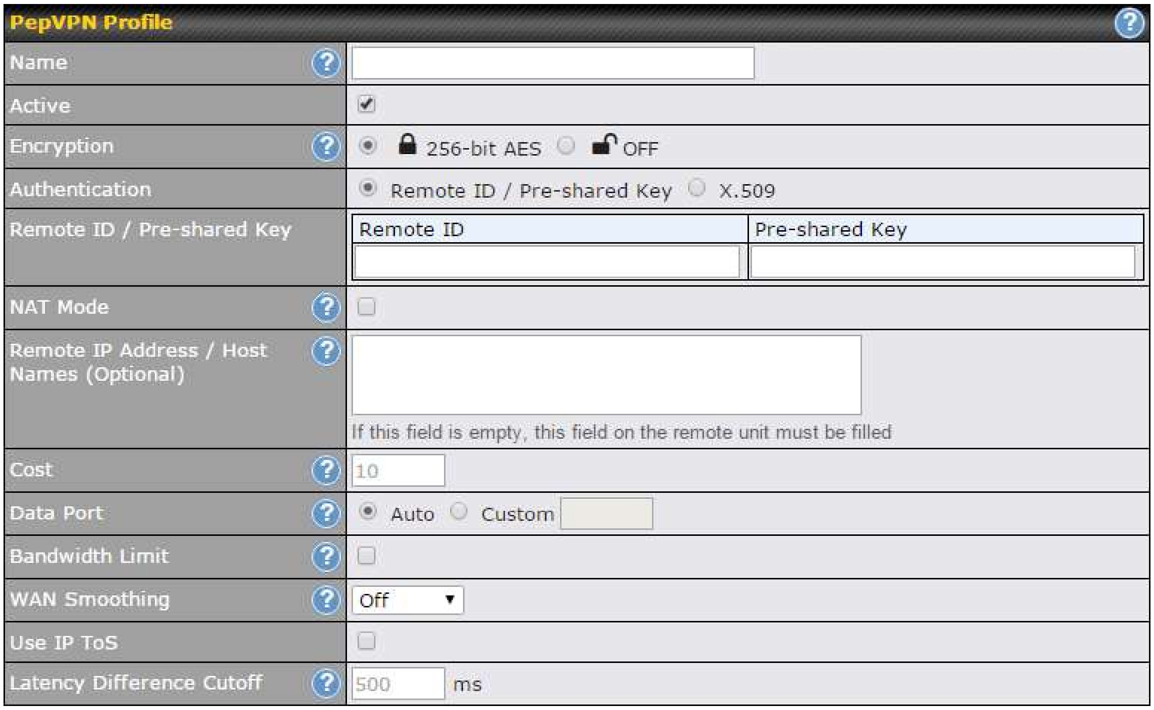
Link Failure Detection	
Link Failure Detection Time	● Recommended (Approx. 15 secs) ○ Fast (Approx. 6 secs) ○ Faster (Approx. 2 secs) ○ Extreme (Under 1 sec) Shorter detection time incurs more health checks and higher bandwidth overhead

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

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

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

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



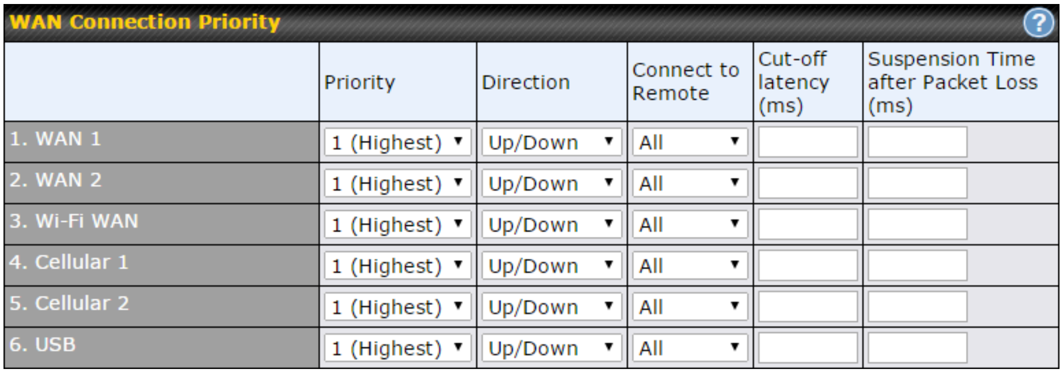
PepVPN Profile	
Name	
Active	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID / Pre-shared Key
NAT Mode	□
Remote IP Address / Host Names (Optional)	If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	□
WAN Smoothing	Off
Use IP ToS	□
Latency Difference Cutoff	500 ms

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

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

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

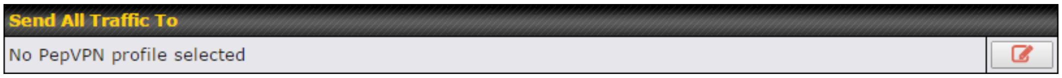
To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>Basic Settings>*LAN Profile Name*** and refer to instructions in section 9.1



WAN Connection Priority ?

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

WAN Connection Priority	
WAN Connection Priority	If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used. To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the ? button.

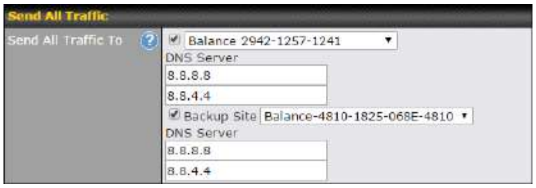


Send All Traffic To

No PepVPN profile selected ✎

Send All Traffic To

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



Send All Traffic

Send All Traffic To ? ☑ Balance 2942-1257-1241 ▾

DNS Server

8.8.8.8

8.8.4.4

☑ Backup Site Balance-4810-1825-068E-4810 ▾

DNS Server

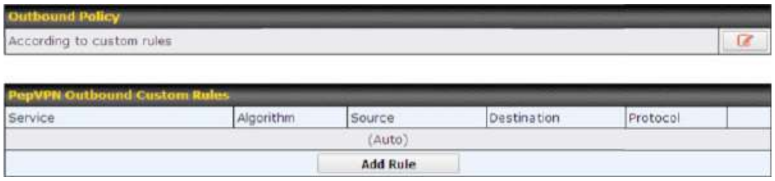
8.8.8.8

8.8.4.4

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

Outbound Policy/PepVPN Outbound Custom Rules

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

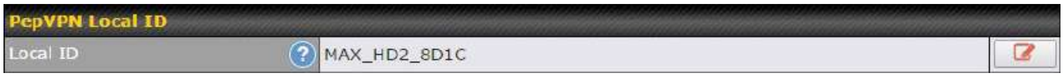


Outbound Policy

According to custom rules

PepVPN Outbound Custom Rules

Service	Algorithm	Source	Destination	Protocol
		(Auto)		

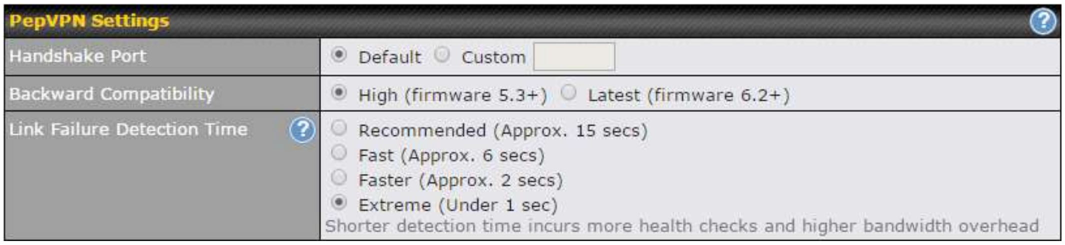


PepVPN Local ID

Local ID	MAX_HD2_8D1C

PepVPN Local ID

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



PepVPN Settings

Handshake Port	● Default ○ Custom
Backward Compatibility	● High (firmware 5.3+) ○ Latest (firmware 6.2+)
Link Failure Detection Time	○ Recommended (Approx. 15 secs) ○ Fast (Approx. 6 secs) ○ Faster (Approx. 2 secs) ● Extreme (Under 1 sec) Shorter detection time incurs more health checks and higher bandwidth overhead

PepVPN Settings

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

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

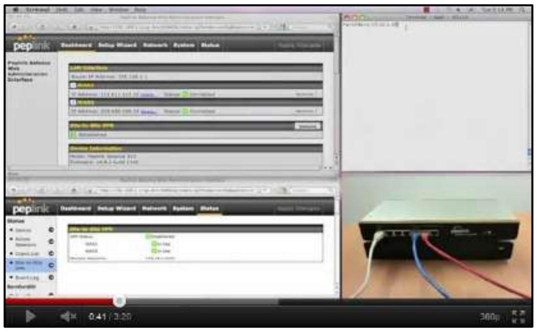
A - Advanced feature, please click the ? button on the top right-hand corner to activate.

Important Note

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

Tip

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



http://youtu.be/TLQgdpPSY88

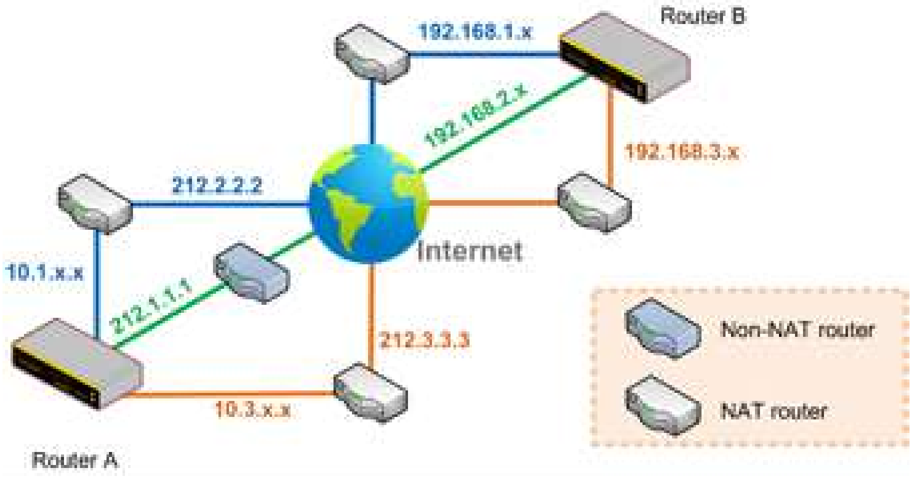
13.2 The Pepwave Router Behind a NAT Router

Pepwave routers support establishing SpeedFusionTM over WAN connections which are behind a NAT (network address translation) router.

To enable a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to inbound port-forward TCP port 32015 to the Pepwave router.

If one or more WAN connections on Unit A can accept VPN connections (by means of port forwarding or not), while none of the WAN connections on the peer Unit B can do so, you should enter all of Unit A's public IP addresses or hostnames into Unit B's **Remote IP Addresses / Host Names** field. Leave the field in Unit A blank. With this setting, a SpeedFusionTM connection can be set up and all WAN connections on both sides will be utilized.

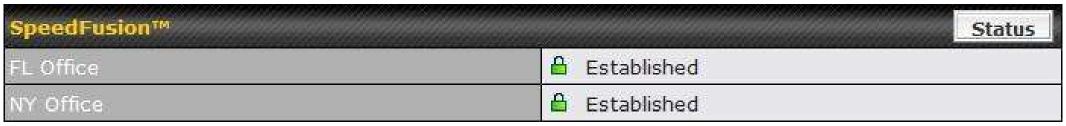
See the following diagram for an example of this setup in use:



One of the WANs connected to Router A is non-NAT'd (*212.1.1.1*). The rest of the WANs connected to Router A and all WANs connected to Router B are NAT'd. In this case, the **Peer IP Addresses / Host Names** field for Router B should be filled with all of Router A's hostnames or public IP addresses (i.e., *212.1.1.1*, *212.2.2.2*, and *212.3.3.3*), and the field in Router A can be left blank. The two NAT routers on WAN1 and WAN3 connected to Router A should inbound port-forward TCP port 32015 to Router A so that all WANs will be utilized in establishing the VPN.

13.3 SpeedFusion™ Status

SpeedFusionTM status is shown in the Dashboard. The connection status of each connection profile is shown as below.



SpeedFusion™	Status
FL Office	🔒 Established
NY Office	🔒 Established

After clicking the **Status** button at the top right corner of the SpeedFusionTM table, you will be forwarded to **Status>SpeedFusionTM**, where you can view subnet and WAN connection information for each VPN peer. Please refer to **Section 22.6** for details.

IP Subnets Must Be Unique Among VPN Peers
The entire interconnected SpeedFusion^{TM} network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

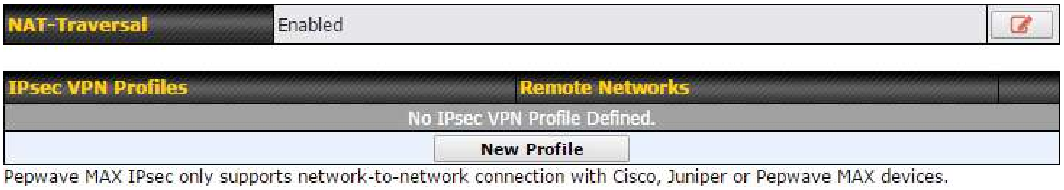
14 IPsec VPN

IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

IPsec VPN on Pepwave routers is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for a multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g., unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

14.1 IPsec VPN Settings

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

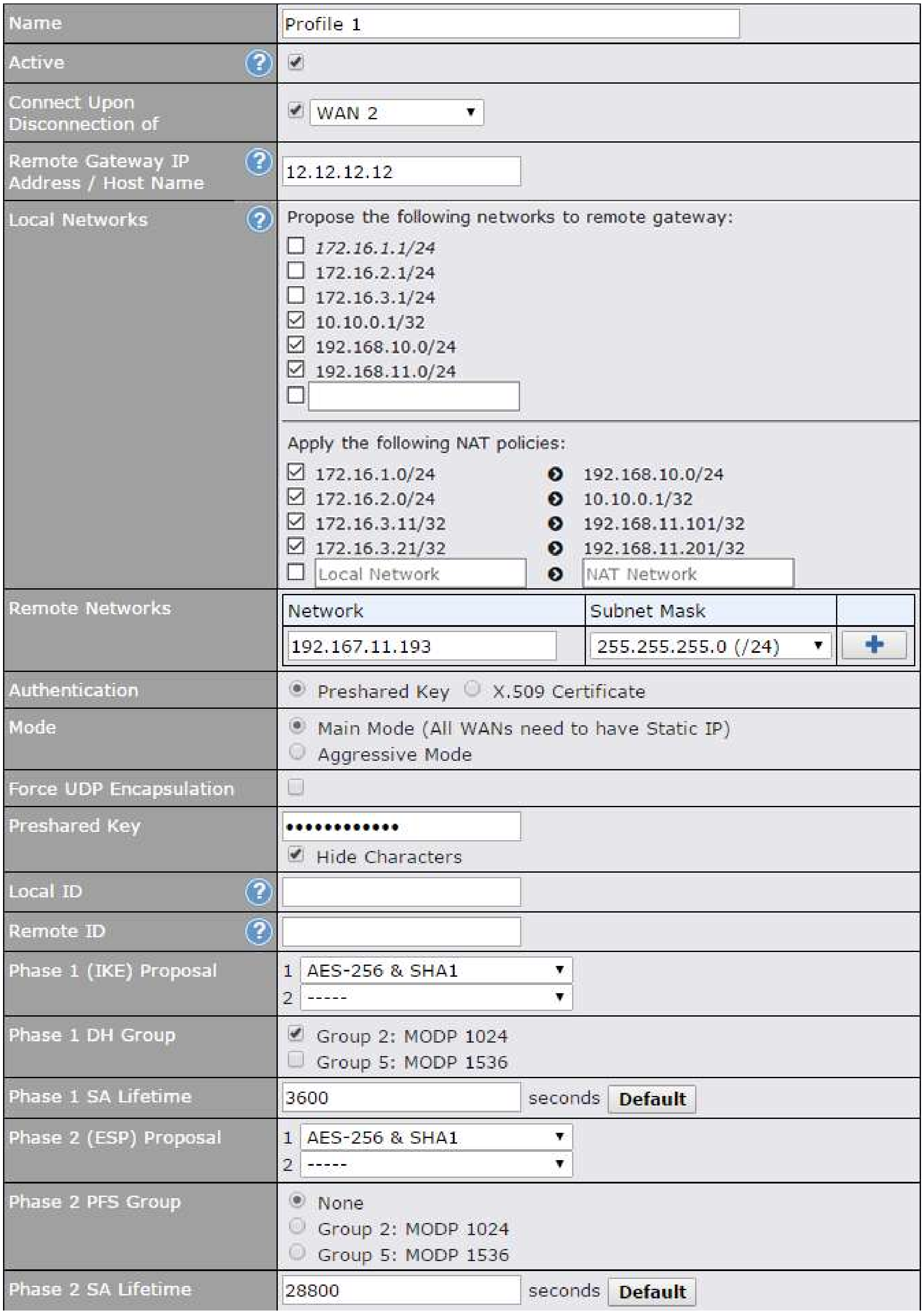


NAT-Traversal	Enabled

IPsec VPN Profiles	Remote Networks
No IPsec VPN Profile Defined.	

Pepwave MAX IPsec only supports network-to-network connection with Cisco, Juniper or Pepwave MAX devices.

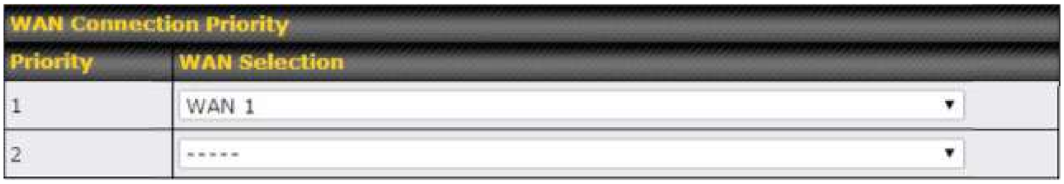
A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown. **NAT-Traversal** should be enabled if your system is behind a NAT router. Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Pepwave, Cisco, or Juniper routers via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



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

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

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



WAN Connection Priority	
Priority	WAN Selection
1	WAN 1 ▾
2	----- ▾

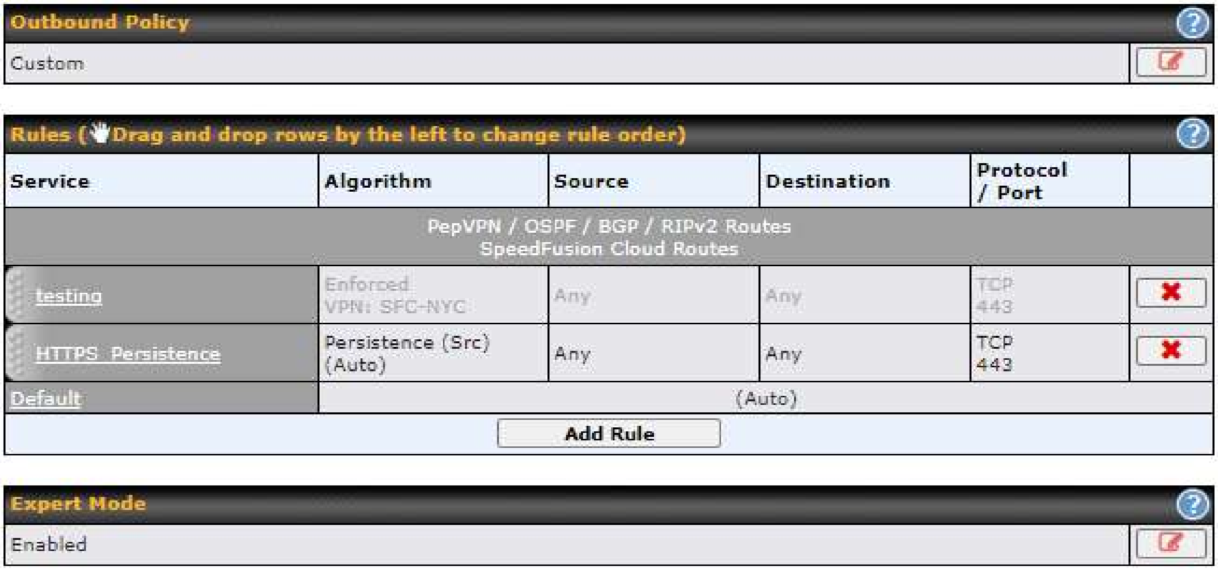
WAN Connection Priority	
WAN Connection	Select the appropriate WAN connection from the drop-down menu.

15 Outbound Policy

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

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

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



Outbound Policy	
Custom	

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

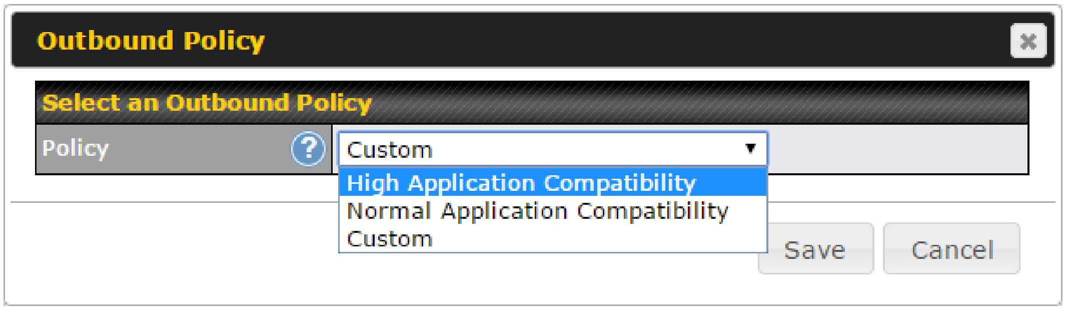
Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes SpeedFusion Cloud Routes					
testing	Enforced VPN: SFC-NYC	Any	Any	TCP 443	✖
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				

Expert Mode	
Enabled	

15.1 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at

Advanced>Outbound Policy> or **Advanced>PepVPN>Outbound Policy.** Click the button beside the **Outbound Policy** box:


Outbound Policy
Select an Outbound Policy
Policy
Custom
High Application Compatibility
Normal Application Compatibility
Custom
Save
Cancel

There are three main selections for the outbound traffic policy:

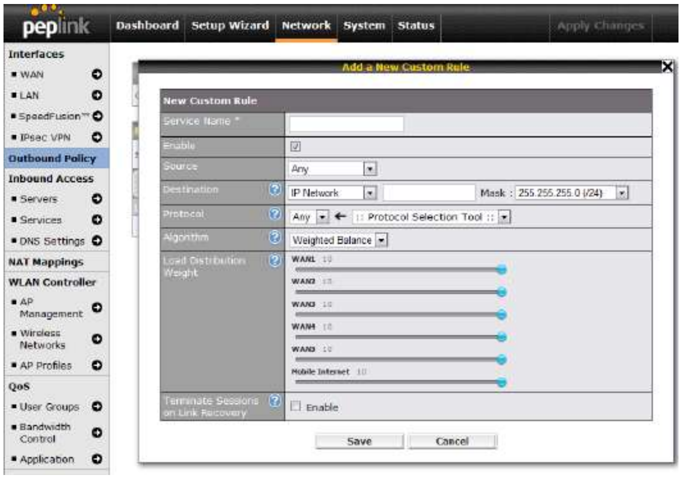
- High Application Compatibility
- Normal Application Compatibility
- Custom

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

Outbound Policy Settings	
High Application Compatibility	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the highest application compatibility.
Normal Application Compatibility	Outbound traffic from a source LAN device to the same destination Internet IP address will be routed through the same WAN connection persistently, regardless of protocol. This option provides high compatibility to most applications, and users still benefit from WAN link load balancing when multiple Internet servers are accessed.
Custom	Outbound traffic behavior can be managed by defining rules in a custom rule table. A default rule can be defined for connections that cannot be matched with any of the rules.

The default policy is **Normal Application Compatibility**.

Tip
Want to know more about creating outbound rules? Visit our YouTube Channel for a video tutorial!

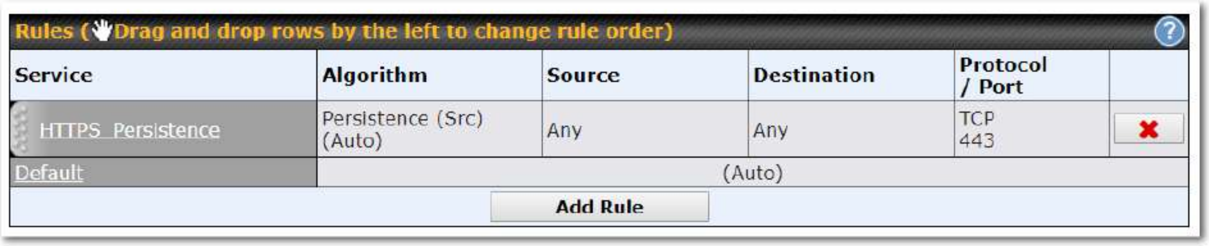


New Custom Rule	
Service Name *	
Enable	☑
Source	Any
Destination	IP Network Mask : 255.255.255.0 (/24)
Protocol	Any ← :: Protocol Selection Tool ::
Algorithm	Weighted Balance
Load Distribution Weight	WAN1 10 WAN2 10 WAN3 10 WAN4 10 WAN5 10 Mobile Internet 10
Terminate Sessions on Link Recovery	□ Enable

http://youtu.be/rKH4AS_bQnE

15.2 Adding Rules for Outbound Policy

The menu underneath enables you to define Outbound policy rules:

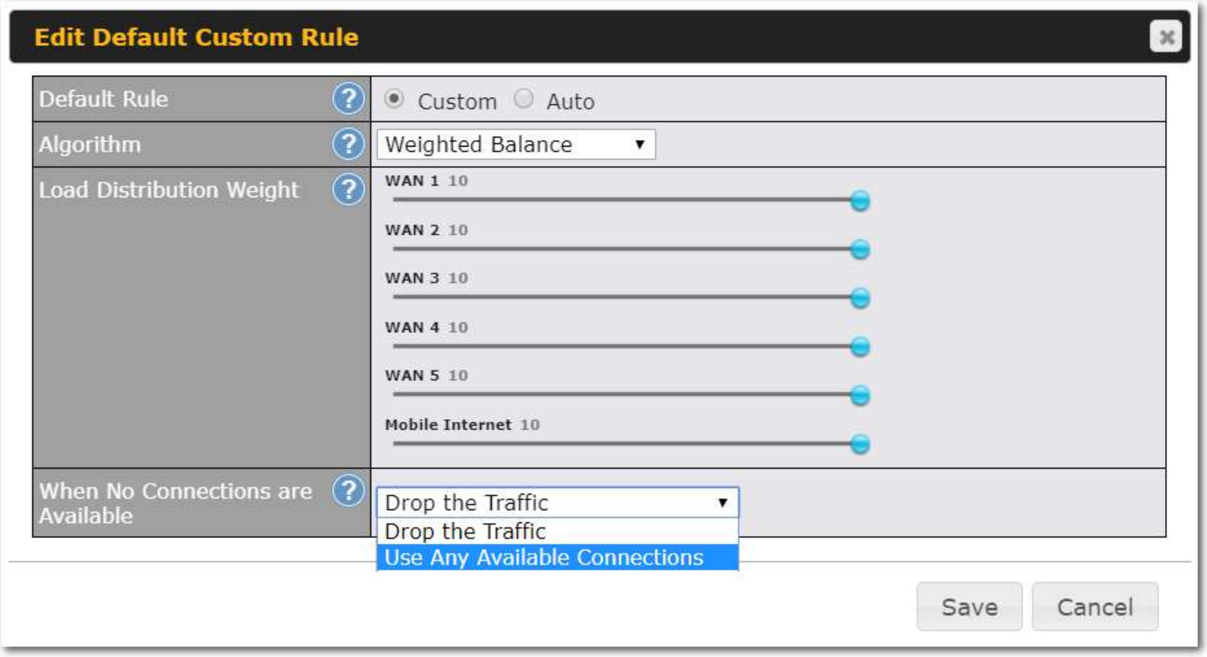


Rules (Drag and drop rows by the left to change rule order)

Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				

The bottom-most rule is **Default**. Edit this rule to change the device's default manner of controlling outbound traffic for all connections that do not match any of the rules above it. Under the **Service** heading, click **Default** to change these settings.

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

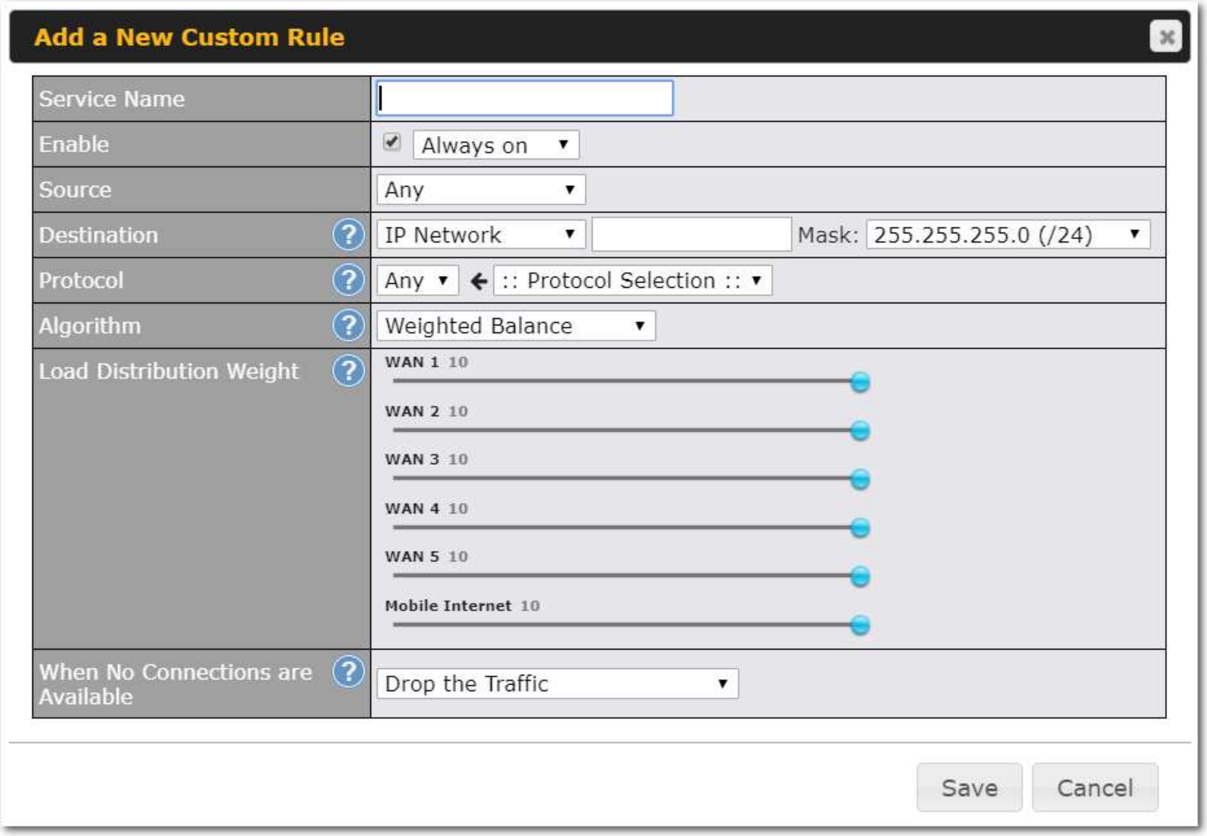


Edit Default Custom Rule

Default Rule	● Custom ○ Auto
Algorithm	Weighted Balance ▾
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic ▾

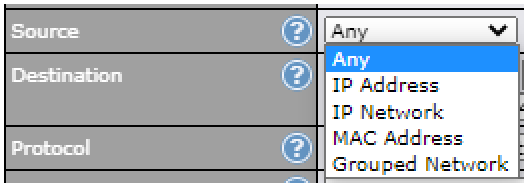
By default, **Auto** is selected as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

To create a custom rule, click **Add Rule** at the bottom of the table.



Add a New Custom Rule

Service Name	
Enable	☑ Always on
Source	Any
Destination	IP Network — Mask: 255.255.255.0 (/24)
Protocol	Any ← :: Protocol Selection ::
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic

New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	This setting specifies whether the outbound traffic rule takes effect. When **Enable** is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When **Enable** is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.
Source	This setting specifies the source IP Address, IP Network, MAC Address or Grouped Network for traffic that matches the rule.  Source Any Destination Protocol Any IP Address IP Network MAC Address Grouped Network
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.