

Pepwave Device Connector User Manual

Pepwave Product:

Device Connector Rugged, Device Connector IP55

Firmware 1.2.1

January 2023

Table of Contents

1. Getting Started	5
1.1. What's in the box	5
1.2. Get to Know Your Device Connector	5
2. Basic Configuration	9
2.1. Accesss the Web Admin Interface	9
2.1.2. Connect by Wi-Fi	10
2.2. Choose Your Connection Mode	10
3. Configuring the LAN Interface(s)	11
3.1. Network Settings	11
3.2. Port Settings	15
4. Configuring the WAN Interface(s)	16
4.1. Wi-Fi WAN (Wi-Fi Mode Only)	17
4.1.1. Wireless Networks	17
4.1.2. Creating Wi-Fi Connection Profiles	25
5. Advanced	28
5.1. SpeedFusion	28
5.2. Port Forwarding	34
5.3. NAT Mappings	36
5.4. QoS	38
5.4.1. Bandwidth Control	38
5.4.2. Application	38
5.5. Misc. Settings	40
5.5.1. RADIUS Server	40
5.5.2. Certificate Manager	42
6. AP Tab	43
6.1. AP	43
6.1.1. Wireless SSID	43
6.1.2. Settings	48
6.2. Status	51
6.2.1. Access Point	51

6.2.2. Wireless SSID	54
6.2.3. Wireless Client	55
6.2.4. Nearby Device	57
6.2.5. Event Log	58
7. System Tab	59
7.1. Admin Security	59
7.2. Operating Mode	62
7.3. Firmware	63
7.4. Time	64
7.5. Schedule	64
7.6. Email Notification	66
7.7. Event Log	69
7.8. SNMP	70
7.9. InControl	72
7.10. Configuration	73
7.11. Feature Add-ons	73
7.12. Reboot	74
8. Tools	75
8.1. Ping	75
8.2. Traceroute	75
8.3. Wake-on-LAN	76
8.4. WAN Analysis	76
9. Status	80
9.1. Device	80
9.2. Client List	81
9.3. SpeedFusion	82
9.4. Event log	86
9.4.1. Device Event Log	86
9.4.2. SpeedFusion Event Log	87
10. WAN Quality	88
11. Usage Reports	89
11.1. Real-Time	89
11.2. Hourly	90

11.3. Daily	91
11.4. Monthly	92
Appendix	93

1. Getting Started

1.1. What's in the box

DCS-RUG

- 12V power supply
- 3x dual-band 5dBi omni antenna

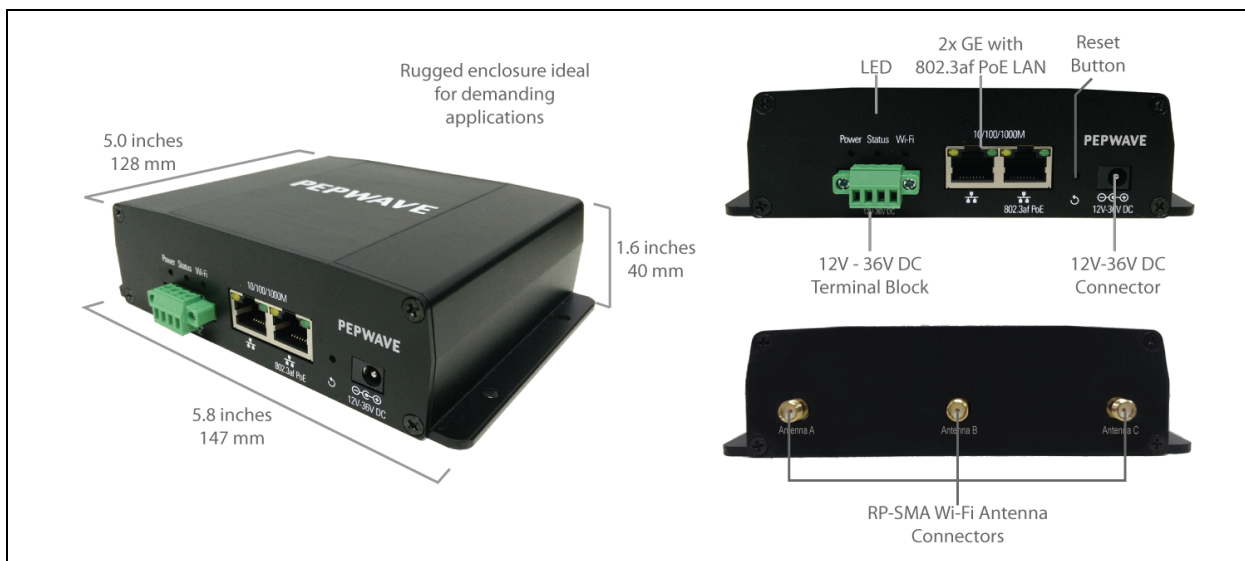
DCS-GN-IP55

- 2 x Plastic Cable Tie

1.2. Get to Know Your Device Connector

1.2.1. Device Connector Rugged

Panel Appearance



LED Indicators

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

Power and Status	
Power	OFF - Power off
	GREEN - Power on

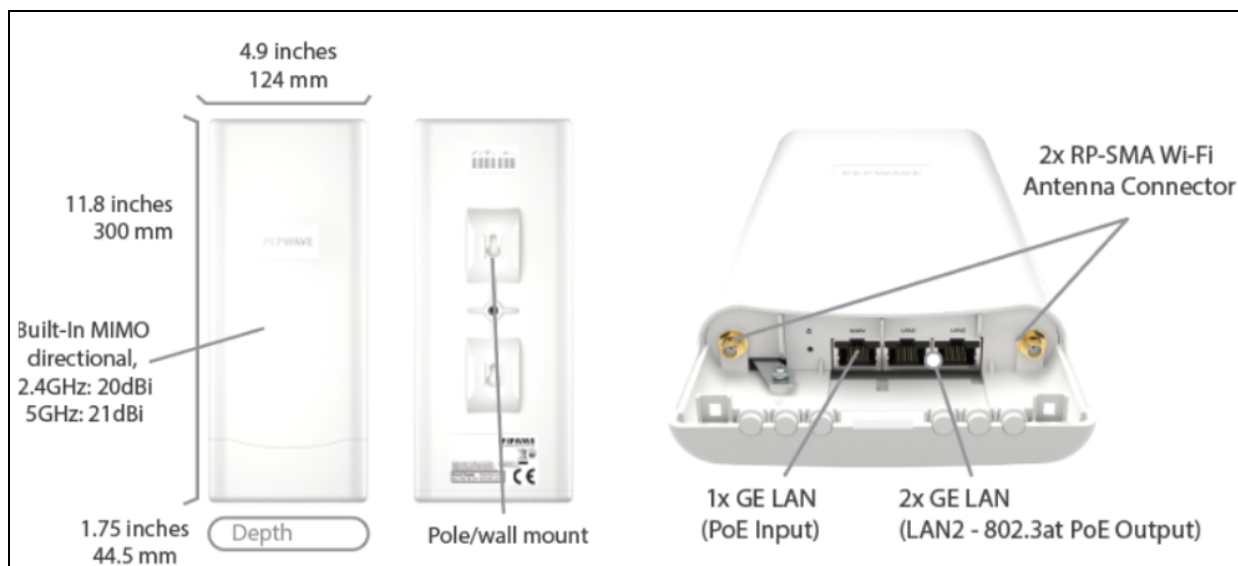
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	GREEN – Ready

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

Wi-Fi Indicators	
Wi-Fi	OFF - WiFi AP disabled
	Green - WiFi AP enabled

1.2.2. Device Connector IP55

Panel Appearance

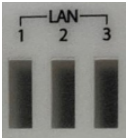
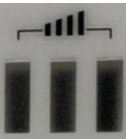


LED Indicators

The statuses indicated by the panel LEDs are as follows:

Status Indicators		
Status	Red	Access point initializing
	Blinking red	Boot up error
	Green	Access point ready

LAN Ports	
Green LED	ON – Powered-on device connected to Ethernet port or 1000Mbps
	OFF – 10 Mbps / 100 Mbps or No device connected to Ethernet port
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

LAN		
	Green LED	ON – Powered-on device connected to Ethernet port OFF – No device connected to Ethernet port
WiFi Signal		
	OFF	No Connection
	Signal Strength	Wi-Fi signal strength (low, medium, and high)

2. Basic Configuration

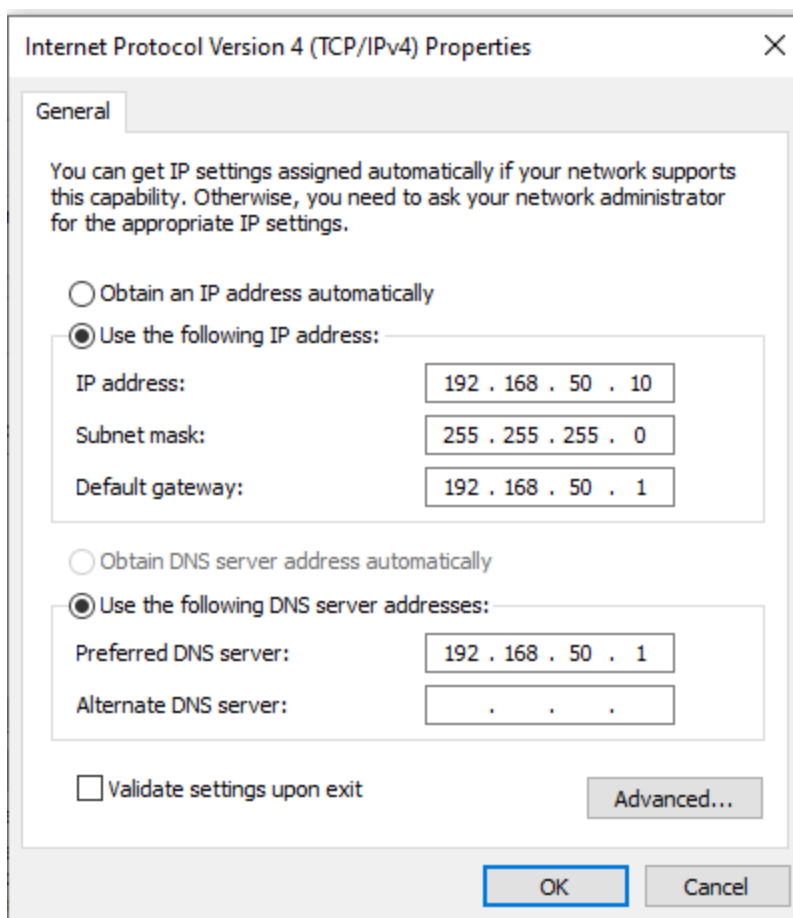
2.1. Accesss the Web Admin Interface

There are two ways to access the **Web Admin** page.

2.1.1. Connect by Ethernet

To access the Web Admin page by Ethernet, your PC must be in the same subnet as the Device Connector (*i.e.* 192.168.50.X).

Your PC should be set up as follow on the **Internet Protocol (TCP/IP) Properties** or **Network** screen:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 50 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 50 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 50 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

2.1.2. Connect by Wi-Fi

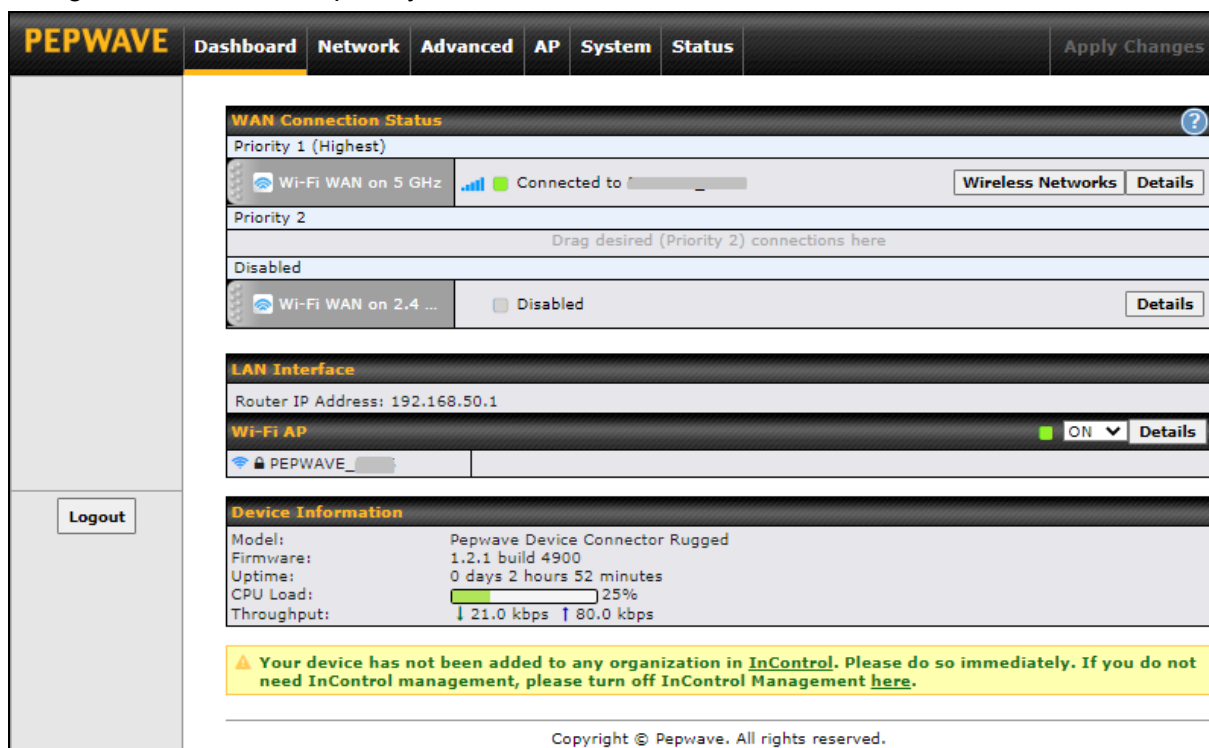
Connect to the SSID: PEPWAVE_XXX where XXXX represents the last four digits of your device's serial number (e.g. 7D6E). Passphrase is the last 8 hexadecimal digits of your device's LAN MAC address (e.g. DDC3CCC0)

Now you are ready to start the first time configuration of the Pepwave Device Connector. On your PC, start a web browser, go to this URL: <http://192.168.50.1/>

2.2. Choose Your Connection Mode

The Device Connector supports only Wi-Fi connection mode.

After successful login The **Dashboard** will be displayed and shows current Wi-Fi WAN connection, LAN Interface, WI-FI AP statuses and Device Information. Here, you can change WAN connection priority and switch on/off the Wi-Fi AP.





The screenshot displays the PEPWAVE Dashboard with the following sections:

- Navigation Bar:** PEPWAVE, Dashboard (selected), Network, Advanced, AP, System, Status, and an Apply Changes button.
- WAN Connection Status:**
 - Priority 1 (Highest): Wi-Fi WAN on 5 GHz, Connected to [redacted], with buttons for Wireless Networks and Details.
 - Priority 2: Drag desired (Priority 2) connections here.
 - Disabled: Wi-Fi WAN on 2.4 GHz, Disabled, with a Details button.
- LAN Interface:** Router IP Address: 192.168.50.1.
- Wi-Fi AP:** Status is ON (indicated by a green dot and a dropdown arrow), with a Details button.
- Device Information:**
 - Model: Pepwave Device Connector Rugged
 - Firmware: 1.2.1 build 4900
 - Uptime: 0 days 2 hours 52 minutes
 - CPU Load: 25% (indicated by a green progress bar)
 - Throughput: 21.0 kbps (down) / 80.0 kbps (up)
- Footer:** A yellow warning box states: "Your device has not been added to any organization in InControl. Please do so immediately. If you do not need InControl management, please turn off InControl Management here." Below this is the copyright notice: Copyright © Pepwave. All rights reserved.

3. Configuring the LAN Interface(s)

3.1. Network Settings


LAN interface settings are located at **Network > LAN > Network Settings**. Begin setting up your physical LAN by entering IP settings (VLAN configuration will be covered following physical LAN setup).

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

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

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

Clicking any of the existing LAN interfaces will result in the following

IP Settings	
IP Address	<input type="text"/> 255.255.255.0 (/24) 

IP Settings

IP Address

The IP address and subnet mask of the Device Connector router on the LAN.

Network Settings 	
Name	<input type="text"/>
VLAN ID	<input type="text"/>
Inter-VLAN routing	<input checked="" type="checkbox"/>

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.

Click the  button found next to the Network Settings and click **here** to define a layer-2 bridging based PepVPN.

Layer 2 PepVPN Bridging 	
PepVPN Profiles to Bridge 	No profile is available
Spanning Tree Protocol	<input type="checkbox"/>
Override IP Address when bridge connected 	<input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None


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, most of the layer 2 protocols will be able to communicate between the peers.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
Override IP Address when bridge connected	<p>Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 SpeedFusion VPN is up.</p> <p>If you choose to override the IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.</p>




DHCP Server											
DHCP Server 	<input checked="" type="checkbox"/> Enable										
DHCP Server Logging	<input type="checkbox"/>										
IP Range	<input type="text"/> - <input type="text"/> 255.255.255.0 (/24) ▼										
Lease Time	<input type="text"/> Days <input type="text"/> Hours <input type="text"/> Mins										
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically										
BOOTP	<input type="checkbox"/>										
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"> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> </td> </tr> <tr> <td colspan="2"> <input type="button" value="Add"/> </td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>		<input type="button" value="Add"/>	
Option	Value										
No Extended DHCP Option											
<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>											
<input type="button" value="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><input type="text"/></td> <td>00:00:00:00:00:00</td> <td><input type="text"/></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>			Name	MAC Address	Static IP		<input type="text"/>	00:00:00:00:00:00	<input type="text"/>	<input type="button" value="+"/>
Name	MAC Address	Static IP									
<input type="text"/>	00:00:00:00:00:00	<input type="text"/>	<input type="button" value="+"/>								


DHCP Server	
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	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	<p>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.</p> <p>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.</p>
DHCP Reservation	<p>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.</p> <p>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</p>

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

Once configuration is complete, click Save to store the changes.

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

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

DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the  icon to disable DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in DHCP Server 1 and DHCP Server 2 .
DHCP Option 82	DCHP 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.
DHCP Relay Logging	Enable logging of DHCP Relay events in the eventlog by selecting the checkbox.

3.2. Port Settings

Port settings can be accessed at **Network > LAN > Port Settings**.

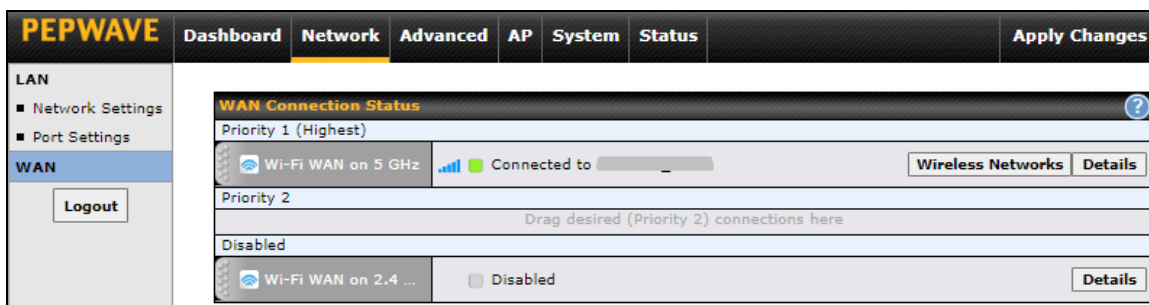
Port Settings						
	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port 1	<input checked="" type="checkbox"/>			Trunk ▼	Any ▼
2	LAN Port 2	<input checked="" type="checkbox"/>	1 Gbps Full Duplex ▼	<input checked="" type="checkbox"/>	Trunk ▼	Any ▼

This section allows you to:

- Enable or disable specific LAN ports
- Configure the negotiation speed of the LAN ports
- Configure the port type (Trunk or Access)
- Assign a VLAN to a LAN port

4. 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.



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

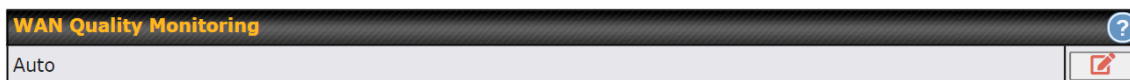
You can also set priorities on the Dashboard. Click the Details button in the corresponding row to modify the connection setting.

Important Note

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

WAN Quality Monitoring

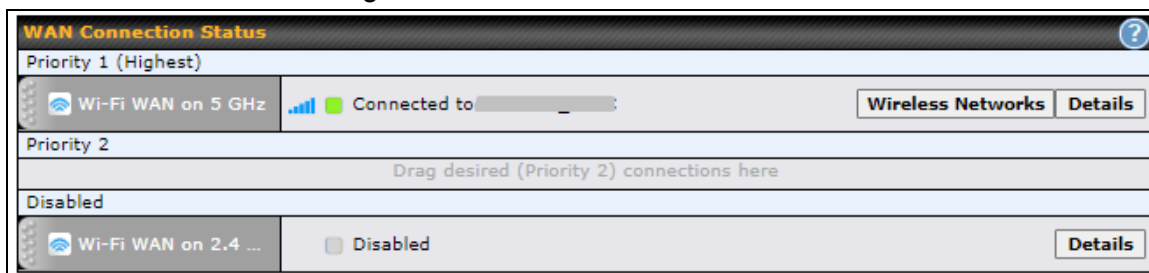
This settings advice how WAN Quality information is being gathered.



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.

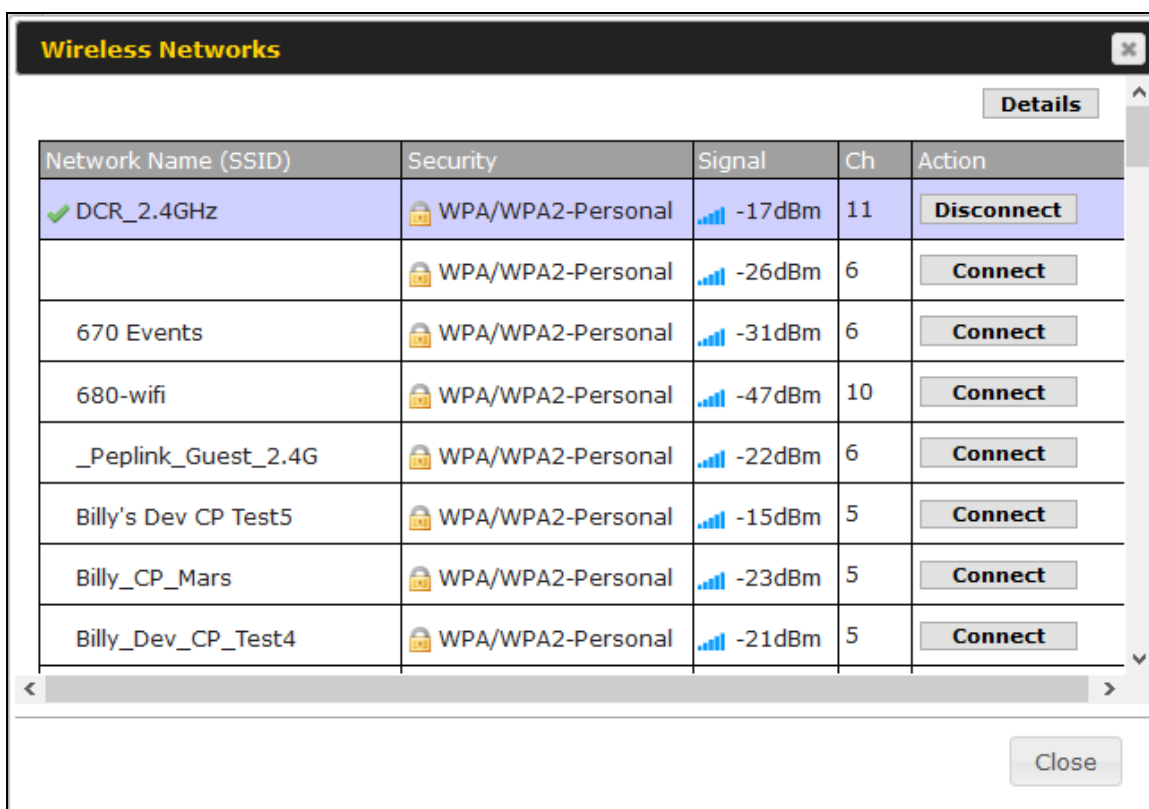
4.1. Wi-Fi WAN (Wi-Fi Mode Only)

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



4.1.1. Wireless Networks

To see a list of available networks, click inside wireless network. To connect to a displayed network, select it from this list. To access wireless network, click **Network > WAN > Wireless Networks**.

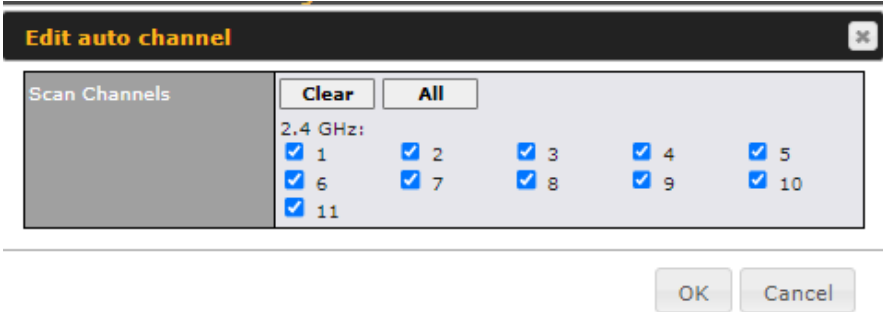



To access detailed WAN settings click, **Network > WAN > Details**.

WAN Connection Settings	
WAN Connection Name	Wi-Fi WAN on 2.4 GHz
Independent from Backup WANs	<input type="checkbox"/>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Reply to ICMP Ping	<input checked="" type="radio"/> Yes <input type="radio"/> No

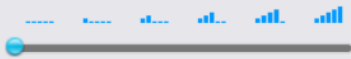
WAN Connection Settings	
WAN Connection Name	Enter a name to represent this Wi-Fi WAN connection.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and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

Wi-Fi WAN Settings	
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	<p>Determine whether the channel will be automatically selected. If you select custom, the following table will appear:</p> 
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.
Data 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.
Roaming	Checking this box will enable Wi-Fi roaming and will display 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^A	This field allows you to set the frequency for the beacon to include delivery traffic indication messages.
Channel Scan Interval^A	Configure Channel Scan Interval in ms.

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

Signal Threshold Settings

Signal Threshold Settings	
Acceptable Level	

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

Signal Threshold Settings	
Signal Strength	RSSI: <input type="text" value="n/a"/> dBm (Recovery: <input type="text" value="n/a"/> dBm)

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

Physical Interface Settings

Physical Interface Settings	
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="1500"/>

This setting specifies the maximum transmission unit. By default, MTU is set to Custom 1500. You may adjust the MTU value by editing the text field. Select Auto and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes.

WAN Health Check

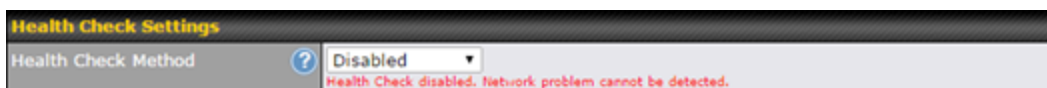
Health Check Settings	
Health Check Method	<input type="text" value="DNS Lookup"/>
Health Check DNS Servers	Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers
Timeout	<input type="text" value="5"/> second(s)
Health Check Interval	<input type="text" value="5"/> second(s)
Health Check Retries	<input type="text" value="3"/>
Recovery Retries	<input type="text" value="3"/>

Health Check Settings

Method	This setting specifies the health check method for the WAN connection. This value can be configured as Disabled, PING, DNS Lookup, or HTTP.
---------------	---

The default method is DNS Lookup. For mobile Internet connections, the value of Method can be configured as Disabled or SmartCheck.

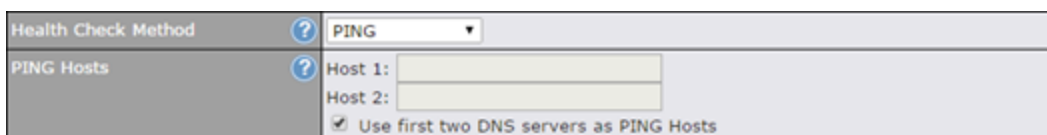
Health Check Disabled



The screenshot shows the 'Health Check Settings' window. The 'Health Check Method' is set to 'Disabled'. A red error message at the bottom states: '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



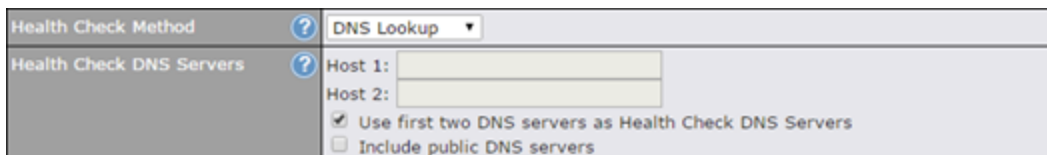
The screenshot shows the 'Health Check Settings' window with 'PING' selected as the method. Below, there are fields for 'Host 1' and 'Host 2'. A checkbox 'Use first two DNS servers as PING Hosts' is checked.

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



The screenshot shows the 'Health Check Settings' window with 'DNS Lookup' selected as the method. Below, there are fields for 'Host 1' and 'Host 2'. Two checkboxes are present: 'Use first two DNS servers as Health Check DNS Servers' (checked) and 'Include public DNS servers' (unchecked).

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

Health Check Method	 HTTP
URL 1	 http:// <input type="text"/> Matching String: <input type="checkbox"/>
URL 2	 http:// <input type="text"/> Matching String: <input type="checkbox"/>

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

URL1

WAN Settings > WAN Edit > Health Check Settings > URL1

The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

URL 2

WAN Settings > WAN Edit > Health Check Settings > URL2

If **URL2** is also provided, a health check will pass if either one of the tests passed.

Others 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.**

Bandwidth Allowance Monitoring

Bandwidth Allowance Monitor	
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable
Action	<input checked="" type="checkbox"/> Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On <input type="text" value="1st"/> of each month at 00:00 midnight
Monthly Allowance	<input type="text" value=""/> MB

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.

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	 <input type="text" value="Disabled"/>

Dynamic DNS Settings	
Dynamic DNS	<p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> <ul style="list-style-type: none"> • Disabled • changeip.com • dyndns.org • no-ip.org • DNS-O-Matic • Others... <p>Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.</p> <p>Select Disabled to disable this feature.</p>
User ID/ Username /	<p>This setting specifies the registered user name for the dynamic DNS service.</p>

Email

Password

This setting specifies the password for the dynamic DNS service.

Hosts

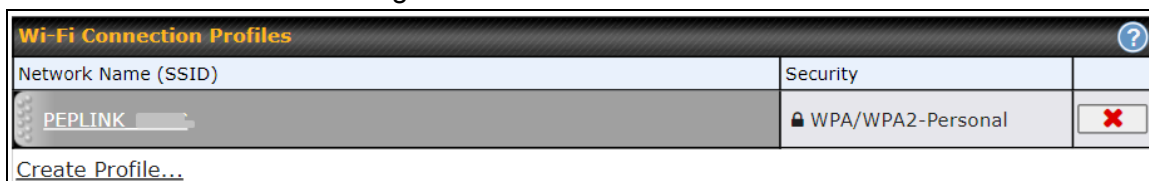
This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

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.

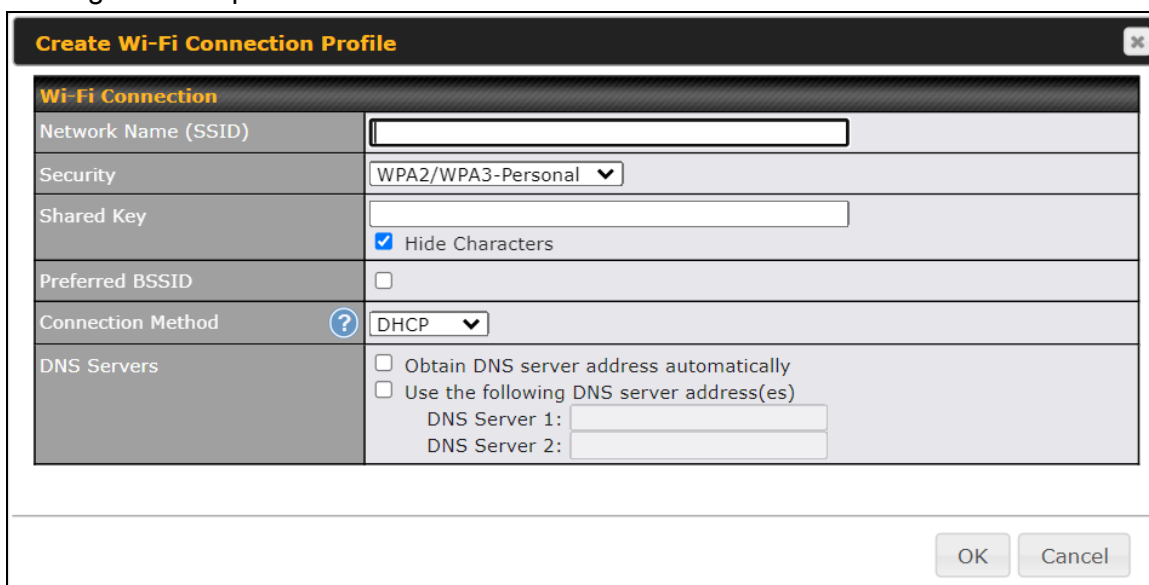
4.1.2. Creating Wi-Fi Connection Profiles

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.



The image shows a window titled "Wi-Fi Connection Profiles" with a help icon in the top right. It contains two main sections: "Network Name (SSID)" and "Security". The "Network Name (SSID)" section has a text input field containing "PEPLINK". The "Security" section has a dropdown menu showing "WPA/WPA2-Personal" and a red "X" icon. At the bottom, there is a "Create Profile..." button.

Clicking this will open a window similar to the one shown below.



The image shows a window titled "Create Wi-Fi Connection Profile" with a close icon in the top right. It contains a "Wi-Fi Connection" section with several fields: "Network Name (SSID)" (text input), "Security" (dropdown menu showing "WPA2/WPA3-Personal"), "Shared Key" (text input with a "Hide Characters" checkbox checked), "Preferred BSSID" (checkbox), "Connection Method" (dropdown menu showing "DHCP" with a help icon), and "DNS Servers" (checkboxes for "Obtain DNS server address automatically" and "Use the following DNS server address(es)", with sub-fields for "DNS Server 1:" and "DNS Server 2:"). At the bottom, there are "OK" and "Cancel" buttons.

Wi-Fi Connection Profile Settings

Network Name (SSID) Enter a name to represent this Wi-Fi connection name.

Security This option allows you to select which security policy is used for this wireless network. Available options:

- **Open**

Security	Open ▼
----------	--------

- **WEP**

Security	WEP ▼
Encryption Key	<input type="text"/>
	<input checked="" type="checkbox"/> Hide Characters

- **WPA/WPA2 – Personal**

Security	WPA/WPA2-Personal ▼
Shared Key	<input type="text"/>
	<input checked="" type="checkbox"/> Hide Characters

- **WPA/WPA2 – Enterprise**

Security	WPA/WPA2-Enterprise ▼
EAP Method	PEAP ▼
EAP Phase 2 Method	EAP/CHAP ▼
Login ID	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
EAP outer authentication identity	<input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/>

- **Enhanced Open (OWE)**

Security	Enhanced Open (OWE) ▼
----------	-----------------------

- **WPA3 - Personal**

Security	WPA3-Personal ▼
Shared Key	<input type="text"/>
	<input checked="" type="checkbox"/> Hide Characters

- **WPA2/WPA3 - Personal**

Security	WPA2/WPA3-Personal ▼
Shared Key	<input type="text"/>
	<input checked="" type="checkbox"/> Hide Characters

Preferred BSSID Configure the BSSID. The BSSID is the MAC address of the wireless access point (WAP).



Connection Method	This option allows you to select the connection method for this WAN connection. Available options are DHCP and Static IP
DNS Servers	Configure the DNS servers that this WAN connection should use.


5. Advanced

5.1. SpeedFusion

To configure PepVPN with SpeedFusion, navigate to **Advanced > SpeedFusion**

PepVPN with SpeedFusion

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

Profile	Remote ID	Remote Address(es)	
No VPN Connection Defined			
<input type="button" value="New Profile"/>			

Send All Traffic To

No PepVPN profile selected

PepVPN Local ID

Local ID

?
DCS_

PepVPN Settings

Link Failure Detection Time
?

☒ Recommended (Approx. 15 secs)
☐ Fast (Approx. 6 secs)
☐ Faster (Approx. 2 secs)
☐ Extreme (Under 1 sec)
Shorter detection time incurs more health checks and higher bandwidth overhead

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 > 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.


PepVPN Profile					
Name	<input type="text"/>				
Enable	<input checked="" type="checkbox"/>				
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF				
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key				
Remote ID / Pre-shared Key	<table border="1"> <thead> <tr> <th>Remote ID</th> <th>Pre-shared Key</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Remote ID	Pre-shared Key	<input type="text"/>	<input type="text"/>
Remote ID	Pre-shared Key				
<input type="text"/>	<input type="text"/>				
NAT Mode	<input type="checkbox"/>				
Remote IP Address / Host Names (Optional)	<input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small>				
Cost	<input type="text" value="10"/>				
Data Port	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>				
Bandwidth Limit	<input type="checkbox"/>				
WAN Smoothing	<input type="text" value="Off"/>				
Forward Error Correction	<input type="text" value="Off"/>				
Receive Buffer	<input type="text" value="0"/> ms				
Use IP ToS	<input type="checkbox"/>				
Latency Difference Cutoff	<input type="text" value="500"/> ms				


Click the **Save** button to create and save a new VPN connection profile for making a VPN connection.

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 ().
Enable	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from By Remote ID Only , Preshared Key . When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field.

Remote ID / Pre-shared Key	This optional field becomes available when Remote ID / Pre-shared Key is selected as the Peplink Balance's VPN Authentication method, as explained above. Pre-shared Key defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	<p>If NAT Mode is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.</p> <p>This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.</p>
Cost	<p>Define path cost for this profile.</p> <p>OSPF will determine the best route through the network using the assigned cost.</p> <p>Default: 10</p>
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.
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 SpeedFusion VPN, 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.

	<p>Off - Disable WAN Smoothing.</p> <p>Normal - The total bandwidth consumption will be at most 2x of the original data traffic.</p> <p>Medium - The total bandwidth consumption will be at most 3x of the original data traffic.</p> <p>High - The total bandwidth consumption depends on the number of connected active tunnels.</p>
Forward Error Correction	<p>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.</p> <p>The expected overhead of Low is 13.3% and High is 26.7%.</p> <p>Require peer using SpeedFusion VPN version 8.0.0 and above.</p>
Receive Buffer	<p>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.</p>
Use IP ToS^A	<p>Checking this button enables the use of IP ToS header field.</p>
Latency Difference Cutoff^A	<p>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)</p>


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

WAN Connection Priority 				
	Priority	Connect to Remote	Cut-off Latency (ms)	Suspension Time after Packet Loss (ms)
1. Wi-Fi WAN on 2.4 GHz	1 (Highest) ▼	All ▼	<input type="text"/>	<input type="text"/>
2. Wi-Fi WAN on 5 GHz	2 (Lowest) ▼	All ▼	<input type="text"/>	<input type="text"/>

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.

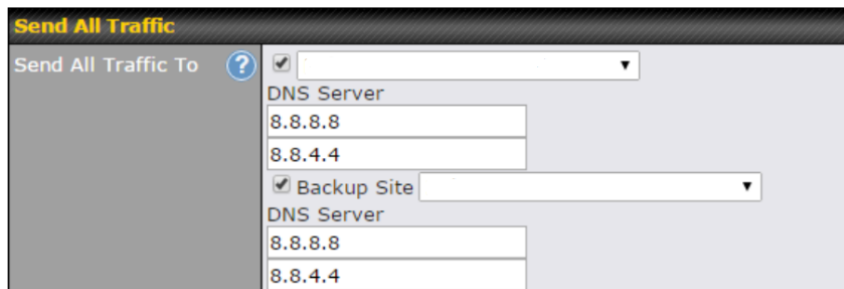
Send All Traffic To

No PepVPN profile selected



Send All Traffic To

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



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 SpeedFusion VPN connection fail.

PepVPN Local ID


Local ID



DCS_B786




PepVPN Local ID

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

PepVPN Settings ?	
Handshake Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>
Link Failure Detection Time ?	<input checked="" type="radio"/> Recommended (Approx. 15 secs) <input type="radio"/> Fast (Approx. 6 secs) <input type="radio"/> Faster (Approx. 2 secs) <input type="radio"/> Extreme (Under 1 sec) <small>Shorter detection time incurs more health checks and higher bandwidth overhead</small>
<input type="button" value="Save"/>	

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

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

5.2. Port Forwarding

Pepwave device connector 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**.

Port Forwarding

Enable

☒

Service Name

Protocol

TCP ⌂ :: Protocol Selection ::

Port

Any Port

Inbound IP Address(es)
(Require at least one IP address)

Connection / IP Address(es)

☐ Wi-Fi WAN on 2.4 GHz

☐ Wi-Fi WAN on 5 GHz

☐ PepVPN

Server IP Address

Save

Cancel

Port Forwarding Settings


Enable	This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.
Protocol	The Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the Servers setting. Please see below for details on the Port and Servers settings. Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After

selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.


Port

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

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

Port		Any Port
------	---	----------

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

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

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

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

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

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

Port Mapping: traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88. (Please see below for details on the **Servers** setting.)

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

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

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.

5.3. NAT Mappings

NAT mappings allow IP address mapping of all inbound and outbound NAT 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
No NAT Mappings Defined		
<input type="button" value="Add NAT Rule"/>		

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

NAT Mappings ✕

LAN Client(s)	?	IP Address ▼
Address	?	<input type="text"/>
Inbound Mappings	?	<div style="background-color: #333; color: white; padding: 2px;">Connection / Inbound IP Address(es)</div> <div> <input type="checkbox"/> Wi-Fi WAN on 2.4 GHz <input type="checkbox"/> Wi-Fi WAN on 5 GHz <input type="checkbox"/> PepVPN </div>
Outbound Mappings	?	<div style="background-color: #333; color: white; padding: 2px;">Connection / Outbound IP Address</div> <div> <div>Wi-Fi WAN on 2.4 GHz</div> <div>Interface IP ▼</div> </div> <div> <div>Wi-Fi WAN on 5 GHz</div> <div>192.168.1.22 (Interface IP) ▼</div> </div>

NAT Mappings 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.
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).

5.4. QoS

5.4.1. Bandwidth Control

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 Manager members. By default, download and upload bandwidth limits are set to unlimited (set as **0**).

Individual Bandwidth Limit			
Enable	<input checked="" type="checkbox"/>		
User Bandwidth Limit	Download	Upload	
	0 <input type="text"/> Mbps <input type="button" value="v"/>	0 <input type="text"/> Mbps <input type="button" value="v"/>	(0: Unlimited)
<input type="button" value="Save"/>			

5.4.2. Application

Application Prioritization

Three application priority levels can be set: **↑High**, **— Normal**, and **↓Low**. Applications not defined in the table are assigned a "Normal" priority level. Pepwave device connectors 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.

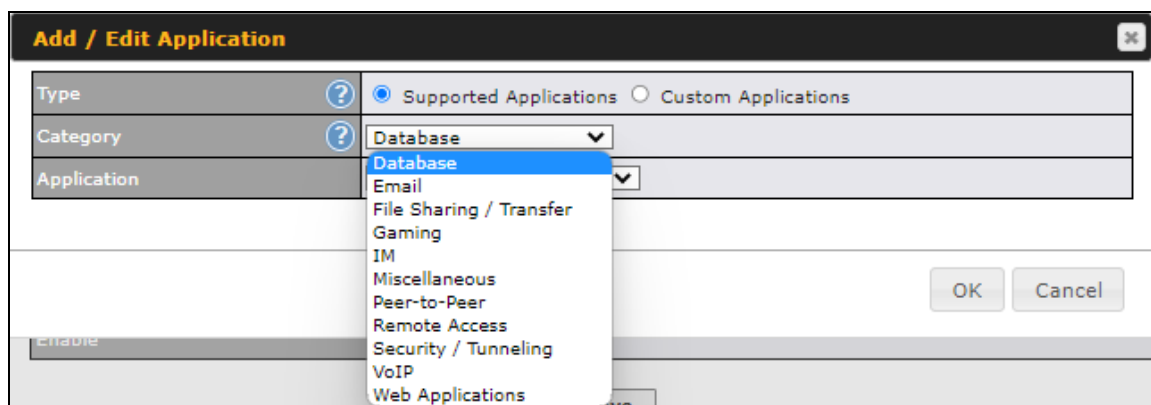
Application	Priority	
All Supported Streaming Applications	↑ High <input type="button" value="v"/>	<input type="button" value="x"/>
<input type="button" value="Add"/>		

Click the **Add** button to define an application's priority. Click the button to delete the application in the corresponding row. Click on a custom application's name to edit.

Prioritization for Custom Applications

Click the **Add** button to define a custom application. Click the button 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: ☒ Supported Applications ☐ Custom Applications

Category: (Dropdown menu open showing: Database, Email, File Sharing / Transfer, Gaming, IM, Miscellaneous, Peer-to-Peer, Remote Access, Security / Tunneling, VoIP, Web Applications)

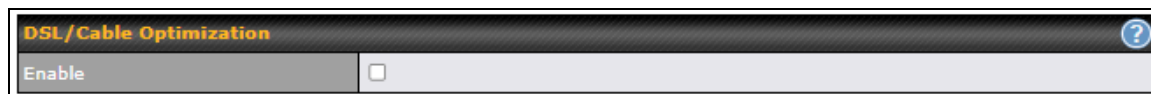
Application:

Enable: ☐

OK Cancel

DSL/Cable Optimization

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

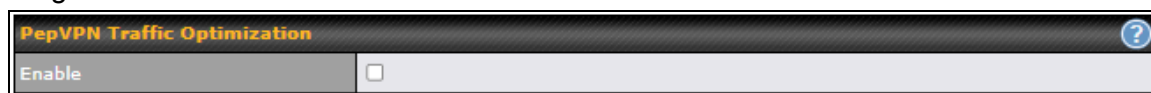


DSL/Cable Optimization

Enable: ☐

PepVPN Traffic Optimization

To enable this option to allow PepVPN traffic has highest priority when WAN is congested.



PepVPN Traffic Optimization

Enable: ☐

5.5. Misc. Settings

5.5.1. RADIUS Server

RADIUS Server settings are located at **Advanced > Misc. Settings > RADIUS Server**.

Authentication Server	Host	Port
No server profiles defined		
New Profile		

Accounting Server	Host	Port
No server profiles defined		
New Profile		

To configure the Authentication Server and Accounting Server, click **New Profile** to display the following screen:

Authentication Server
✕

Name	<input type="text"/>
Host	<input type="text"/>
Port	<input type="text" value="1812"/>
Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

[Save](#)
[Cancel](#)

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

Accounting Server

Name

Host

Port

1813

Secret

☐ Hide Characters


Save

Cancel

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

5.5.2. Certificate Manager

This section allows you to assign certificates for SpeedFusion, Web Admin SSL, Wi-Fi WAN Client certificate and Wi-Fi WAN CA Certificate.

Certificate		
SpeedFusion	No Certificate	
Web Admin SSL	Default Certificate is in use	

Wi-Fi WAN Client Certificate
No Certificates defined
Add Certificate

Wi-Fi WAN CA Certificate
No Certificates defined
Add Certificate

The following knowledge base article describes how to create self-signed certificates and import it to a Peplink Product.

<https://forum.peplink.com/t/how-to-create-a-self-signed-certificate-and-import-it-to-a-peplink-product/>


6. AP Tab

Use the controls on the **AP** tab to set the wireless SSID and AP settings.


6.1. AP


6.1.1. Wireless SSID


Wireless network settings, including the name of the network (SSID) and security policy, can be defined and managed in this section.

SSID	Security Policy	
PEPWAVE	WPA2 - Personal	
New SSID		

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

SSID


SSID Settings


SSID	<input type="text"/>
Schedule	Always on ▼
VLAN	Untagged LAN ▼
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed <input type="radio"/> Minimum
Multicast Filter	<input type="checkbox"/>
Multicast Rate	MCS16/MCS8/MCS0/6M ▼
IGMP Snooping	<input type="checkbox"/>
Layer 2 Isolation	<input type="checkbox"/>
Maximum number of clients	2.4 GHz: <input type="text"/> 5 GHz: <input type="text"/> (0: Unlimited)
Band Steering	 Disable ▼

SSID Settings

SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Schedule	Click the drop-down menu to apply a time schedule to this interface
VLAN	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi

	segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is 0 , which means VLAN tagging is disabled (instead of tagged with zero).
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate ^A	Select Auto to allow the Pepwave router to set the data rate automatically, or select Fixed and choose a rate from the displayed drop-down menu.
Multicast Filter ^A	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate ^A	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected Protocol and Channel Bonding settings will affect the rate options and values available here.
IGMP Snooping ^A	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
Layer 2 Isolation ^A	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
Maximum number of clients ^A	Indicate the maximum number of clients that should be able to connect to each frequency.
Band Steering ^A	To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency. Choose between: Force - Clients capable of 5 GHz operation are only offered with 5 GHz frequency. Prefer - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered. Disable - Default

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Shared Key	<div> ? <input type="password" value="....."/> </div> <input checked="" type="checkbox"/> Hide Characters

Security Settings

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

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

Security Policy

When **WPA/WPA2 - Enterprise** is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the **Shared Key** option should be disabled. When using this method, select the appropriate version using the **V1/V2** controls. The security level of this method is known to be very high.

When **WPA/WPA2- Personal** is configured, a shared key is used for data encryption and authentication. When using this configuration, the **Shared Key** option should be enabled. Key length must be between eight and 63 characters (inclusive). The security level of this method is known to be high.

NOTE:

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

Access Control	
Restricted Mode	Deny all except listed ▼
MAC Address List	<div></div>

Access Control	
Restricted Mode	The settings allow administrator to control access using MAC address filtering. Available options are None , Deny all except listed , Accept all except listed and Radius MAC Authentication .
MAC Address List	Connection coming from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field. If more than one MAC address needs to be entered, you can use a carriage return to separate them.

Guest Protect			
Block All Private IP	<input type="checkbox"/>		
Custom Subnet	Network	Subnet Mask	
	<div></div>	255.255.255.0 (/24) ▼	<div>+</div>
Block Exception	Network	Subnet Mask	
	<div></div>	255.255.255.0 (/24) ▼	<div>+</div>

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

Firewall Settings	
Firewall Mode	<div> Disable ▼ </div>

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

6.1.2. Settings

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

AP Settings	
SSID	<div>2.4 GHz 5 GHz</div> <div><input checked="" type="checkbox"/> <input checked="" type="checkbox"/> PEPWAVE_B786</div>
Operating Country	United States
	2.4 GHz 5 GHz
Protocol	<div>802.11n 802.11n/ac</div> <div>Integrated AP supports 802.11n/ac only</div>
Channel Width	Auto Auto
Channel	<div>Auto Edit</div> <div>Channels: 1 2 3 4 5 6 7 8 9 10 11 Channels: 36 40 44 48 149 153 157 161 165</div>
Auto Channel Update	<div>Daily at Clear All</div> <div> <input type="checkbox"/> 00:00 <input type="checkbox"/> 01:00 <input type="checkbox"/> 02:00 <input checked="" type="checkbox"/> 03:00 <input type="checkbox"/> 04:00 <input type="checkbox"/> 05:00 <input type="checkbox"/> 06:00 <input type="checkbox"/> 07:00 <input type="checkbox"/> 08:00 <input type="checkbox"/> 09:00 <input type="checkbox"/> 10:00 <input type="checkbox"/> 11:00 <input type="checkbox"/> 12:00 <input type="checkbox"/> 13:00 <input type="checkbox"/> 14:00 <input type="checkbox"/> 15:00 <input type="checkbox"/> 16:00 <input type="checkbox"/> 17:00 <input type="checkbox"/> 18:00 <input type="checkbox"/> 19:00 <input type="checkbox"/> 20:00 <input type="checkbox"/> 21:00 <input type="checkbox"/> 22:00 <input type="checkbox"/> 23:00 <input checked="" type="checkbox"/> Wait until no active client associated </div>
Output Power	<div>Max Boost</div> <div>Max Boost</div>
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)
Discover Nearby Networks	<input checked="" type="checkbox"/> <div>Note: Feature will be automatically turned on with Auto Channel / Dynamic Output Power</div>
Beacon Rate	1 Mbps
Beacon Interval	100 ms
DTIM	1
RTS Threshold	0
Fragmentation Threshold	0 (0: Disable)
Distance / Time Converter	<div>4050 m</div> <div>Note: Input distance for recommended values</div>
Slot Time	<input type="radio"/> Auto <input checked="" type="radio"/> Custom 9 μs
ACK Timeout	48 μs
Save	


AP Settings

SSID

These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Pepwave does not detect whether the

	AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.
Operating Country	This option sets the country whose regulations the Pepwave router follows.
Protocol	This option allows you to specify which client association requests will be accepted. By default, 802.11ng is selected.
Channel Width	<p>Auto (20/40 MHz) and 20 MHz are available. The default setting is Auto (20/40 MHz), which allows both widths to be used simultaneously.</p> <p>Auto (80 MHz) and (20/40 MHz) are available. The default setting is 80 MHz.</p> <p>The two default settings are for 802.11ng and 802.11ac accordingly.</p>
Channel	This option allows you to select which 802.11 RF channel will be used.
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^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Discover Nearby Networks	<p>This option is to turn on and off to scan the nearby the AP.</p> <p>Note: Feature will be automatically turned on with Auto Channel / Dynamic Output Power</p>
Beacon Rate^A	This option is for setting the transmit bit rate for sending a beacon. By default, 1Mbps is selected.
Beacon Interval^A	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM^A	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to 1 ms .

RTS Threshold	Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.
Fragmentation Threshold^A	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.
Distance/Time Converter^A	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
Slot Time^A	This field is for specifying the wait time before the Device Connector transmits a packet. By default, this field is set to 9 μs .
ACK Timeout^A	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 μs .

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

Important Note

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

6.2. Status

6.2.1. Access Point

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







AP Status		
Name	IP Address	
DCS_B786/2933-2...	(Local)	 

AP Status

AP Status


This table shows the detailed information on each AP, including channel, number of clients, upload traffic, and download traffic. Click the blue arrows at the left of the table to expand and collapse information on each device group.

On the right of the table, you will see the following icons:   .

Click the  icon to see a usage table for each client:

Client List						
MAC Address	IP Address	Type	Signal	SSID	Upload	Download
80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB


Close

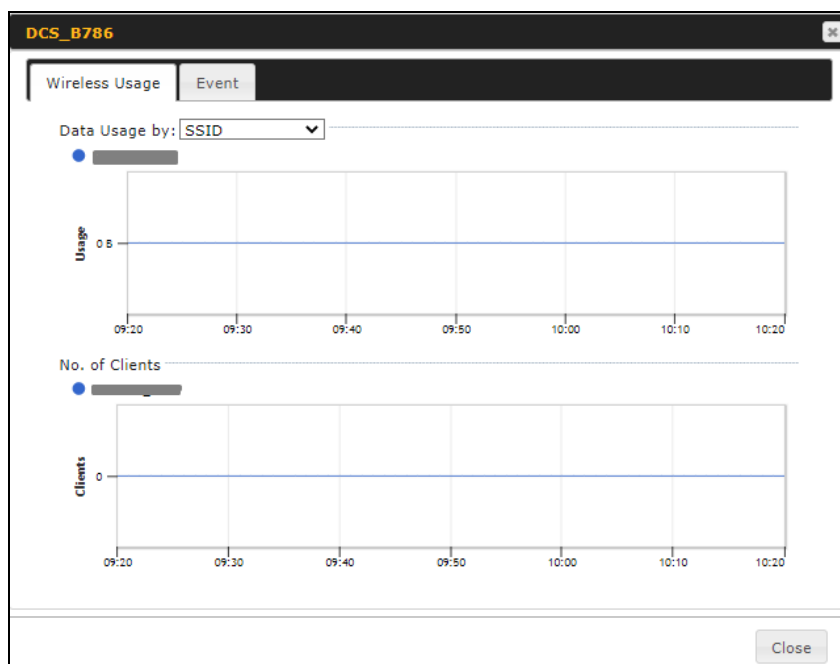
Click the  icon to configure each client

AP Details	
Serial Number	
MAC Address	
Product Name	Pepwave Device Connector Rugged
Firmware Version	1.2.1 build 4900
SSID List	2.4 GHz: 5 GHz:
Current Channel	2.4 GHz: 11 5 GHz: 36
Current Output Power	2.4 GHz: 25 dBm 5 GHz: 25 dBm

Close

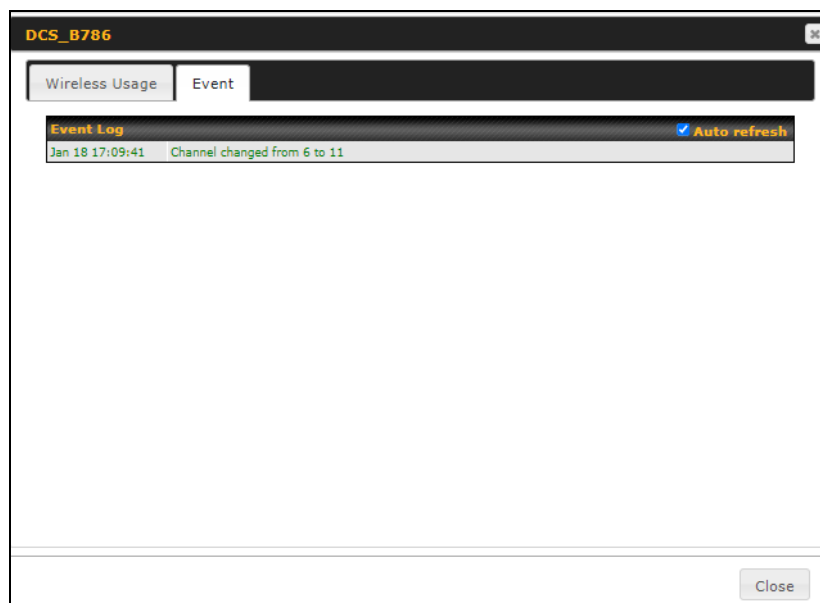
For easier network management, you can give each client a name and designate its location. You can also designate which firmware pack (if any) this client will follow, as well as the channels on which the client will broadcast.

Click the  icon to see a graph displaying usage:



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

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

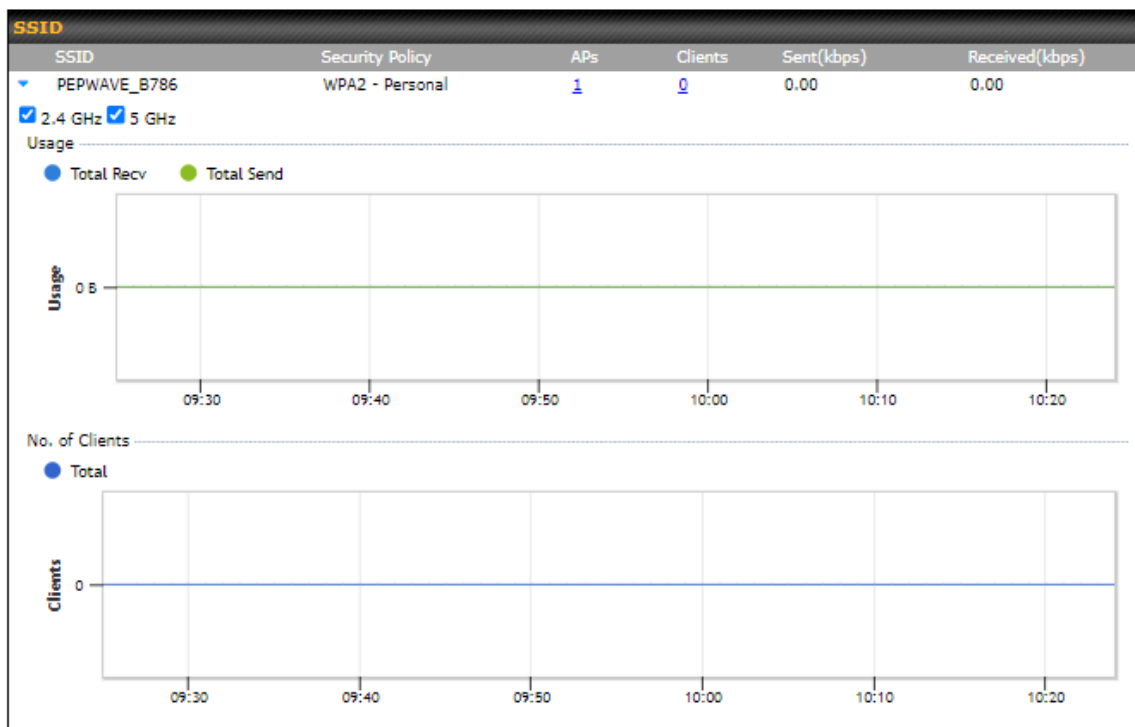


6.2.2. Wireless SSID

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

SSID					
SSID	Security Policy	APs	Clients	Sent(kbps)	Received(kbps)
▶ PEPWAVE_B786	WPA2 - Personal	1	0	0.00	0.00

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



6.2.3. Wireless Client

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

Search Filter

Search Key

Client MAC Address / SSID / AP Serial Number

Maximum Result (1-256)

50


Show Associated Clients Only

☐

Search Result


Search

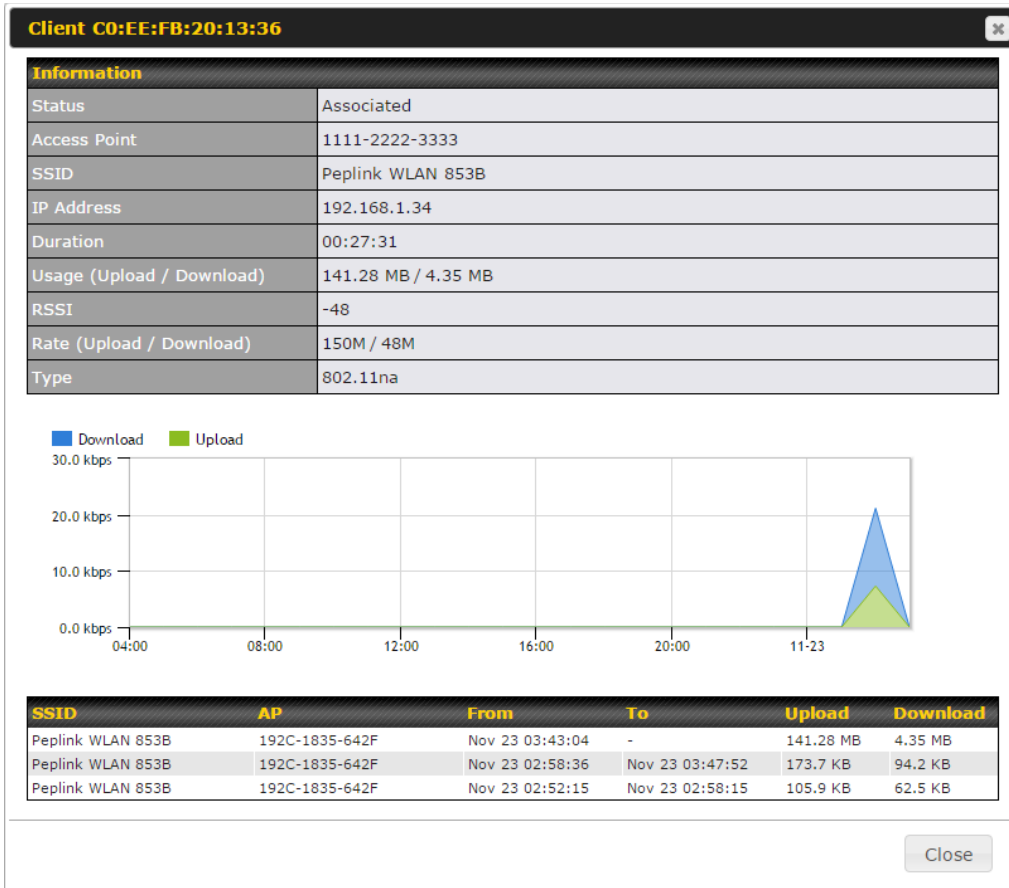
Wireless Clients

Name / MAC Address ▲	IP Address	Type	Mode	RSSI (dBm)	SSID	AP	Duration	
HUAWEI_Mate_40_P...	-	802.11ng		-	-	-	-	☆ 

Top 10 Clients of last hour (Updated at 16:00)

Client	Upload	Download
No information		

Here, you will be able to see your network's heaviest users as well as search for specific users. Click the ☆ icon to bookmark specific users, and click the  icon for additional details about each user:



6.2.4. Nearby Device

A listing of near devices can be accessed by navigating to **AP > Status > Nearby Device**.

Search Filter

Search Key

MAC Address / SSID

Type

All

Maximum Result (1-999)

200

Time

From









































hh:mm

to

hh:mm



Search

Nearby Devices

Mark	Type	MAC Address	SSID	Channel	Encryption	Last Seen	Mark as
	Station Probe	8C:F8:C5:BE:3B:C9	-	36		1 minute ago	 
	Station Probe	F8:5E:A0:A4:68:F7	-	36		1 minute ago	 
	Station Probe	70:3E:97:05:C5:30	-	11		1 minute ago	 
	Station Probe	A8:C0:EA:37:8F:E8	-	36		1 minute ago	 
	Station Probe	68:5D:43:F5:C6:93	-	11		1 minute ago	 
	Station Probe	84:1B:77:37:D3:4F	-	36		1 minute ago	 
	Station Probe	DC:21:48:1D:D3:1F	-	11		1 minute ago	 
	Station Probe	F4:7B:09:EA:E0:ED	-	36		1 minute ago	 
	AP	A8:C0:EA:34:D9:85	Pismo Research	6	WPA2	1 minute ago	 
	AP	A8:C0:EA:34:D9:86	Guest	6	WPA2	1 minute ago	 
	AP	A8:C0:EA:34:D9:87	Pismo Research Tech	6	WPA2	1 minute ago	 
	Station Probe	00:21:6B:D5:B5:7E	-	36		1 minute ago	 
	Station Probe	10:56:CA:83:43:C8	-	36		1 minute ago	 
	Station Probe	40:F0:2F:88:2F:1E	-	36		1 minute ago	 
	Station Probe	E8:1C:BA:73:EB:07	-	11		1 minute ago	 
	Station Probe	C8:94:02:1B:00:65	-	11		1 minute ago	 
	AP	A8:C0:EA:26:F9:24	PEPWAVE_34CC	3	WPA2	1 minute ago	 
	Station Probe	54:14:F3:C0:5D:C3	-	36		1 minute ago	 
	AP	10:56:CA:66:F7:28	PEPLINK_465C	1	WPA2	1 minute ago	 
	AP	A8:C0:EA:73:12:E9	P WiFi	1	WPA2/WPA3	1 minute ago	 

Prev 1-20 (200) Next

Suspected Rogue Devices

Hovering over the device MAC address will result in a popup with information on how this device was detected. Click the   icons and the device will be moved to the bottom table of identified devices.

6.2.5. Event Log

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

Filter	
Search key	<input type="text" value="Client MAC Address / Wireless SSID"/>
Time	From <input type="text" value=""/> hh:mm to <input type="text" value=""/> hh:mm
Alerts only	<input type="checkbox"/>
<input type="button" value="Search"/>	

Event Log ✓ Auto refresh	
Jan 18 17:09:41	Channel changed from 6 to 11

Events

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

7. System Tab

7.1. Admin Security

There are two types of user accounts available for accessing the web admin: *admin* and *user*. They represent two user levels: the admin level has full administrative access, while the user level is read-only. The user level can access only the device's status information; users cannot make any changes on the device.

A web login session will be logged out automatically when it has been idle longer than the **Web Session Timeout**. Before the session expires, you may click the **Logout** button in the web admin to exit the session.

0 hours 0 minutes signifies an unlimited session time. This setting should be used only in special situations, as it will lower the system security level if users do not log out before closing the browser. The **default** is 4 hours, 0 minutes.

For security reasons, after logging in to the web admin Interface for the first time, it is recommended to change the administrator password. Configuring the administration interface to be accessible only from the LAN can further improve system security. Administrative settings configuration is located at **System > Admin Security**.

Admin Settings ?		
Device Name	DCS_B786	hostname: dcs-b786
Admin User Name	admin	
Admin Password	••••••••	
Confirm Admin Password	••••••••	
Read-only User Name	user	
User Password		
Confirm User Password		
Web Session Timeout ?	4 Hours 0 Minutes	
Authentication Method ?	<input checked="" type="radio"/> Local Account <input type="radio"/> RADIUS <input type="radio"/> TACACS+	
Security	HTTP / HTTPS ▼ <input checked="" type="checkbox"/> Redirect HTTP to HTTPS	
Web Admin Access	HTTP: LAN Only HTTPS: LAN Only ▼	
Web Admin Port	HTTP: 80 HTTPS: 443	

Admin Settings	
Device Name	This field allows you to define a name for this Pepwave router. By default, Device Name is set as DCS_XXXX , where XXXX refers to the last 4 digits of the unit's serial number.
Admin User Name	Admin User Name is set as <i>admin</i> by default, but can be changed, if desired.
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	Read-only User Name is set as <i>user</i> by default, but can be changed, if desired.
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm User Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to 4 hours .
Authentication Method	<p>With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.</p> <p>Available options:</p> <ul style="list-style-type: none"> • Local Account • RADIUS

Authentication Method	? <input type="radio"/> Local Account <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+
Authentication Protocol	MS-CHAP v2 ▼
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles
Authentication Host	
Authentication Port	1812
Authentication Secret	<input type="password"/> <input checked="" type="checkbox"/> Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles
Accounting Host	
Accounting Port	1813
Accounting Secret	<input type="password"/> <input checked="" type="checkbox"/> Hide Characters
Authentication Timeout	3 seconds

Authentication Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
Authentication Host	This specifies the IP address or hostname of the RADIUS server host.
Authentication Port	This setting specifies the UDP destination port for authentication requests.
Authentication Secret	This field is for entering the secret key for accessing the RADIUS server.
Accounting Host	This specifies the IP address or hostname of the RADIUS server host.
Accounting Port	This setting specifies the UDP destination port for accounting requests.
Accounting Secret	This field is for entering the secret key for accessing the accounting server.
Authentication Timeout	This option specifies the time value for authentication timeout

- TACACS+

Authentication Method	? <input type="radio"/> Local Account <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+
TACACS+ Server	
TACACS+ Server Secret	<input type="password"/> <input checked="" type="checkbox"/> Hide Characters
TACACS+ Server Timeout	3 seconds

TACACS+ Server	This specifies the access address of the
-----------------------	--

	external TACACS+ server.
TACACS+ Server Secret	This field is for entering the secret key for accessing the RADIUS server.
TACACS+ Server Timeout	This option specifies the time value for TACACS+ timeout
Security	<p>This option is for specifying the protocol(s) through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/HTTPS <p>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface</p>
Web Admin Access	<p>This option is for specifying the network interfaces through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> • LAN only • LAN/WAN <p>If LAN/WAN is chosen, the WAN Connection Access Settings form will be displayed.</p>
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.

7.2. Operating Mode

Operating Mode can be accessed at **System > Operating Mode**. The operating mode can be changed between **Router or Bridge Mode or Bridge Mode, without LAN IP address**.

Operating Mode

Select the operating mode you want to use for this device:

☒ Router Mode
 ☐ Bridge Mode
 ☐ Bridge Mode, without LAN IP address

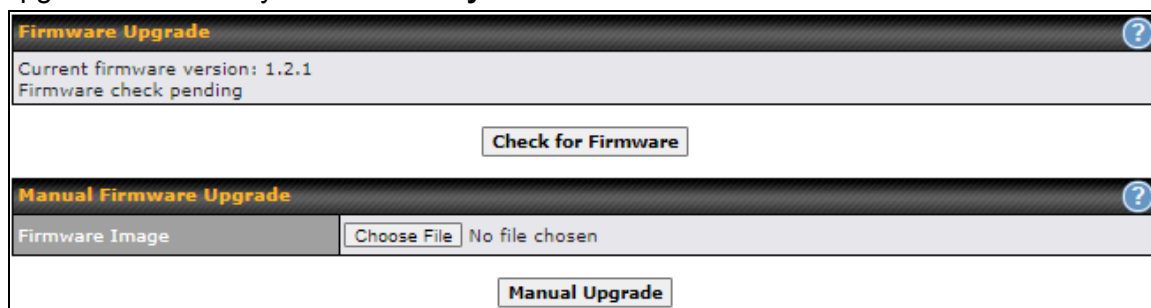
Save and Apply

Operating Mode

Operating Mode Your device can act as a bridge or as a router, depending on your selection here.

7.3. Firmware

Pepwave router firmware is upgradeable through the web admin interface. Firmware upgrade functionality is located at **System > Firmware**.



There are two ways to upgrade the unit. The first method is through an online download. The second method is to upload a firmware file manually.

To perform an online download, click on the **Check for Firmware** button. The Pepwave router will check online for new firmware. If new firmware is available, the Pepwave router will automatically download the firmware. The rest of the upgrade process will be automatically initiated.

You may also download a firmware image from the Peplink website and update the unit manually. To update using a firmware image, click **Choose File** to select the firmware file from the local computer, and then click **Manual Upgrade** to send the firmware to the Pepwave router. It will then automatically initiate the firmware upgrade process.

Please note that all Peplink devices can store two different firmware versions in two different partitions. A firmware upgrade will always replace the inactive partition. If you want to keep the inactive firmware, you can simply reboot your device with the inactive firmware and then perform the firmware upgrade.

Important Note

The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. Do not disconnect the power during firmware upgrade process. Do not attempt to upload a non-firmware file or a

firmware file that is not supported by Peplink. Upgrading the Pepwave router with an invalid firmware file will damage the unit and may void the warranty.

Important Note

If the firmware is rolled back from 5.x to 4.x, the configurations will be lost.

7.4. Time

Time Settings enables the system clock of the Pepwave router to be synchronized with a specified time server. Time settings are located at **System > Time**.

Time Settings	
Time Zone	<div>(GMT) Casablanca</div> <div><input type="checkbox"/> Show all</div>
Time Server	0.pepwave.pool.ntp.org
<div>Save</div>	

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

7.5. Schedule

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

Name	Time	Used by
No schedule profile defined		
<div>New Schedule</div>		

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

[illegible]

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

7.6. Email Notification

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

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	<input type="text"/> <input checked="" type="checkbox"/> Require authentication
Connection Security	None ▼
SMTP Port	25
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Confirm SMTP Password	<input type="password"/>
Sender's Email Address	<input type="text"/>
Recipient's Email Address	<input type="text"/>
<input type="button" value="Test Email Notification"/> <input type="button" value="Save"/>	

Email Notification Settings	
Email Notification	This setting specifies whether or not to enable email notification. If Enable is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If Enable is not checked, email notification is disabled and the Pepwave router will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check Require authentication .
Connectivity Security	This setting specifies via a drop-down menu one of the following valid Connection Security: <ul style="list-style-type: none"> None STARTTLS SSL/TLS
SSL Encryption	Check the box to enable SMTPS. When the box is checked, SMTP Port will be changed to 465 automatically.

SMTP Port	<p>This field is for specifying the SMTP port number. By default, this is set to 25. If Connection Security is selected “STARTTLS”, the default port number will be set to 587. If Connection Security is selected “SSL/TLS”, the default port number will be set to 465.</p> <p>You may customize the port number by editing this field.</p>
SMTP User Name / Password	<p>This setting specifies the SMTP username and password while sending email. These options are shown only if Require authentication is checked in the SMTP Server setting.</p>
Confirm SMTP Password	<p>This field allows you to verify and confirm the new administrator password.</p>
Sender's Email Address	<p>This setting specifies the email address the Pepwave router will use to send reports.</p>
Recipient's Email Address	<p>This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the enter key.</p>

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

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com
<div> <input type="button" value="Send Test Notification"/> <input type="button" value="Cancel"/> </div>	

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

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

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	<input type="text"/> <input checked="" type="checkbox"/> Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Confirm SMTP Password	<input type="password"/>
Sender's Email Address	<input type="text"/>
Recipient's Email Address	<input type="text"/>

Test Email Notification Save

Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
<- 220 smtp.gmail.com ESMTP h11sm3907691pjj.46 - gsmt
-> EHLO balance.peplink.com
<- 250-smtp.gmail.com at your service, [14.192.209.255]
<- 250-SIZE 35882577
<- 250-8BITMIME
<- 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
<- 250-ENHANCEDSTATUSCODES
<- 250-PIPELINING
<- 250-CHUNKING
<- 250 SMTPUTF8
-> AUTH PLAIN AGdwc2dhbjk0QGdtVWlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

7.7. Event Log

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

Send Events to Remote Syslog Server	
Remote Syslog	<input type="checkbox"/>
Remote Syslog Host	<input type="text"/>
Port:	<input type="text" value="514"/>
Push Events to Mobile Devices	
Push Events	<input type="checkbox"/>
URL Logging	
Enable	<input type="checkbox"/>
Session Logging	
Enable	<input type="checkbox"/>
<input type="button" value="Save"/>	

Event Log Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
Push Events	The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature.
URL Logging	This setting is to enable event logging at the specified log server.
URL Logging Host	This setting specifies the IP address or hostname of the URL log server.
Session Logging	This setting is to enable event logging at the specified log server.
Session Logging Host	This setting specifies the IP address or hostname of the Session log server.



For more information on the Router Utility, go to:
www.peplink.com/products/router-utility

7.8. SNMP

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

SNMP Settings	
SNMP Device Name	DCS_####6
Location	<input type="text"/>
SNMP Port	<input type="text" value="161"/> <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
SNMP Trap	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		
<input type="button" value="Add SNMP Community"/>		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		
<input type="button" value="Add SNMP User"/>		

SNMP Settings

SNMP Device Name	This field shows the router name defined at System>Admin Security .
SNMP Port	This option specifies the port which SNMP will use. The default port is 161 .
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.
SNMP Trap	This option allows you to enable SNMP Trap. If enabled, the following entry fields will appear.

SNMP Trap Community	This setting specifies the SNMP Trap community name.
SNMP Trap Server	Enter the IP address of the SNMP Trap server.

To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:

SNMP Community

Community Name	<input type="text" value="My Company"/>
Allowed Network	<input type="text" value="192.168.1.25"/> / <input type="text" value="255.255.255.0 (/24)"/>

SNMP Community	
Community Name	This setting specifies the SNMP community name.
Allowed Network	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., 192.168.1.0) and select the appropriate subnet mask.

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

SNMPv3 User

User Name	<input type="text" value="SNMPUser"/>
Authentication	<input type="text" value="SHA"/> <input type="text" value="password"/>
Privacy	<input type="text" value="DES"/> <input type="text" value="privacypassword"/>

SNMPv3 User	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication	<p>This setting specifies via a drop-down menu one of the following valid authentication protocols:</p> <ul style="list-style-type: none"> • NONE • MD5 • SHA <p>When MD5 or SHA is selected, an entry field will appear for the password.</p>
Privacy	<p>This setting specifies via a drop-down menu one of the following valid privacy protocols:</p> <ul style="list-style-type: none"> • NONE • DES <p>When DES is selected, an entry field will appear for the password.</p>

7.9. InControl

Controller Management Settings	
Controller	<input data-bbox="548 1077 576 1108" type="button" value="?"/> <input type="text" value="InControl"/> <input type="checkbox"/> Restricted to Status Reporting Only
Privately Host InControl	<input type="checkbox"/>

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

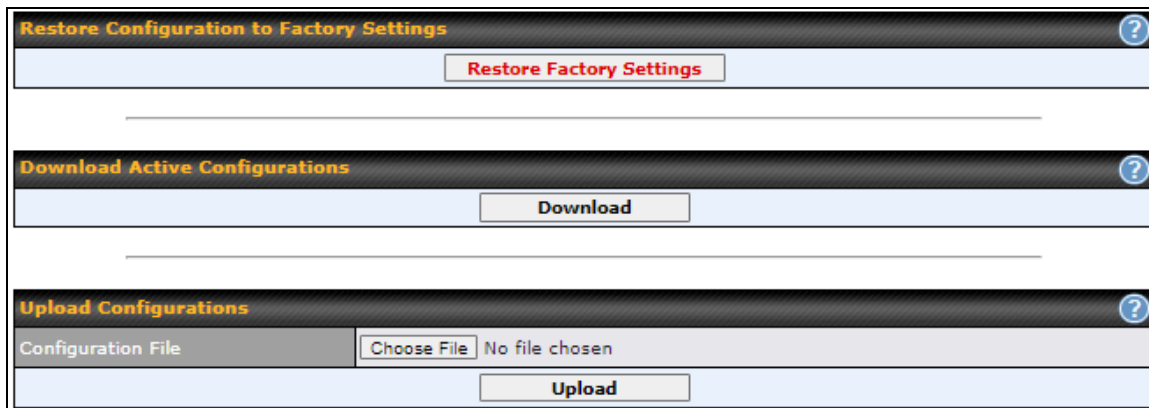
When this check box is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

Alternately, you could also privately host InControl. Simply check the box beside the "Privately Host InControl" open, and enter the IP Address of your InControl Host.

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

7.10. Configuration

Backing up Pepwave router settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Pepwave router settings is found at **System > Configuration**. Note that available options vary by model.



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

7.11. Feature Add-ons

Pepwave devices have features that can be activated upon purchase. Once the purchase is complete, you will receive an activation key. Enter the key in the **Activation Key** field, click **Activate**, and then click **Apply Changes**

Feature Activation	
Activation Key	

7.12. Reboot

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

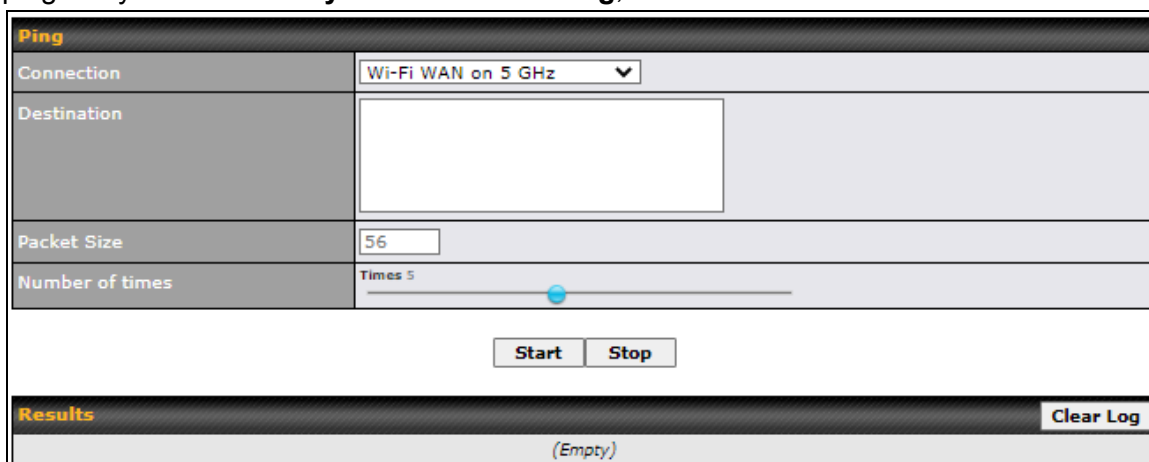
Please note that a firmware upgrade will always replace the inactive firmware partition.

Reboot System ?	
Select the firmware you want to use to start up this device:	
<input checked="" type="radio"/> Firmware 1: 1.2.1 build 4900 (Running)	
<input type="radio"/> Firmware 2: 1.2.0s003 build 4892	
<input type="button" value="Reboot"/>	

8. Tools

8.1. Ping

The ping test tool sends pings through a specified Ethernet interface or a VPN connection. You can specify the number of pings in the field Number of times, to a maximum number of 10 times. Packet Size can be set to a maximum of 1472 bytes. The ping utility is located at **System > Tools > Ping**, illustrated below:



The screenshot shows the 'Ping' utility interface. It has a title bar 'Ping' and a 'Clear Log' button in the top right. The interface is divided into two main sections: 'Configuration' and 'Results'.

Connection	Wi-Fi WAN on 5 GHz ▼
Destination	<input type="text"/>
Packet Size	56
Number of times	Times 5 <input type="range"/>

Below the configuration fields are 'Start' and 'Stop' buttons. The 'Results' section at the bottom shows '(Empty)' and a 'Clear Log' button.

Tip

A system administrator can use the ping utility to manually check the connectivity of a particular LAN/WAN connection.

8.2. Traceroute

The traceroute test tool traces the routing path to the destination through a particular Ethernet interface or a SpeedFusion connection. The traceroute test utility is located at **System > Tools > Traceroute**.

Traceroute

Connection

WAN 1

Destination

64.233.189.99

Start

Stop

Results

Clear Log

```

Traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 100 bytes packet size
 0 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 1 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 2 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 3 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 4 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 5 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 6 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 7 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 8 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 9 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 10 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 11 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 12 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 13 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 14 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 15 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 16 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 17 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 18 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 19 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 20 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 21 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 22 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 23 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 24 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 25 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 26 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 27 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 28 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 29 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
 30 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.000 ms 0.000 ms 0.000 ms
  
```

Tip

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

8.3. Wake-on-LAN

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

Wake-on-LAN

Wake-on-LAN Target

Custom MAC Address... 00:00:00:00:00:00

Send

Select a client from the drop-down list and click **Send** to send a “magic packet”.

8.4. WAN Analysis

The WAN Analysis feature allows you to run a WAN to WAN speed test between 2 Pepwave devices .

You can set a device up as a **Server** or a **Client**. One device must be set up as a server to run the speed tests and the server must have a public IP address.

WAN Performance Analysis

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



As a server

For the peer who has public IP addresses to accept connection.



As a client

For the peer to initiate connection.

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

WAN Performance Analysis

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

Server Settings

Status	<input checked="" type="checkbox"/> Listening (Control Port: 6000)
Control Port	<input type="text" value="6000"/>

WAN Connection Status

1 WAN 1	<input checked="" type="checkbox"/> 10.22.1.182
2 WAN 2	<input type="checkbox"/> Disabled
3 WAN 3	<input type="checkbox"/> Disabled
4 WAN 4	<input type="checkbox"/> Disabled
5 WAN 5	<input type="checkbox"/> Disabled
Mobile Internet	<input type="checkbox"/> Disabled

The client side has a few more settings that can be changed. Make sure that the **Control Port** matches what's been entered on the server side. Select the WAN(s) that will be used for testing and enter the Servers WAN IP address. Once all of the options have been set, click the **Start Test** button.

WAN Performance Analysis

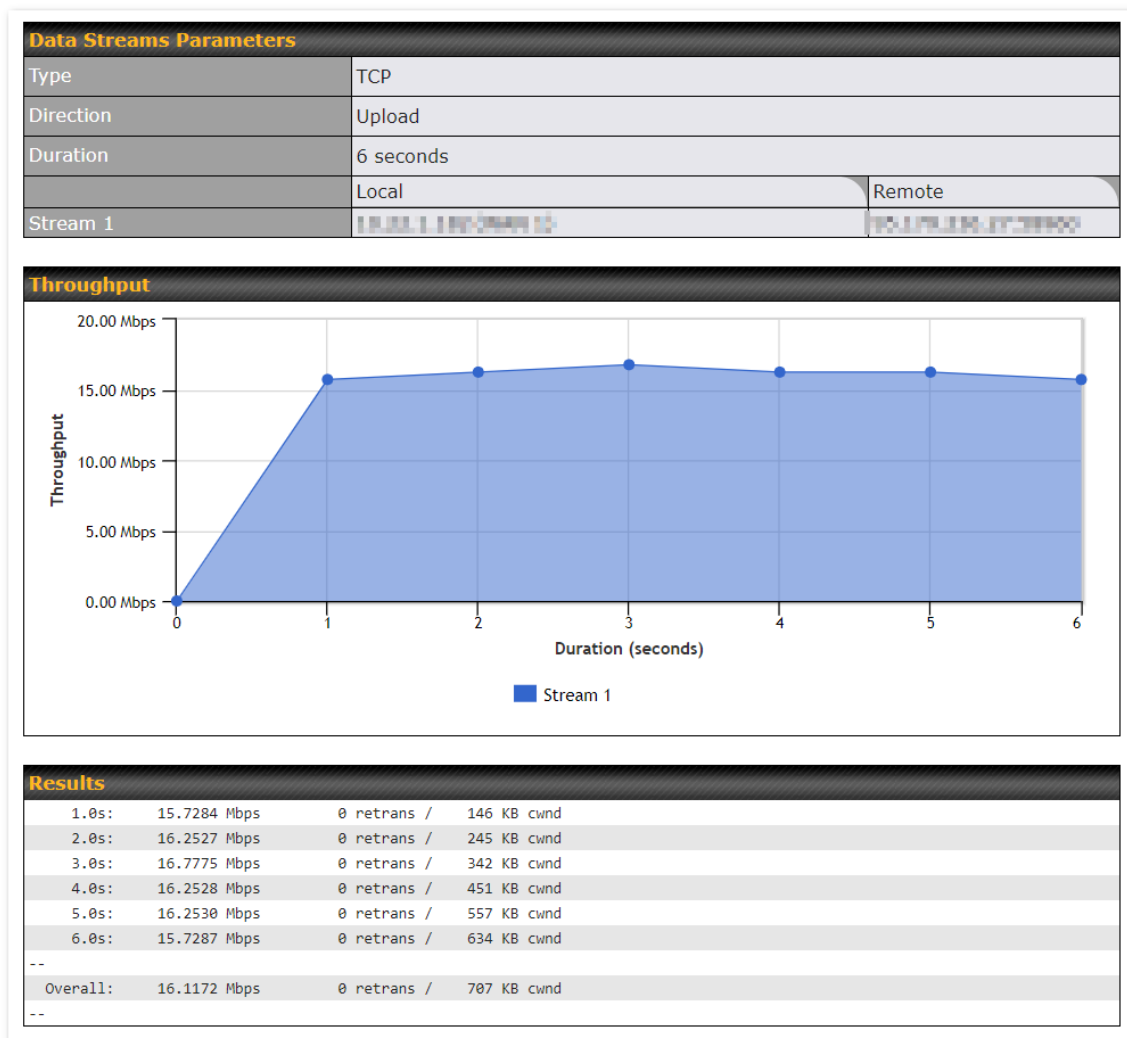
Check your point-to-point WAN performance with another peer

Client Settings	
Control Port	6000
Data Port	57280 - 57287
Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download
Duration	20 seconds (5 - 600)

Data Streams	
Local WAN Connection	Remote IP Address
1. -- Not Used --	
2. -- Not Used --	
3. -- Not Used --	
4. -- Not Used --	
5. -- Not Used --	
6. -- Not Used --	
7. -- Not Used --	
8. -- Not Used --	

[Start Test](#)

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



The test can be run again once it's complete by clicking the **Start** button or you can click **Close** and change the parameters for the test.

9. Status

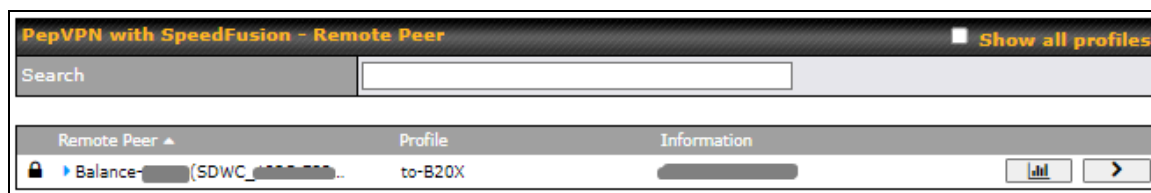
9.1. Device

System information is located at **Status > Device**.

System Information	
Device Name	DCS-B786
Model	Pepwave Device Connector Rugged
Hardware Revision	1
Serial Number	2933-2411-B786
Firmware	1.2.1 build 4900
PepVPN Version	10.0.0
Host Name	dcs-b786
Uptime	1 day 11 hours 53 minutes
System Time	Fri Jan 20 00:29:02 +08 2023
Diagnostic Report	Download


System Information	
Device Name	This is the name specified in the Device Name field located at System > Admin Security .
Model	This shows the model name and number of this device.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version this device is currently running.
PepVPN Version	This shows the current PepVPN version.
Host Name	The host name assigned to the Pepwave router appears here.
Uptime	This shows the length of time since the device has been rebooted.
System Time	This shows the current system time.

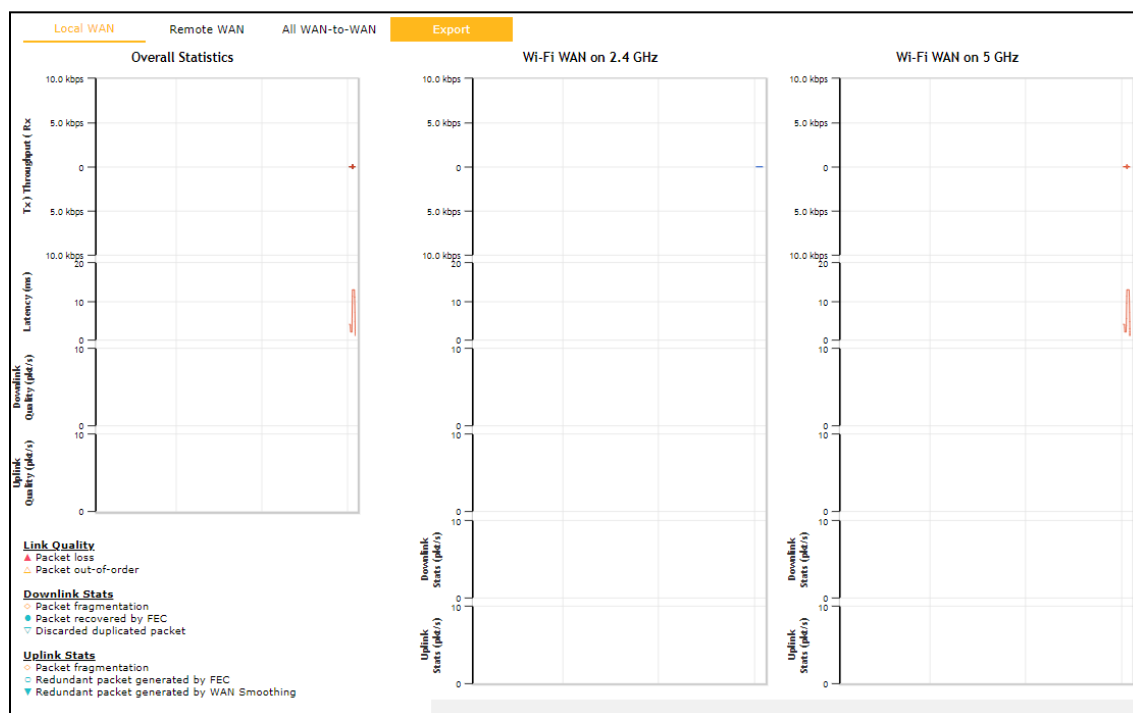
9.3. SpeedFusion



Current PepVPN with SpeedFusion Remote Peer status information is located at **Status > SpeedFusion**. Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.

PepVPN with SpeedFusion - Remote Peer		Show all profiles
Search		
Remote Peer	Profile	Information
Balance- (SDWC_...)	to-B20X	
Wi-Fi WAN on 2.4 GHz		Not available - WAN disabled
Wi-Fi WAN on 5 GHz	Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 1 ms	
Total	Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s	

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



When pressing the  button, the following menu will appear:

PepVPN Details

Connection Information

Profile

to-B20X

Remote ID

Device Name

Serial Number

More information

WAN Statistics

Remote Connections

☐ Show remote connections

WAN Label

☒ WAN Name
☐ IP Address and Port

Wi-Fi WAN on 2.4 GHz

Not available - WAN disabled

Wi-Fi WAN on 5 GHz

Rx:

< 1 kbps

Tx:

< 1 kbps

Loss rate:

0.0 pkt/s

Latency:

1 ms

Total

Rx:

< 1 kbps

Tx:

< 1 kbps

Loss rate:

0.0 pkt/s

PepVPN Test Configuration

Type

☒ TCP
☐ UDP

Streams

4

Direction

☒ Upload
☐ Download

Duration

20 seconds (5 - 600)

Start

PepVPN Test Results

No information

Close

The **connection information** shows the details of the selected PepVPN profile, consisting of the Profile name, **Router ID**, **Router Name** and **Serial Number** of the remote router

Advanced features for the PepVPN profile will also be shown when the **More Information** checkbox is selected.




The **WAN statistics** show information about the local and remote WAN connections (when **show Remote connections**) is selected.

The available details are **WAN Name**, **IP address** and **port** used for the Speedfusion connection. **Rx and Tx rates**, **Loss rate** and **Latency**.


Connections can be temporarily disabled by sliding the switch button next to a WAN connection to the left.

The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15 minutes without any action.

This can be used when testing the PepVPN speed between two locations to see if there is interference or network congestion between certain WAN connections.

WAN Statistics 									
Remote Connections		<input checked="" type="checkbox"/> Show remote connections							
WAN Label		<input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port							
 Wi-Fi WAN on 2.4 GHz		Not available - WAN disabled							
 Wi-Fi WAN on 5 GHz									
<input checked="" type="radio"/> WAN		Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s	Latency:	1 ms
Total		Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s		
The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15 minutes without any action.									

The PepVPN test configuration allows us to configure and perform thorough tests. This is usually done after the initial installation of the routers and in case there are problems with aggregation.

PepVPN Test Configuration 				
Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP		<div>Start</div>	
Streams	4 ▼			
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download			
Duration	20 seconds (5 - 600)			

Press the **Start** button to perform throughput test according to the configured options.

If **TCP** is selected, 4 parallel streams will be generated to get the optimal results by default. This can be customized by selecting a different value of streams.

Using more streams will typically get better results if the latency of the tunnel is high.

SpeedFusion VPN Test Results			
1.0s:	16.2527 Mbps	0 retrans /	306 KB cwnd
2.0s:	20.4445 Mbps	0 retrans /	306 KB cwnd
3.0s:	18.3526 Mbps	0 retrans /	306 KB cwnd
4.0s:	17.8258 Mbps	0 retrans /	306 KB cwnd
5.0s:	17.3014 Mbps	0 retrans /	306 KB cwnd
6.0s:	14.1558 Mbps	0 retrans /	306 KB cwnd
7.0s:	18.3500 Mbps	0 retrans /	306 KB cwnd
8.0s:	15.7252 Mbps	0 retrans /	306 KB cwnd
9.0s:	17.2932 Mbps	0 retrans /	306 KB cwnd
10.0s:	20.4591 Mbps	0 retrans /	306 KB cwnd
11.0s:	11.5347 Mbps	0 retrans /	306 KB cwnd
12.0s:	15.2043 Mbps	0 retrans /	306 KB cwnd
13.0s:	12.0584 Mbps	0 retrans /	306 KB cwnd
14.0s:	13.1074 Mbps	0 retrans /	306 KB cwnd
15.0s:	10.4849 Mbps	0 retrans /	306 KB cwnd
16.0s:	12.5838 Mbps	0 retrans /	306 KB cwnd
17.0s:	15.2043 Mbps	0 retrans /	306 KB cwnd
18.0s:	16.2486 Mbps	0 retrans /	306 KB cwnd
19.0s:	18.8789 Mbps	0 retrans /	306 KB cwnd
20.0s:	18.3491 Mbps	0 retrans /	306 KB cwnd
--			
Stream 1:	3.9913 Mbps	0 retrans /	78 KB cwnd
Stream 2:	3.9728 Mbps	0 retrans /	74 KB cwnd
Stream 3:	3.9879 Mbps	0 retrans /	75 KB cwnd
Stream 4:	4.0044 Mbps	0 retrans /	79 KB cwnd
Overall:	15.9564 Mbps	0 retrans /	306 KB cwnd
--			
TEST DONE			

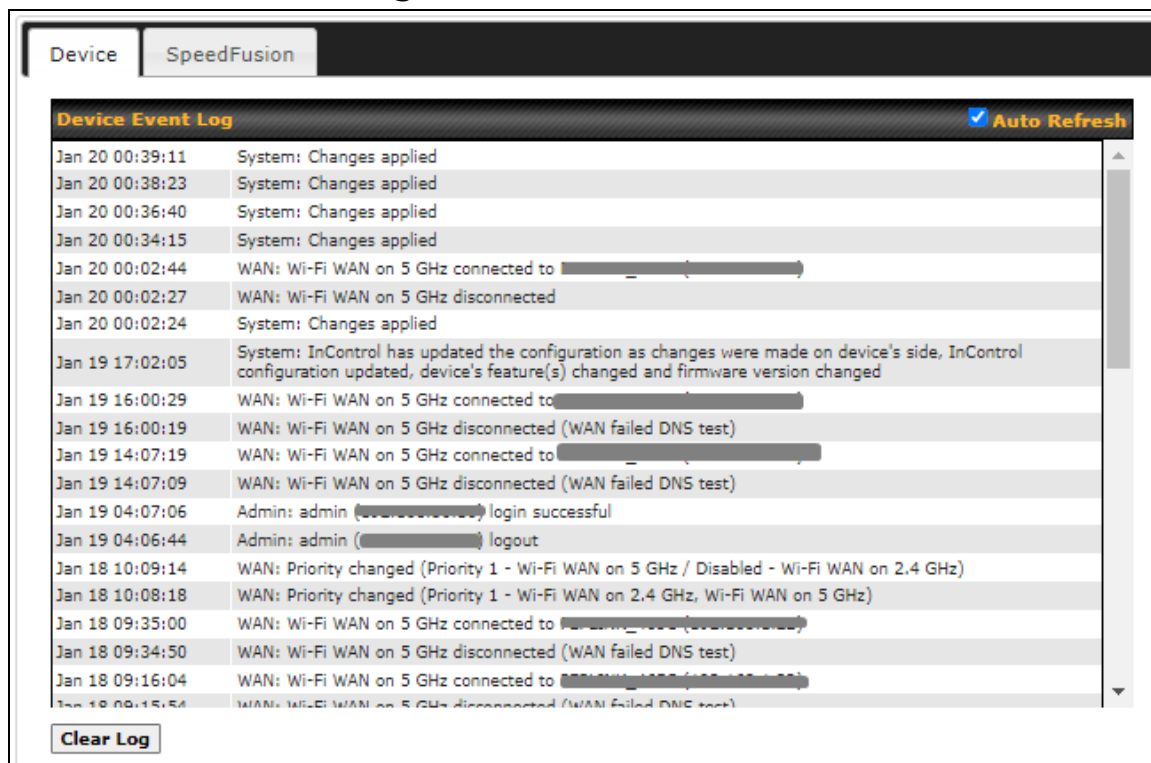
Peplink also published a whitepaper about Speedfusion which can be downloaded from the following url:

<http://download.peplink.com/resources/whitepaper-speedfusion-and-best-practices-2019.pdf>

9.4. Event log

Event log information is located at **Status > Event Log**.

9.4.1. Device Event Log



The screenshot displays the 'Device Event Log' for a device named 'SpeedFusion'. The log contains the following entries:

Timestamp	Event Description
Jan 20 00:39:11	System: Changes applied
Jan 20 00:38:23	System: Changes applied
Jan 20 00:36:40	System: Changes applied
Jan 20 00:34:15	System: Changes applied
Jan 20 00:02:44	WAN: Wi-Fi WAN on 5 GHz connected to [REDACTED]
Jan 20 00:02:27	WAN: Wi-Fi WAN on 5 GHz disconnected
Jan 20 00:02:24	System: Changes applied
Jan 19 17:02:05	System: InControl has updated the configuration as changes were made on device's side, InControl configuration updated, device's feature(s) changed and firmware version changed
Jan 19 16:00:29	WAN: Wi-Fi WAN on 5 GHz connected to [REDACTED]
Jan 19 16:00:19	WAN: Wi-Fi WAN on 5 GHz disconnected (WAN failed DNS test)
Jan 19 14:07:19	WAN: Wi-Fi WAN on 5 GHz connected to [REDACTED]
Jan 19 14:07:09	WAN: Wi-Fi WAN on 5 GHz disconnected (WAN failed DNS test)
Jan 19 04:07:06	Admin: admin ([REDACTED]) login successful
Jan 19 04:06:44	Admin: admin ([REDACTED]) logout
Jan 18 10:09:14	WAN: Priority changed (Priority 1 - Wi-Fi WAN on 5 GHz / Disabled - Wi-Fi WAN on 2.4 GHz)
Jan 18 10:08:18	WAN: Priority changed (Priority 1 - Wi-Fi WAN on 2.4 GHz, Wi-Fi WAN on 5 GHz)
Jan 18 09:35:00	WAN: Wi-Fi WAN on 5 GHz connected to [REDACTED]
Jan 18 09:34:50	WAN: Wi-Fi WAN on 5 GHz disconnected (WAN failed DNS test)
Jan 18 09:16:04	WAN: Wi-Fi WAN on 5 GHz connected to [REDACTED]
Jan 18 09:15:54	WAN: Wi-Fi WAN on 5 GHz disconnected (WAN failed DNS test)

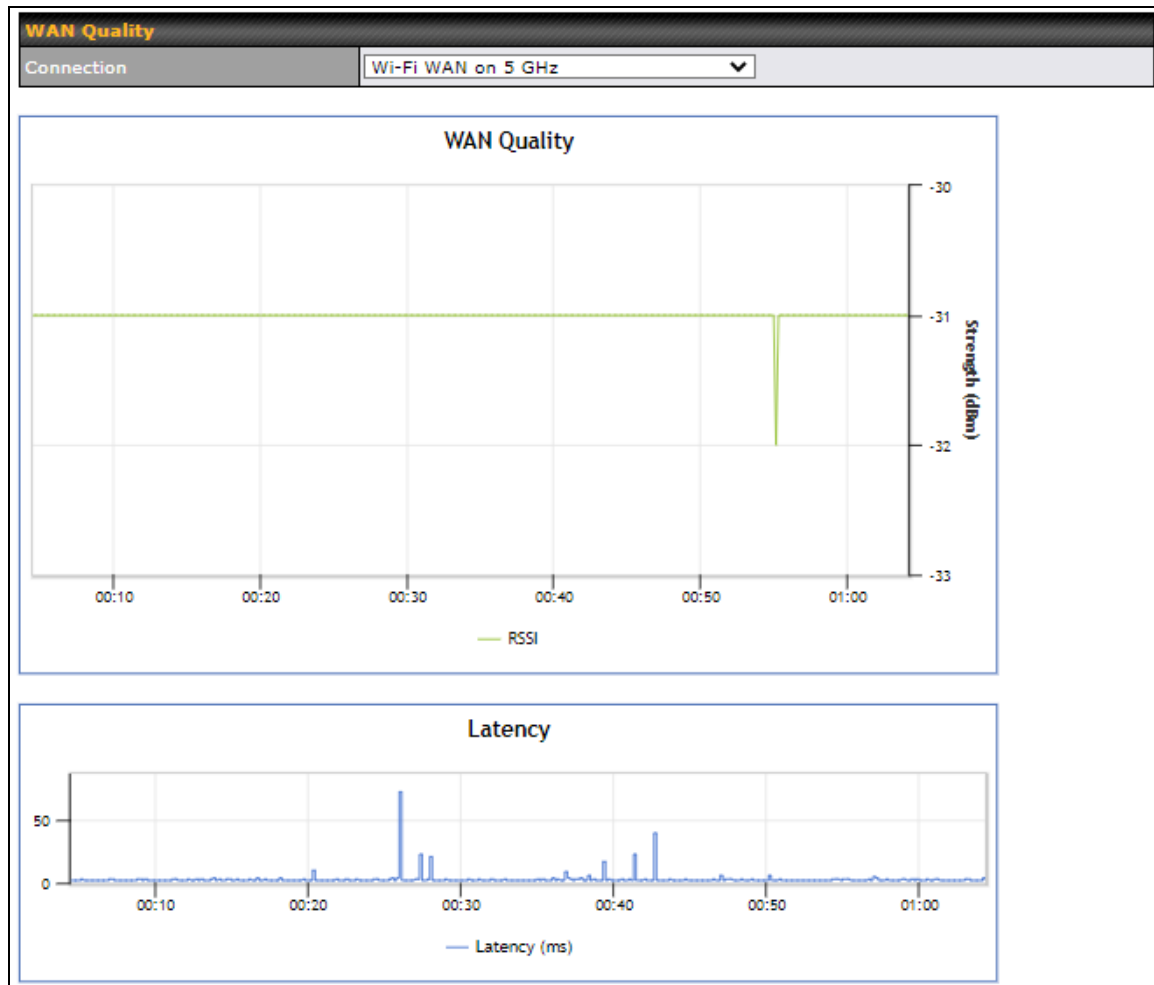
At the bottom of the log, there is a 'Clear Log' button.

The log section displays a list of events that has taken place on the Pepwave router. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

9.4.2. SpeedFusion Event Log

10. WAN Quality

The **Status > WAN Quality** allow to show detailed information about each connected WAN connection.



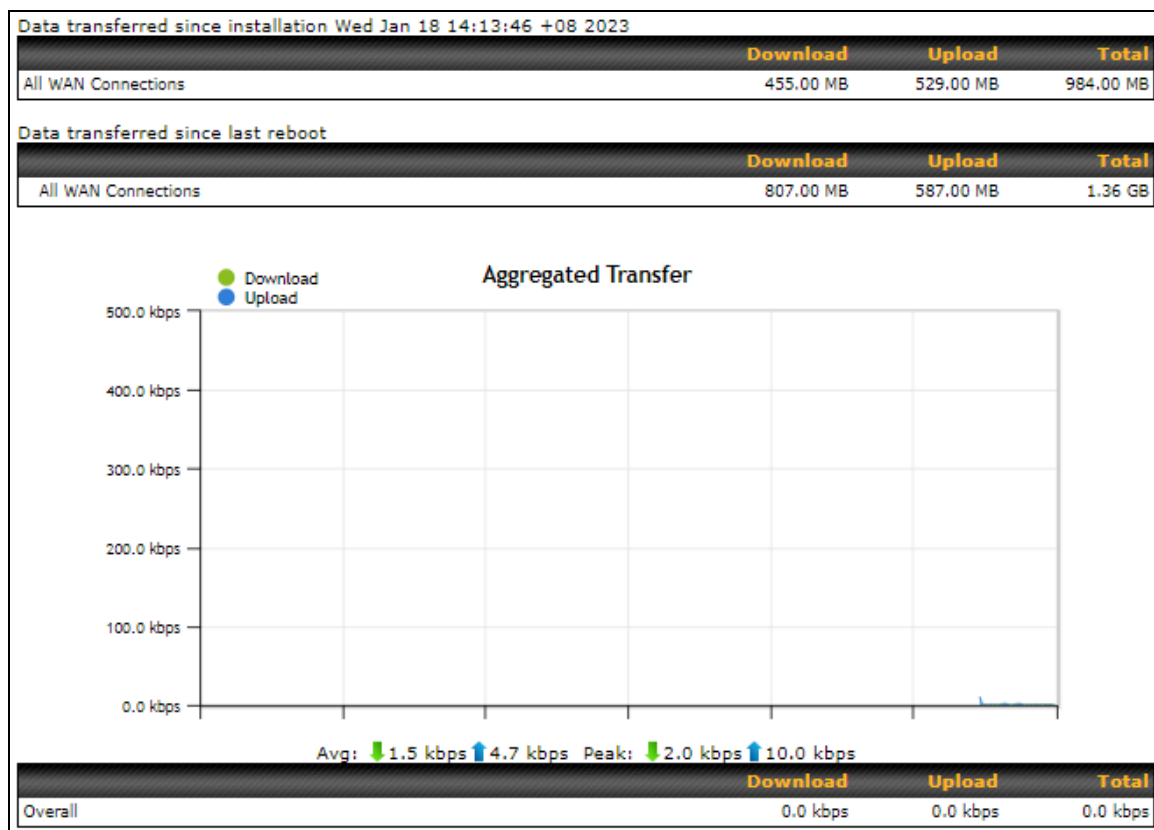
11. Usage Reports

This section shows bandwidth usage statistics and is located at **Status > Usage Reports**

Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

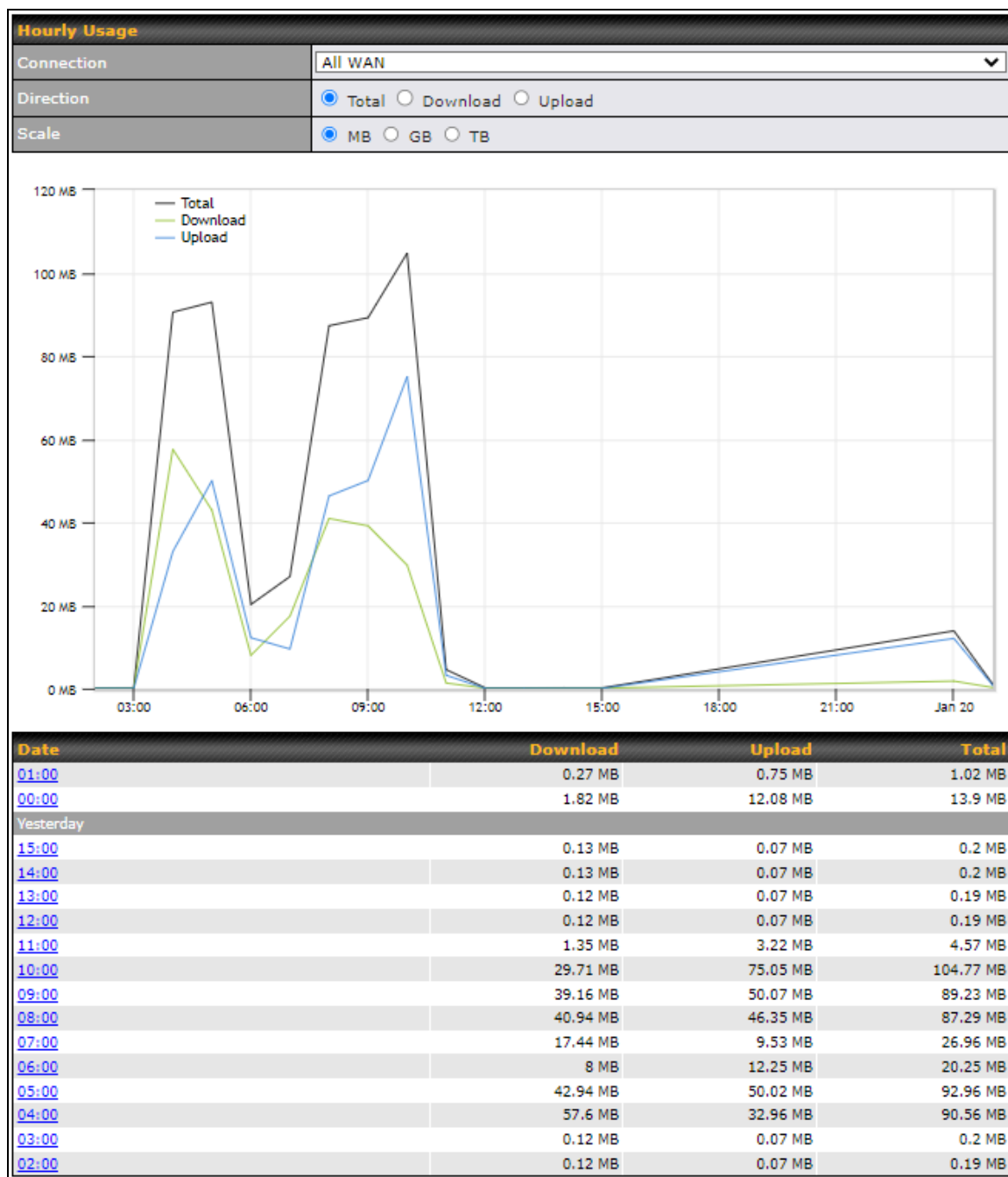
11.1. Real-Time

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



11.2. Hourly

This page shows the hourly bandwidth usage for all WAN connections, with the option of viewing each individual connection. Select the desired connection to check from the drop-down menu.

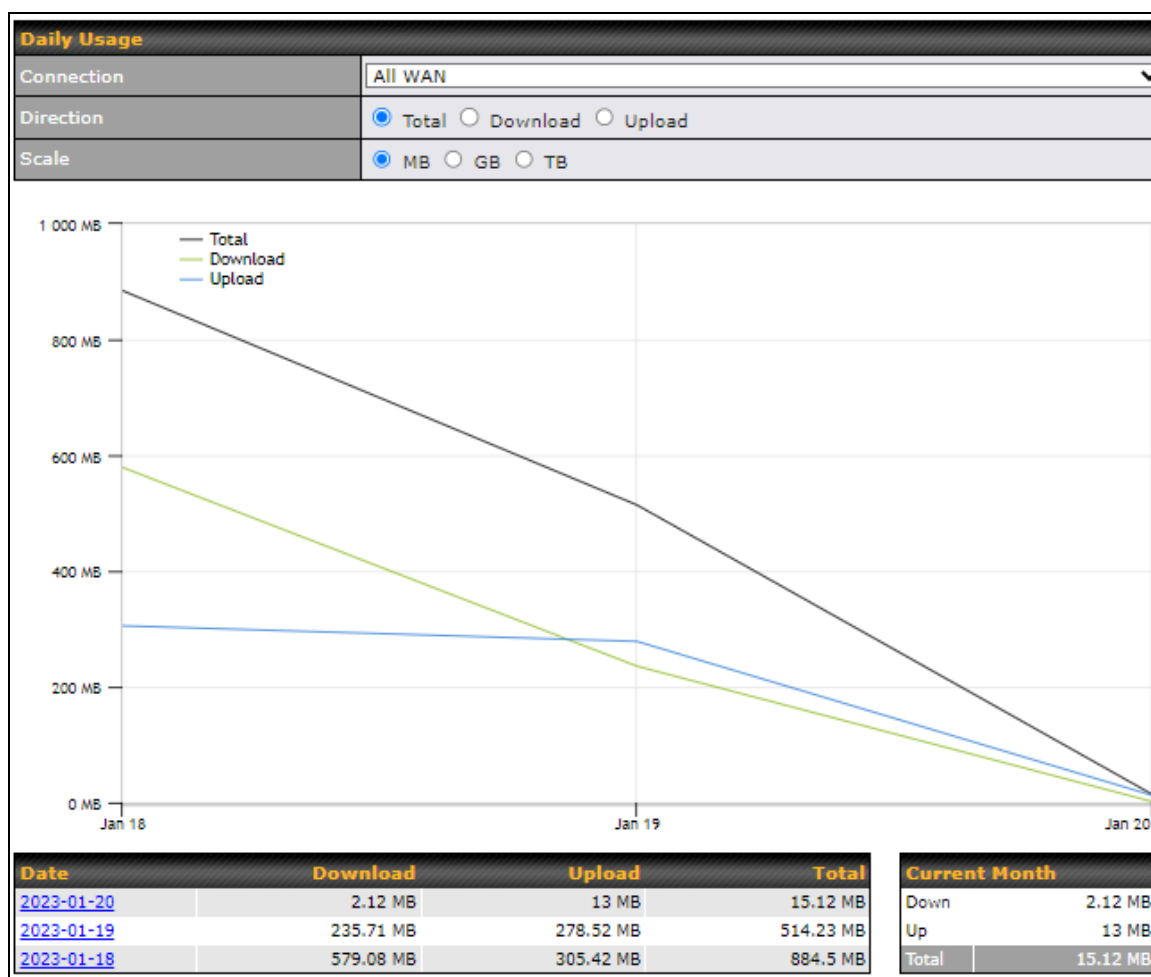


11.3. Daily

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

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

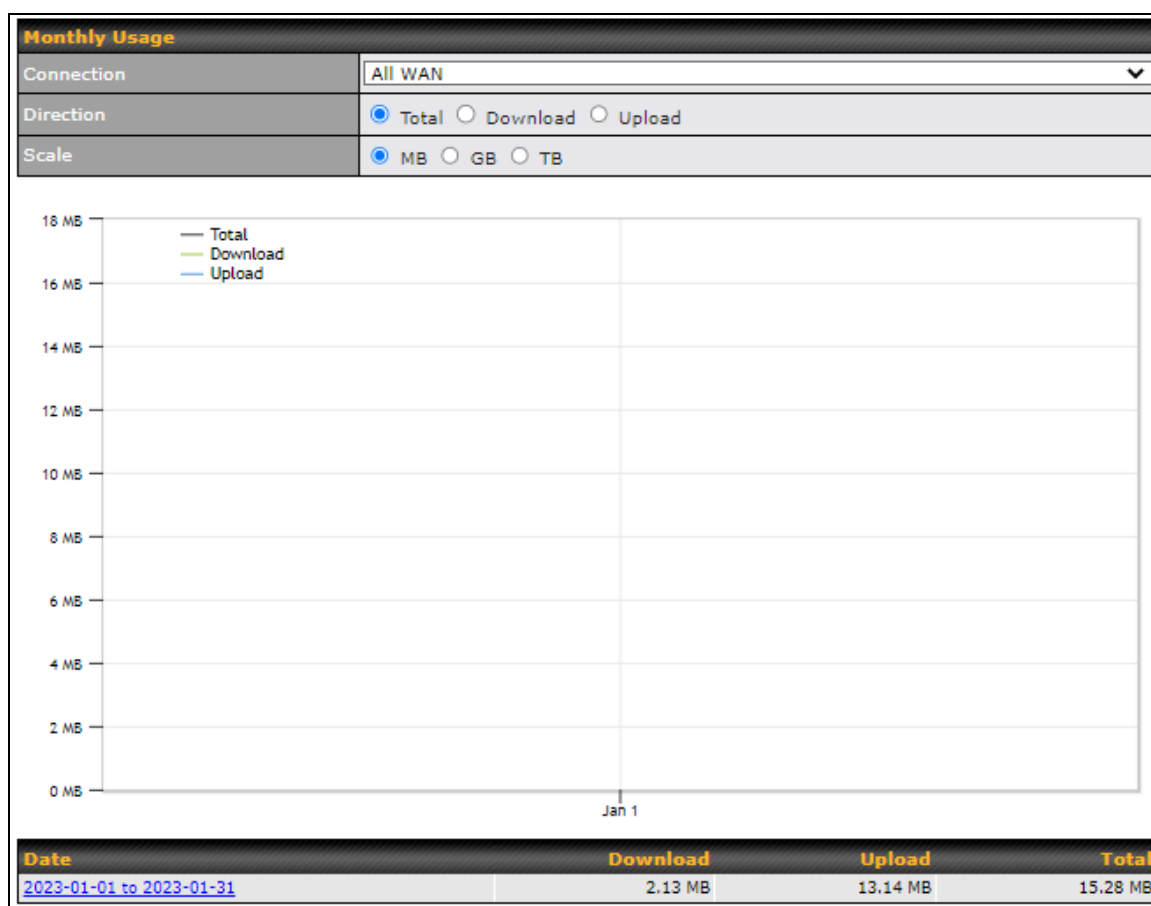
Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).



11.4. Monthly

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

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



Appendix

Federal Communication Commission Interference Statement

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

- 1) Reorient or relocate the receiving antenna.
- 2) Increase the separation between the equipment and receiver.
- 3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4) Consult the dealer or an experienced radio/TV technician for help.

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

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

IMPORTANT NOTE: FCC Radiation Exposure Statement

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

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

Taiwan NCC Statement

經型式認證合格之低功率射頻電機,非經許可,公司、商號或使用者均不得擅自 變更頻率、加大功率或變更原設計之特性及功能

低功率射頻電機之使用不得影響飛航安全及干擾合法通信;經發現有干擾現象 時,應改善至無干擾時方得繼續使用。前項合法通信,指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電 機設備之干擾。

Copyright

Copyright © 2016 Peplink

The content of this documentation may not be reproduced in any part or as a whole without the prior written permission of Peplink.

Disclaimer

Peplink does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent right nor the patent rights of others. Peplink further reserves the right to make changes in any products described herein without notice. This documentation is subject to change without notice.