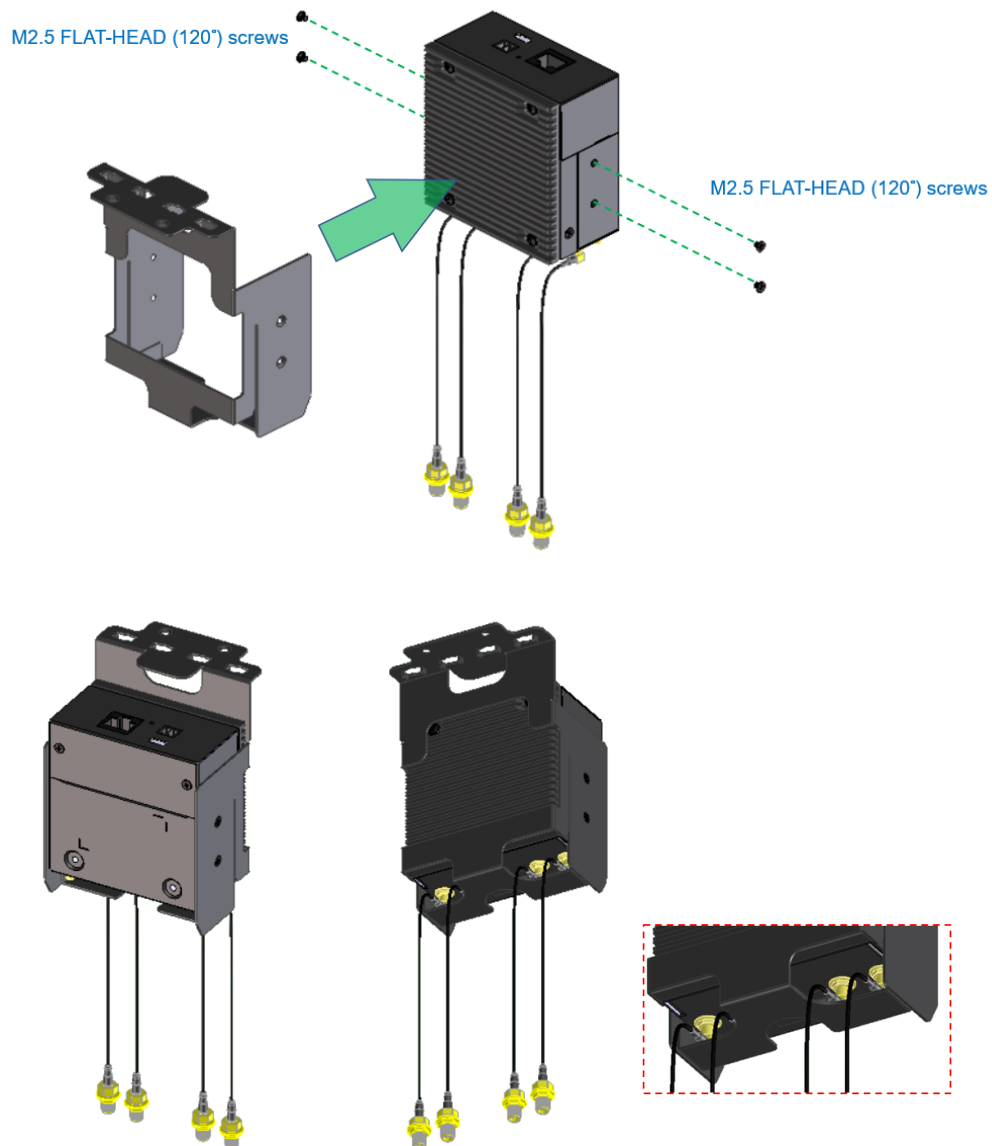
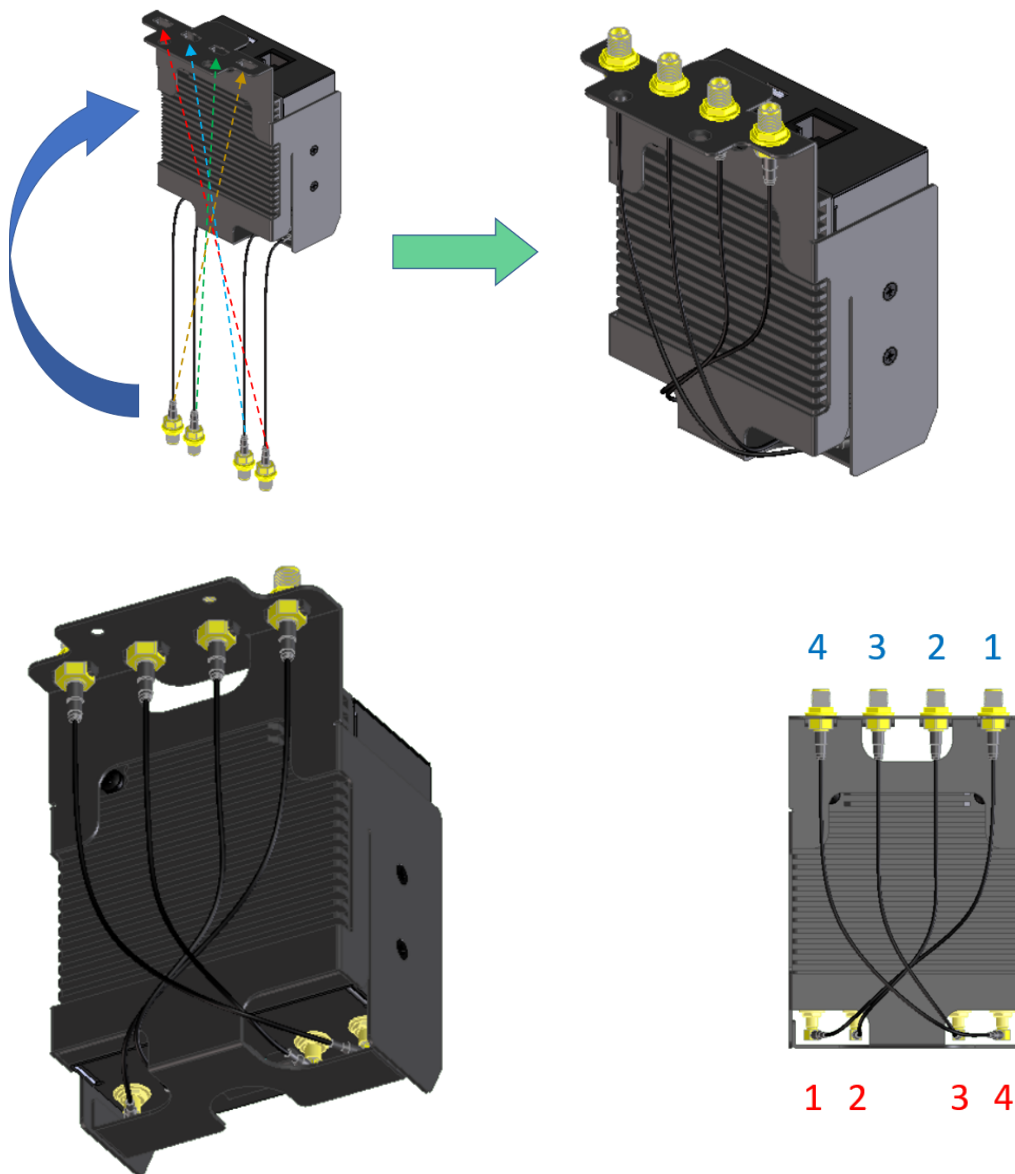
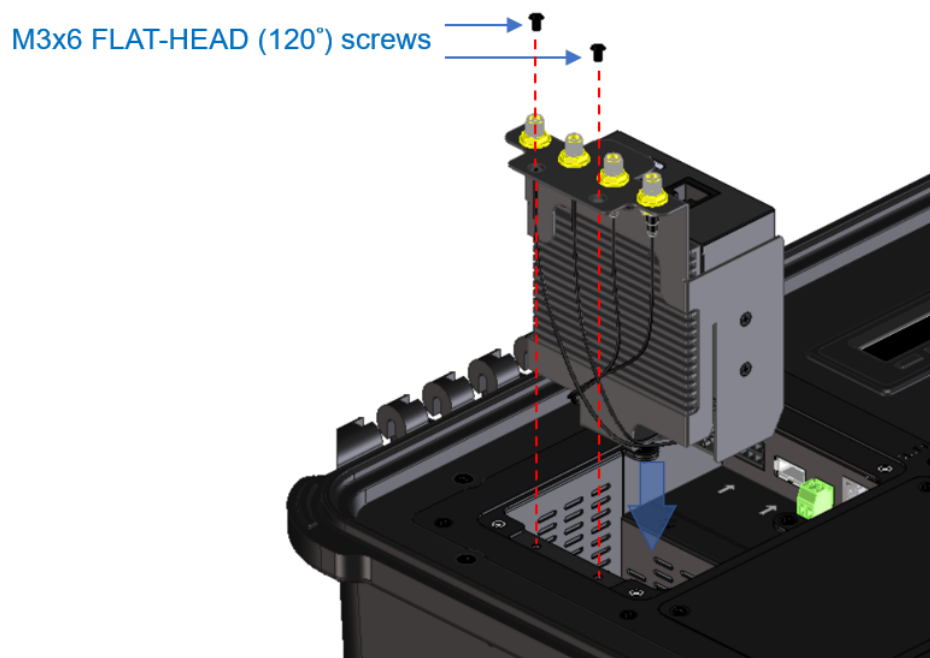




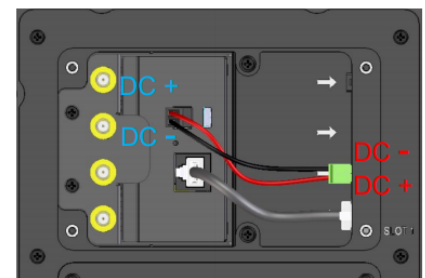
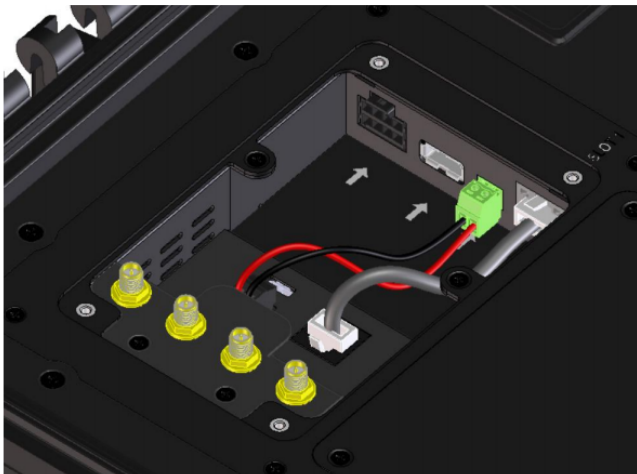
- STEP 3: Assemble SMA connectors to the bracket



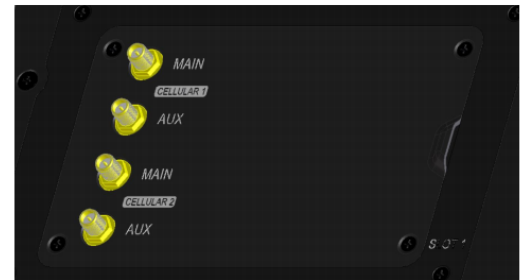
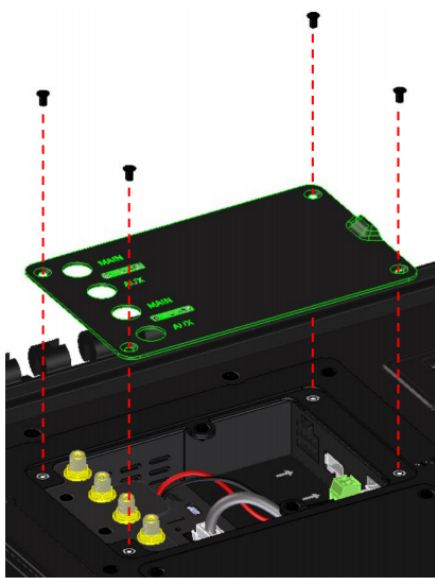
- STEP 4: Lock the SFE-Duo set in the slot with 2 pcs M3 screws.



- STEP 5: Connect DC power & ETH port



- STEP 6: Lock the slot cover with 4 pcs M3 screws.



0

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

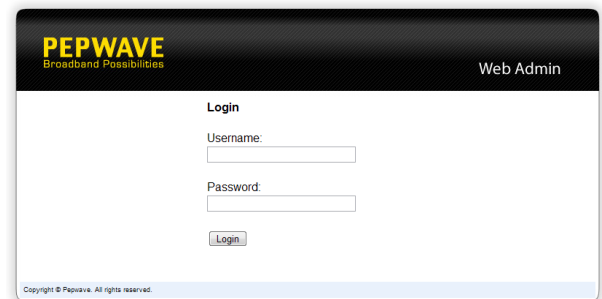
(This is the default LAN IP address for Pepwave routers.)

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

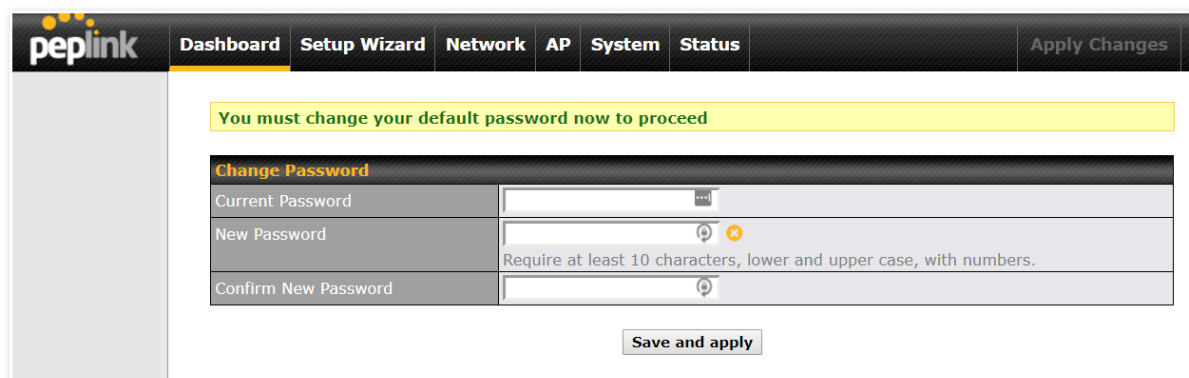
Username: admin

Password: admin

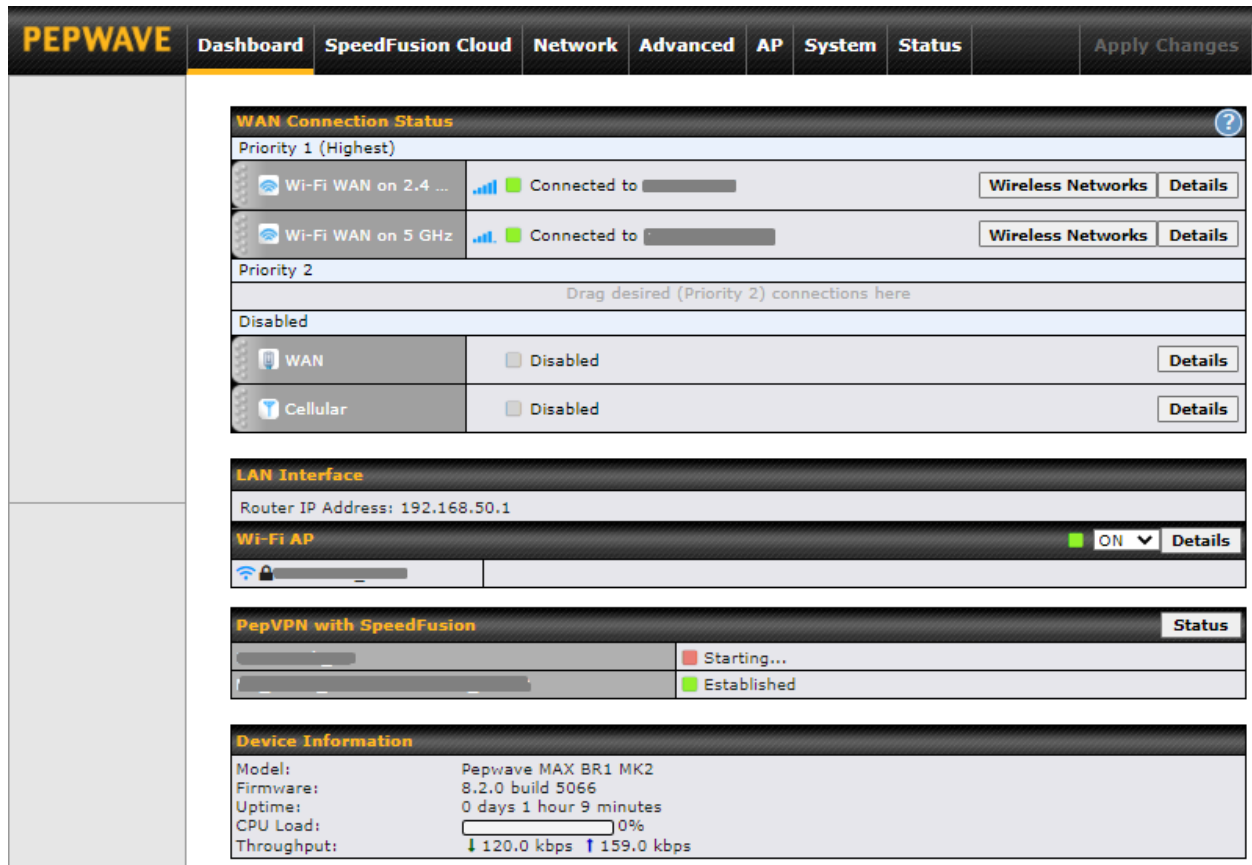
(This is the default username and password for Pepwave routers).



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



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



The screenshot shows the Peplink PEPWAVE web admin interface. The top navigation bar includes tabs for Dashboard, SpeedFusion Cloud, Network, Advanced, AP, System, and Status, along with an 'Apply Changes' button. The main content area is divided into several sections:

- WAN Connection Status:** This section shows two priority levels. Priority 1 (Highest) includes 'Wi-Fi WAN on 2.4 GHz' and 'Wi-Fi WAN on 5 GHz', both connected to wireless networks. Priority 2 is currently empty, with a prompt to 'Drag desired (Priority 2) connections here'. Below this, 'WAN' and 'Cellular' connections are shown as disabled.
- LAN Interface:** Displays the 'Router IP Address: 192.168.50.1'.
- Wi-Fi AP:** Shows the status as 'ON' with a dropdown menu and a 'Details' button.
- PepVPN with SpeedFusion:** Displays the status of VPN connections, with one shown as 'Starting...' and another as 'Established'.
- Device Information:** Provides details about the device, including Model (Pepwave MAX BR1 MK2), Firmware (8.2.0 build 5066), Uptime (0 days 1 hour 9 minutes), CPU Load (0%), and Throughput (120.0 kbps down, 159.0 kbps up).

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

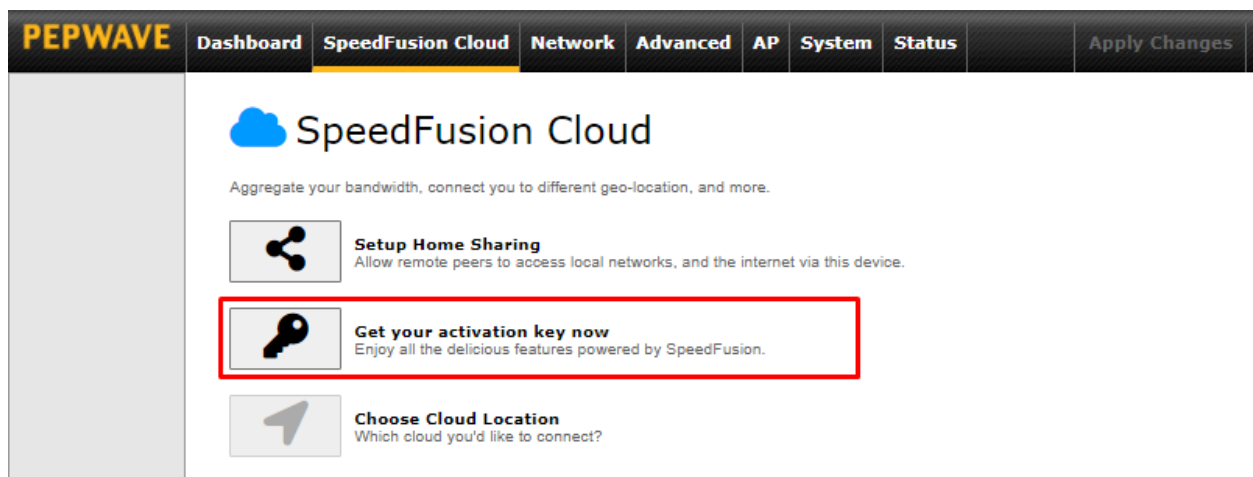
With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*



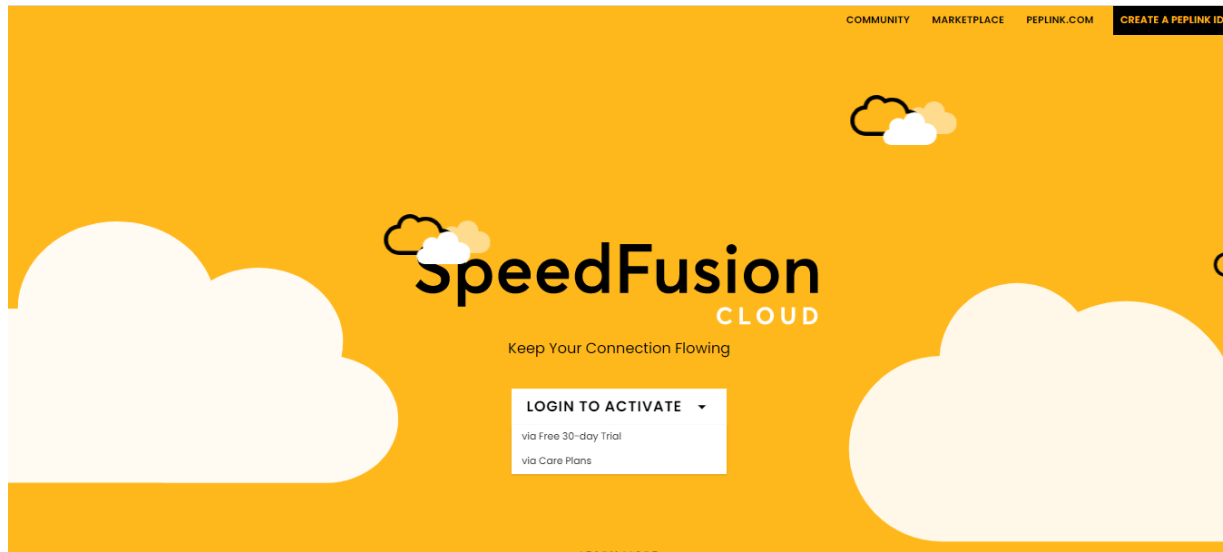
*SpeedFusion Cloud is supported in firmware version 8.1.0 and above. SpeedFusion Cloud is a subscription basis. SpeedFusion Cloud license can be purchased at <https://store.peplink.com/> > Cloud Solutions > SpeedFusion Cloud Service.

7.1 Activate SpeedFusion Cloud Service

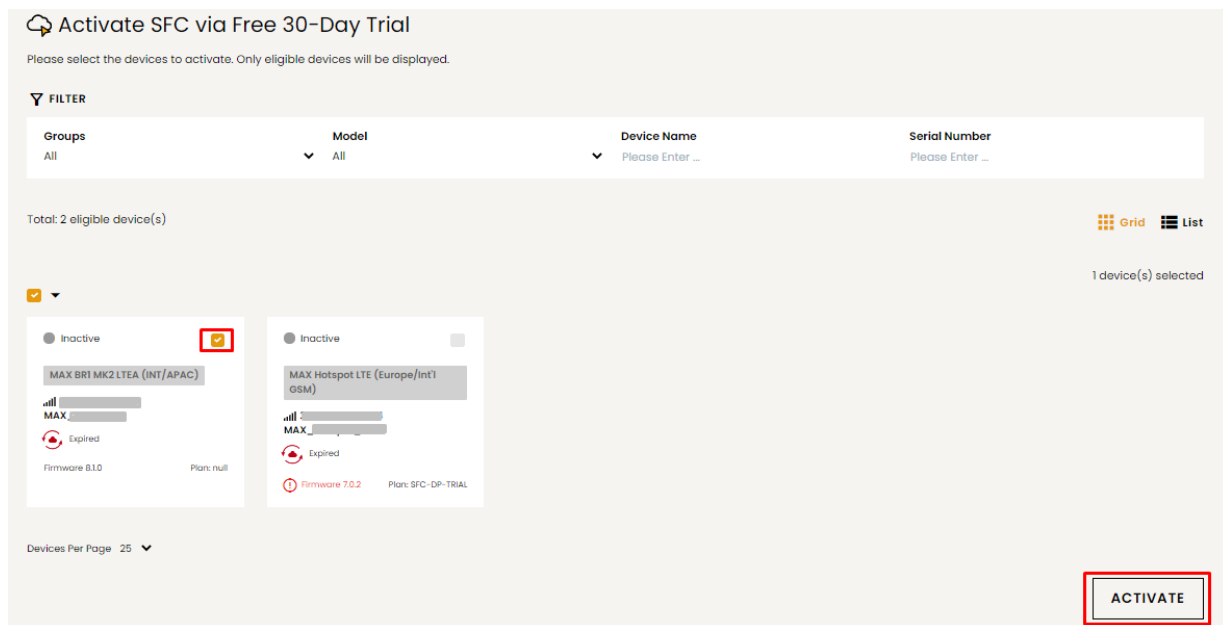
You are entitled to a 30-day free period with 100GB of SpeedFusion usage upon activation of the SpeedFusion Cloud service. This offer is limited to once per device. To get your activation key please visit SpeedFusion Cloud.



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**.

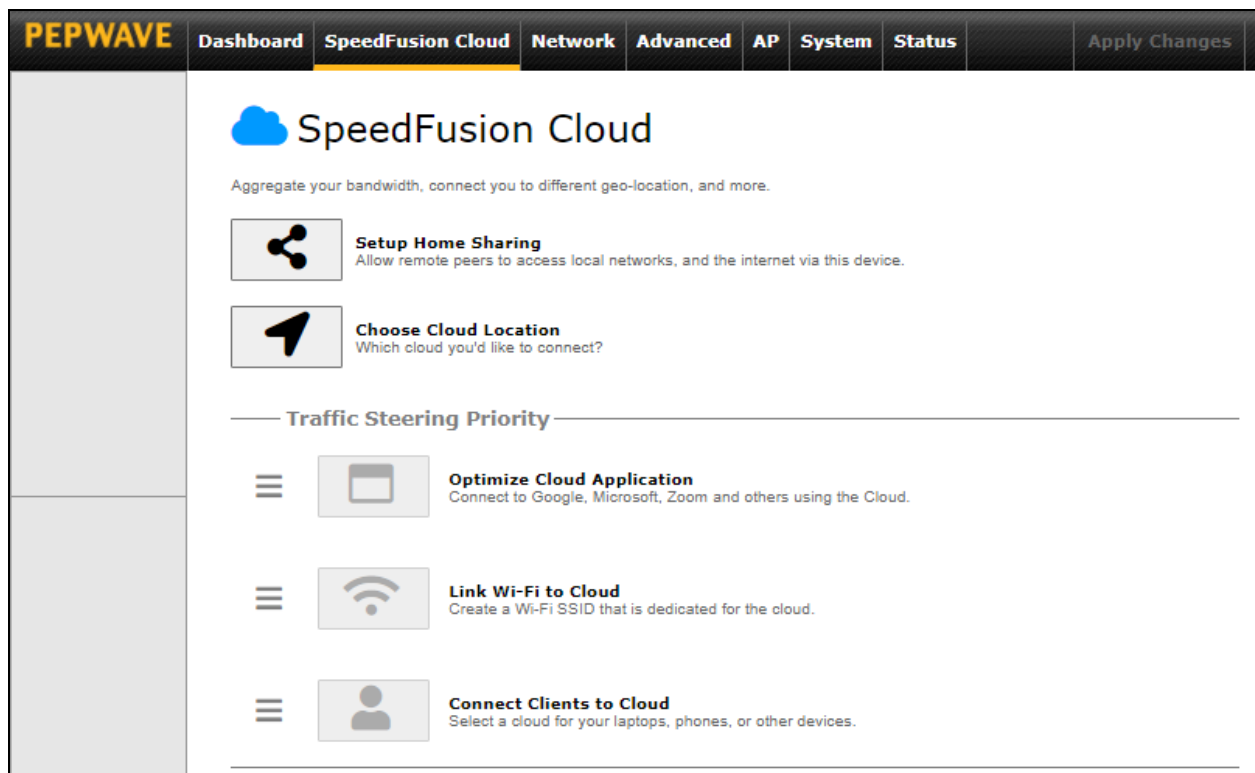


From **System > Features Add-ons**, paste the license key into the window and click on **Activate** once you have received the license key.

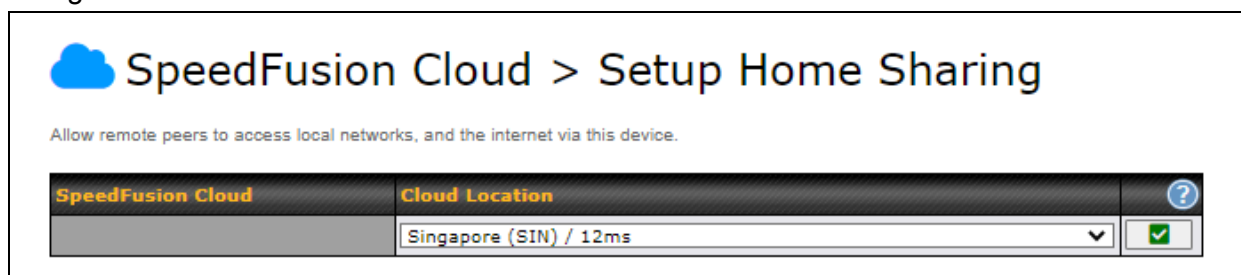
PEPWAVE		Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System	Status	Apply Changes
System - Admin Security - Firmware - Time - Schedule - Email Notification - Event Log - SNMP - SMS Control - InControl - Configuration Feature Add-ons - Reboot Tools - Ping - Traceroute - Wake-on-LAN - WAN Analysis Feature Activation Activation Key 9629a523e54fe148f876e75cf95df776f248e248b618b618a6199b23e54fe148f876e75cf95df776f351e640e450b618b618a310ae10a711a219a6249c5af05ef747c958e346e248c95bf75df309a709a3199c7ae64cf34dd05ce540f947b66afa46e34db668f55dff5ff75dff46f809dd4cef09be18a619d16bbfa96c3083b48a7d337ade187a5ce2e4e1 Activate									

7.2 Enable SpeedFusion Cloud

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



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



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



SpeedFusion Cloud > Setup Home Sharing

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

SpeedFusion Cloud	Cloud Location	
SFH-SHARE-SIN	Home Sharing Code: ----- COPY	

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



SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	
SDWC_SFC-HKG	Hong Kong (HKG)	
	---	

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

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes



SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	
	--- Automatic --- --- Automatic --- Australia (SYD) Germany (FRA) Japan (TYO) Singapore (SIN) United Kingdom (LON) United States (NYC) United States (SFO)	

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



SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	
	[Home Sharing] ▼	☒
	e.g. 1234-5678-1234-5678	

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

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

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



SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

Changes applied successfully.



SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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

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

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

WAN Connection Status

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

Priority 2

1
Cellular 1

Connected to MY MAXIS LTE-A

Details

2
Cellular 2

Connected to MY MAXIS LTE-A

Details

Priority 3
Drag desired (Priority 3) connections here

Disabled

1
WAN 1

☐ Disabled

Details

2
WAN 2

☐ Disabled

Details

3
Cellular 3

☐ Disabled

Details

4
Cellular 4

☐ Disabled

Details

Wi-Fi WAN

☐ Disabled

Details

3
LAN 1 as WAN

☐ Disabled

Details

4
LAN 2 as WAN

☐ Disabled

Details

5
LAN 3 as WAN

☐ Disabled

Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP

ON

Details

Wi-Fi
PEPWAVE_EBB4

SpeedFusion Cloud

SFC

Established

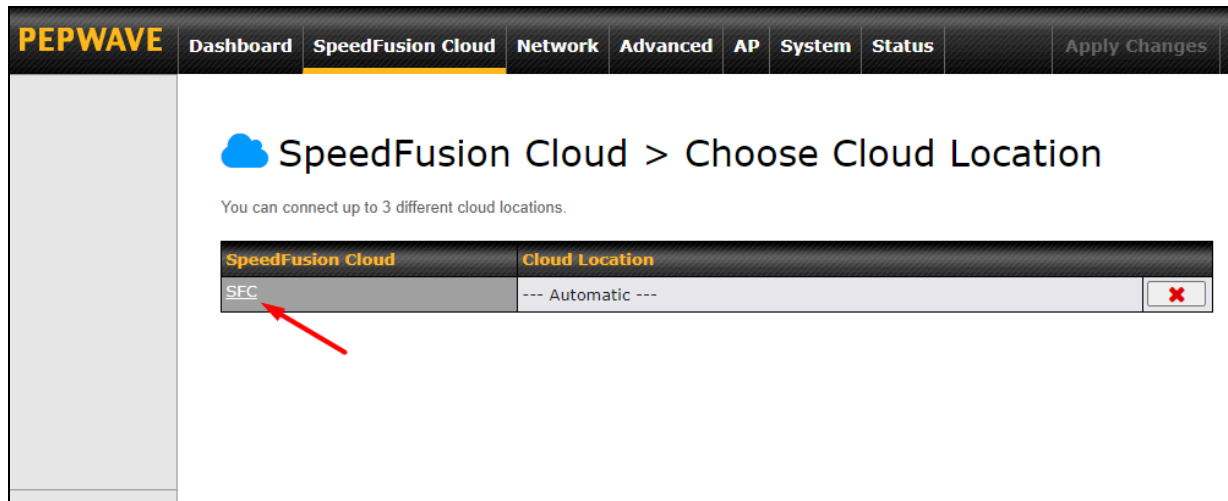
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)

<https://www.peplink.com>

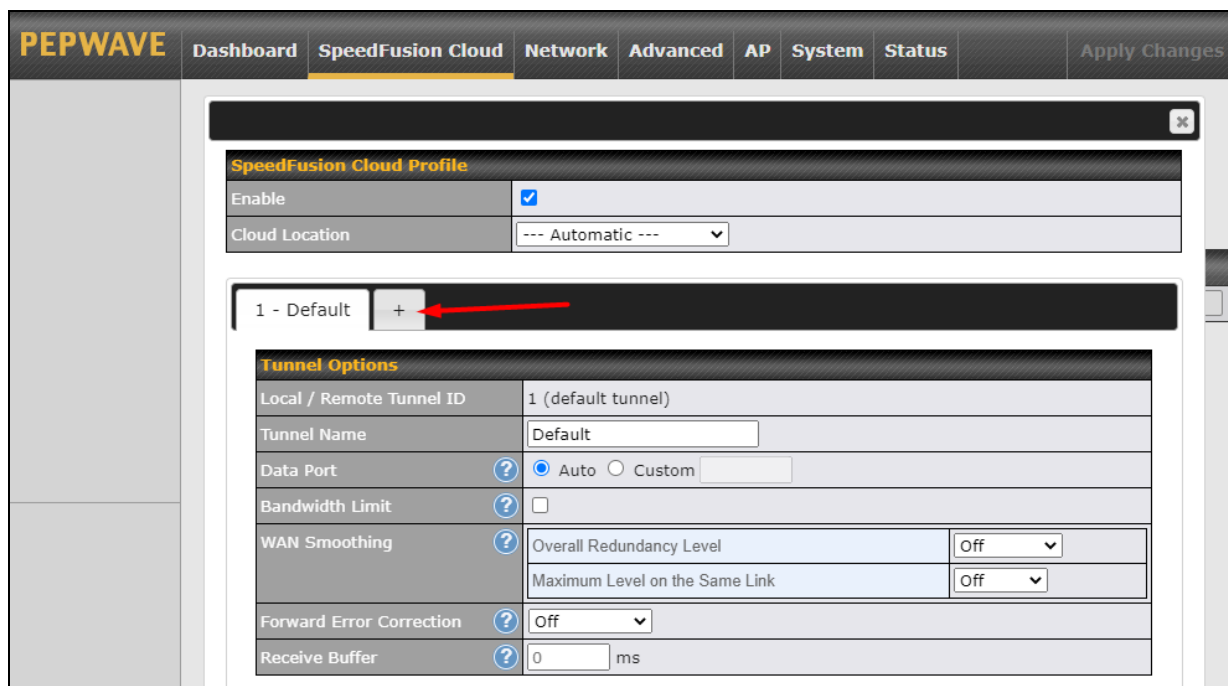
39

Copyright @ 2021 Peplink

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



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



PEPWAVE

Dashboard

SpeedFusion Cloud

Network

Advanced

AP

System

Status

Apply Changes

SpeedFusion Cloud Profile

Enable

☒

Cloud Location

--- Automatic ---

1 - Default

2 - WAN Smoo...

+

Tunnel Options

Local / Remote Tunnel ID

2

Tunnel Name

WAN Smoothing

Data Port

☒ Auto
 ☐ Custom

Bandwidth Limit

☐

WAN Smoothing

Overall Redundancy Level

Normal

Maximum Level on the Same Link

Normal

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.

PEP WAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

WAN Connection Status

Priority 1 (Highest)

Drag desired (Priority 1) connections here

Priority 2

1

Cellular 1

Connected to MY MAXIS LTE-A

Details

2

Cellular 2

Connected to MY MAXIS LTE-A

Details

Priority 3

Drag desired (Priority 3) connections here

Disabled

1

WAN 1

☐

Disabled

Details

2

WAN 2

☐

Disabled

Details

3

Cellular 3

☐

Disabled

Details

4

Cellular 4

☐

Disabled

Details

Wi-Fi WAN

☐

Disabled

Details

3

LAN 1 as WAN

☐

Disabled

Details

4

LAN 2 as WAN

☐

Disabled

Details

5

LAN 3 as WAN

☐

Disabled

Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP

ON

Details

PEPWAVE_EBB4

SpeedFusion Cloud

SFC (1 - Default)

Established

SFC (2 - WAN Smoothing)

Established

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

https://www.peplink.com

42

Copyright @ 2021 Peplink

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

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

Advanced

- SpeedFusion
- IPsec VPN
- GRE Tunnel
- Outbound Policy**
- Port Forwarding

NAT Mappings

QoS

- User Groups
- Bandwidth Control
- Application

Firewall

- Access Rules
- Content Blocking

Routing Protocols

- OSPF & RIPv2
- BGP

Remote User Access

Misc. Settings

- High Availability
- RADIUS Server
- Certificate Manager
- Service Forwarding
- Service Passthrough
- GPS Forwarding
- NTP Server
- Grouped Networks

Outbound Policy

Custom

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

When No Connections are Available: Drop the Traffic

Terminate Sessions on Connection Recovery: ☐ Enable

Save Cancel

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.


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

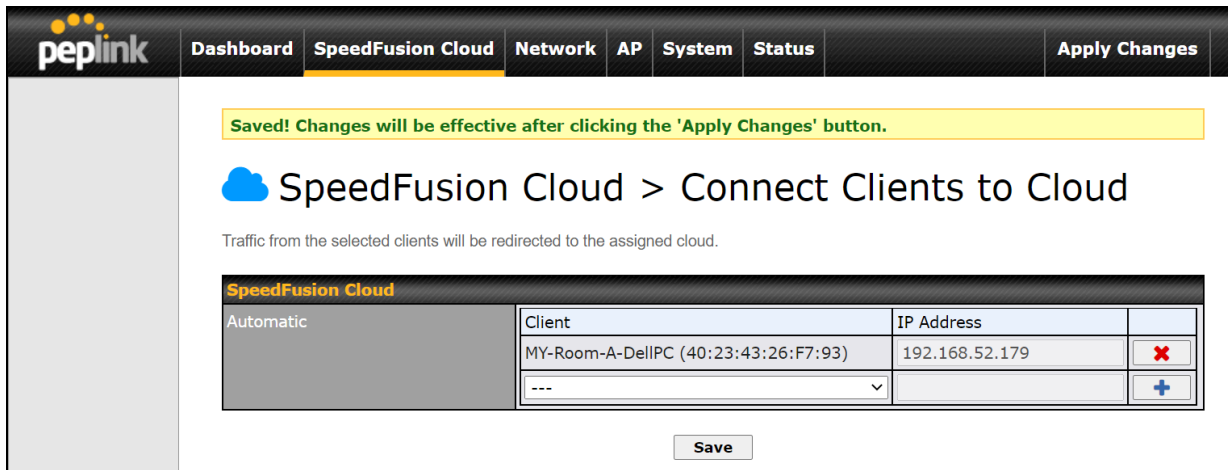

Choose Cloud Location
 Which cloud you'd like to connect?

Traffic Steering Priority




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

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



SpeedFusion Cloud > Connect Clients to Cloud

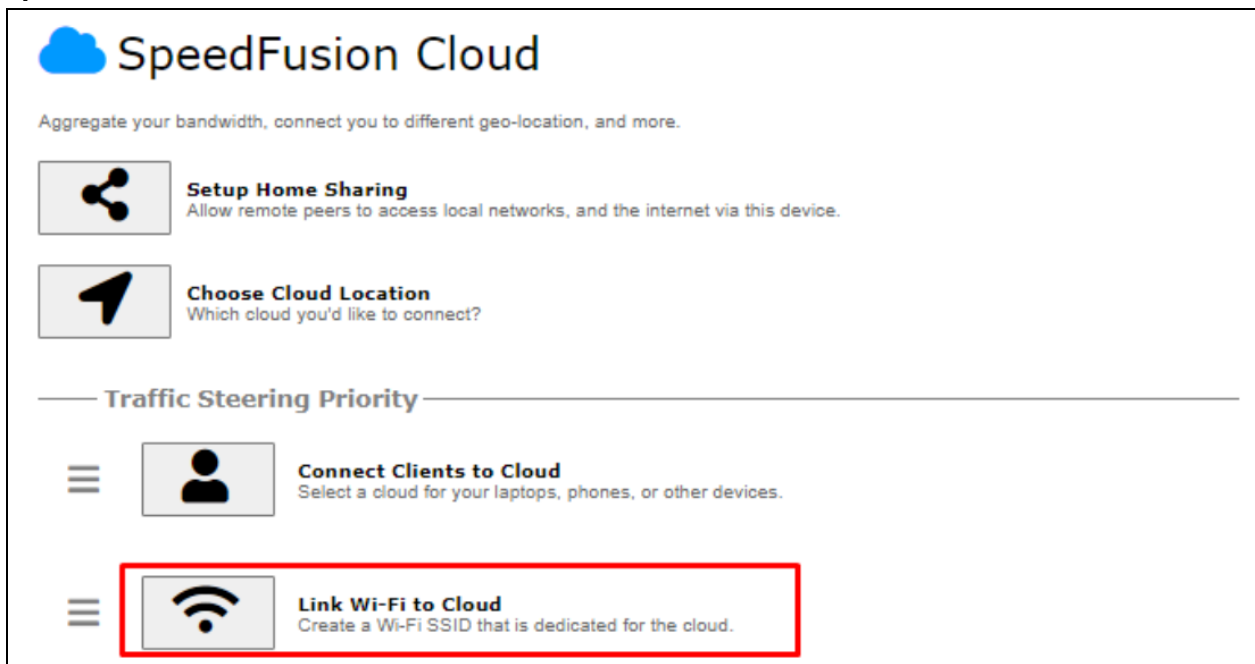
Traffic from the selected clients will be redirected to the assigned cloud.

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

Save

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**.



SpeedFusion Cloud

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

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

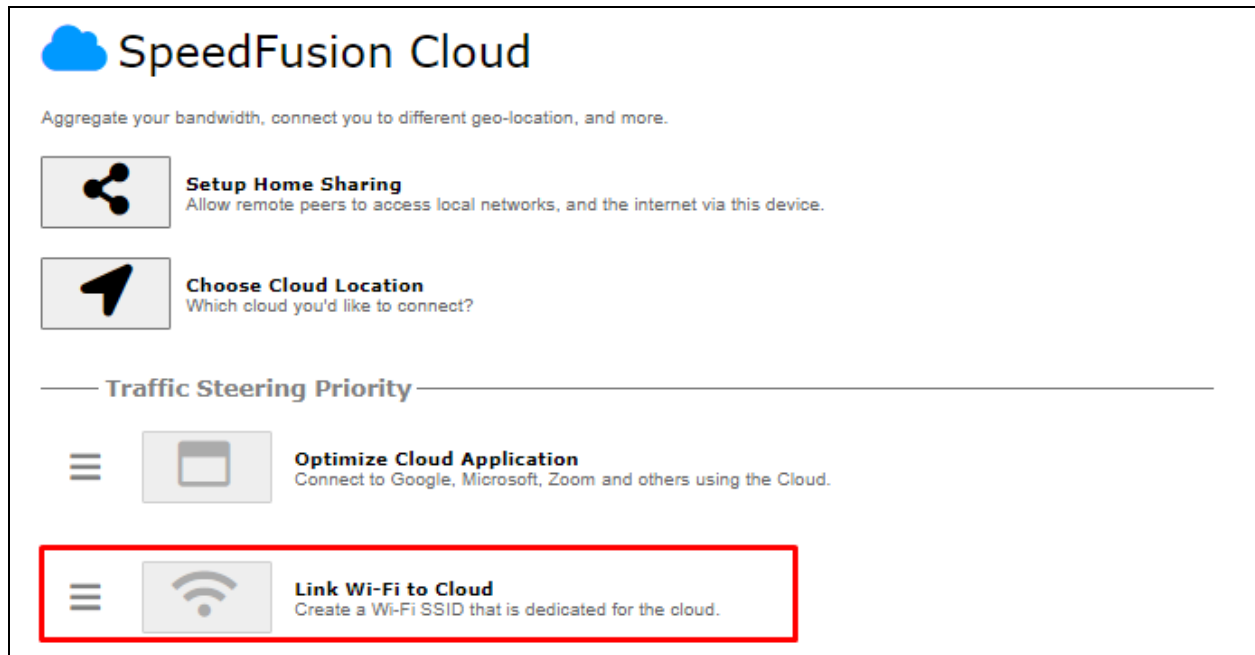
Choose Cloud Location
Which cloud you'd like to connect?

Traffic Steering Priority

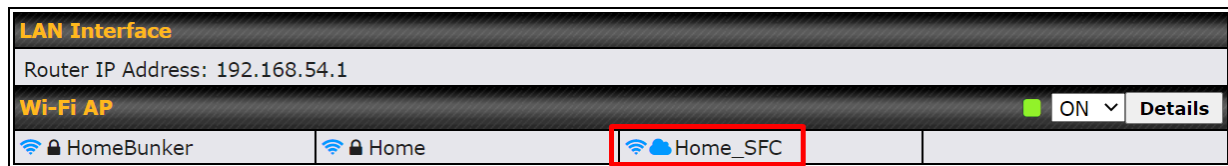
Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

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**.

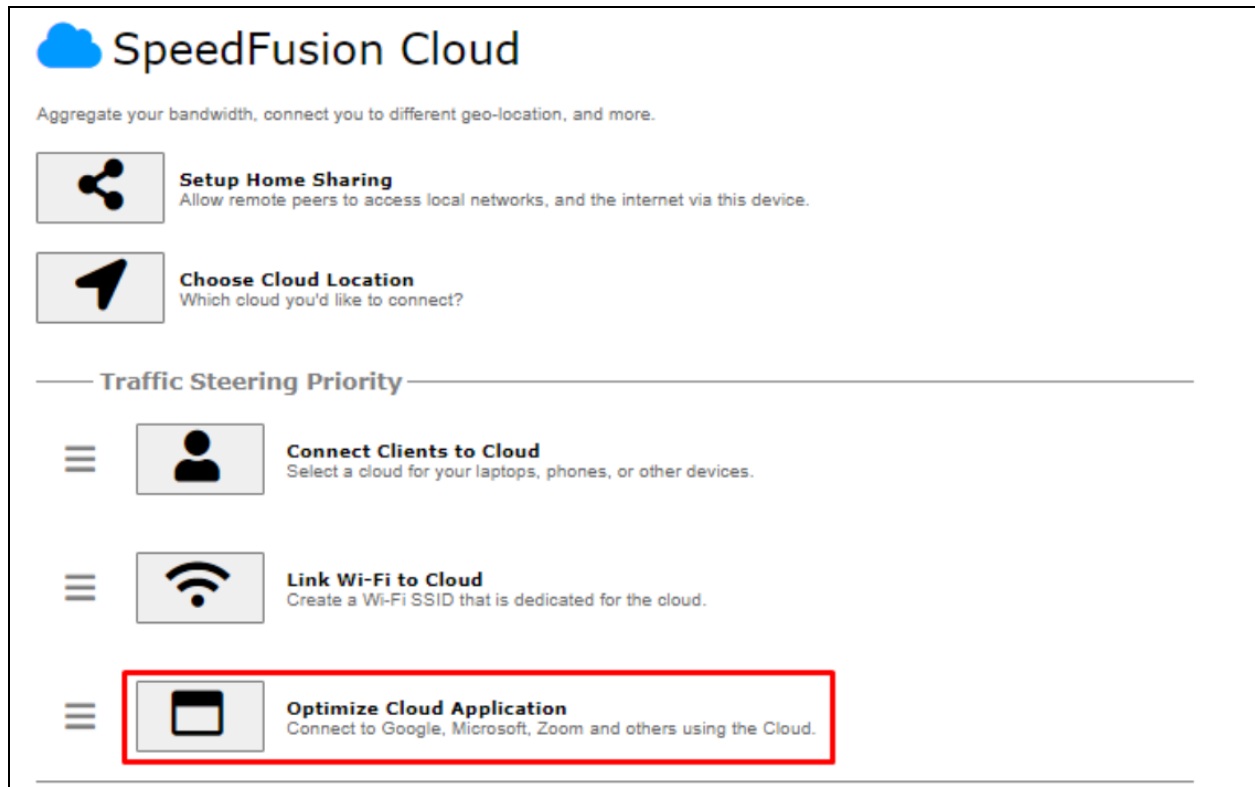


SpeedFusion Cloud SSID will be shown on **Dashboard**.



7.5 Optimize Cloud Application

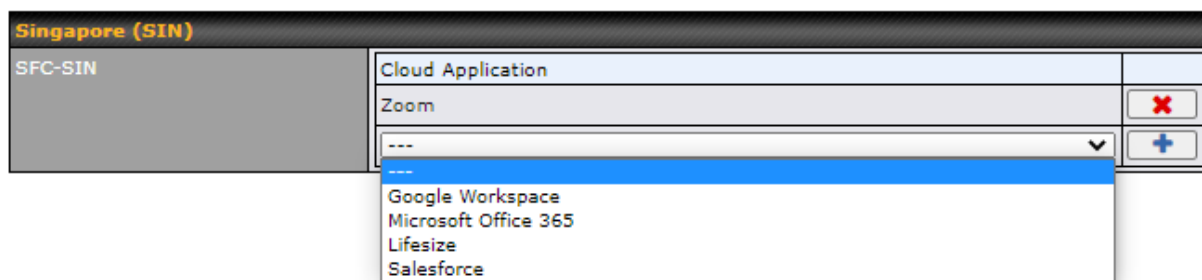
Optimize Cloud Application allows you to route Internet traffic to SpeedFusion Cloud based on the application. Go to **SpeedFusion Cloud > Optimize Cloud Application**.



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.



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	
New LAN			

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

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

Clicking 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		<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;">Add</td> </tr> </tbody> </table>		Option	Value	No Extended DHCP Option		Add			
Option	Value										
No Extended DHCP Option											
Add											
DHCP Reservation		<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>00:00:00:00:00:00</td> <td></td> <td></td> </tr> </tbody> </table>		Name	MAC Address	Static IP			00:00:00:00:00:00		
Name	MAC Address	Static IP									
	00:00:00:00:00:00										

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™, 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.

^A - Advanced feature, please click the  button on the top right hand corner of the Static Route section to activate and configure Virtual Network Mapping to resolve network address conflict with remote peers.

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

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

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

For further details on virtual network mapping watch this video:

<https://youtu.be/C1FMdZCn3Z8>

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

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 .

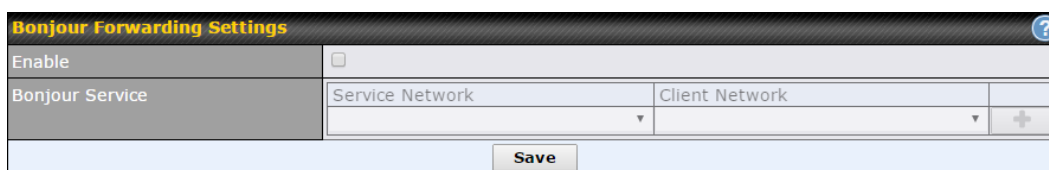
DNS Proxy Settings																				
Enable	☒																			
DNS Caching	☐																			
Include Google Public DNS Servers	☐																			
Local DNS Records	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>+</td> </tr> </tbody> </table>		Host Name	IP Address				+												
Host Name	IP Address																			
		+																		
DNS Resolvers	<table border="1"> <thead> <tr> <th>Connection</th> <th>Current Status</th> </tr> </thead> <tbody> <tr> <td>☐ WAN 1</td> <td>10.88.3.1</td> </tr> <tr> <td>☐ WAN 2</td> <td></td> </tr> <tr> <td>☐ Wi-Fi WAN</td> <td></td> </tr> <tr> <td>☐ Cellular 1</td> <td></td> </tr> <tr> <td>☐ Cellular 2</td> <td></td> </tr> <tr> <td>☐ USB</td> <td></td> </tr> <tr> <th>Connection</th> <th>DNS Servers</th> </tr> <tr> <td>☐ LAN</td> <td></td> </tr> </tbody> </table>		Connection	Current Status	☐ WAN 1	10.88.3.1	☐ WAN 2		☐ Wi-Fi WAN		☐ Cellular 1		☐ Cellular 2		☐ USB		Connection	DNS Servers	☐ LAN	
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™ 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™ 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.



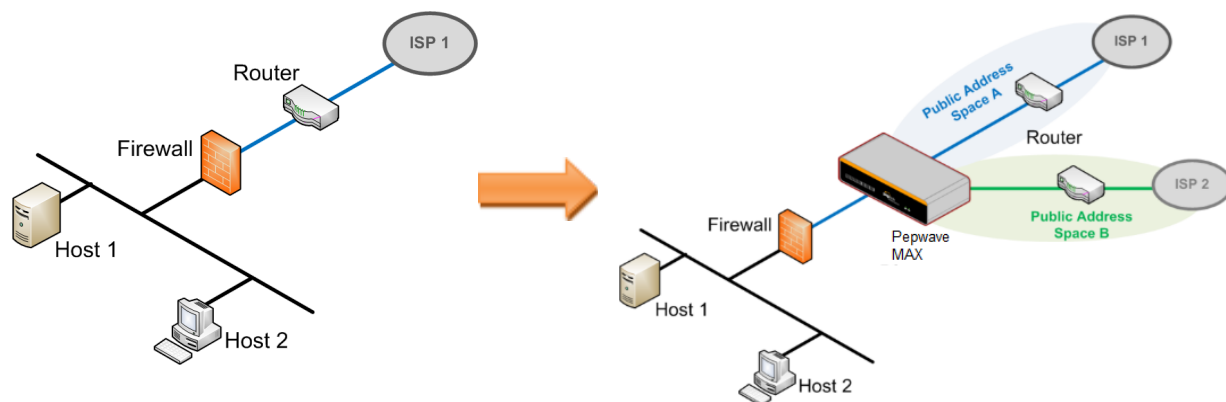
Bonjour Forwarding Settings		
Enable	☐	
Bonjour Service	Service Network	Client Network
		
Save		

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	<table border="1"> <thead> <tr> <th>Destination Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td>255.255.255.0 (/24) ▼</td> <td> + </td> </tr> </tbody> </table>	Destination Network	Subnet Mask			255.255.255.0 (/24) ▼	+
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

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

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

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



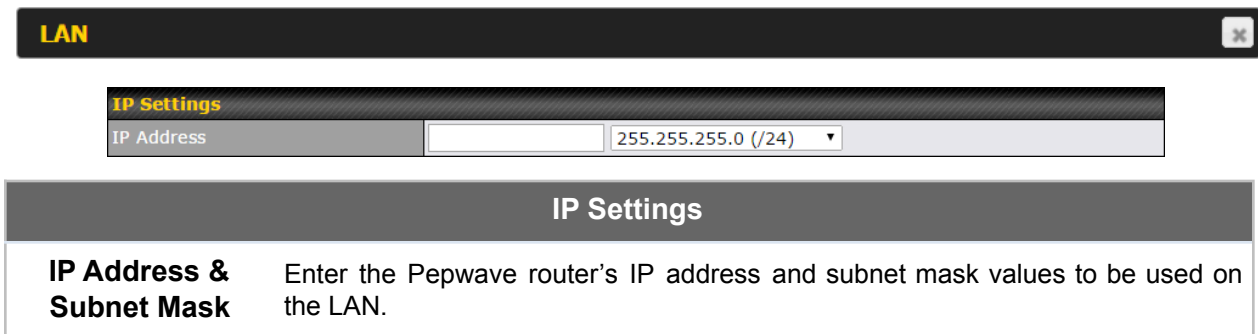
To add a new LAN, click the **New LAN** button. To change LAN settings, click the name of the LAN to change under the **LAN** heading.



LAN	VLAN	Network
Untagged LAN	None	192.168.50.1/24

New LAN

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



LAN

IP Settings
IP Address: Subnet Mask: 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	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Extended DHCP Option</td> </tr> <tr> <td colspan="2">Add</td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		Add	
Option	Value								
No Extended DHCP Option									
Add									
DHCP Reservation	☒	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>		Name	MAC Address	Static IP			
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™, 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	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

Address	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: <table border="1"> <tbody> <tr> <td>Authentication</td><td>RADIUS Server</td></tr> <tr> <td>Auth Server</td><td> Port 1812 Default</td></tr> <tr> <td>Auth Server Secret</td><td> ☒ Hide Characters</td></tr> <tr> <td>CoA-DM</td><td>☐</td></tr> <tr> <td>Accounting Server</td><td> Port 1813 Default</td></tr> <tr> <td>Accounting Server Secret</td><td> ☒ Hide Characters</td></tr> <tr> <td>Accounting Interim Interval</td><td> seconds</td></tr> </tbody> </table> Fill in the necessary information to complete your connection to the server and enable authentication.	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
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														
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.

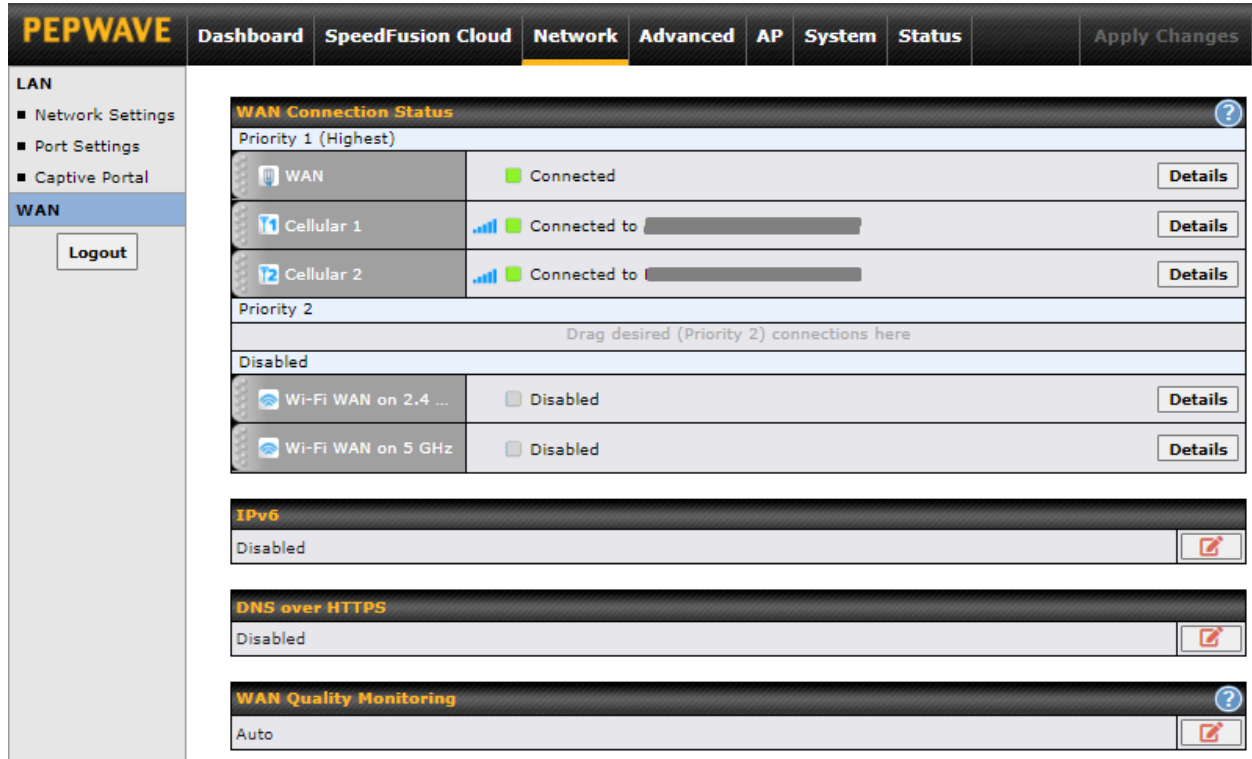
The **Portal Customization** menu has two options:  and . Clicking  displays a pop-up previewing the captive portal that your clients will see. Clicking  displays the following menu:

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.



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

LAN

- Network Settings
- Port Settings
- Captive Portal

WAN

Logout

WAN Connection Status

Priority 1 (Highest)

WAN	Connected	Details
Cellular 1	Connected to [Signal Bar]	Details
Cellular 2	Connected to [Signal Bar]	Details

Priority 2

Drag desired (Priority 2) connections here

Disabled

Wi-Fi WAN on 2.4 ...	Disabled	Details
Wi-Fi WAN on 5 GHz	Disabled	Details

IPv6

Disabled

DNS over HTTPS

Disabled

WAN Quality Monitoring

Auto

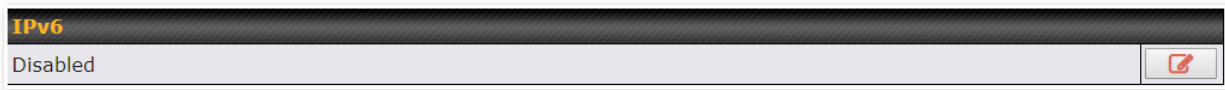
To enable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it to the **Disabled** row, and drop it by releasing the mouse button.

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

Important Note

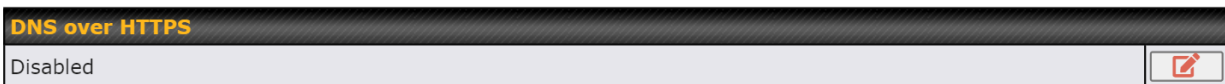
Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.

IPv6

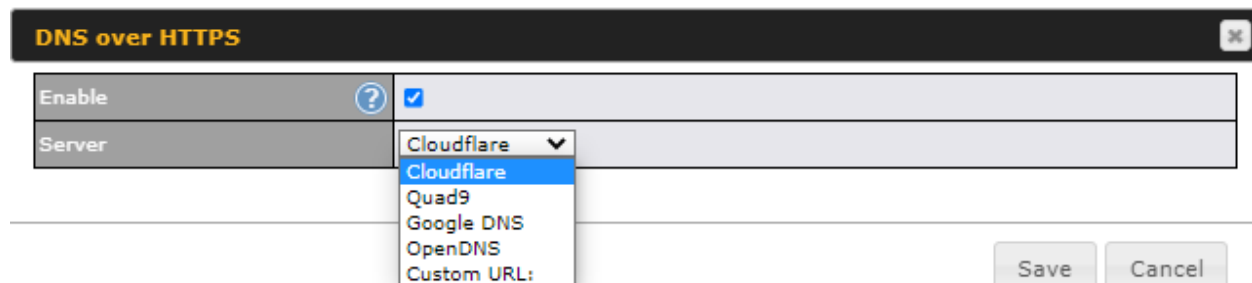


You can also enable IPv6 support in this section.

DNS over HTTPS (DoH)



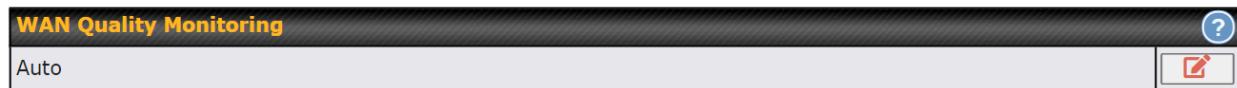
You can enable DoH (DNS over HTTPS) support in this section.



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

WAN Quality Monitoring

This settings advice how WAN Quality information is being gathered.



By default, WAN Quality will always be observed and gathered automatically. With customized choice of WAN connections, the device will always observe WAN Quality of those selected WAN connections. Other WAN connections may stop observing WAN Quality information if it is not necessary for the underlying features.

9.1 Ethernet WAN

9.1.2 DHCP Connection

There are four possible connection methods:

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

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.).

WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	? DHCP ▼
Routing Mode	? ☒ NAT
Hostname (Optional)	? ☐ Use custom hostname
Management IP Address	255.255.255.0 (/24) ▼
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	? ☐
Independent from Backup WANs	? ☐
Standby State	? ☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	? ☒ Yes ☐ No
Upload Bandwidth	? 1 Gbps ▼
Download Bandwidth	? 1 Gbps ▼

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.
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.

Management IP Address	Management IP Address is available for configuration when you click the link in the help  icon via the Hostname. This option allows you to configure the management IP address for the DHCP WAN connection.
DNS Servers	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.
IP Passthrough	When this IP Passthrough option is active, after the ethernet WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT. Regardless the WAN connection's state, the router always binds to the LAN IP address (Default: 192.168.50.1). So when the ethernet WAN is connected, the LAN client could access the router's web admin by manually configuring its IP address to the same subnet as the router's LAN IP address (e.g. 192.168.50.10). Note: when this option is firstly enabled, the LAN client may not be able to refresh its IP address to the ethernet WAN IP address in a timely fashion. The LAN client may have to manually renew its IP address from DHCP server. After this option is enabled, the DHCP lease time will be 2 minutes. I.e. the LAN client could refresh its IP address and access the network at most one minute after the ethernet WAN connection goes up.
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 when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, upon bringing up this WAN connection to active, it will be immediately available for use. If this WAN connection is charged by connection time, you may want to set

	this option to Disconnect so that connection will be made only when needed. PepVPN may use connected standby WAN for failover if link failure detected on the higher priority WAN, you can set this option to Disconnect to avoid data passing through.
Reply to ICMP PING	If the checkbox is unticked, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: ticked (Yes)
Upload Bandwidth	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

9.1.3 Static IP Connection

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

WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	Static IP ▼
Routing Mode	☒ NAT
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:
IP Passthrough	☐
Independent from Backup WANs	☐
Standby State	☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	☒ Yes ☐ No
Upload Bandwidth	1 Gbps ▼
Download Bandwidth	1 Gbps ▼

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.

9.1.4 PPPoE Connection

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

WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	PPPoE
Routing Mode	☒ NAT
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
Keep-Alive Interval	6 seconds(s)
Keep-Alive Retry	6
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
Reply to ICMP Ping	☒ Yes ☐ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

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.
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	If your ISP provides a PPPoE IP address, enter it here.

(Optional)	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.

9.1.5 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.

WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	L2TP
Routing Mode	☒ NAT
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 ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Independent from Backup WANs	☐
Standby State	☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	☒ Yes ☐ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

L2TP 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.
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.

9.1.6 GRE Connection

This connection method is suitable if your ISP provides a static WAN IP and Tunnel IP via GRE.

WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	? GRE ▾
Routing Mode	? ☒ NAT
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24) ▾
WAN Default Gateway	
Remote GRE Host	
Tunnel Local IP Address	
Tunnel Remote IP Address	
Outgoing NAT IP Address	
DNS Servers	☒ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Independent from Backup WANs	? ☐
Standby State	? ☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	? ☒ Yes ☐ No
Upload Bandwidth	? 1 Gbps ▾
Download Bandwidth	? 1 Gbps ▾

L2TP 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.
WAN 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.
Remote GRE Host	This field allows you to enter the IP address of the remote GRE.
Tunnel Local IP Address	This field allows you to enter the IP address of the local tunnel for the GRE tunnel connection.
Tunnel Remote IP Address	This field allows you to enter the IP address of the remote tunnel for the GRE tunnel connection.

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 ☐ Alternate periodically between SIM A Only and SIM B Only ☐ Use Remote SIM Only	
Preferred SIM Card	☒ No preference ☐ SIM A ☐ SIM B	
	SIM Card A	SIM Card B
Carrier Selection	☒ Auto	☒ Auto
LTE/3G	☒ LTE Only	☒ Auto
Optimal Network Discovery	☐	☐
Band Selection	Auto	Auto
Data Roaming	☒ Any countries	☐
Authentication	Auto	Auto
Operator Settings	☒ Auto ☐ Custom	☒ Auto ☐ Custom
APN		
Username		
Password		
Confirm Password		
SIM PIN (Optional)	 (Confirm)	 (Confirm)
Bandwidth Allowance Monitor	☒ Enable	☐ 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	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	On 1st of each month at 00:00 midnight
Monthly Allowance	GB	GB

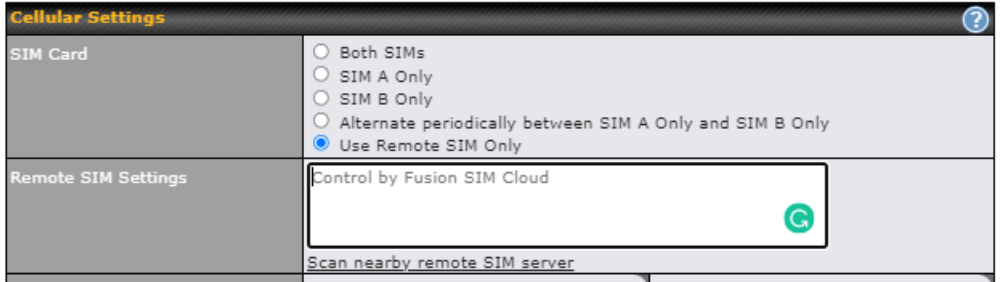
Cellular Settings

SIM Card

Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards. For routers that support the SIM Injector, you may select the "Use Remote SIM Only" to provision a SIM from a SIM Injector. Further details on the SIM Injector found is available here: <https://www.peplink.com/products/sim-injector/>.

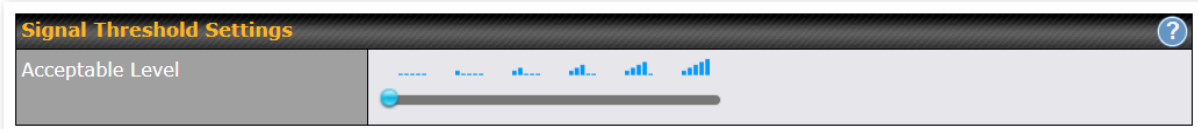
Preferred SIM

If "Both SIMs" were selected on the above field, then you can designate the priority

Card	of the SIM card slots here.
Remote SIM Settings	If “Use Remote SIM Only” is selected in the SIM card section, the Remote SIM Settings will be shown.  You may need to enable the remote SIM Host settings in the Remote SIM management, see the section 22.10 or Appendix B for more details on FusionSIM. After that, click on “Scan nearby remote SIM server” to show the serial number(s) of the connected SIM Injector(s). If you want to select a specific SIM, in the Cellular Settings, type “:” and then the number of the SIM slot, eg.1111-2222-3333:7.
LTE/3G	This drop-down menu allows restricting cellular to particular band. Click the  button to enable the selection of specific bands.
Optimal Network Discovery	Cellular WANs by default will only handover from 3G to LTE network when there is no active 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 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



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 / RSRP	-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.

The screenshot shows the 'Signal Threshold Settings' window with the manual input fields visible. It includes sections for LTE and 3G, each with fields for RSRP/SINR and RSSI, and a 'Recovery' field. The units are dBm for RSRP/SINR and dB for RSSI.

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

9.3 Wi-Fi WAN

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

WAN Connection Settings	
WAN Connection Name	Wi-Fi WAN
Independent from Backup WANs	☐
Standby State	☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	☒ Yes ☐ No

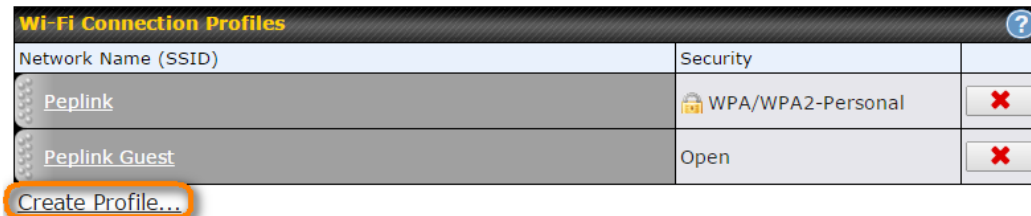
WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be 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	Auto
Channel	☒ Auto ☐ Custom
Output Power	Max ☐ Boost
Data Rate	☒ Auto ☐ Fixed
Roaming	☐ Enable
Connect to Any Open Mode AP	☐ Yes ☒ No
Beacon Miss Counter	5
Channel Scan Interval	50 ms

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	Determine whether the channel will be automatically selected. If you select custom, the following table will appear: Scan Channels Clear All 2.4GHz: ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ 6 ☒ 7 ☒ 8 ☒ 9 ☒ 10 ☒ 11 OK Cancel
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.
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.
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.
Channel Scan Interval	Configure Channel Scan Interval in ms.

9.3.2 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.



This will open a window similar to the one shown below

Create Wi-Fi Connection Profile

Wi-Fi Connection

Network Name (SSID)	
Security	WPA2/WPA3-Personal ▼
Shared Key	☒ Hide Characters
Preferred BSSID	☐
Connection Method	? DHCP ▼
DNS Servers	☐ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

OK

Cancel

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
Shared Key	Enter the password for the wireless network.
Preferred BSSID	Configure the BSSID. The BSSID is the MAC address of the wireless access point (WAP).
Connected Method	Choose DHCP or Static IP.
DNS Servers	Configure the DNS servers that this WAN connection should use.

9.4 WAN Connection Settings (Common)

The remaining WAN-related settings are common to the WAN connection:

Physical Interface Settings	
Port Speed	Auto
MTU	☐ Auto ☒ Custom 1440
MSS	☒ Auto ☐ Custom
MAC Address Clone	☒ Default ☐ Custom 10:56:CA:15:92:5D
VLAN	☐

Physical Interface Settings	
Speed	This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device. Default: Auto

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. Default value is 1440.
MSS	This field is for specifying the Maximum Segment Size of the WAN connection. When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections. Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections. Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size. Default: Auto
MAC Address Clone	Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.
VLAN	Check the box to assign a VLAN to the interface.

9.5 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://

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.

9.6 Bandwidth Allowance Monitoring

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 ?	GB

Bandwidth Allowance Monitor	
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.

Disclaimer

Due to different network protocol overheads and conversions, the amount of data reported by this Peplink device is not representative of actual billable data usage as metered by your network provider. Peplink disclaims any obligation or responsibility for any events arising from the use of the numbers shown here.

9.7 Additional Public IP address

Additional IP Address Settings	
Additional IP Address ?	IP Address Subnet Mask 255.255.255.255 (/32) ▼ ↓ ✕

Additional Public IP Settings	
IP Address List	IP Address List represents the list of fixed Internet IP addresses assigned by the ISP in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the Down Arrow button to populate IP address entries to the IP Address List.

9.8 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...

Account Name / Email Address

Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.

Select **Disabled** to disable this feature.

Password / TZO Key

This setting specifies the registered user name for the dynamic DNS service.

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: 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	Clients with signal strength lower than this value will not be allowed to connect.
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 Default μs
ACK Timeout	 48 Default μs
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 Converter	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 <button>Generate</button>

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 MediaFast Configuration

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

11.1 Setting Up MediaFast Content Caching

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

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 caching 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	<table border="1"> <thead> <tr> <th>File Extension</th> <th>Lifetime (days)</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>+</td> </tr> </tbody> </table>	File Extension	Lifetime (days)				+
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.

11.2 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 .

Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:

New Schedule

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

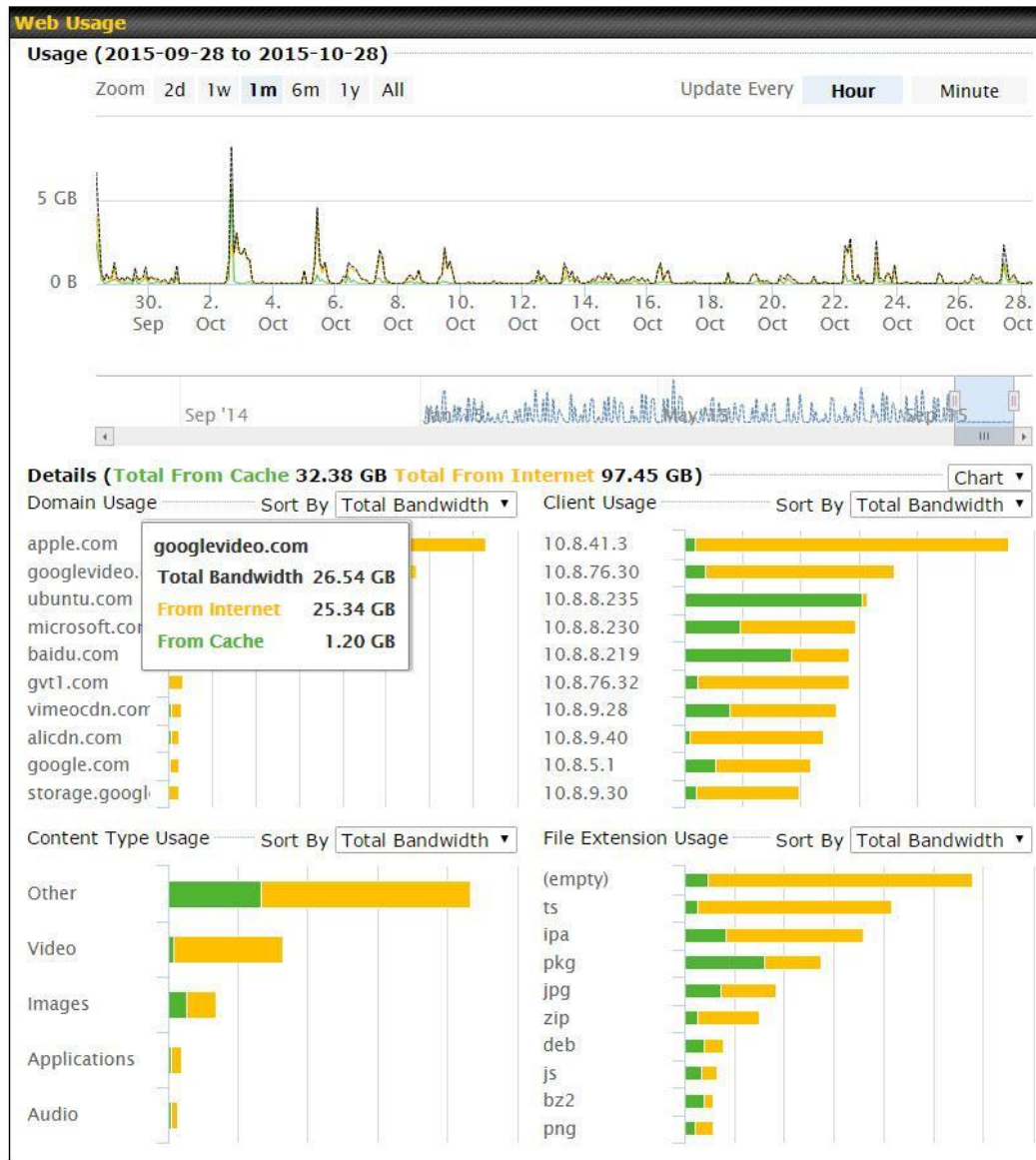
To clear all cached content, click this button. Note that this action cannot be undone.

Clear Statistics

To clear all prefetch and status page statistics, click this button.

11.3 Viewing MediaFast Statistics

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



12 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.

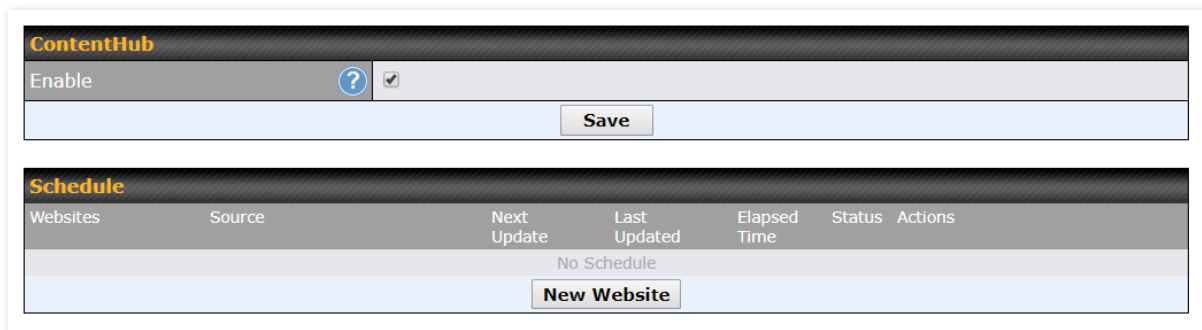
The ContentHub can be used to provide infotainment to connected users on transport.

12.1 Configuring the ContentHub

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

ContentHub storage has not been configured. Click [here](#) to review storage configuration

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



ContentHub						
Enable		☒				
Save						
Schedule						
Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
No Schedule						
New Website						

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

To configure a website or application as content, follow the steps below.

Configure a website for 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 you sync it with ContentHub.

Click **New Website** and a window with 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)

Save & Apply Now

Cancel

Schedule	
Active	Checking the box toggles the activation of the content.
Type	Select the type of content: Website or Application.
Protocol	Configure the protocol to be used: HTTP, HTTPS or both.
Domain/Path	Enter the URL for the ContentHub to use as the domain name for client access (such as http://mytest.com).
Method	Only applicable for Application type content. Choose between sync or file upload.
Source	Enter the details of the server that the content will be downloaded from. Enter credentials under Username and Password .
Period	This field determines how often the router will search for updates to the source content.
Bandwidth Limit	Set a bandwidth limit for clients.

Click “**Save & Apply Now**” to activate the changes. A screenshot of the display after configuration is shown below:

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 synced regularly according to the time set in the **Period** that was configured earlier.

If you want to activate the sync manually, you can click the “” icon. The “Status” column will display the sync progress. When the sync is completed, a summary will be displayed, 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 the MFA's client and enter the domain details that were configured earlier (such as <http://mytest.com>).

Configure an application for ContentHub

MediaFast routers allow you to configure and publish any application from the router itself by using one of the supported frameworks below:

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

Install the desired framework under “Package Manager” as shown below:



The screenshot shows the PEPWAVE router web interface. The top navigation bar includes tabs for Dashboard, SpeedFusion Cloud, Network, Advanced, AP, System (selected), and Status. An 'Apply Changes' button is on the right. The left sidebar lists various system and tool options. The main content area displays the 'Package List' for the selected 'System' tab, showing details for Node.js, Python, and Ruby, each with a download button.

System	Package List	Action
■ Admin Security ■ Firmware ■ Time ■ Schedule ■ Email Notification ■ Event Log ■ SNMP ■ InControl ■ Configuration ■ Feature Add-ons ■ Reboot	(Last Update: Tue May 23 04:02:36 UTC 2017) Package List Update All 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	Download Download Download

After installing the framework, change 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)

Save & Apply Now

Cancel

The setting is the same as the Website type (refer to the description in the section above).

Application type content need to be packed as explained below:

1. Implement two bash script files, start.sh and stop.sh in the 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 the application files and the bash script to .tar.gz format.
3. Upload this tar file to the router.

13 Docker

MediaFast enabled routers can host Docker containers when running Firmware 7.1 or later.

Docker is an open platform for developing, shipping, and running applications.

From Firmware version 7.1.0 and upwards, it is possible to install and run Docker Containers on your Pepwave routers with MediaFast, such as the MAX HD2 and the MAX HD4.

Due to the nature of Docker and its unlimited variables, this feature is supported by Pepwave up to the point of creating a running Docker Container.

Information about Docker can be found on the Docker Documentation site:

<https://docs.docker.com/> 2

This will allow you to run a file sharing platform (ownCloud), a web server (WordPress, Joomla!), a learning platform (Moodle), or a visualisation tool for viewing large scale data (Kibana).

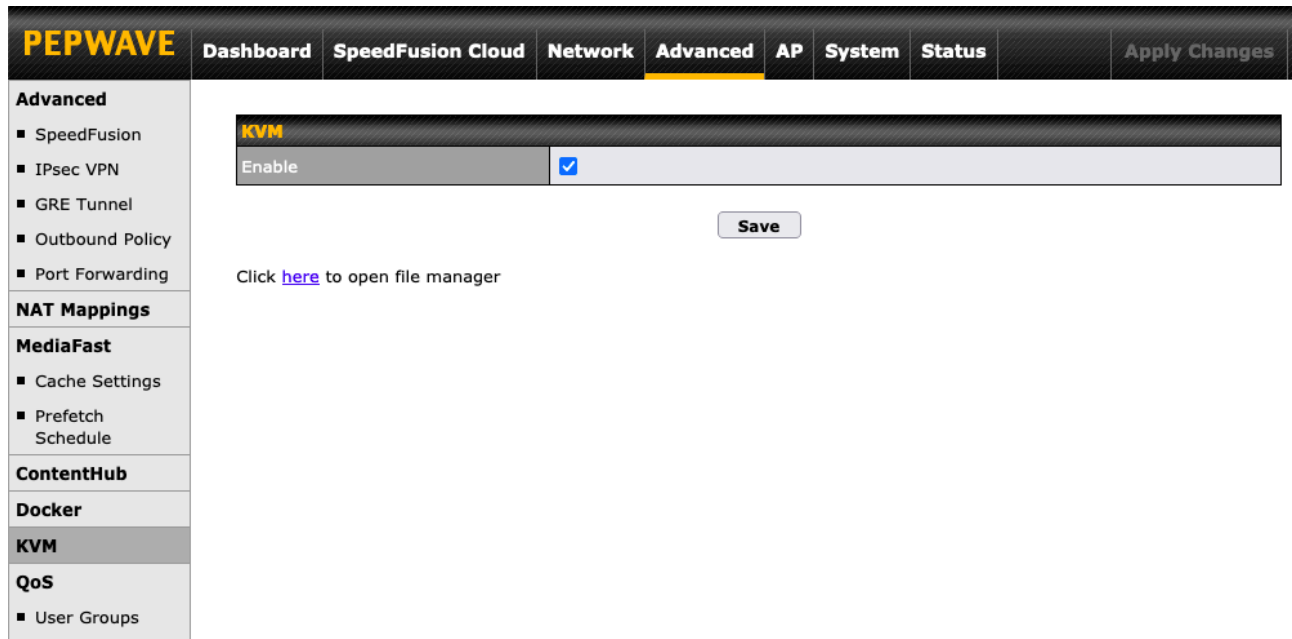
When creating a new Docker Container, the Pepwave router will search through the Docker Hub repository. <https://hub.docker.com/explore/> 7

For detailed configuration instructions, refer to our knowledge base:

<https://forum.peplink.com/t/how-to-run-a-docker-application-on-a-peplink-mediafast-router/1602>
1

14 KVM

MediaFast enabled routers now support KVM. Users will have to download and install Virtual Machine Manager to manage the KVM virtual machines. Through this, users are able to virtualise a Linux environment.



The screenshot shows the Peplink PEPWAVE web interface. The top navigation bar includes tabs for Dashboard, SpeedFusion Cloud, Network, Advanced (selected), AP, System, Status, and an Apply Changes button. The left sidebar lists various configuration categories: Advanced (with sub-items: SpeedFusion, IPsec VPN, GRE Tunnel, Outbound Policy, Port Forwarding), NAT Mappings, MediaFast (with sub-items: Cache Settings, Prefetch Schedule), ContentHub, Docker, KVM (highlighted), QoS, and User Groups. The main content area is titled 'KVM' and contains a single setting: 'Enable', which is currently checked with a blue checkbox. Below this setting is a 'Save' button and a text link that says 'Click [here](#) to open file manager'.

For detailed configuration instructions, refer to our knowledge base articles:

1. [How to install a Virtual Machine on Peplink/Peplink - MediaFast/ContentHub Routers](#)
2. [How to Install Virtual Machine with USB storage on Peplink/Peplink - MediaFast/ContentHub Routers](#)

15 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.

15.1 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)	?
 EL Office	8345-5F7A-DE97		
New Profile			

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					
Enable	☒				
Encryption	☒ 256-bit AES ☐ OFF				
Authentication	☒ Remote ID / Pre-shared Key				
Remote ID / Pre-shared Key	<table border="1"> <tr> <td>Remote ID</td> <td>Pre-shared Key</td> </tr> <tr> <td> </td> <td> </td> </tr> </table>	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				
Forward Error Correction	Off				
Receive Buffer	0 ms				
Packet Fragmentation	☒ Always ☐ Use DF Flag				
Use IP ToS	☐				
Latency Difference Cutoff	500 ms				

PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from By Remote ID Only , Preshared Key , 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 Certificate	These optional fields become available when X.509 is selected as the Pepwave MAX's VPN authentication method, as explained above. To authenticate VPN 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.
WAN Smoothing	While using PepVPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN's available bandwidth.

	Off - Disable WAN Smoothing. Normal - The total bandwidth consumption will be at most 2x of the original data traffic. Medium - The total bandwidth consumption will be at most 3x of the original data traffic. High - The total bandwidth consumption depends on the number of connected active tunnels.
Forward Error Correction	Forward Error Correction (FEC) can help to recover packet loss by using extra bandwidth to send redundant data packets. Higher FEC level will recover packets on a higher loss rate link. The expected overhead of Low is 13.3% and High is 26.7%. Require peer using PepVPN version 8.0.0 and above.
Receive Buffer	Receive Buffer can help to reduce out-of-order packets and jitter, but will introduce extra latency to the tunnel. Default is 0 ms, which disables the buffer, and maximum buffer size is 2000 ms.
Packet Fragmentation	If the packet size is larger than the tunnel's MTU, it will be fragmented inside the tunnel in order to pass through. Select Always to fragment any packets that are too large to send, or Use DF Flag to only fragment packets with Don't Fragment bit cleared. This can be useful if your application does Path MTU Discovery, usually sending large packets with DF bit set, if allowing them to go through by fragmentation, the MTU will not be detected correctly.
Use IP ToS^A	Checking this button enables the use of IP ToS header field.
Latency Difference Cutoff^A	Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)

^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

Traffic Distribution	
Policy	 Bonding

Traffic Distribution		
Policy		Dynamic Weighted Bonding ▼
Congestion Latency Level		Default ▼
Ignore Packet Loss Event		☐
Disable Bufferbloat Handling		☐
Disable TCP ACK Optimization		☐
Packet Jitter Buffer		150 ms

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

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 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.

The screenshot shows two configuration windows. The top window, titled 'Outbound Policy', has a dropdown menu set to 'According to custom rules' and an edit icon. The bottom window, titled 'PepVPN Outbound Custom Rules', is a table with columns: Service, Algorithm, Source, Destination, Protocol, and an empty row below. Below the table is an 'Add Rule' button.

The screenshot shows the 'PepVPN Local ID' configuration window. It has a label 'Local ID', a text input field containing 'MAX_HD2_8D1C', a help icon, and an edit icon.

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**.

The screenshot shows the 'PepVPN Settings' configuration window. It has a title bar with a question mark icon. The settings are as follows:

- Handshake Port:** Radio buttons for 'Default' (selected) and 'Custom' (with an empty text field).
- Backward Compatibility:** Radio buttons for 'High (firmware 5.3+)' (selected) and 'Latest (firmware 6.2+)'. Below this is a note: 'Shorter detection time incurs more health checks and higher bandwidth overhead'.
- Link Failure Detection Time:** Radio buttons for 'Recommended (Approx. 15 secs)' (selected), 'Fast (Approx. 6 secs)', 'Faster (Approx. 2 secs)', and 'Extreme (Under 1 sec)'. Below this is a note: '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.

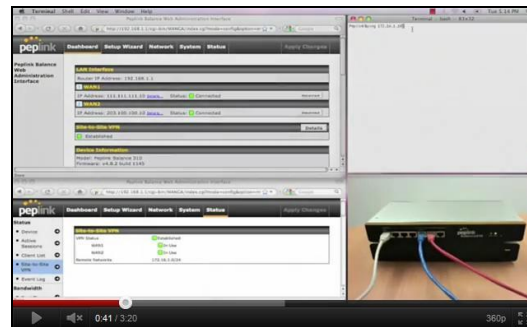
^A - Advanced feature, please click the  button on the top right-hand corner to activate.

Important Note

Peplink proprietary SpeedFusion™ 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>

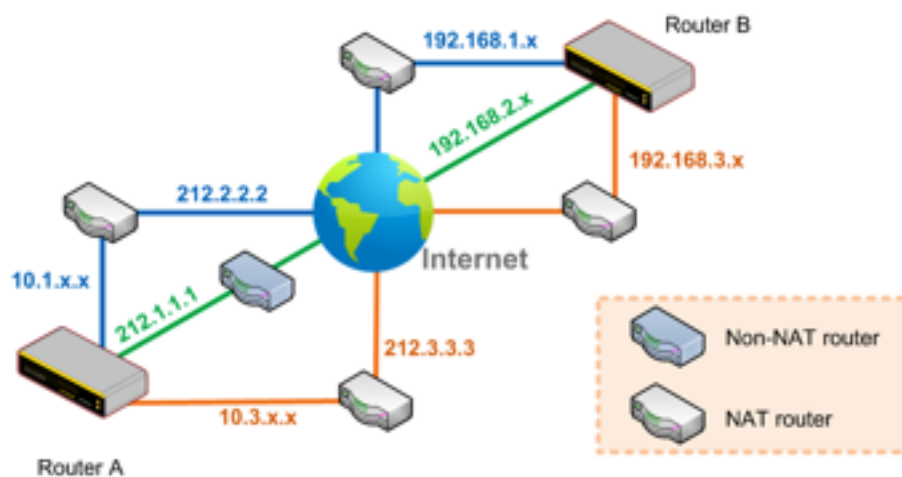
15.2 The Pepwave Router Behind a NAT Router

Pepwave routers support establishing SpeedFusion™ 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 SpeedFusion™ 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.

15.3 SpeedFusion™ Status

SpeedFusion™ 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 SpeedFusion™ table, you will be forwarded to **Status>SpeedFusion™**, 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™ network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

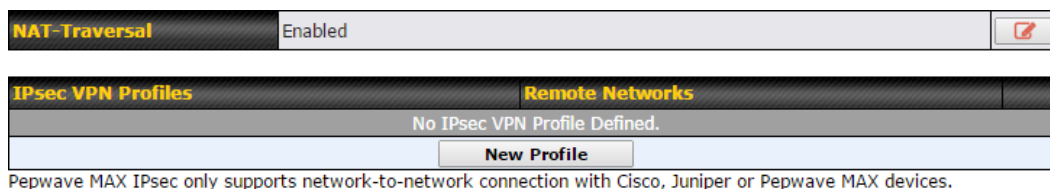
16 IPsec VPN

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.

16.1 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**.



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			
Active ?	☒		
IKE Version	☒ IKEv1 ☐ IKEv2		
Connect Upon Disconnection of	☒ WAN ▼		
Remote Gateway IP Address / Host Name ?			
IPsec Type ?	☒ Policy-based ☐ Route-based		
Local Networks ?	Propose the following networks to remote gateway: ☒ 192.168.50.0/24 ☐ Apply the following NAT policies: ☐ Local Network ☒ NAT Network		
Remote Networks	Network	Subnet Mask	
		255.255.255.0 (/24) ▼	+
Authentication	☒ Preshared Key		
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 ?	1 Group 2 ▼ 2 ----- ▼		
Phase 1 SA Lifetime	3600 seconds		
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 ▼ 2 ----- ▼		
Phase 2 PFS Group	None ▼		
Phase 2 SA Lifetime	28800 seconds		

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.

IKE Version	Two versions of the IKE standards are available: • IKEv1 • IKEv2
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.
IPsec Type	Policy-based - (default) All the matched traffic as defined in Local Networks and Remote Networks will be routed to this IPsec connection, this cannot be overridden by other routing methods. Route-based - Outbound Policy rule is required to route traffic to this tunnel and comes with more flexibility to control how to route traffic compared to Policy-based. If you want to modify the traffic selector instead of using the default (0.0.0.0/0). Note: This option is available for certain following models only: • MAX: BR1 ENT, Transit, 700 HW3 or above, HD2 HW5 or above, HD4
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	Enter the LAN and subnets that are located at the remote site here.

Networks	
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 Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
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 Certificate 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.

16.2 GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. A GRE tunnel is similar to IPSec or PepVPN.

To configure a GRE Tunnel, navigate to **Advanced > GRE Tunnel**.

GRE Tunnel Profiles	Remote Networks	
No GRE profile defined		
New Profile		

Click the **New Profile** button to create new GRE tunnel profiles that establish tunnel connections to remote tunnel endpoints via available WAN connections. To edit the profiles, click on its associated connection name in the leftmost column.

GRE Tunnel Profile
✕

Name			
Active	☒		
Remote GRE IP Address			
Tunnel Local IP Address			
Tunnel Remote IP Address			
Tunnel Subnet Mask	☒ Auto ☐ 255.255.255.0 (/24)		
Connection	WAN ▼		
Remote Networks	Network	Subnet Mask	
		255.255.255.0 (/24)	+

Save

Cancel

GRE Tunnel Profile Settings

Name	This field is for specifying a name to represent this GRE Tunnel connection profile.
Active	When this box is checked, this GRE Tunnel connection profile will be enabled. Otherwise, it will be disabled.
Remote GRE IP Address	This field is for entering the remote GRE's IP address
Tunnel Local IP Address	This field is for specifying the tunnel source IP address.
Tunnel Remote IP Address	This field is for specifying the tunnel destination IP address
Tunnel Subnet Mask	This field is to select the subnet mask that is to be used for the GRE tunnel.
Connection	Select the appropriate WAN connection from the drop-down menu.
Remote Networks	Input the LAN and subnets that are located at the remote site here.

17 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					
<u>testing</u>	Enforced VPN: SFC-NYC	Any	Any	TCP 443	
<u>HTTPS Persistence</u>	Persistence (Src) (Auto)	Any	Any	TCP 443	
<u>Default</u>	(Auto)				
Add Rule					

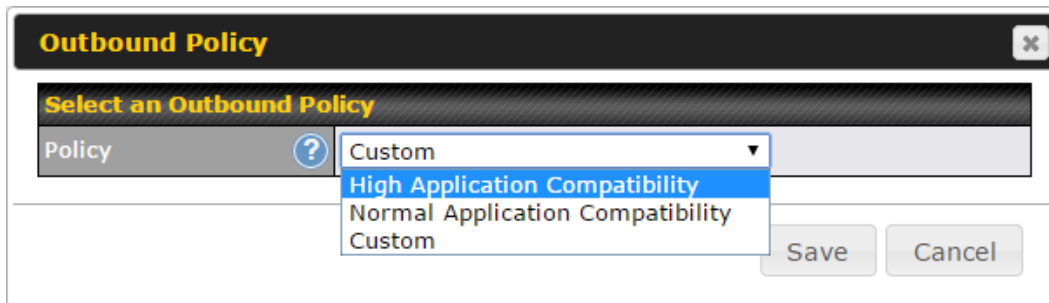
Expert Mode
?

Enabled

17.1 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:



There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

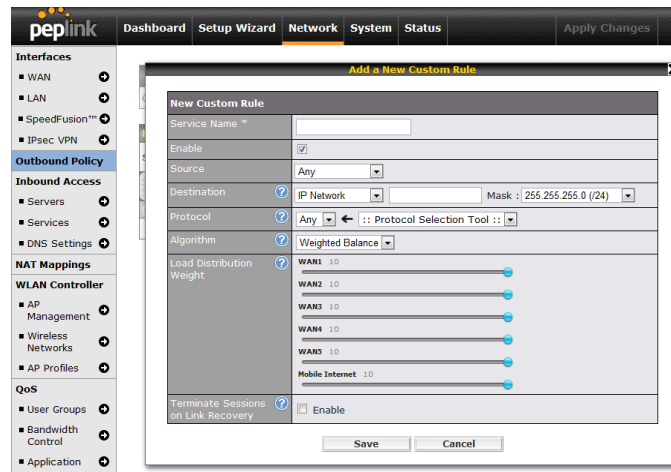
Note that some Pepwave routers provide only the **Send All Traffic To** setting here. See **Section 12.1** for details.

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!



http://youtu.be/rKH4AS_bQnE

17.2 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)				
Add Rule					

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 Drop the Traffic Use Any Available Connections

Save

Cancel

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	

Save
Cancel

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 Destination Protocol ? ? ? Any 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.

Destination	?	IP Network
Protocol	?	Any
Algorithm	?	IP Address
Load Distribution Weight	?	IP Network
		Domain Name
		SpeedFusion Cloud
		PepVPN Profile
		Grouped Network

If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (.) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *foobar.**, for example, *www.foobar.com*, *www.foobar.co.jp*, or *foobar.co.uk* will also match. Placing wildcards in any other position is not supported.

Note: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, access to any one of the server names will also match this rule.

Protocol and Port

This setting specifies the IP protocol and port of traffic that matches this rule. Via a drop-down menu, the following protocols can be specified:

- Any
- TCP
- UDP
- IP
- DSCP

Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.

Algorithm

This setting specifies the behavior of the Pepwave router for the custom rule.

One of the following values can be selected (Note that some Pepwave routers provide only some of these options):

- Weighted Balance
- Persistence
- Enforced
- Priority
- Overflow
- Least Used
- Lowest Latency
- Fastest Response Time

For a full explanation of each Algorithm, please see the following article:

<https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithms-work/8059>

Load Distribution Weight

This is to define the outbound traffic weight ratio for each WAN connection.

When No connections are available	This field allows you to configure the default action when all the selected Connections are not available. Drop the Traffic - Traffic will be discarded. Use Any Available Connections - Traffic will be routed to any available Connection, even it is not selected in the list. Fall-through to Next Rule - Traffic will continue to match the next Outbound Policy rule just like this rule is inactive.
Terminate Sessions on Connection Recovery	This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the Priority algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.

17.2.2 Algorithm: Weighted Balance

This setting specifies the ratio of WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Weighted Balance**.

Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 Wi-Fi WAN 10 Cellular 1 10 Cellular 2 10 USB 10

The amount of matching traffic that is distributed to a WAN connection is proportional to the weight of the WAN connection relative to the total weight. Use the sliders to change each WAN's weight.

For example, with the following weight settings:

- Ethernet WAN1: 10
- Ethernet WAN2: 10
- Wi-Fi WAN: 10
- Cellular 1: 10
- Cellular 2: 10

- USB: 10

Total weight is 60 = (10 +10 + 10 + 10 + 10 + 10).

Matching traffic distributed to Ethernet WAN1 is 16.7% = (10 / 60 x 100%.

Matching traffic distributed to Ethernet WAN2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Wi-Fi WAN is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 1 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to USB is 16.7% = (10 / 60) x 100%.

17.2.3 Algorithm: Persistence

The configuration of persistent services is the solution to the few situations where link load distribution for Internet services is undesirable. For example, for security reasons, many e-banking and other secure websites terminate the session when the client computer's Internet IP address changes mid-session.

In general, different Internet IP addresses represent different computers. The security concern is that an IP address change during a session may be the result of an unauthorized intrusion attempt. Therefore, to prevent damages from the potential intrusion, the session is terminated upon the detection of an IP address change.

Pepwave routers can be configured to distribute data traffic across multiple WAN connections. Also, the Internet IP depends on the WAN connections over which communication actually takes place. As a result, a LAN client computer behind the Pepwave router may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Pepwave router with three WAN connections may communicate on the Internet using three different IP addresses.

With the persistence feature, rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate using one IP address, eliminating the issues mentioned above.

Algorithm	Persistence
Persistence Mode	☒ By Source ☐ By Destination
Load Distribution	☐ Auto ☒ Custom
Load Distribution Weight	WAN 1 10 WAN 2 10 Wi-Fi WAN 10 Cellular 1 10 Cellular 2 10 USB 10

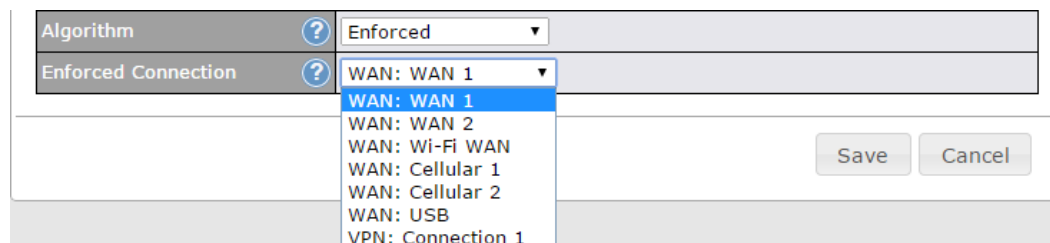
There are two persistent modes: **By Source** and **By Destination**.

By Source:	The same WAN connection will be used for traffic matching the rule and originating from the same machine, regardless of its destination. This option will provide the highest level of application compatibility.
By Destination:	The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute loads to WAN connections when there are only a few client machines.

The default mode is **By Source**. When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. If you choose **Auto** in **Load Distribution**, the weights will be automatically adjusted according to each WAN's **Downstream Bandwidth** which is specified in the WAN settings page). If you choose **Custom**, you can customize the weight of each WAN manually by using the sliders.

17.2.4 Algorithm: Enforced

This setting specifies the WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Enforced**.



Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Starting from Firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

17.2.5 Algorithm: Priority

This setting specifies the priority of the WAN connections used to route the specified network service. The highest priority WAN connection available will always be used for routing the specified type of traffic. A lower priority WAN connection will be used only when all higher priority connections have become unavailable.

Algorithm	Priority	
Priority Order	Highest Priority	Not In Use
	WAN: WAN	
	WAN: Cellular 1	
	WAN: Cellular 2	
	WAN: USB	
	WAN: LAN 1 as WAN	
	WAN: GRE WAN 1	
	WAN: GRE WAN 2	
	WAN: OpenVPN WAN 1	
	Lowest Priority	
When No Connections are Available	Drop the Traffic	
Terminate Sessions on Connection Recovery	☐ Enable	

Starting from Firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion™ connection(s). By default, VPN connections are not included in the priority list.

Tip

Configure multiple distribution rules to accommodate different kinds of services.

17.2.6 Algorithm: Overflow

The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.

Algorithm	Overflow	
Overflow Order	Highest Priority	
	WAN: WAN 1	
	WAN: WAN 2	
	WAN: Wi-Fi WAN	
	WAN: Cellular 1	
	WAN: Cellular 2	
	WAN: USB	
	Lowest Priority	

Drag and drop to specify the order of WAN connections to be used for routing traffic. Only the highest priority healthy connection that is not in full load will be used.

17.2.7 Algorithm: Least Used

Algorithm	Least Used
Connection	☒ WAN 1 ☒ WAN 2 ☒ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB

The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the most available download bandwidth. The available download bandwidth of a WAN connection is calculated from the total download bandwidth specified on the WAN settings page and the current download usage. The available bandwidth and WAN selection is determined every time an IP session is made.

17.2.8 Algorithm: Lowest Latency

Algorithm	Lowest Latency Note: Use of Lowest Latency will incur additional network usage.
Connection	☒ WAN 1 ☒ WAN 2 ☒ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB

The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the lowest latency. Latency checking packets are issued periodically to a nearby router of each WAN connection to determine its latency value. The latency of a WAN is the packet round trip time of the WAN connection. Additional network usage may be incurred as a result.

Tip

The roundtrip time of a 6M down/640k uplink can be higher than that of a 2M down/2M up link because the overall round trip time is lengthened by its slower upload bandwidth, despite its higher downlink speed. Therefore, this algorithm is good for two scenarios:

- All WAN connections are symmetric; or
- A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN's available bandwidth.

17.2.9 Expert Mode

Expert Mode is available on some Pepwave routers for use by advanced users. To enable the feature, click on the help icon and click **turn on Expert Mode**.

In Expert Mode, a new special rule, **SpeedFusion™ Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion™ routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets will be routed to the corresponding VPN peer. You can create custom **Priority** or **Enforced** rules and move them

above the bar to override the SpeedFusion™ routes.

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

Help

Close

This table allows you to fine tune how the outbound traffic should be distributed to the WAN connections.

Click the *Add Rule* button to add a new rule. Click the *X* button to remove a rule. Drag a rule to promote or demote its precedence. A higher position of a rule signifies a higher precedence. You may change the default outbound policy behavior by clicking the *Default* link.

If you require advanced control of PepVPN traffic, [turn on Expert Mode](#).

18 Port Forwarding

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

Service	IP Address(es)	Server	Protocol
No Services Defined			
Add Service			

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

Enable	☒ Yes ☐ No																												
Service Name	Service_1																												
IP Protocol	TCP ← :: Protocol Selection Tool :: →																												
Port	Any Port																												
Inbound IP Address(es) (Require at least one IP address)	<table> <tr> <th colspan="2">Connection / IP Address(es)</th><th> All </th><th> Clear </th></tr> <tr> <td>☒ WAN 1</td><td>☒ 10.88.3.158 (Interface IP)</td><td></td><td></td></tr> <tr> <td>☐ WAN 2</td><td></td><td></td><td></td></tr> <tr> <td>☐ Wi-Fi WAN</td><td></td><td></td><td></td></tr> <tr> <td>☐ Cellular 1</td><td></td><td></td><td></td></tr> <tr> <td>☐ Cellular 2</td><td></td><td></td><td></td></tr> <tr> <td>☐ USB</td><td></td><td></td><td></td></tr> </table>	Connection / IP Address(es)		All	Clear	☒ WAN 1	☒ 10.88.3.158 (Interface IP)			☐ WAN 2				☐ Wi-Fi WAN				☐ Cellular 1				☐ Cellular 2				☐ USB			
Connection / IP Address(es)		All	Clear																										
☒ WAN 1	☒ 10.88.3.158 (Interface IP)																												
☐ WAN 2																													
☐ Wi-Fi WAN																													
☐ Cellular 1																													
☐ Cellular 2																													
☐ USB																													
Server IP Address	120.78.95.7																												

Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.

IP Protocol

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

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

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

Port		Any Port ▼
------	---	------------

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

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

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

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

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

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

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

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

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

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

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

Port

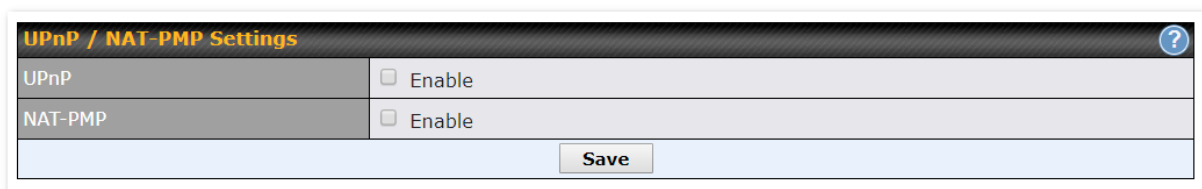
Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Server IP Address	This setting specifies the LAN IP address of the server that handles the requests for the service.

18.1 UPnP / NAT-PMP Settings

UPnP and NAT-PMP are network protocols which allow a computer connected to the LAN port to automatically configure the router to allow parties on the WAN port to connect to itself. That way, the process of inbound port forwarding becomes automated.

When a computer creates a rule using these protocols, the specified TCP/UDP port of all WAN connections' default IP address will be forwarded.

Check the corresponding box(es) to enable UPnP and/or NAT-PMP. Enable these features only if you trust the computers connected to the LAN ports.



UPnP / NAT-PMP Settings	
UPnP	☐ Enable
NAT-PMP	☐ Enable
Save	

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

19 NAT Mappings

NAT mappings allow IP address mapping of all inbound and outbound NAT'd traffic to and from an internal client IP address. Settings to configure NAT mappings are located at **Advanced > NAT Mappings**.

LAN Clients	Inbound Mappings	Outbound Mappings	
192.168.1.23	(WAN 1):10.88.3.158 (Interface IP)	Use Interface IP only	
Add NAT Rule			

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

LAN Client(s)	 IP Address ▾												
Address													
Inbound Mappings	 Connection / Inbound IP Address(es) ☐ WAN 1 ☐ WAN 2 ☐ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB												
Outbound Mappings	 Connection / Outbound IP Address <table> <tr> <td>WAN 1</td> <td>10.88.3.158 (Interface IP) ▾</td> </tr> <tr> <td>WAN 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 1</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>USB</td> <td>Interface IP ▾</td> </tr> </table>	WAN 1	10.88.3.158 (Interface IP) ▾	WAN 2	Interface IP ▾	Wi-Fi WAN	Interface IP ▾	Cellular 1	Interface IP ▾	Cellular 2	Interface IP ▾	USB	Interface IP ▾
WAN 1	10.88.3.158 (Interface IP) ▾												
WAN 2	Interface IP ▾												
Wi-Fi WAN	Interface IP ▾												
Cellular 1	Interface IP ▾												
Cellular 2	Interface IP ▾												
USB	Interface IP ▾												

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

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

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

Important Note

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

20 QoS

20.1 User Groups

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

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

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

Subnet / IP Address	User Group	Action
Guest Computer	Guest	
All DHCP reservation clients	Manager	
Everyone		

Add / Edit User Group

Client	Staff A		
Subnet / IP Address	IP Address	192.168.1.99	
Group	Manager	Staff A (192.168.1.99)	

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

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

20.2 Bandwidth Control

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

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

Group Bandwidth Reservation			
Enable	☒		
	Manager	Staff	Guest
Bandwidth %	50%	30%	20%
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M
WAN 2	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M

You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Managers. By default, download and upload bandwidth limits are set to unlimited (set as 0).

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

20.3 Application

20.3.2 Application Prioritization

On many Pepwave routers, you can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.

Application Prioritization	
☒	Apply same settings to all users
☐	Customize

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

table. Custom applications are at the bottom.

Application	Priority			?
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High	— Normal	↑ High	✖
All Email Protocols	↑ High	↑ High	↑ High	✖
MySQL	↑ High	— Normal	↓ Low	✖
SIP	↑ High	↓ Low	↓ Low	✖
Add				

20.3.3 Prioritization for Custom Applications

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

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

Add / Edit Application

Type
Category
Application

☒ Supported Applications
☐ Custom Applications

Audio Video Streaming
Database
Email
File Sharing / Transfer
IM
Miscellaneous
Remote Access
Security / Tunneling
VoIP

OK
Cancel

Add / Edit Application

Type

☐ Supported Applications
☒ Custom Applications

Application Name

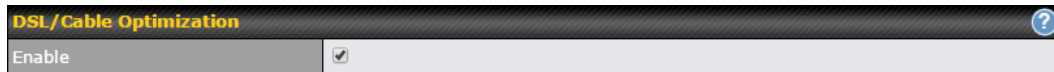
Scope / Protocol
TCP

Port
Single Port

OK
Cancel

20.3.4 DSL/Cable Optimization

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



21 Firewall

A firewall is a mechanism that selectively filters data traffic between the WAN side (the Internet) and the LAN side of the network. It can protect the local network from potential hacker attacks, access to offensive websites, and/or other inappropriate uses.

The firewall functionality of Pepwave routers supports the selective filtering of data traffic in both directions:

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)
- Internal Network (VLAN to VLAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion™ enabled, the firewall rules also apply to VPN tunneled traffic.

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

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

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

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

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

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

Intrusion Detection and DoS Prevention

Disabled
 

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

Rule	Service	WAN	Source	Action	
Default	Any	Any	Any	✓	
Add Rule					