

Client(s)	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	<p>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.</p> <p>Note that inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Also note that each WAN IP address can be associated to one NAT mapping only.</p>
Outbound Mappings	<p>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).</p> <p>Note that if you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the Outbound Policy section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.</p>

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

Important Note

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


18 QoS

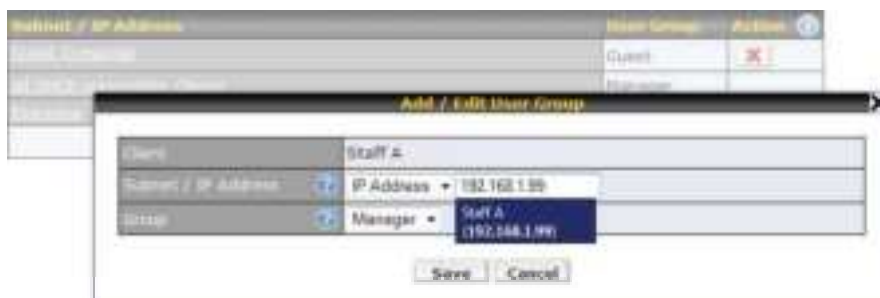
18.1 User Groups

LAN and PPTP clients can be categorized into three user groups: **Manager, Staff, and Guest**.

This menu allows you to define rules and assign client IP addresses or subnets to a user group. You can apply different bandwidth and traffic prioritization policies on each user group in the **Bandwidth Control** and **Application** sections (note that the options available here vary by model).

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

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



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

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

18.2 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**).

Group Bandwidth Reservation			
Enable	<input checked="" type="checkbox"/>		
	Manager	Staff	Guest
Bandwidth %	50%	30%	30%
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M
WAN 2	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M

18.3 Application

18.3.1 Application Prioritization


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

Application Prioritization	
<input checked="" type="radio"/> Apply same settings to all users	
<input type="radio"/> Customize	

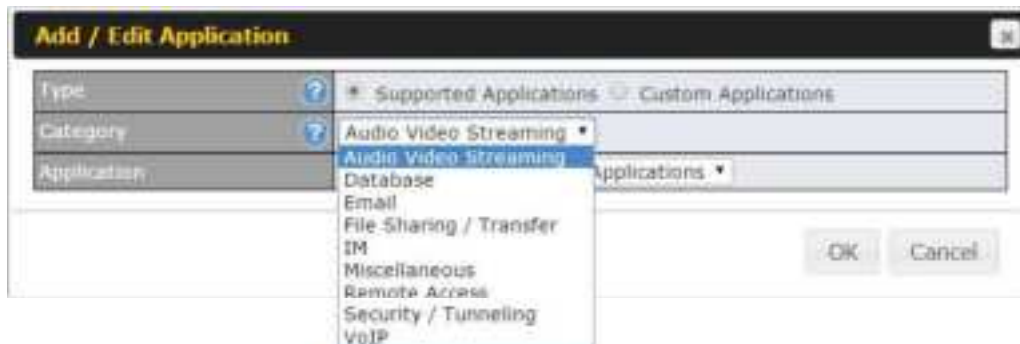
Three application priority levels can be set: ↑ High, — Normal, and ↓ Low. Pepwave routers can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference of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

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

18.3.2 Prioritization for Custom Applications

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

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



18.3.3 DSL/Cable Optimization

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



19 Firewall

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

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

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

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

Rule	Protocol	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Allow

Add Rule

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

Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Any	Allow

Add Rule

Apply Firewall Rules to PpVPN Traffic:

Enabled

Intrusion Detection and DDoS Prevention:

Disabled

19.1 Outbound and Inbound Firewall Rules

19.1.1 Access Rules

The outbound firewall settings are located at **Advanced>Firewall>Access Rules>Outbound Firewall Rules**.

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

Rule	Protocol	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Allow

Add Rule

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	<input checked="" type="checkbox"/> Always on
Protocol	Any <small>Protocol Selection Tool</small>
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save **Cancel**

Inbound firewall settings are located at **Advanced>Firewall>Access Rules>Inbound Firewall Rules**.

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

Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Any	Allow

Add Rule

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

Add a New Inbound Firewall Rule



New Firewall Rule

Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/>
WAN Connection	Any
Protocol	Any :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save Cancel

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

Inbound / Outbound Firewall Settings	
Rule Name	This setting specifies a name for the firewall rule.
Enable	<p>This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by the Pepwave router based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Pepwave router will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	<p>This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> • TCP • UDP • ICMP • IP

	<p>Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)</p> <p>After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remains manually modifiable.</p>
Source IP & Port	<p>This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the Source IP & Port setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the Source IP & Port settings.</p>
Destination IP & Port	<p>This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the Destination IP & Port setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the Destination IP & Port settings.</p>
Action	<p>This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:</p> <ul style="list-style-type: none"> • Source IP & port • Destination IP & port <p>With the value of Allow for the Action setting, the matching traffic passes through the router (to be routed to the destination). If the value of the Action setting is set to Deny, the matching traffic does not pass through the router (and is discarded).</p>
Event Logging	<p>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page Status>Event Log. A sample message is as follows:</p> <p>Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80</p> <ul style="list-style-type: none"> • CONN: The connection where the log entry refers to • SRC: Source IP address • DST: Destination IP address • LEN: Packet length • PROTO: Protocol • SPT: Source port • DPT: Destination port

Click **Save** to store your changes. To create an additional firewall rule, click **Add Rule** and repeat the above steps.

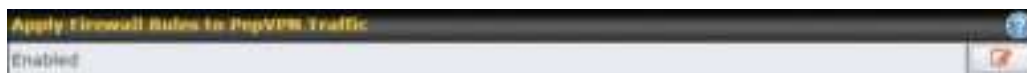
To change a rule's priority, simply drag and drop the rule:


- Hold the left mouse button on the rule.
- Move it to the desired position.
- Drop it by releasing the mouse button.

Tip

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


19.1.2 Apply Firewall Rules to PepVpn Traffic



When this option is enabled, Outbound Firewall Rules will be applied to PepVPN traffic. To turn on this feature, click , check the **Enable** check box, and press the **Save** button.

19.1.3 Intrusion Detection and DoS Prevention

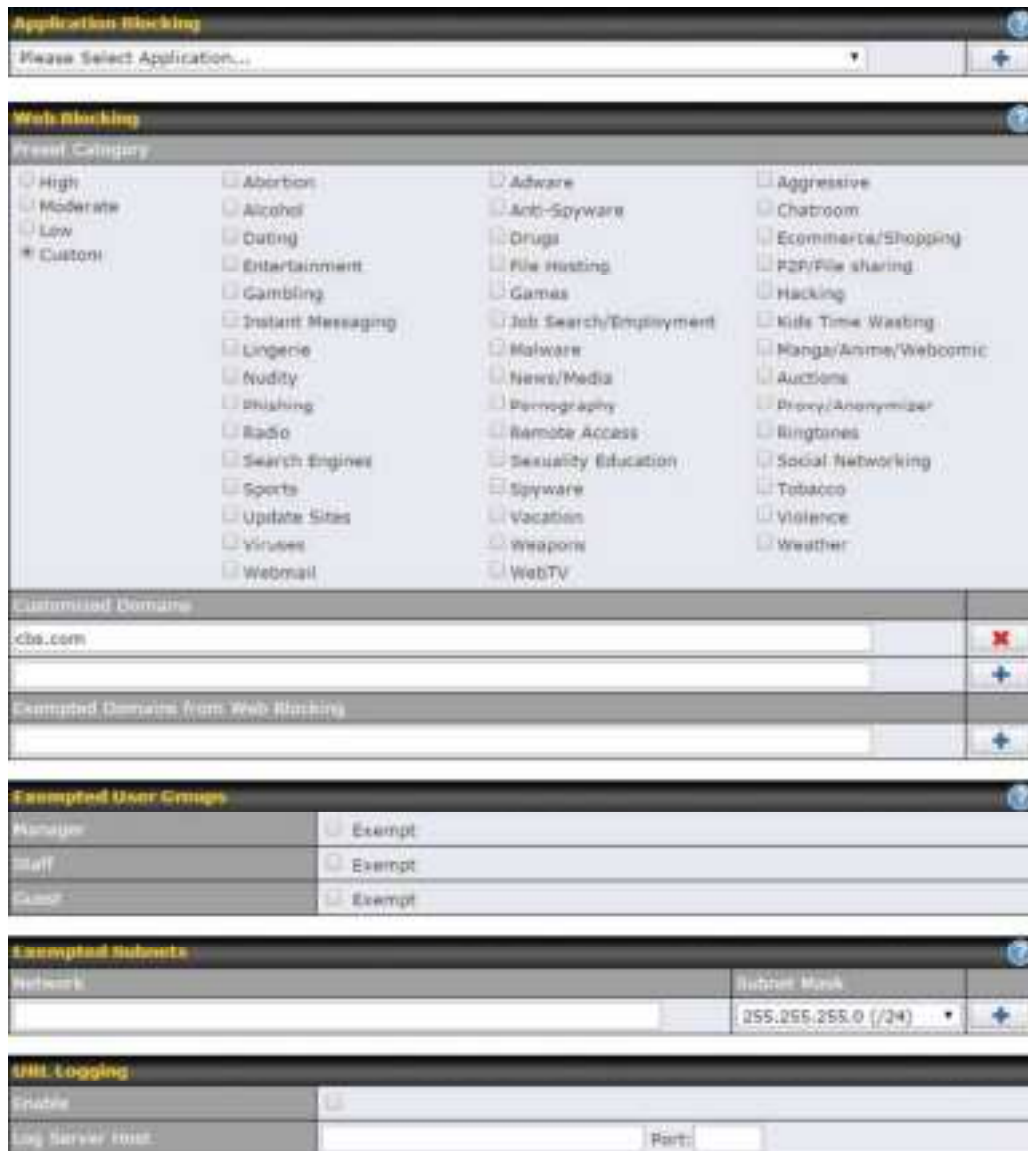


Pepwave routers can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click , check the **Enable** check box, and press the **Save** button.

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

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

19.2 Content Blocking



Application Blocking

Please Select Application...

Web Blocking

Select Category

<input type="checkbox"/> High	<input type="checkbox"/> Abortion	<input type="checkbox"/> Adware	<input type="checkbox"/> Aggressive
<input type="checkbox"/> Moderate	<input type="checkbox"/> Alcohol	<input type="checkbox"/> Anti-Spyware	<input type="checkbox"/> Chatroom
<input type="checkbox"/> Low	<input type="checkbox"/> Dating	<input type="checkbox"/> Drugs	<input type="checkbox"/> Ecommerce/Shopping
<input checked="" type="checkbox"/> Custom	<input type="checkbox"/> Entertainment	<input type="checkbox"/> File Hosting	<input type="checkbox"/> P2P/File sharing
<input type="checkbox"/> Gambling	<input type="checkbox"/> Games	<input type="checkbox"/> Hacking	<input type="checkbox"/> Kids Time Wasting
<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Job Search/Employment	<input type="checkbox"/> Manga/Anime/Webcomic	<input type="checkbox"/> Auctions
<input type="checkbox"/> Lingerie	<input type="checkbox"/> Malware	<input type="checkbox"/> Pornography	<input type="checkbox"/> Proxy/Anonymizer
<input type="checkbox"/> Nudity	<input type="checkbox"/> News/Media	<input type="checkbox"/> Remote Access	<input type="checkbox"/> Ringtones
<input type="checkbox"/> Smoking	<input type="checkbox"/> Sexuality Education	<input type="checkbox"/> Spyware	<input type="checkbox"/> Social Networking
<input type="checkbox"/> Radio	<input type="checkbox"/> Vacation	<input type="checkbox"/> Weapons	<input type="checkbox"/> Tobacco
<input type="checkbox"/> Search Engines	<input type="checkbox"/> WebTV	<input type="checkbox"/> Violence	<input type="checkbox"/> Weather
<input type="checkbox"/> Sports			
<input type="checkbox"/> Update Sites			
<input type="checkbox"/> Viruses			
<input type="checkbox"/> Webmail			

Customized Domains

cbs.com	<input type="button" value="X"/>
	<input type="button" value="+"/>

Exempted Domains from Web Blocking

	<input type="button" value="+"/>
--	----------------------------------

Exempted User Groups

Manager	<input type="checkbox"/> Exempt
Staff	<input type="checkbox"/> Exempt
Guest	<input type="checkbox"/> Exempt

Exempted Subnets

Subnet	Subnet Mask
	255.255.255.0 (/24)
	<input type="button" value="+"/>

URL Logging

Enable	<input type="checkbox"/>
Log Server IP	Port:

19.2.1 Application Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted User Groups or Exempted Subnets defined below.

19.2.2 Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for those on the Exempted User Groups or Exempted Subnets defined below.

If "foobar.com" is entered, any web site with a host name ending in foobar.com will be blocked, e.g. www.foobar.com, foobar.com, etc. However, "myfoobar.com" will not be blocked.

You may enter the wild card "." at the end of a domain name to block any web site with a host name having the domain name in the middle. If you enter "foobar.*", then "www.foobar.com", "www.foobar.co.jp", or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The device will inspect and look for blocked domain names on all HTTP and HTTPS traffic.

19.2.3 Customized Domains

Enter an appropriate website address, and the Peplink Balance will block and disallow LAN/PPTP/SpeedFusion™ peer clients to access these websites. Exceptions can be added using the instructions in Sections 20.1.3.2 and 20.1.3.3.

You may enter the wild card "." at the end of a domain name to block any web site with a host name having the domain name in the middle. For example, If you enter "foobar.*", then "www.foobar.com", "www.foobar.co.jp", or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The Peplink Balance will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

19.2.4 Exempted User Groups

Check and select pre-defined user group(s) who can be exempted from the access blocking rules. User groups can be defined at **QoS>User Groups** section. Please refer to **Section 17.1** for details.

19.2.5 Exempted Subnets

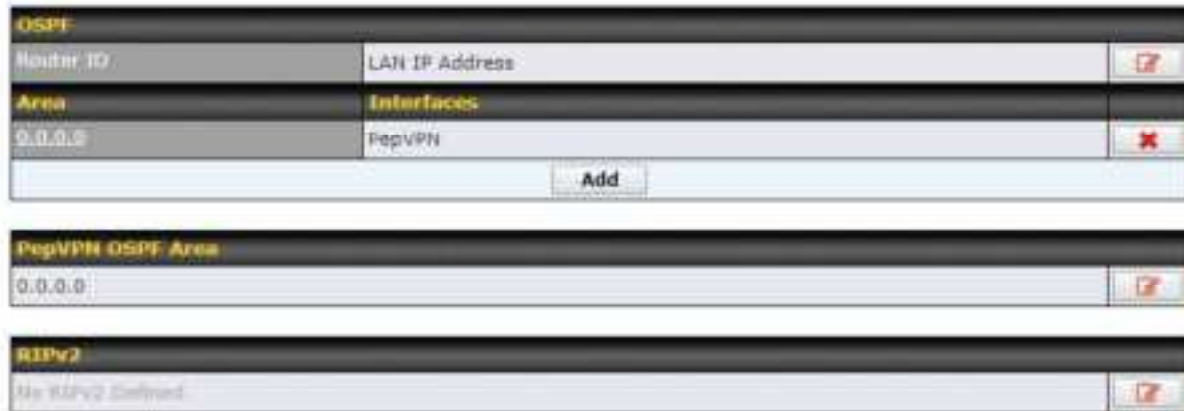
With the subnet defined in the field, clients on the particular subnet(s) can be exempted from the access blocking rules.

19.2.6 URL Logging


Click **enable**, and then enter the ip address and port (if applicable) where your remote syslog server is located.

20 OSPF & RIPv2

The Pepwave supports OSPF and RIPv2 dynamic routing protocols. Click the **Advanced** tab from the top bar, and then click the **Routing Protocols >OSPF & RIPv2** item on the sidebar to reach the following menu:



OSPF


Router ID	LAN IP Address	
Area	Interfaces	
0.0.0.0	PepVPN	
Add		

PepVPN OSPF Area

0.0.0.0	
---------	---

RIPv2


No RIPv2 Defined	
------------------	---

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

OSPF settings

Area ID	0.0.0.0
Link Type	<input checked="" type="radio"/> Broadcast <input type="radio"/> Point-to-Point
Authentication	None ▼
Interfaces	<div style="display: flex; align-items: flex-start;"> <div style="width: 20px; text-align: center; color: blue;">?</div> <div> <input type="checkbox"/> Untagged LAN <input type="checkbox"/> V167 (192.168.167-1/24) <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input checked="" type="checkbox"/> PepVPN </div> </div>

OSPF Settings	
Area ID	Determine the name of your Area ID to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.
Link Type	Choose the network type that this area will use.
Authentication	Choose an authentication method, if one is used, from this drop-down menu. Available options are MD5 and Text . Enter the authentication key next to the drop-down menu.
Interfaces	Determine which interfaces this area will use to listen to and deliver OSPF packets

To access RIPv2 settings, click .



RIPv2 settings

Authentication	None ▼
Interfaces	<input type="checkbox"/> Untagged LAN <input type="checkbox"/> V167 (192.168.167.1/24) <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5

Save Cancel

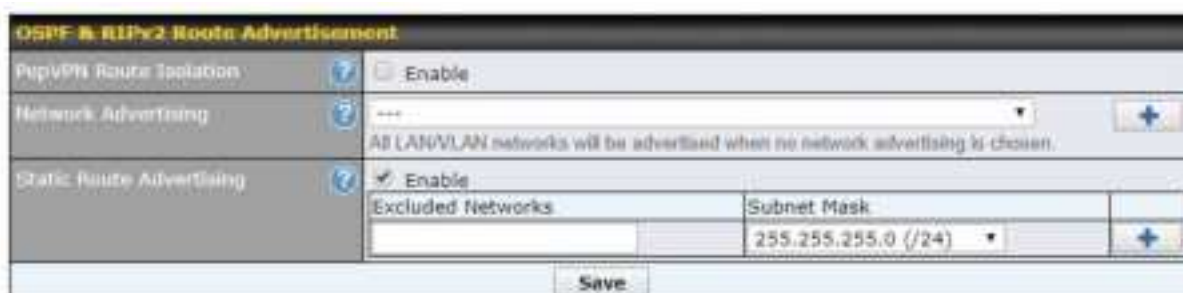
RIPv2 Settings

Authentication

Choose an authentication method, if one is used, from this drop-down menu. Available options are **MD5** and **Text**. Enter the authentication key next to the drop-down menu.

Interfaces

Determine which interfaces this group will use to listen to and deliver RIPv2 packets.



OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation	<input type="checkbox"/> Enable				
Network Advertising	+ + + ... ▼ + All LAN/VLAN networks will be advertised when no network advertising is chosen.				
Static Route Advertising	<input checked="" type="checkbox"/> Enable <table border="1"> <thead> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td></td> <td>255.255.255.0 (/24) ▼</td> </tr> </tbody> </table>	Excluded Networks	Subnet Mask		255.255.255.0 (/24) ▼
Excluded Networks	Subnet Mask				
	255.255.255.0 (/24) ▼				

Save

OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation

Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption..

Network Advertising

Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.

Static Route Advertising

Enable this option to advertise LAN static routes over OSPF & RIPv2. Static routes that match the Excluded Networks table will not be advertised.

21 BGP

Click the **Advanced** tab from the top bar, and then click the **Routing Protocols>BGP** item on the sidebar to configure BGP.

BGP	AS	Neighbors	
Uplink	54520	172.16.51.1	X
Add			

Click "x" to delete a BGP profile

Click "Add" to add a new BGP profile

BGP Profile						
Profile Name						
Enable	<input checked="" type="checkbox"/>					
Interface	WAN 1					
Router ID	<input checked="" type="radio"/> LAN IP Address <input type="radio"/> Custom:					
Autonomous System						
Neighbor	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
			disable			+
Hold Time	<input type="text" value="240"/>					

BGP	
Name	This field is for specifying a name to represent this profile.
Enable	When this box is checked, this BGP profile will be enabled. Otherwise, it will be disabled.
Interface	The interface where BGP neighbor is located
Autonomous System	The Autonomous System Number (ASN) of this profile
Neighbor	BGP Neighbor's details
IP address	Neighbor's IP address
Autonomous System	Neighbor's ASN
Multihop/TTL	Time-to-live (TTL) of BGP packet. Leave it blank if BGP neighbor is directly connected, otherwise you must specify a TTL value. Accurately, this option should be used if the configured neighbor IP

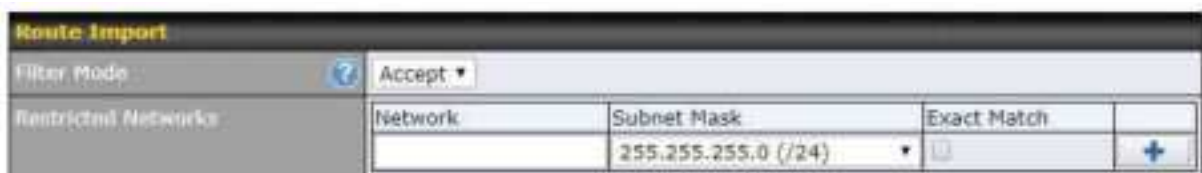
	address does not match the selected Interface's network subnets. TTL value must be between 2 to 255.
Password	Optional password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this neighbor. The value must be a comma separated ASN. For example "64530,64531" will prepend "64530, 64531" to received routes.
Hold Time	Time in seconds to wait for a keepalive message from the neighbor before considering the BGP connection is staled. This value must be either 0 (infinite hold time) or between 3 and 65535 inclusively.



The **Route Advertisement** window contains the following fields:

- Network Advertising:** A dropdown menu with a question mark icon and a plus button.
- Static Route Advertising:** A section with a question mark icon containing:
 - ☒ **Enable**
 - Excluded Networks:** A text input field.
 - Subnet Mask:** A dropdown menu showing "255.255.255.0 (/24)" and a plus button.
- Advertise OSPF Route:** A checkbox with a question mark icon.

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



The **Route Import** window contains the following fields:

- Filter Mode:** A dropdown menu showing "Accept" and a question mark icon.
- Restricted Networks:** A table with columns:

Network	Subnet Mask	Exact Match
	255.255.255.0 (/24)	<input type="checkbox"/>

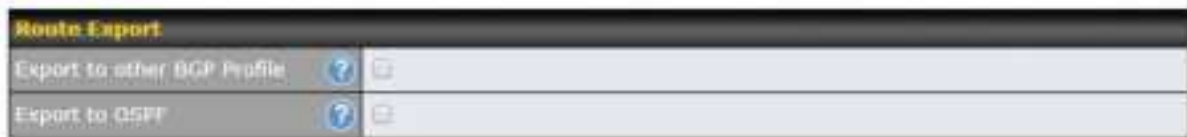
 A plus button is located to the right of the table.

Filter Mode	<p>This option selects the route import filter mode.</p> <p>None: all BGP routes will be accepted.</p> <p>Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p>Reject: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.</p>
--------------------	---

Restricted Networks

This specifies the network in the “route import” entry

Exact Match: When this box is checked, only routes with the same Networks and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnet will be filtered.

**Export to other BGP Profile**

When this box is checked, routes learnt from this BGP profile will export to other BGP profiles.

Export to OSPF

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


22 Remote User Access

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

22.1 L2TP with IPsec



The screenshot shows the 'Remote User Access Settings' window. The 'Enable' checkbox is checked. Under 'VPN Type', 'L2TP with IPsec' is selected with a radio button. The 'PPTP' and 'OpenVPN' options are unselected. The 'Pre-shared Key' field is empty, and the 'Hide Characters' checkbox is checked.

L2TP with IPsec Remote User Access Settings	
Pre-shared Key	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
Listen On	This setting is for specifying the WAN IP addresses that allow remote user access.
Disable Weak Ciphers	Click the  button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.

Continue to configure the authentication method.

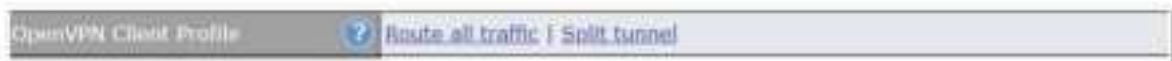
22.2 OpenVPN



The screenshot shows the 'Remote User Access Settings' window. The 'Enable' checkbox is checked. Under 'VPN Type', 'OpenVPN' is selected with a radio button. A note below the radio buttons states: 'You can obtain the OpenVPN client profile from the [status page](#)'.

Select OpenVPN and continue to configure the authentication method.

The OpenVPN Client profile can be downloaded from the **Status > device** page after the configuration has been saved.



The screenshot shows the 'OpenVPN Client Profile' selection window. There are two radio buttons: 'Route all traffic' (selected) and 'Split tunnel'.

You have a choice between 2 different OpenVPN Client profiles.

- **"route all traffic" profile**
Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel
- **"split tunnel" profile**
Using this profile, VPN clients will ONLY send those traffic designated to the untagged LAN and VLAN segment through the OpenVPN tunnel.

22.3 PPTP



The screenshot shows the 'Remote User Access Settings' window. The 'Enable' checkbox is checked. Under 'VPN Type', three radio buttons are visible: 'L2TP with IPsec' (selected), 'PPTP', and 'OpenVPN'.

No additional configuration required.

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

Continue to configure authentication method.

22.4 Authentication Methods



The screenshot shows the 'Authentication Methods' configuration window. It has three main sections: 'Connect to Network' with a dropdown menu showing 'Untagged LAN', 'Authentication' with a dropdown menu showing 'Local User Accounts', and 'User Accounts' which contains a table with columns for 'Username' and 'Password', and an 'Add' button.

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

User accounts:


This setting allows you to define the Remote User Accounts. Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

Note:

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





The password must be between 8 and 12 characters long.

LDAP Server:

Connect to Network	 Untagged LAN ▾
Authentication	LDAP Server ▾
LDAP Server	<input type="text"/> Port 389 
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server
Base DN	<input type="text"/>
Base Filter	<input type="text"/>

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

Radius Server:

Authentication	RADIUS Server ▾
Auth Protocol	MS-CHAP v2 ▾
Auth Server	<input type="text"/> Port 1812 
Auth Server Secret	<input type="text"/> 
Accounting Server	<input type="text"/> Port 1813 
Accounting Server Secret	<input type="text"/> 

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

Active Directory:

Connect to Network	 Untagged LAN ▾
Authentication	Active Directory ▾
Server Hostname	<input type="text"/>
Domain	<input type="text"/>
Admin Username	<input type="text"/>
Admin Password	<input type="text"/> 

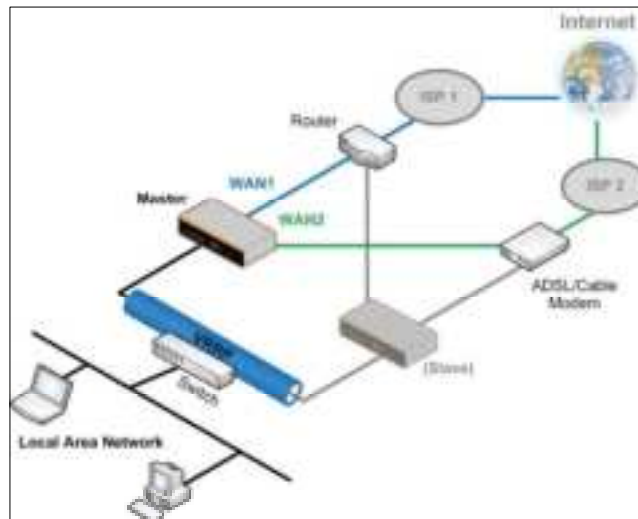
Enter the matching Active Directory details to allow for Active Directory server authentication.

23 Miscellaneous Settings

The miscellaneous settings include configuration for High Availability, Certificate Manager, service forwarding, service passthrough, GPS forwarding, GPIO, Groupe Networks and SIM Toolkit (depending the feature is supported on the model of Peplin router that is being used).

23.1 High Availability

Many Pepwave routers support high availability (HA) configurations via an open standard virtual router redundancy protocol (VRRP, RFC 3768). In an HA configuration, two Pepwave routers provide redundancy and failover in a master-slave arrangement. In the event that the master unit is down, the slave unit becomes active. High availability will be disabled automatically where there is a drop-in connection configured on a LAN bypass port.



In the diagram, the WAN ports of each Pepwave router connect to the router and to the modem. Both Pepwave routers connect to the same LAN switch via a LAN port.

An elaboration on the technical details of the implementation of the virtual router redundancy protocol (VRRP, RFC 3768) by Pepwave routers follows:

- In an HA configuration, the two Pepwave routers communicate with each other using VRRP over the LAN.
- The two Pepwave routers broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the master Pepwave router is received in 3 seconds (or longer) since the last heartbeat signal, the slave Pepwave router becomes active.
- The slave Pepwave router initiates the WAN connections and binds to a previously configured LAN IP address.
- At a subsequent point when the master Pepwave router recovers, it will once again

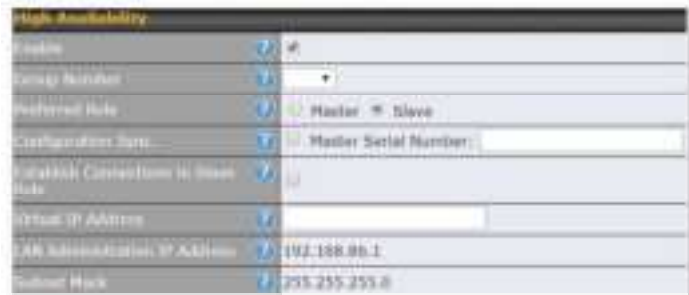
become active.

You can configure high availability at **Advanced>Misc. Settings>High Availability**.

Interface for Master Router



Interface for Slave Router



High Availability	
Enable	Checking this box specifies that the Pepwave router is part of a high availability configuration.
Group Number	This number identifies a pair of Pepwave routers operating in a high availability configuration. The two Pepwave routers in the pair must have the same Group Number value.
Preferred Role	This setting specifies whether the Pepwave router operates in master or slave mode. Click the corresponding radio button to set the role of the unit. One of the units in the pair must be configured as the master, and the other unit must be configured as the slave.
Resume Master Role Upon Recovery	This option is displayed when Master mode is selected in Preferred Role . If this option is enabled, once the device has recovered from an outage, it will take over and resume its Master role from the slave unit.
Configuration Sync.	This option is displayed when Slave mode is selected in Preferred Role . If this option is enabled and the Master Serial Number entered matches with the actual master unit's, the master unit will automatically transfer the configuration to this unit. Please make sure the LAN IP Address and the Subnet Mask fields are set correctly in the LAN settings page. You can refer to the Event Log for the configuration synchronization status.
Master Serial Number	If Configuration Sync. is checked, the serial number of the master unit is required here for the feature to work properly.
Virtual IP	The HA pair must share the same Virtual IP . The Virtual IP and the LAN Administration IP must be under the same network.

LAN Administration IP

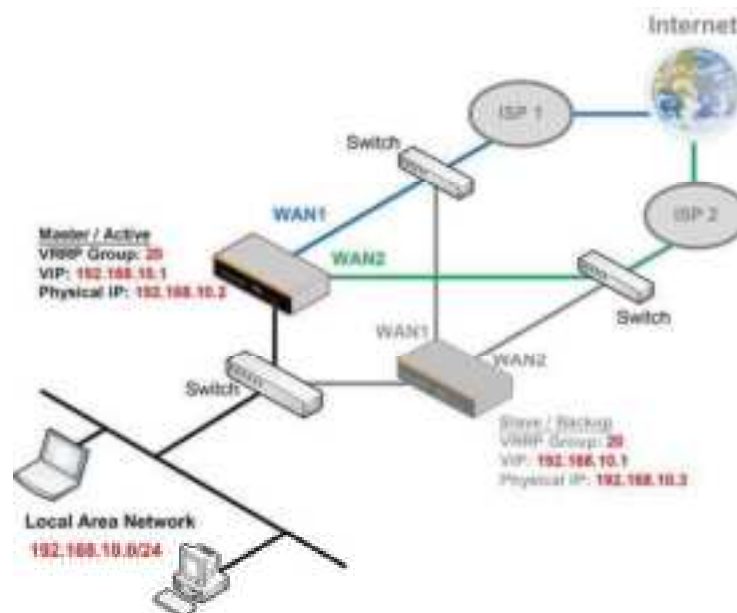
This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN.

Subnet Mask

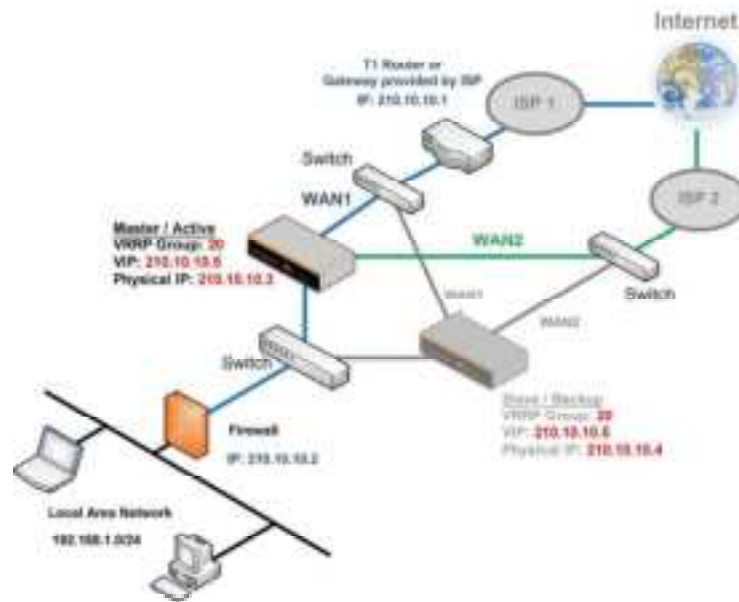
This setting specifies the subnet mask of the LAN.

Important Note

For Pepwave routers in NAT mode, the virtual IP (VIP) should be set as the default gateway for all hosts on the LAN segment. For example, a firewall sitting behind the Pepwave router should set its default gateway as the virtual IP instead of the IP of the master router.



In drop-in mode, no other configuration needs to be set.



Please note that the drop-in WAN cannot be configured as a LAN bypass port while it is configured for high availability.

23.2 Certificate Manager

Certificate		
Specifications/Types: VPNs	No Certificate	
Web Admin SSL	Default Certificate is in use	
Captive Portal SSL	Default Certificate is in use	
OpenVPN CA 	Default Certificate is in use	

Wi-Fi WAN Client Certificate	
No Certificates defined	
Add Certificate	

Wi-Fi WAN CA Certificate	
No Certificates defined	
Add Certificate	

This section allows for certificates to be assigned to the local VPN, Web Admin SSL, Captive Portal SSL, OpenVPN CA, Wi-Fi WAN Client certificate and Wi-Fi WAN CA 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/>

23.3 Service Forwarding

Service forwarding settings are located at **Advanced>Misc. Settings>Service Forwarding**.



Service Forwarding	
SMTP Forwarding	When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting Enable .
Web Proxy Forwarding	When this option is enabled, all outgoing connections destined for the proxy server specified in Web Proxy Interception Settings will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting Enable .
DNS Forwarding	When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down.
Custom Service Forwarding	When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number.

23.3.1 SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP's SMTP server. All outgoing SMTP

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



SMTP Forwarding Setup

SMTP Forwarding: ☒ Enable

Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	<input type="checkbox"/>		
WAN 2	<input type="checkbox"/>		
Wi-Fi WAN	<input type="checkbox"/>		
Cellular 1	<input type="checkbox"/>		
Cellular 2	<input type="checkbox"/>		
USB	<input type="checkbox"/>		

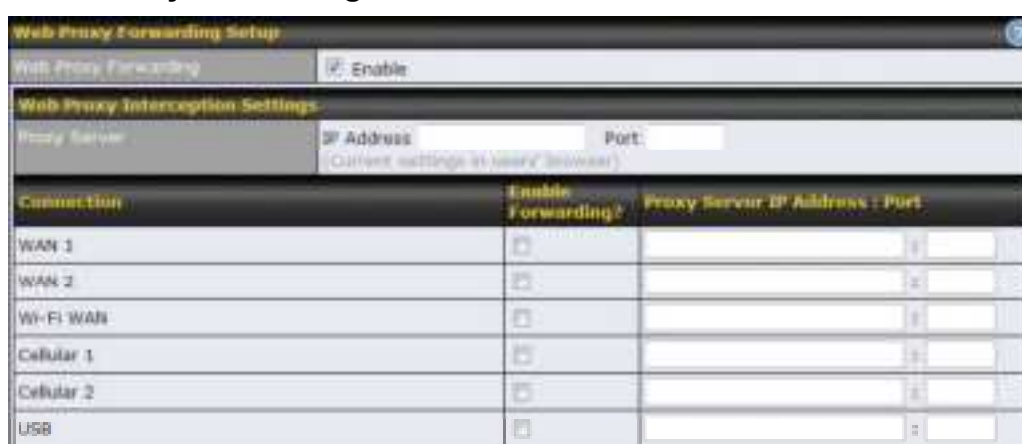
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

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

Note

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see **Section 14.2**).

23.3.2 Web Proxy Forwarding



Web Proxy Forwarding Setup

Web Proxy Forwarding: ☒ Enable

Web Proxy Interception Settings

Proxy Server: IP Address: Port:
(Current settings in proxy browser)

Connection	Enable Forwarding?	Proxy Server IP Address : Port
WAN 1	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
WAN 2	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
Wi-Fi WAN	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
Cellular 1	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
Cellular 2	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
USB	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>

When this feature is enabled, the Pepwave router will intercept all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings**, choose a WAN connection with reference to the outbound policy, and then forward them to the specified web

proxy server and port number. Redirected server settings for each WAN can be set here. If forwarding is disabled for a WAN, web proxy connections for the WAN will be simply forwarded to the connection's original destination.

23.3.3 DNS Forwarding



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

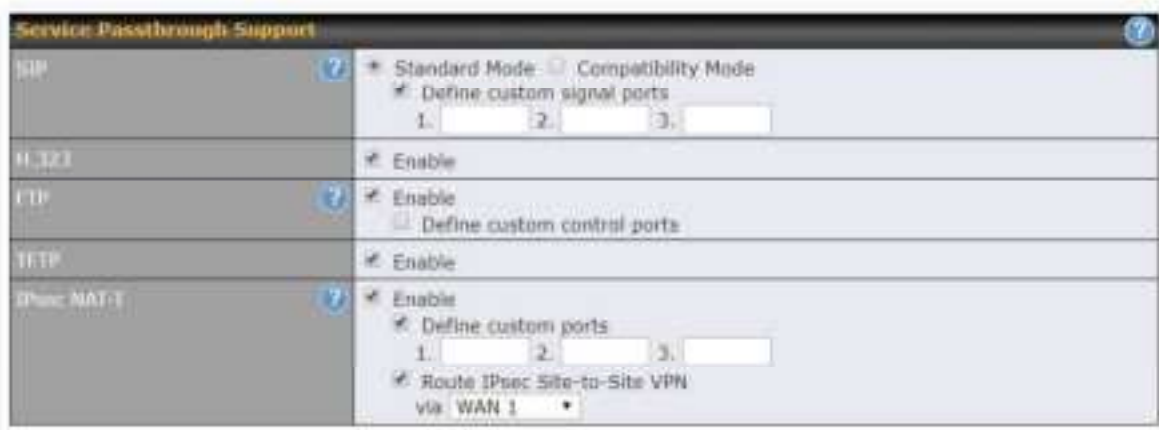
23.3.4 Custom Service Forwarding



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

23.4 Service Passthrough

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



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

Service Passthrough Support

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

23.5 UART

Selected Pepwave MAX routers feature a RS-232 serial interface on the built-in terminal block. The RS-232 serial interface can be used to connect to a serial device and make it accessible over an TCP/IP network.

The serial interface can be enabled and parameters can be set on the web admin page under **Advanced > UART**. Make sure they match the serial device you are connecting to.

Serial to Network	
Enable	<input checked="" type="checkbox"/>
Allowed Source IP Subnets	* Any <input type="checkbox"/> Allows access from the following IP subnets only
Web Console	<input type="checkbox"/>

Serial Parameters	
Baud Rate	9600 ▾
Data Bits	8 ▾
Stop Bits	1 ▾
Parity	None ▾
Flow Control	None ▾
Interface	RS232 ▾

Operating Settings	
Operation Mode	TCP Server Mode ▾
Local TCP Port	4001
Max Connection	1
TCP Alive Check Time	7 min(s)
Inactivity Time	0 ms

Data Packing	
Packing Length	0 byte(s)
Delimiter	<input type="text"/>
Delimiter process	Do Nothing ▾
Force Transmit	0 ms

There are 4 pins i.e. TX, RX, RTS, CTS on the terminal block for serial connection and they correspond to the pins in a DB-9 connector as follows:

DB-9 Pepwave MAX Terminal Block

Pin 1 –

Pin 2 Rx (rated -+25V)

Pin 3 Tx (rated -+12V)

Pin 4 –

Pin 5 –

Pin 6 –

Pin 7 RTS

Pin 8 CTS

Pin 9 –

The RS232 serial interface is not an isolated RS232. External galvanic isolation may be added if required.


Be sure to check whether your serial cable is a null modem cable, commonly known as crossover cable, or a straight through cable. If in doubt, swap Rx and Tx, and RTS and CTS, at the other end and give it another go.

Once connected, your serial device should be accessible on your Pepwave MAX router LAN IP address at the specified TCP port.

23.6 GPS Forwarding

Using the GPS forwarding feature, some Pepwave routers can automatically send GPS reports to a specified server. To set up GPS forwarding, navigate to **Advanced>GPS Forwarding**.



GPS Forwarding	
Enable	Check this box to turn on GPS forwarding.
Server	Enter the name/IP address of the server that will receive GPS data. Also specify a port number, protocol (UDP or TCP), and a report interval of between 1 and 10 seconds. Click  to save these settings.
GPS Report Format	Choose from NMEA or TAIP format for sending GPS reports.
NMEA Sentence Type	If you've chosen to send GPS reports in NMEA format, select one or more sentence types for sending the data (GPRMC , GPGGA , GPVTG , GPGSA , and GPGSV).
Vehicle ID	The vehicle ID will be appended in the last field of the NMEA sentence. Note that the NMEA sentence will become customized and non-standard.
TAIP Sentence Type/TAIP ID (optional)	If you've chosen to send GPS reports in TAIP format, select one or more sentence types for sending the data (PV—Position / Velocity Solution and CP—Compact Velocity Solution). You can also optionally include an ID number in the TAIP ID field.


23.7 Ignition Sensing

Ignition Sensing detects the ignition signal status of a vehicle it is installed in.

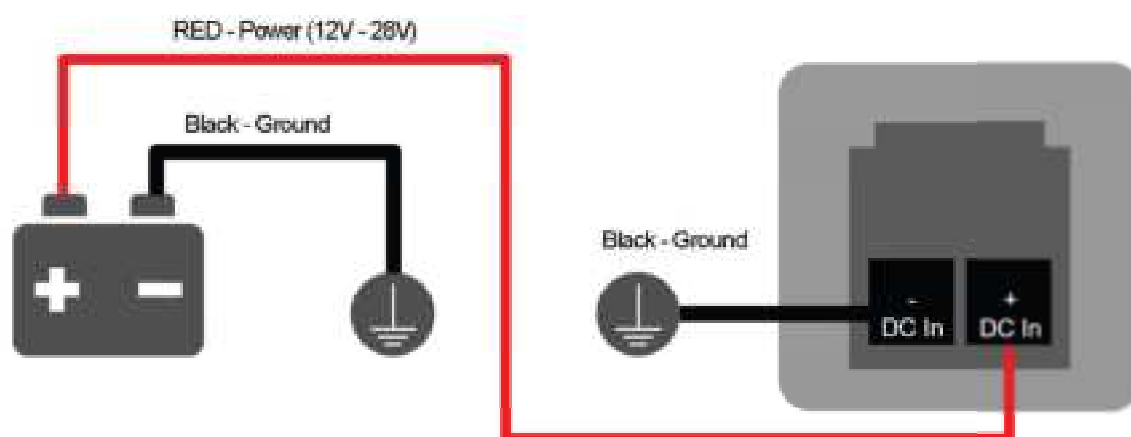
This feature allows the cellular router to start up or shut down when the engine of that vehicle

is started or turned off. The time delay setting between ignition off and power down of the router is a configurable setting, which allows the router to stay on for a period of time after the engine of a vehicle is turned off.

Ignition Sensing installation

Function		Colour Wire
	I/O optional*	Brown
	IGN I/P connected to positive feed on the ignition .	Orange
	DC IN - connected to permanent negative feed (ground)	Black
	DC IN + connected to permanent positive feed (power 12VDC, 2A)).	Red
* Currently not functional; will be used for additional features in future firmware		

Connectivity diagram for devices with 2-pin connector



GPIO Menu

The Ignition Sensing options are available in **Advanced > GPIO**

The configurable option for Ignition Input is **Delay**; the time in seconds the router stays powered on after the ignition is turned off.

IGN I/P	
Enable	<input checked="" type="checkbox"/>
Type	Digital Input ▼
Mode	Ignition Sensing ▼
Delay	<input type="text"/> seconds

Still under development:

O/P (connected to I/O pin on 4 pin connector) can be configured as a digital input, digital output or analog input.

Digital Input - the connection supports input sensing; it reads the external input and determine if the settings should be 'High' (on) or 'Low' (off).

Digital Output - when there is a healthy WAN connection, the output pin is marked as 'High' (on). Otherwise, it will be marked as 'Low' (off)

Analog Input - to be confirmed. In most cases should read the external input and determine the voltage level.

O/P	
Enable	<input checked="" type="checkbox"/>
Type	Digital Output ▾
Mode	WAN Status ▾

23.8 Grouped Networks

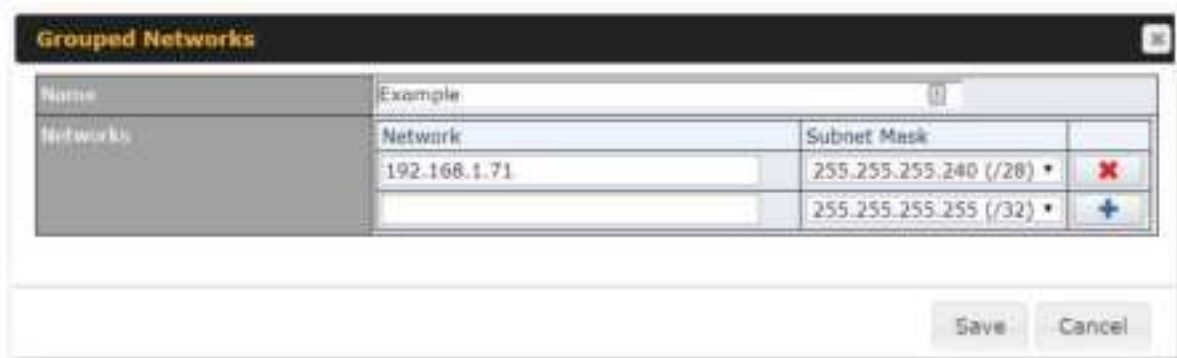
Advanced > Grouped Networks allows to configure destination networks in grouped format.



Name	Networks
Example	192.168.1.71/28

Add Group

Select Add group to create a new group with single IPAddresses or subnets from different VLANs.



Name	Networks						
Example	<table border="1"> <thead> <tr> <th>Network</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>192.168.1.71</td> <td>255.255.255.240 (/28) *</td> </tr> <tr> <td></td> <td>255.255.255.255 (/32) *</td> </tr> </tbody> </table>	Network	Subnet Mask	192.168.1.71	255.255.255.240 (/28) *		255.255.255.255 (/32) *
Network	Subnet Mask						
192.168.1.71	255.255.255.240 (/28) *						
	255.255.255.255 (/32) *						

Save Cancel

The created network groups can be used in outbound policies, firewall rules.

23.9 SIM Toolkit

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

USSD

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

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	856195002100538
Tool	USSD

USSD	
USSD Code	<input type="text"/> <input type="button" value="Submit"/>

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

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	856195002100538
USSD Code	*138# <input type="button" value="Submit"/>
Receive SMS	<input type="button" value="Get"/>

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

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	856195002100538
USSD Code	*138# <input type="button" value="Submit"/>
USSD Status	Request is sent successfully
Receive SMS	<input type="button" value="Get"/>

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

Received SMS	
May 27 20:02	PCX As of May 27th Account Balance: 1 0.00 Amount Unbilled Voice Calls: 0 minutes Video Calls: 0 minutes SMS (Roaming): 0 SMS (Within Network): 0 MMS (Roaming): 0 MMS (Within Network): 0 Data Usage: 7364KB (For reference only, please refer to bill)
Aug 8, 2013 14:51	PCX iPhone & Android users need to make sure "PCX" is entered as the APN under "Settings" > "Mobile network setting" for web browsing and mobile data service. Other handset models will receive handset settings via SMS shortly (PIN: 1234) (Consumer Service Hotline: 1000 / Business Customer Hotline: 10008)

SMS

The SMS option allows you to read SMS (text) messages that have been sent to the SIM

in your Peplink router.

SIM Status	
WAN Connection	Cellular ▼
SIM Card	1
IMEI	734373056298
Tool	SMS ▼

SMS		Refresh
Jun 21, 2017 16:00	Hi, Thank you, your work performance is excellent - you can always rely on me when you first begin at work as we	✖
May 06, 2017 12:33	SMS Hi there, your new cell is ready to use. Go to your M3 account on your desktop or go to mobile phone click here http://m3link.com/activation	✖
Mar 15, 2017 10:03	Pepple News Hello, there is planned maintenance at the company this week. If your service is affected, you can get updates from us by 24x7.	✖
Mar 06, 2017 14:50	SMS Hi there, your new cell is ready to use. Go to your M3 account on your desktop or go to mobile phone click here http://m3link.com/activation	✖
Dec 28, 2016 09:53	Pepple News Hi, we have your appointment in monthly call price offer but we cannot give this offer again to your first in order, your monthly earnings change will affect to future in your first set. Thank	✖
Dec 06, 2016 12:09	SMS Hi there, your new cell is ready to use. Go to your M3 account on your desktop or go to mobile phone click here http://m3link.com/activation	✖
Nov 08, 2016 11:29	Pepple News Hello, there is planned maintenance at the company this week. If your service is affected, you can get updates from us by 24x7.	✖
Sep 07, 2016 17:05	Pepple News Hello there, thank you for supporting our service. We are happy to hear that you are using our service. We are happy to hear that you are using our service. We are happy to hear that you are using our service.	✖

24 AP - access point

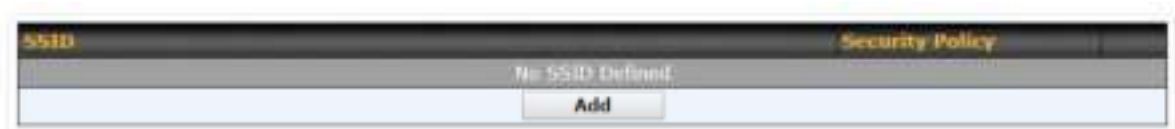
25 AP Controller

The AP controller acts as a centralized controller of Pepwave Access Points. With this feature, users can customize and manage up to 1500 Access Points from a single Pepwave router interface. To configure, navigate to the **AP** tab. and the following screen appears.

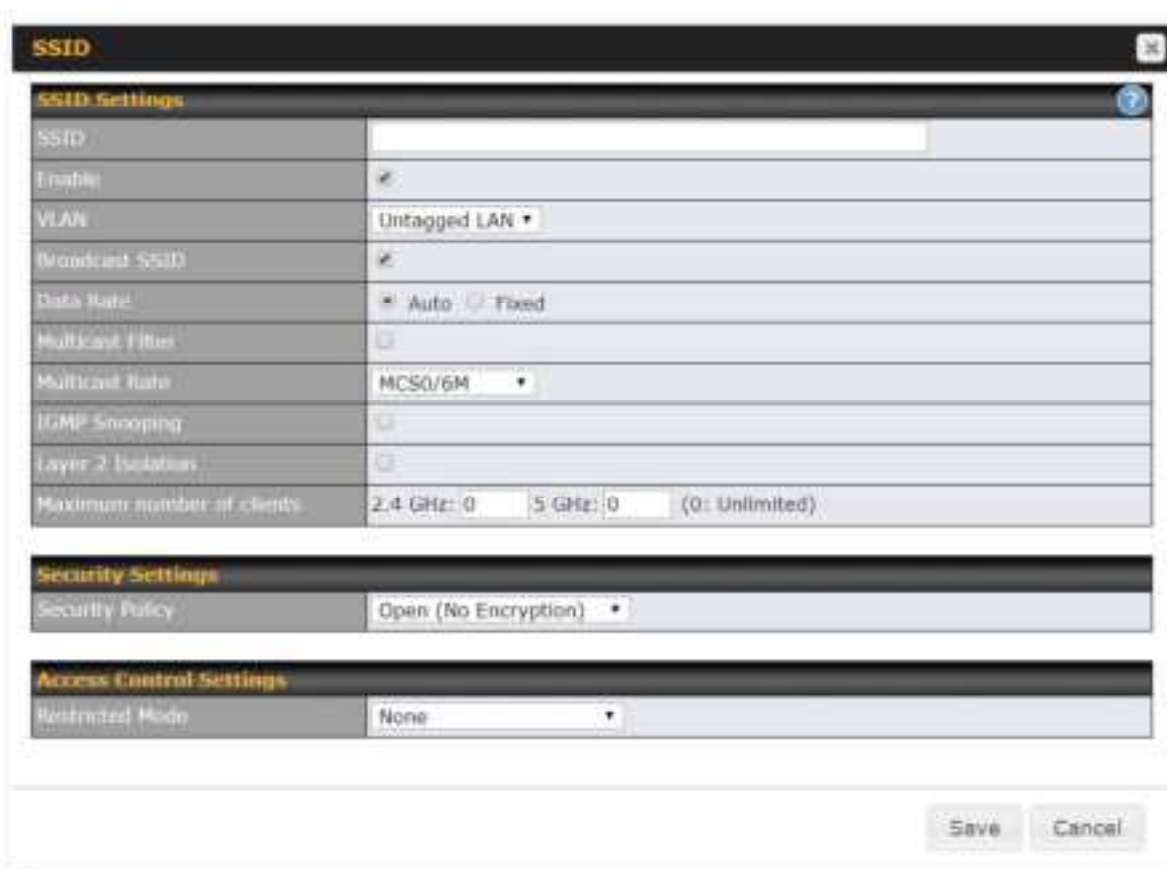


AP Controller	
AP Management	The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, CAPWAP Access Controller addresses (field 138), will be added to the DHCP server. A local DNS record, AP Controller , will be added to the local DNS proxy.
Sync Method	<ul style="list-style-type: none"> • As soon as possible • Progressively • One at a time
Permitted AP	Access points to manage can be specified here. If Any is selected, the AP controller will manage any AP that reports to it. If Approved List is selected, only APs with serial numbers listed in the provided text box will be managed.

25.1 Wireless SSID




Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model. The below settings shows a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Enable	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.
DHCP Option 82 ^A	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
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	Indicate the maximum number of clients that should be able to connect to each frequency.

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



Security Settings	
Security Policy	<p>This setting configures the wireless authentication and encryption methods. Available options are :</p> <ul style="list-style-type: none"> • Open (No Encryption) • WPA2 -Personal (AES:CCMP) • WPA2 – Enterprise • WPA/WPA2 - Personal (TKIP/AES: CCMP) • WPA/WPA2 – Enterprise <p>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</p>

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.



The screenshot shows the 'Access Control Settings' window. It has two main sections: 'Restricted Mode' and 'MAC Address List'. The 'Restricted Mode' section has a dropdown menu currently set to 'Deny all except listed'. The 'MAC Address List' section has a large text input area with a question mark icon to its left.

Access Control

Restricted Mode

The settings allow administrator to control access using MAC address filtering. Available options are **None**, **Deny all except listed**, and **Accept all except listed**

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.



The screenshot shows the 'RADIUS Server Settings' window. It is divided into two columns: 'Primary Server' and 'Secondary Server'. Each column has fields for 'Host', 'Secret', 'Authentication Port', and 'Accounting Port'. The 'Secret' fields have a 'Hide Characters' checkbox. The 'Authentication Port' and 'Accounting Port' fields have 'Default' buttons. The 'NAS Identifier' field at the bottom has a 'Device Name' dropdown menu.

RADIUS Server Settings

Host

Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.

Secret

Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.

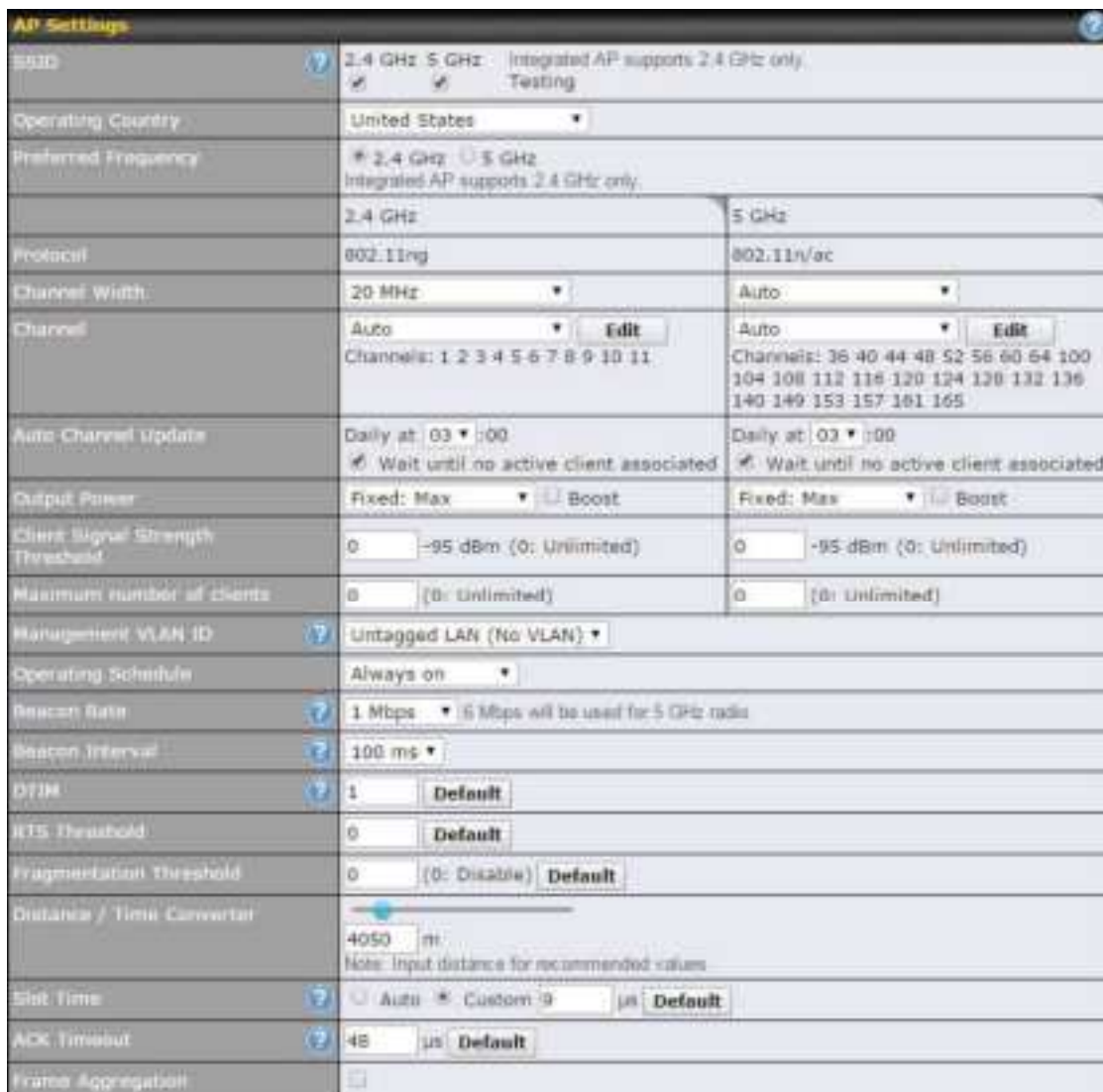
Authentication

In field, enter the UDP authentication port(s) used by your RADIUS server(s) or click

Port	the Default button to enter 1812 .
Accounting Port	In field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the Default button to enter 1813 .
NAS-Identifier	Choose between Device Name , LAN MAC address , Device Serial Number and Custom Value

25.2 Settings

On many Pepwave models, the AP settings screen (**AP>Settings**) looks similar to the example below:



AP Settings

2.4 GHz 5 GHz Integrated AP supports 2.4 GHz only, Testing

Operating Country: United States

Preferred Frequency: 2.4 GHz 5 GHz Integrated AP supports 2.4 GHz only

Protocol: 802.11n 802.11n/ac

Channel Width: 20 MHz Auto

Channel: Auto Edit Channels: 1 2 3 4 5 6 7 8 9 10 11

Auto Channel update: Daily at 03:00 Wait until no active client associated

Output Power: Fixed: Max Boost

Client Signal Strength Threshold: 0 -95 dBm (0: Unlimited)

Maximum number of clients: 0 (0: Unlimited)

Management VLAN ID: Untagged LAN (No VLAN)

Operating Schedule: Always on

Beacon Rate: 1 Mbps 6 Mbps will be used for 5 GHz radio

Beacon Interval: 100 ms

DTIM: 1 Default

RTS Threshold: 0 Default

Fragmentation Threshold: 0 (0: Disable) Default

Distance / Time Converter: 4050 m Note: Input distance for recommended values


Slot Time: Auto Custom: 9 Default

ACK Timeout: 48 Default

Frame Aggregation: ☒

AP Settings	
SSID	<p>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 Peplink Balance 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.</p>
Operating Country	<p>This drop-down menu specifies the national / regional regulations which the AP should follow.</p> <ul style="list-style-type: none"> • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). <p>NOTE: Users are required to choose an option suitable to local laws and regulations.</p> <p>Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.</p>
Preferred Frequency	<p>These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies.</p>
Protocol	<p>This section displays the 2.4 GHz protocols your APs are using.</p>
Channel Width	<p>There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.</p>
Channel	<p>This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.</p>
Auto Channel Update	<p>Indicate the time of day at which update automatic channel selection.</p>
Output Power^A	<p>This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When Dynamic settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance.</p> <p>The Dynamic: Auto setting will set the AP to do this automatically. Otherwise, the Dynamic: Manual setting will set the AP to dynamically adjust only if instructed to do so. If you have set Dynamic: Manual, you can go to AP>Toolbox>Auto Power Adj. to give your AP further instructions.</p> <p>If you click the Boost checkbox, the AP under this profile will transmit using</p>

	additional power. Please note that using this option with several APs in close proximity will lead to increased interference.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Max number of Clients^A	This field determines the maximum clients that can be connected to APs under this profile.
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is 0 by default, meaning that no VLAN tagging will be applied. NOTE: change this value with caution as alterations may result in loss of connection to the AP controller.
Operating Schedule	Choose from the schedules that you have defined in System>Schedule . Select the schedule for the integrated AP to follow from the drop-down menu.
Beacon Rate^A	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are 1Mbps , 2Mbps , 5.5Mbps , 6Mbps , and 11Mbps .
Beacon Interval^A	This drop-down menu provides the option to set the time between each beacon send. Available options are 100ms , 250ms , and 500ms .
DTIM^A	This field provides the option to set the frequency for beacon to include delivery traffic indication message (DTIM). The interval unit is measured in milliseconds.
RTS Threshold^A	This field provides the option to set the minimum packet size for the unit 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 provides the option to modify the unit wait time before it transmits. The default value is 9μs .
ACK Timeout^A	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is 48μs .
Frame Aggregation^A	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.
Frame Length	This field is only available when Frame Aggregation is enabled. It specifies the frame length for frame aggregation. By default, it is set to 50000 .

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



Web Administration Settings (on External AP)

Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	443
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username	admin
Admin Password	25db591396e0 <input type="button" value="Generate"/>

Web Administration Settings	
Enable	Check the box to allow the Pepwave router to manage the web admin access information of the AP.
Web Access Protocol	These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are HTTP and HTTPS .
Management Port	This field specifies the management port used for accessing the device.
HTTP to HTTPS Redirection	This option will be available if you have chosen HTTPS as the Web Access Protocol . With this enabled, any HTTP access to the web admin will redirect to HTTPS automatically.
Admin User Name	This field specifies the administrator username of the web admin. It is set as <i>admin</i> by default.
Admin Password	This field allows you to specify a new administrator password. You may also click the Generate button and let the system generate a random password automatically.

Navigating to **AP>Settings** on some Pepwave models displays a screen similar to the one shown below:



WiControl Management enabled. Settings can now be configured on WiControl.

Wi-Fi Radio Settings

Operating Country	United States
Wi-Fi Mode	<input checked="" type="radio"/> Internal <input type="radio"/> External

Wi-Fi AP Settings

Profile	002.11ng
Channel	1 (2.412 GHz)
Channel Width	Auto
Output Power	Max <input type="checkbox"/> Boost
Beacon Rate	1 Mbps
Beacon Interval	100ms
DTIM	3
WMM	9 <input type="checkbox"/> 10
ACE Threshold	95 <input type="checkbox"/> 10
Frame Aggregation	<input checked="" type="checkbox"/> Enable
Guard Interval	<input type="checkbox"/> Short <input checked="" type="checkbox"/> Long

Wi-Fi Radio Settings

Operating Country	This option sets the country whose regulations the Pepwave router follows.
Wi-Fi Antenna	Choose from the router's internal or optional external antennas, if so equipped.

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.

Wi-Fi AP Settings

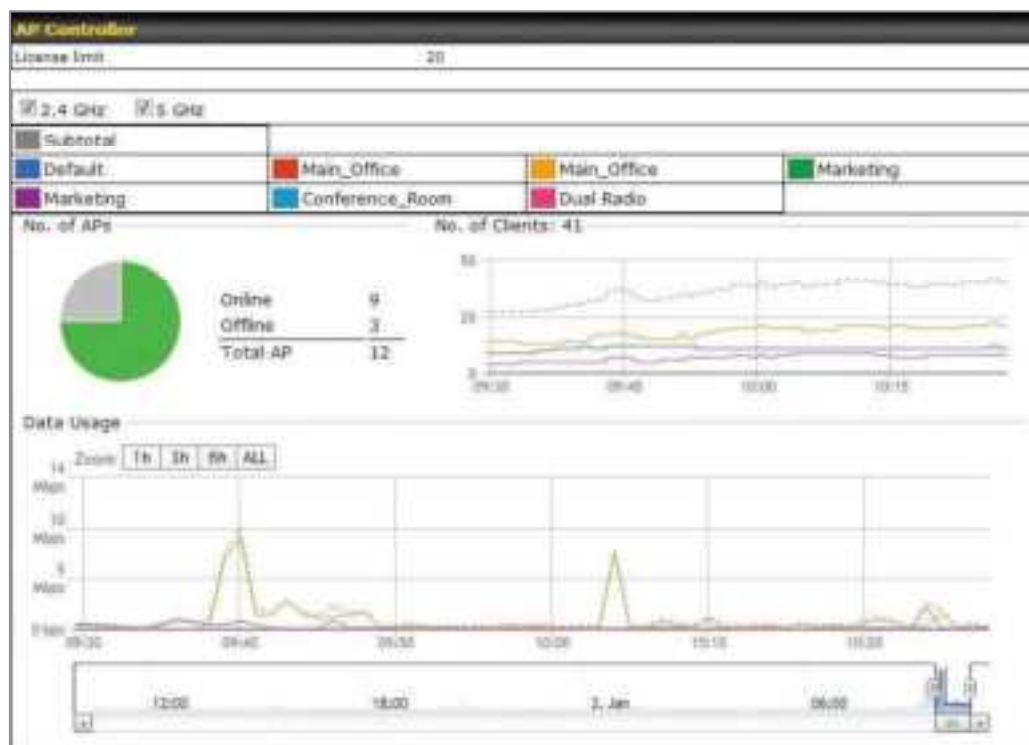
Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are 802.11ng and 802.11na . By default, 802.11ng is selected.
Channel	This option allows you to select which 802.11 RF channel will be used. Channel 1 (2.412 GHz) is selected by default.
Channel Width	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.
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.
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 .
Slot Time^A	This field is for specifying the wait time before the Router 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 .
Frame Aggregation^A	This option allows you to enable frame aggregation to increase transmission throughput.
Guard Interval^A	This setting allows choosing a short or long guard period interval for your transmissions.

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

26 AP Controller Status

26.1 Info

A comprehensive overview of your AP can be accessed by navigating to **AP > Controller Status > Info**.



AP Controller	
License Limit	This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage.
Frequency	Underneath, there are two check boxes labeled 2.4 Ghz and 5 Ghz . Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.
SSID	The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs.
No. of APs	This pie chart and table indicates how many APs are online and how many are offline.
No. of Clients	This graph displays the number of clients connected to each network at any given time. Mouse over any line on the graph to see how many clients connected to a

specific SSID for that point in time.

Data Usage

This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to **Zoom** to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client 54:EA:48:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:02:42	AP One 300M: Client 54:EA:48:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:03:38	AP One 300M: Client 54:EA:48:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:03:38	AP One 300M: Client 00:21:64:35:39:AA associated with Balance_11a	
Jan 2 11:03:20	AP One 300M: Client 60:67:20:24:88:4C disassociated from Marketing_11a	
Jan 2 11:03:09	AP One 300M: Client 54:EA:48:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:21:64:35:39:AA disassociated from Balance_11a	
Jan 2 10:59:08	Office Floor AP: Client 18:00:2D:3D:4E:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:48:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 10:8F:48:2B:76:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:48:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:48:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:05	AP One 300M: Client 54:EA:48:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:48:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:48:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:26:8B:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:05	AP One 300M: Client 6C:D4:EB:13:29:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:48:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:48:2D:A0:D5 associated with Marketing_11a	

Events

This event log displays all activity on your AP network, down to the client level. Click **View Alerts** to see only alerts, and click the **More...** link for additional records.

26.2 Access Point (Usage)

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

Search Filter	
AP Name / Serial Number / SSID	All
	<input type="checkbox"/> Include Offline APs
Search Result:	

Managed APs							Expand	Collapse
Name	IP Address	MAC	Location	Firmware Pack III	Configuration			
Default (3/9 online)								
000-0000-0000	10.0.0.11	00:1A:00:00:00:00		3.3.3	None			



Usage




AP Name/Serial Number


This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.

Online Status

This button toggles whether your search will include offline devices.

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. You could also expand and collapse all groups by using the   buttons.


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

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



AP Name	AP ID	AP Type	AP Model	AP Status	AP Channel	AP Clients	AP Upload	AP Download
00:00:00:00:00:00	00:00:00	000.11ng	Excellent (27)	Balance	88.24 MB	26.24 MB		
04-0a-00-00-00-00	00:00:00	000.11ng	Excellent (42)	Balance	8.03 MB	2.24 MB		
00:00:00:00:00:00	00:00:00	000.11ng	Good (23)	Balance	1.84 MB	88.43 MB		
00:00:00:00:00:00	00:00:00	000.11ng	Excellent (39)	Balance	3.42 MB	474.52 MB		
00:00:00:00:00:00	00:00:00	000.11ng	Excellent (28)	Balance	88.24 MB	481.57 MB		
14-0a-00-00-00-00	00:00:00	000.11ng	Excellent (28)	Balance	2.24 MB	3.47 MB		
00:00:00:00:00:00	00:00:00	000.11ng	Excellent (29)	Wireless	5.35 MB	5.75 MB		
00:00:00:00:00:00	00:00:00	000.11ng	Excellent (25)	Wireless	6.24 MB	11.14 MB		
00:00:00:00:00:00	00:00:00	000.11ng	Good (20)	Wireless	118.05 MB	7.32 MB		
00:00:00:00:00:00	00:00:00	000.11ng	Excellent (35)	Marketing	74.75 MB	4.55 MB		
04:00:00:00:00:00	00:00:00	000.11ng	Poor (22)	Marketing	84.34 MB	118.02 MB		


Managed Wireless Devices

Click the  icon to configure each client



Serial Number	1111-2222-3333
MAC Address	00:1A:00:00:00:00
Product Name	Pepwave AP Pro Dual
Name	
Location	
Hardware Version	1.1.1
Hardware Pack	Default (None)
AP Client List	<input checked="" type="radio"/> Follow AP Profile <input type="radio"/> Custom
2.4 GHz SSID List	24Open
5 GHz SSID List	5GOpen
Last Config Applied by	Admin User 11:15:00:00 HKT 2015
Uptime	66d 18h 11:15:00:00 HKT 2015
Current Channel	1 (2.4 GHz)
Channel	2.4 GHz: Follow AP Profile • 5 GHz: Follow AP Profile •
Output Power	2.4 GHz: Follow AP Profile • 5 GHz: Follow AP Profile •

For easier network management, you can give each client a name and designate

Click the  icon to see a graph displaying usage:

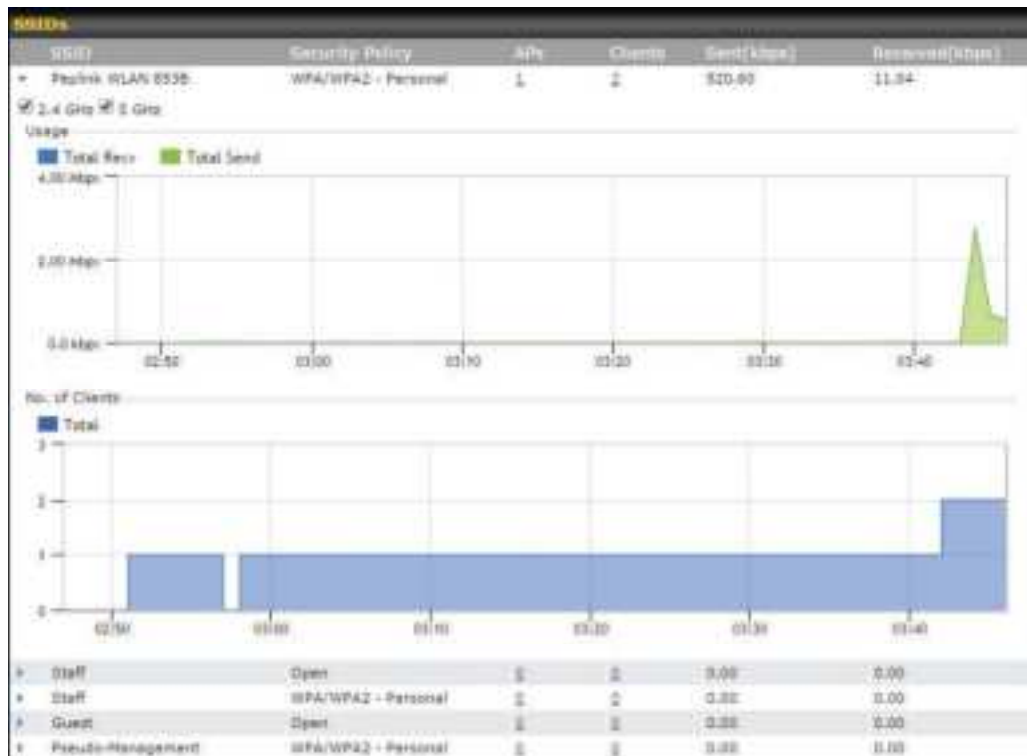


Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:

Event Information	
Events	
Jan 2 21:23:39	Client 22:26:5D:89:AC:FD associated with Wireless_11a
Jan 2 21:28:31	Client 22:67:23:31:68:8C disassociated from Marketing_11a
Jan 2 21:35:51	Client 22:68:2F:61:3F:10 disassociated from Sales_11a
Jan 2 21:33:44	Client 22:68:2F:61:3F:10 associated with Wireless_11a
Jan 2 21:38:45	Client 22:67:23:31:68:8C associated with Marketing_11a
Jan 2 21:38:36	Client 22:31:6A:52:58:44 associated with Sales_11a
Jan 2 21:56:30	Client 22:67:23:31:68:8C disassociated from Marketing_11a
Jan 2 22:03:39	Client 22:31:6A:52:58:44 disassociated from Sales_11a
Jan 2 22:42:28	Client FA:67:22:19:33:29 associated with Wireless_11a
Jan 2 22:39:51	Client 24:7A:07:73:12:40 associated with Wireless_11a
Jan 2 22:04:27	Client 22:68:2F:61:3F:10 disassociated from Marketing_11a
Jan 2 22:04:17	Client 22:68:2F:61:3F:10 named to Marketing_11a as 2268-2F6C-2330
Jan 2 22:12:12	Client 22:6D:10:30:42:62 associated with Sales_11a
Jan 2 22:12:21	Client 22:6D:10:30:42:62 named to Wireless_11a from 226D-1030-426C
Jan 2 22:07:02	Client 0C:5A:61:35:07:F9 associated with Wireless_11a
Jan 2 22:04:35	Client 22:67:23:31:68:8C associated with Marketing_11a
Jan 2 22:03:06	Client 22:67:23:31:68:8C disassociated from Marketing_11a
Jan 2 22:08:27	Client 22:26:5D:89:AC:FD associated from Wireless_11a
Jan 2 22:02:46	Client 22:26:5D:89:AC:FD associated with Wireless_11a
Jan 2 22:05:26	Client 3C:3A:83:3F:17:62 associated with Sales_11a

26.3 Wireless SSID

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



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



26.4 Wireless Client

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

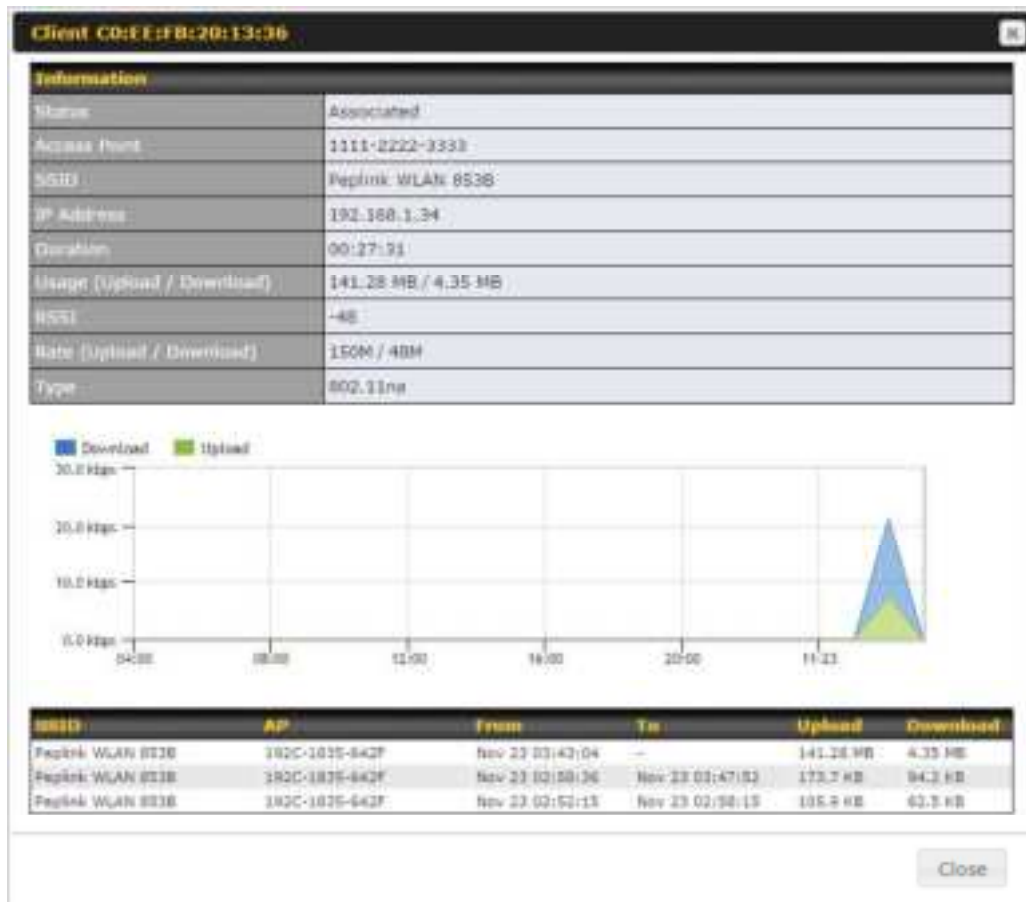


Client MAC / SSID / AP Serial Number	Maximum Result (1-256)	Search Result
	50	

Top 10 Clients of last hour (Updated at 03:00)		
Client MAC Address	Sent(kbps)	Received(kbps)
C0:EE:FE:20:33:36	00.3 KB	101.4 KB












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:





26.5 Nearby Device

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

Suspected Rogue APs					
Client MAC Address	Client Name	Count	Security Profile	Time	Actions
00:1A:0D:0E:03:03	Wireless...	15	WPA2	18 hours ago	 
00:1A:0D:0E:03:03	Accounting	15	WPA2	18 hours ago	 
00:1A:0D:0E:03:04	Marketing	15	WPA2	18 hours ago	 
00:03:7F:00:00:00	HYBRUSH	1	WPA & WPA2	11 minutes ago	 
00:03:7F:00:00:01	HYBRUSH	1	WPA2	15 minutes ago	 
00:1A:0D:0E:00:00	PEPWAVER_C87E	1	WPA & WPA2	5 minutes ago	 
00:1A:0D:0E:00:01	Mini_E1_1	6	WPA & WPA2	1 hour ago	 
00:1A:0D:0E:02:48	MAX_H02_G001	15	WPA & WPA2	2 minutes ago	 
00:1A:0D:0E:03:01	PEPLINK_0588	4	WPA & WPA2	1 minute ago	 
00:1A:0D:0E:03:02	UK_0588	4	WPA2	1 minute ago	 
00:1A:0D:0E:03:03	UK_0588_VLAN22	4	WPA2	1 minute ago	 
00:1A:0D:0E:03:04	dev_captive_portal_test	1	WPA & WPA2	3 minutes ago	 
00:1A:0D:0E:03:05	PEPWAVER_7092	15	WPA & WPA2	2 hours ago	 
00:1A:0D:0E:03:06	dev_captive_portal_test	6	WPA & WPA2	6 minutes ago	 
00:1A:0D:0E:03:07	void_test	8	WPA & WPA2	2 minutes ago	 
00:1A:0D:0E:03:08	SSID New	8	WPA & WPA2	2 minutes ago	 
00:1A:0D:0E:03:09	Guest SSID	8	WPA2	2 minutes ago	 
00:1A:0D:0E:03:0A	PEPWAVER_6788	5	WPA & WPA2	5 minutes ago	 
00:1A:0D:0E:03:0B	G 891 Portal	1	WPA2	2 minutes ago	 
00:1A:0D:0E:03:0C	void_test	8	WPA & WPA2	2 hours ago	 

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.

26.6 Event Log

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

Filter	
Search key	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name
Time	From <input type="text"/> <input type="text"/> to <input type="text"/> <input type="text"/>
Alerts only	<input type="checkbox"/>
<input type="button" value="Search"/>	

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client 54:EA:48:2D:AD:D5 disassociated from Marketing_11a	
Jan 2 11:02:42	AP One 300M: Client 54:EA:48:2D:AD:D5 associated with Marketing_11a	
Jan 2 11:03:38	AP One 300M: Client 54:EA:48:2D:AD:D5 disassociated from Marketing_11a	
Jan 2 11:05:36	AP One 300M: Client 00:11:64:33:38:AA associated with Science_11a	
Jan 2 11:05:20	AP One 300M: Client 60:67:20:54:88:4C disassociated from Marketing_11a	
Jan 2 11:05:09	AP One 300M: Client 54:EA:48:2D:AD:D5 associated with Marketing_11a	
Jan 2 10:59:04	AP One 300M: Client 00:21:64:33:38:AA disassociated from Science_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Science	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:48:2D:AD:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office Inwall: Client 18:0F:48:29:76:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:48:2D:AD:D5 associated with Marketing_11a	
Jan 2 10:57:14	AP One 300M: Client 54:EA:48:2D:AD:D5 disassociated from Marketing_11a	
Jan 2 10:57:06	AP One 300M: Client 54:EA:48:2D:AD:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:48:2D:AD:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:48:2D:AD:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:26:8B:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:06	AP One 300M: Client 9C:D4:CB:11:29:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:48:2D:AD:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:48:2D:AD:D5 associated with Marketing_11a	

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.

27 Toolbox

Tools for managing firmware packs can be found at **AP>Toolbox**.

Firmware Packs			
Pack ID	Release Date	Details	Action
1.1.26	2017-09-26		
Check for updates Manual Upload Default (no default defined)			

Firmware Packs

Here, you can manage the firmware of your AP. Clicking on  will result in information regarding each firmware pack. To receive new firmware packs, you can click **Check for Updates** to download new packs, or you can click **Manual Upload** to manually upload a firmware pack. Click **Default** to define which firmware pack is default.

28 System Settings

28.1 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.

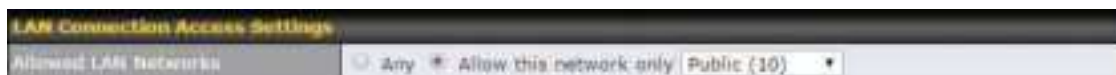
For security reasons, after logging in to the web admin Interface for the first time, it is recommended to change the administrator password. Configuring the administration interface to be accessible only from the LAN can further improve system security. Administrative settings configuration is located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



Admin Settings	
Router Name	MBX-345A <small>hostname: mbx-345a</small>
<small>This configuration is being managed by InControl.</small>	
Admin User Name	admin
Admin Password	*****
Confirm Admin Password	*****
Read-only User Name	DemoPep
User Password	*****
Confirm User Password	*****
Web Session Timeout	4 Hours 0 Minutes
Authentication by RADIUS	<input type="checkbox"/> Enable
CLI SSH & Console	<input type="checkbox"/> Enable
Security	HTTP / HTTPS * <input type="checkbox"/> Redirect HTTP to HTTPS
Web Admin Access	HTTP: LAN Only * HTTPS: LAN Only *
Web Admin Port	HTTP: 80 HTTPS: 443 Default
LAN Connection Access Settings	
Allowed LAN Networks	* Any <input type="checkbox"/> Allow this network only
Save	

Admin Settings	
Router Name	This field allows you to define a name for this Pepwave router. By default, Router Name is set as MAX_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 by RADIUS	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.
Auth Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.

Network Connection	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
CLI SSH	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to Section 30.5 .
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
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
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
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>



LAN Connection Access Settings

Allowed LAN Networks

This field allows you to permit only specific networks or VLANs to access the Web UI.



WAN Connection Access Settings

Allowed Source IP Subnets

This field allows you to restrict web admin access only from defined IP subnets.

- **Any** - Allow web admin accesses to be from anywhere, without IP address restriction.
- **Allow access from the following IP subnets only** - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:

The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of *w.x.y.z/m*, where *w.x.y.z* is an IP address (e.g., 192.168.0.0), and *m* is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, 192.168.0.0/24).

To define multiple subnets, separate each IP subnet one in a line. For example:

- 192.168.0.0/24
- 10.8.0.0/16

Allowed WAN IP Address(es)

This is to choose which WAN IP address(es) the web server should listen on.

28.2 Firmware

28.2.1 Web admin interface : automatically check for updates

Upgrading firmware can be done in one of three ways. Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

The automatic upgrade can be done from **System > Firmware**.



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



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

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



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

Firmware Upgrade

It may take up to 8 minutes.



*Upgrading the firmware will cause the router to reboot.

28.2.2 Web admin interface : install updates manually

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

site may also be recommended or required for a couple of reasons.

All of the Peplink/Pepwave GA firmware can be found [here](#). Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the Balance line.



Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual
Balance 1300	HW2	7.1.2	Download	PDF	PDF
Balance 1500	HW1	6.3.4	Download	PDF	PDF
Balance 20	HW1-B	7.1.2	Download	PDF	PDF
Balance 210	HW4	7.1.2	Download	PDF	PDF

If the device has more than one firmware version the current hardware revision will be required to know what firmware to download.

Navigate to System > Firmware and click the Choose File button under the Manual Firmware Upgrade section. Navigate to the location that the firmware was downloaded to select the “.img” file and click the Open button.

Click on the Manual Upgrade button to start the upgrade process.



A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the Ok button to start the upgrade process. The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will depend on the router that's being upgraded.

Firmware Upgrade

It may take up to 8 minutes.



***Upgrading the firmware will cause the router to reboot.**

28.2.3 The InControl method

[Described in this knowledgebase article on our forum.](#)

28.3 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**.



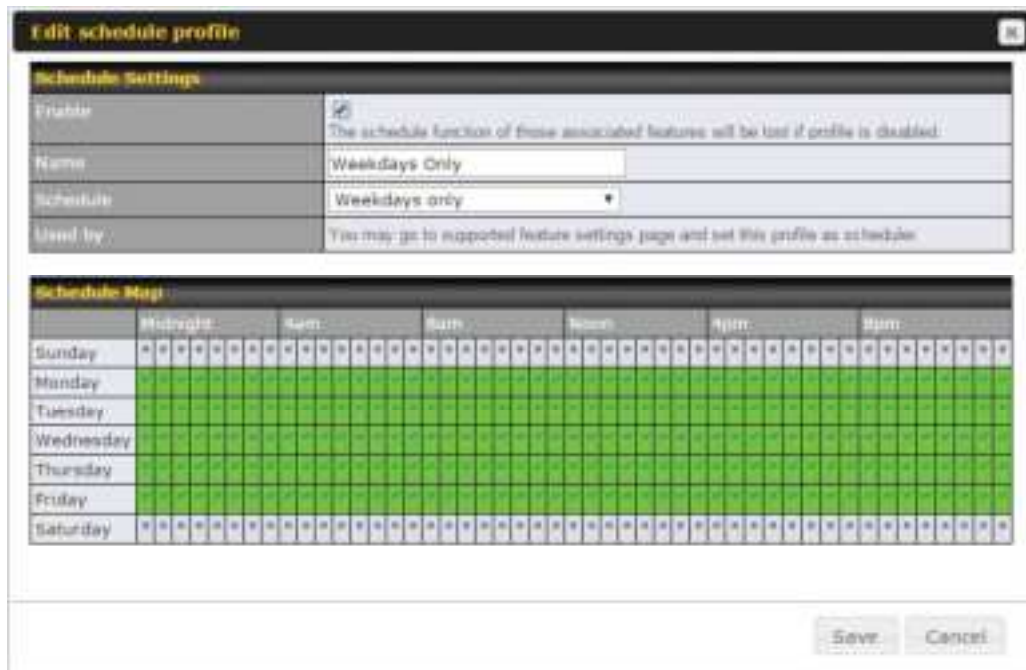
Time Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme). The Time Zone value affects the time stamps in the Pepwave router's event log and e-mail notifications. Check Show all to show all time zone options.
Time Server	This setting specifies the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

28.4 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**



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



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

28.5 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 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 .
SSL Encryption	Check the box to enable SMTPS. When the box is checked, SMTP Port will be changed to 465 automatically.
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to 25 ; when SSL Encryption is checked, the default port number will be set to 465 . You may customize the port number by editing this field. Click Default to restore the number to its default setting.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if Require authentication is checked in the SMTP Server setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address the Pepwave router will use to send reports.
Recipient's Email Address	This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the

enter key.

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

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

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

Test email sent. Email notification settings are not saved, it will be saved after clicked the 'Save' button.

Test Result


```
[INFO] Try email through connection #3
[<-] 220 ESMTP
[->] EHLO balance
[<-] 250-smtp Hello balance [210.210.210.210]
250-SIZE 100000000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250-UNIQUE
```

28.6 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**.

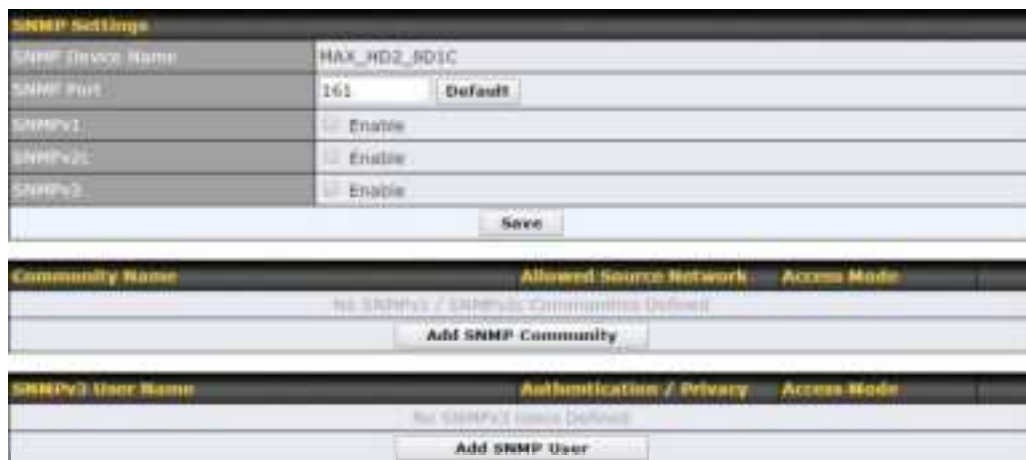
Send Events to Remote Syslog Server	
Remote Syslog	<input checked="" type="checkbox"/>
Remote Syslog Host	

Push Events to Mobile Devices	
Push Events	<input checked="" type="checkbox"/>

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

28.7 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	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.

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:



The image shows a configuration window titled "SNMP Community". It contains a table with two rows: "Community Name" and "Allowed Network". The "Community Name" row has a text input field containing "My Company". The "Allowed Network" row has a text input field containing "192.168.1.25 / 255.255.255.0 (/24)" followed by a small asterisk icon. At the bottom right of the window are "Save" and "Cancel" buttons.

SNMP Community	
Community Name	My Company
Allowed Network	192.168.1.25 / 255.255.255.0 (/24) *

Save Cancel

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

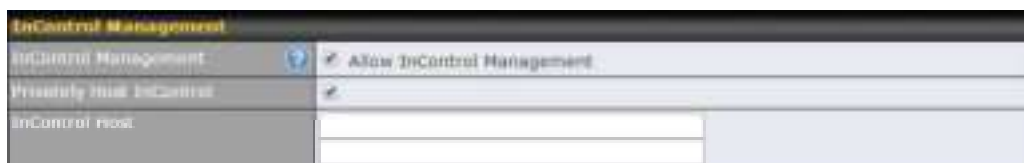
To define a user name for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:



The image shows a configuration window titled "SNMPv3 User". It contains three rows of settings: "User Name" with the value "SNMPUser", "Authentication" with a dropdown menu set to "SHA" and a text field for "password", and "Privacy" with a dropdown menu set to "DES" and a text field for "privacypassword". At the bottom right, there are "Save" and "Cancel" buttons.

SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	<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 Protocol	<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>

28.8 InControl



The image shows a configuration window titled "InControl Management". It contains three rows: "InControl Management" with a checkbox labeled "Allow InControl Management" that is checked, "Presets must be InControl" with a checkbox that is checked, and "InControl host" with a text input field.

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.

28.9 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.

Upload Configurations from High Availability Pair

In a high availability (HA) configuration, a Pepwave router can quickly load the configuration of its HA counterpart. To do so, click the **Upload** button. After loading the settings, configure the LAN IP address of the Pepwave router so that it is different from the HA counterpart.

28.10 Feature Add-ons

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



28.11 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.

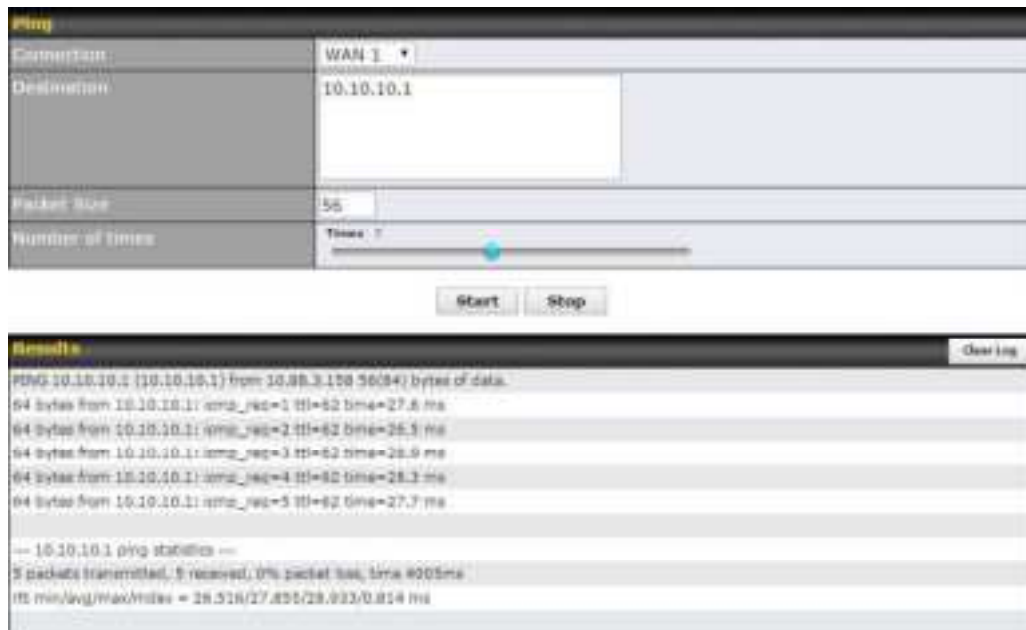


29 Tools

29.1 Ping

The ping test tool sends pings through a specific Ethernet interface or a SpeedFusion™ VPN

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



The screenshot shows the 'Ping' utility window. The 'Connection' is set to 'WAN 1'. The 'Destination' is '10.10.10.1'. The 'Packet Size' is '55'. The 'Number of times' is set to 'Times 7'. There are 'Start' and 'Stop' buttons. Below the configuration is a 'Results' window showing the output of the ping command.

```

PING 10.10.10.1 (10.10.10.1) from 10.30.3.150 56(84) bytes of data:
64 bytes from 10.10.10.1: icmp_seq=1 ttl=62 time=27.6 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=62 time=26.3 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=62 time=26.9 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=62 time=26.3 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=62 time=27.7 ms


--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 26.516/27.856/29.933/0.814 ms
  
```

Tip

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

29.2 Traceroute Test

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**.



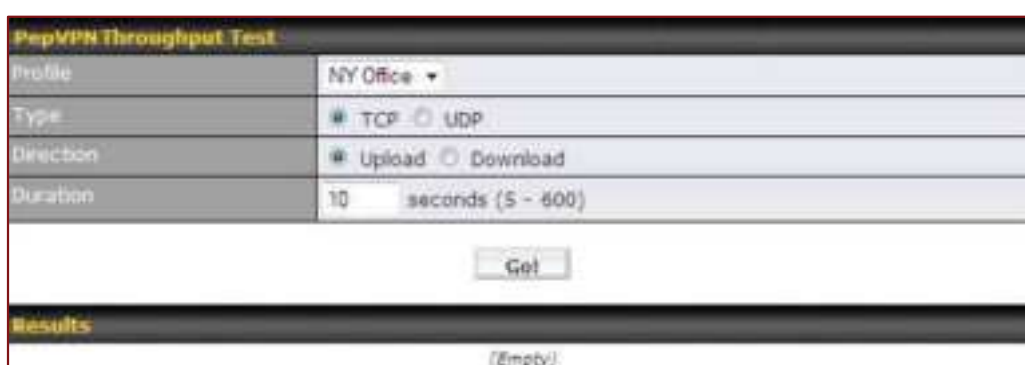
Tip

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

29.3 PepVPN Test

The **PepVPN Test** tool can help to test the throughput between different VPN peers.

You can define the **Test Type**, **Direction**, and **Duration** of the test, and press **Go!** to perform the throughput test. The VPN test utility is located at **System>Tools>PepVPN Test**, illustrated as follows:



29.4 Wake-on-LAN

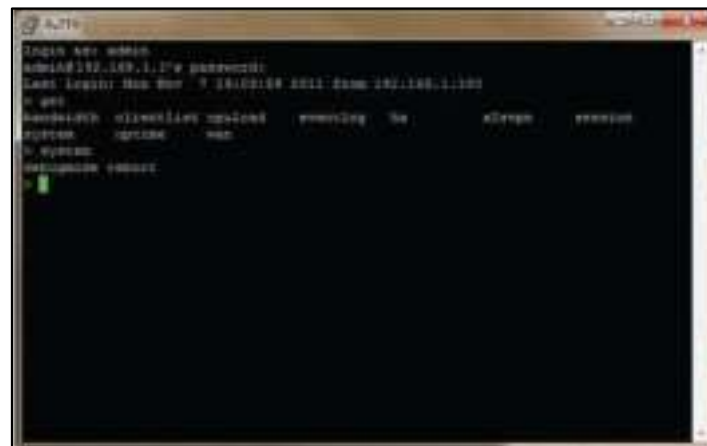
Peplink routers can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**



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

29.5 CLI (Command Line Interface Support)

The CLI (command line interface) can be accessed via SSH. This field enables CLI support. The below settings specify which TCP port and which interface(s) should accept remote SSH CLI access. The user name and password used for remote SSH CLI access are the same as those used for web admin access.



30 Status

30.1 Device

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


System Information	
Router Name	MBX-345A
Model	Pepwave MAX HD4 MBX
Product Code	MAX-HD4-MBX-LTEA-R
Hardware Revision	2
Serial Number	2836-0803-0FLA
Firmware	8.0.0 build 1218
OpenVPN Version	8.0.0
Modem Support Version	1023 (Modem Support List)
InControl Managed Configurations	Firmware, LAN
Host Name	mbx-345a
Uptime	3 days 3 minutes
System Time	Fri Mar 22 13:57:08 GMT 2019
OpenVPN Client Profile	Boson all traffic Split tunnel
Diagnostic Report	Download
Remote Assistance	Turn On

MAC Address	
LAN	00:1A:3C:4E:00:30
WAN 1	00:1A:3C:4E:00:11
WAN 2	00:1A:3C:4E:00:11
WAN 3	00:1A:3C:4E:00:11


[Legal](#)

System Information	
Router Name	This is the name specified in the Router Name field located at System>Admin Security .
Model	This shows the model name and number of this device.
Product Code	If your model uses a product code, it will appear here.
Hardware	This shows the hardware version of this device.

Revision	
Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version this device is currently running.
PepVPN Version	This shows the current PepVPN version.
Modem Support Version	This shows the modem support version. For a list of supported modems, click Modem Support List .
InControl Managed Configuration	InControl Managed Configurations (firmware, VLAN, Captive Portal, etcetera)
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.
OpenVPN Client Profile	Link to download OpenVpn Client profile when this is enabled in Remote User Access
Diagnostic Report	The Download link is for exporting a diagnostic report file required for system investigation.
Remote Assistance	Click Turn on to enable remote assistance.

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

30.2 GPS Data

GPX File 	2019-03-22 (Today) ▾	Download
Diagnostic Report	2019-03-22 (Today)	
Remote Assistance	2019-03-21	
	2019-03-20	
	2019-03-19	
MAC Address	2019-03-18	
	2019-03-17	
LAN	2019-03-16	

GPS enabled models automatically store up to seven days of GPS location data in GPS

eXchange format (GPX). To review this data using third-party applications, click **Status>Device** and then download your GPX file.

The Pepwave GPS enabled devices export real-time location data in NMEA format through the LAN IP address at TCP port 60660. It is accessible from the LAN or over a SpeedFusion connection. To access the data via a virtual serial port, install a virtual serial port driver. Visit <http://www.peplink.com/index.php?view=faq&id=294> to download the driver.

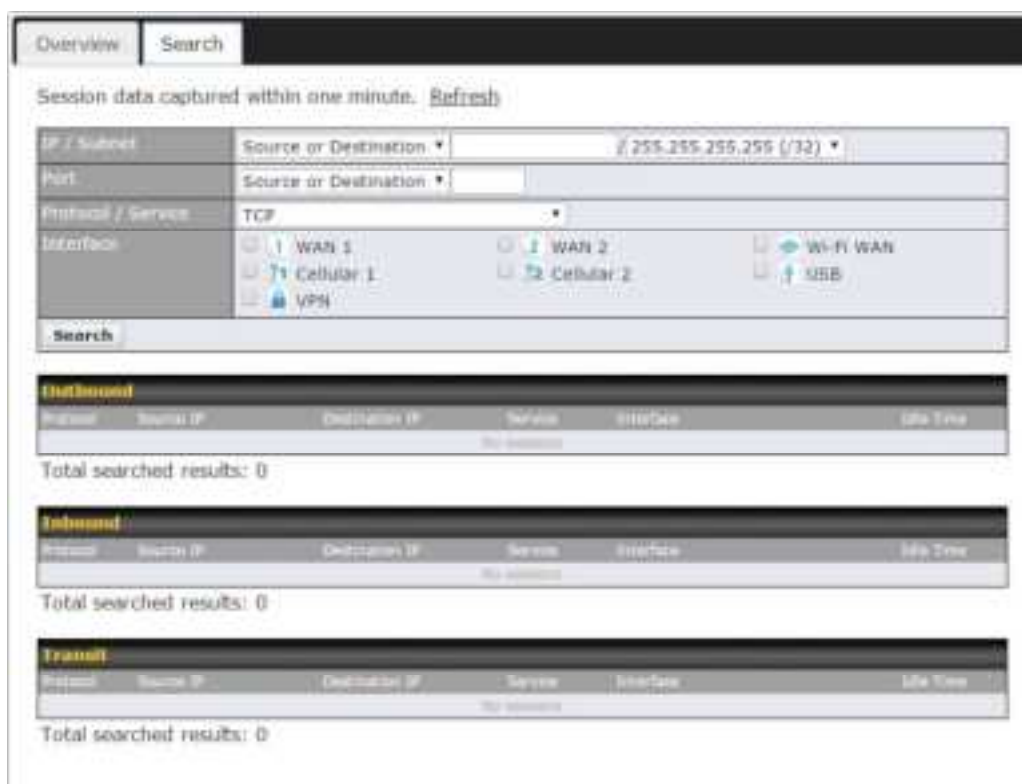
30.3 Active Sessions

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

Overview Search		
Session data captured within one minute. Refresh		
Service	Inbound Sessions	Outbound Sessions
ATM/ICQ	0	1
Bittorrent	0	32
DNS	0	51
Flash	0	1
HTTPS	0	76
Jabber	0	5
MSN	0	11
NTP	0	4
QQ	0	1
Remote Desktop	0	3
SSH	0	12
SSL	0	64
XMPP	0	4
Yahoo	0	1
Interface	Inbound Sessions	Outbound Sessions
WAN 1	0	176
WAN 2	0	32
Wi-Fi WAN	0	51
Cellular 1	0	64
Cellular 2	0	0
USB	0	0
Top Clients		
Client IP Address	Total Sessions	
10.9.66.66	1069	
10.9.98.144	147	
10.9.2.18	53	
10.9.66.14	56	
10.9.2.25	33	

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

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



Overview Search

Session data captured within one minute. [Refresh](#)

IP / Subnet Source or Destination

Port Source or Destination

Protocol / Service TCP

Interface ☐ WAN 1 ☐ WAN 2 ☐ Wi-Fi WAN
☐ Cellular 1 ☐ Cellular 2 ☐ USB
☐ VPN

Search

Outbound

Source	Source IP	Destination IP	Service	Interface	Life Time
No sessions					

Total searched results: 0

Inbound

Source	Source IP	Destination IP	Service	Interface	Life Time
No sessions					

Total searched results: 0

Transit


Source	Source IP	Destination IP	Service	Interface	Life Time
No sessions					

Total searched results: 0

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

30.4 Client List

The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses, names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address.

Clients can be imported into the DHCP reservation table by clicking the  button on the right. You can update the record after import by going to **Network>LAN**.



Filter ☐ Online Clients Only ☐ DHCP Clients Only

Client List

IP Address	Name	Download (Kbps)	Upload (Kbps)	MAC Address	Import
192.168.1.100		0	0	00:30:86:00:01:76	

Scale: ☐ kbps ☐ Mbps

If the PPTP server (see **Section 19.2**), SpeedFusion™ (see **Section 12.1**), or AP controller (see **Section 20**) is enabled, you may see the corresponding connection name listed in the **Name** field.

30.5 WINS Client

The WINS client list table is located at **Status>WINS Client**.

WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.20.1
UserC	10.9.2.4
Flush All	


The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server (navigation: **Network>Interfaces>LAN**). The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush All** to flush all WINS client records.

WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.20.1
UserC	10.9.2.4
Flush All	


30.6 UPnP / NAT-PMP

The table that shows the forwarded ports under UPnP and NAT-PMP protocols is located at **Status>UPnP/NAT-PMP**. This section appears only if you have enabled UPnP / NAT-PMP as mentioned in **Section 16.1.1**.

Forwarded Ports						
External ▲	Internal	Internal Address	Type	Protocol	Description	
47453	3392	192.168.1.100	UPnP	UDP	Application 031	
35892	11285	192.168.1.50	NAT-PMP	TCP	NAT-PMP 38	
4500	3560	192.168.1.20	UPnP	TCP	Application 013	
3821	236	192.168.1.30	UPnP	TCP	Application 047	
22409	8943	192.168.1.70	NAT-PMP	UDP	NAT-PMP 97	
2388	27549	192.168.1.40	UPnP	TCP	Application 004	
Delete All						

Click  to delete a single UPnP / NAT-PMP record in its corresponding row. To delete all records, click **Delete All** on the right-hand side below the table.

Important Note

UPnP / NAT-PMP records will be deleted immediately after clicking the button  or **Delete All**, without the need to click **Save** or **Confirm**.

30.7 OSPF & RIPv2

Shows status of OSPF and RIPv2



30.8 BGP

Shows status of BGP



30.9 SpeedFusion Status

Current SpeedFusion™ status information is located at **Status>SpeedFusion™**.

Details about SpeedFusion™ connection peers appears as below:




The screenshot shows the 'Peplink with SpeedFusion - Remote Peer Details' page. It has a search bar at the top. Below the search bar is a table with columns for 'Remote Peer', 'Profile', and 'Information'. The table contains two entries:

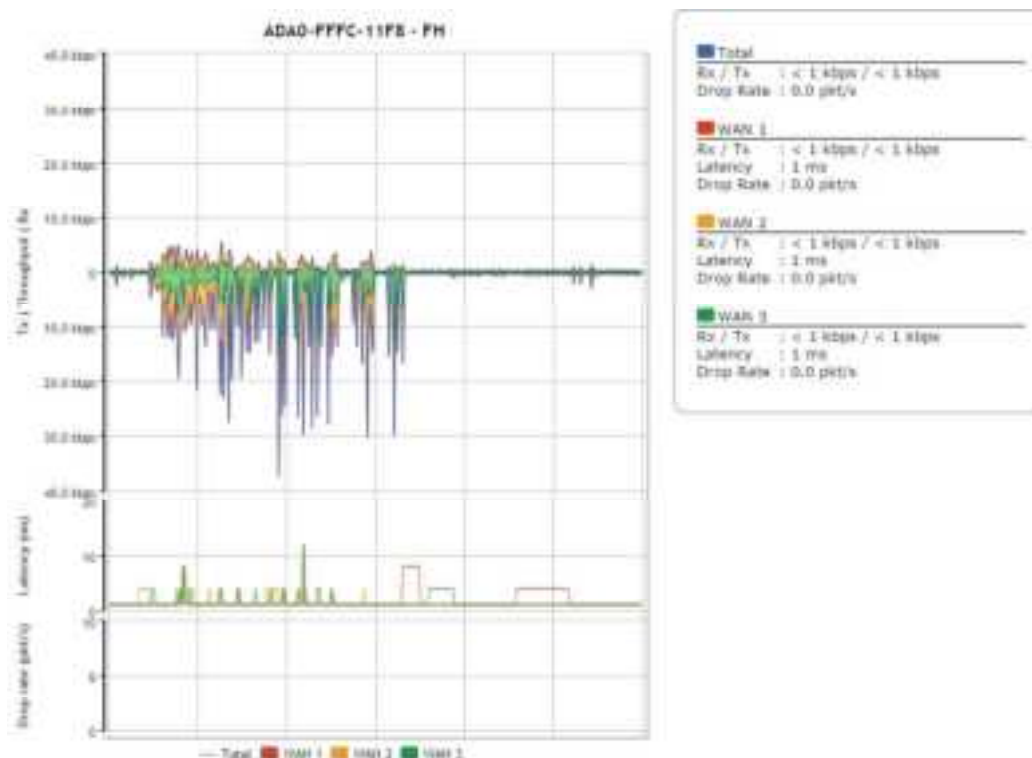
Remote Peer	Profile	Information
AD40-PPFC-11FE	PP	192.168.77.0/24
3002-BF63-102A	100-S - NO NAT	192.168.3.0/24

Each entry has a 'Wi' button and a 'Wi' button next to it. There is also a 'Show disconnected profiles' button in the top right corner.

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

Interface	Profile	Information		
AD40-PFPC-11PB	FW	192.168.77.0/24		
WAN 1	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms		
WAN 2	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms		
WAN 3	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms		
Total	Rx: < 1 kbps Tx: 1.1 kbps	Drop rate: 0.0 pkt/s		
380-S - NO NAT		192.168.3.0/24		
WAN 1	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms		
WAN 2	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms		
WAN 3	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms		
Total	Rx: 1.6 kbps Tx: < 1 kbps	Drop 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

SAL-LAB (1 - 700)

Remote ID

LAB-NET-GW

Router Name

LAB-NET-GW

Serial Number

PL11-8898-547C

[More information](#)

WAN Statistics

Remote Connections

☐ Show remote connections

WAN Label

☒ WAN Name
 ☐ IP Address and Port

ST	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s	Latency:	25 ms
Virgin Media	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s	Latency:	17 ms
WAN 3	Not available - WAN disabled							
WAN 4	Not available - link failure, no data received							
PepLink HK Network	Not available - link failure, no data received							
Mobile Internet	Not available - WAN down							
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

The Speedfusion status page shows all related information about the PepVPN connection. This screen also allows you to run PepVPN Tests allowing throughput tests.

30.10 Event Log

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

Device Event Log	
Device Event Log Auto Refresh	
Mar 22 14:29:44	System: Changes applied
Mar 22 14:29:29	System: Changes applied
Mar 22 14:00:26	WAN: Wi-Fi WAN connected to PEPLINK_1 (10.22.1.152)
Mar 22 11:47:45	Admin: DemoPep (10.22.1.160) login successful
Mar 22 11:47:38	Admin: admin (10.22.1.160) login failed
Mar 22 11:46:59	System: Changes applied
Mar 22 11:45:42	System: Changes applied
Mar 20 15:43:27	System: Changes applied
Mar 20 11:20:15	System: Changes applied
Mar 19 15:23:26	System: Changes applied
Mar 19 15:21:35	System: Changes applied
Mar 19 15:21:31	System: InControl has updated the configuration as InControl configuration updated
Mar 19 15:21:31	System: LAN Configuration has been updated by InControl
Mar 19 15:07:38	System: Changes applied
Mar 19 14:09:27	System: WAN Analysis server stopped
Mar 19 14:09:22	System: WAN Analysis server started (control port: 8000, max. streams: 8)
Mar 19 14:05:30	WAN: WAN 2 connected (10.22.1.155)
Mar 19 14:05:30	WAN: WAN 1 connected (10.22.1.151)
Mar 19 14:05:18	WAN: WAN 2 disconnected
Mar 19 14:05:18	WAN: WAN 1 disconnected
Mar 19 14:05:18	System: Changes applied
Mar 19 13:54:31	WAN: WAN 2 connected (10.22.1.155)
Clear Log	

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.

31 WAN Quality



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

For cellular connections it shows signal strength, quality, throughput and latency for the past hour.

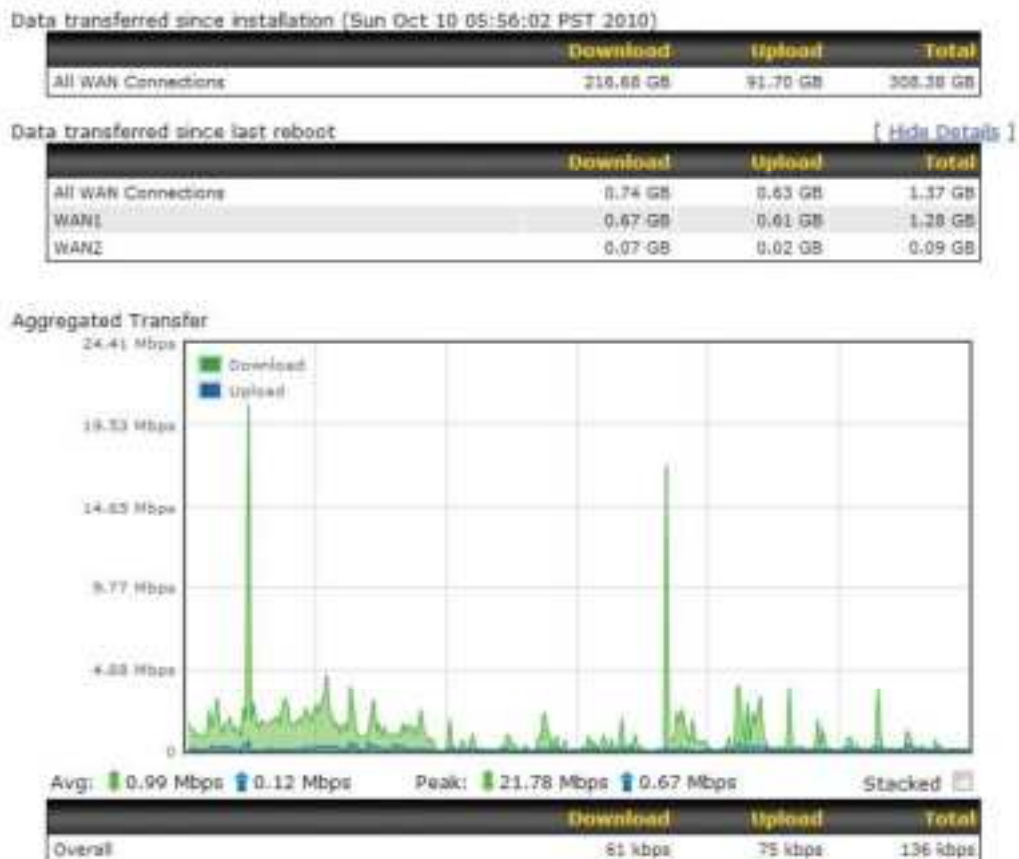
32 Usage Reports

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.

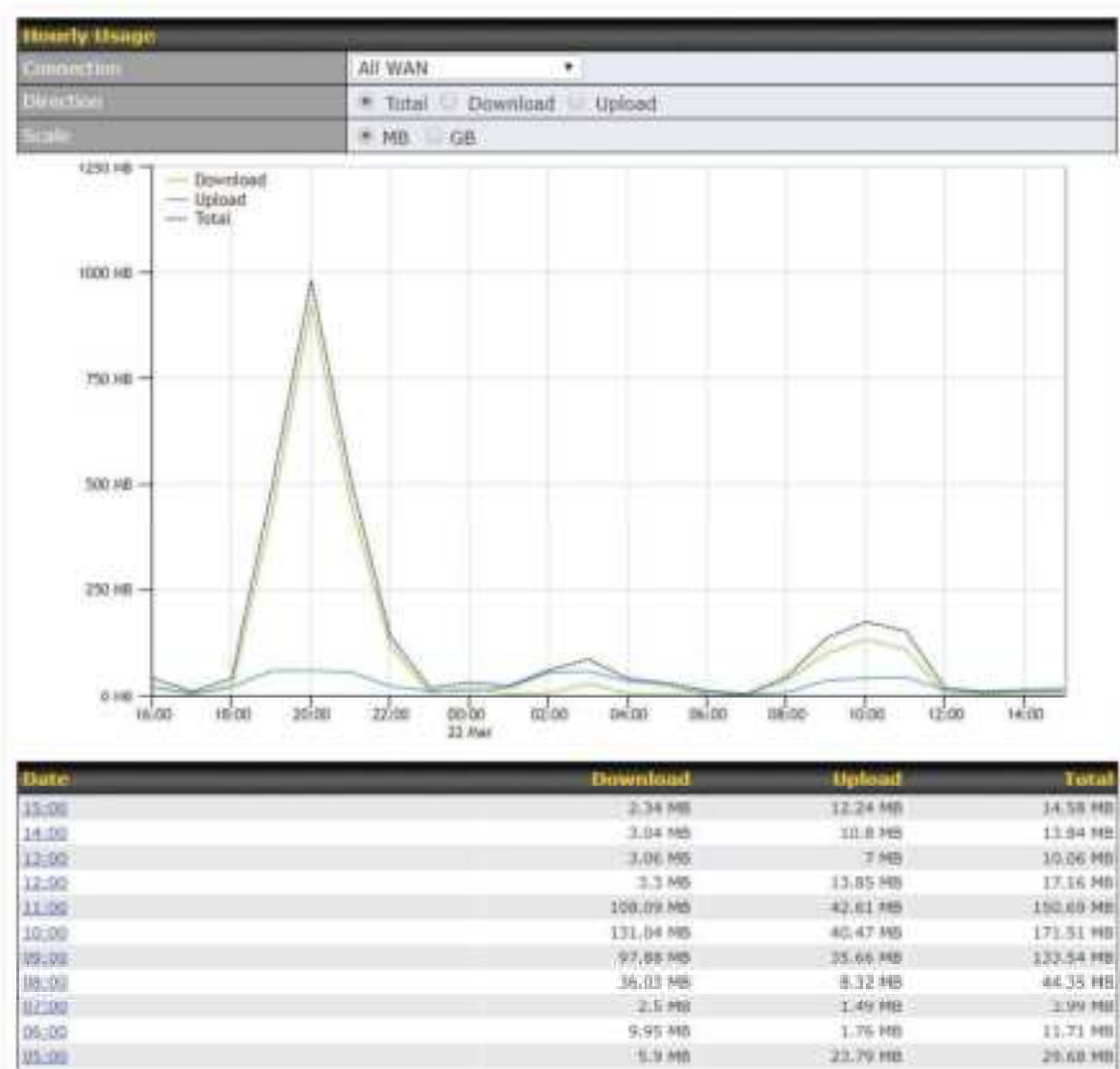
32.1 Real-Time

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.



32.2 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.



32.3 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**).



All WAN Daily Bandwidth Usage

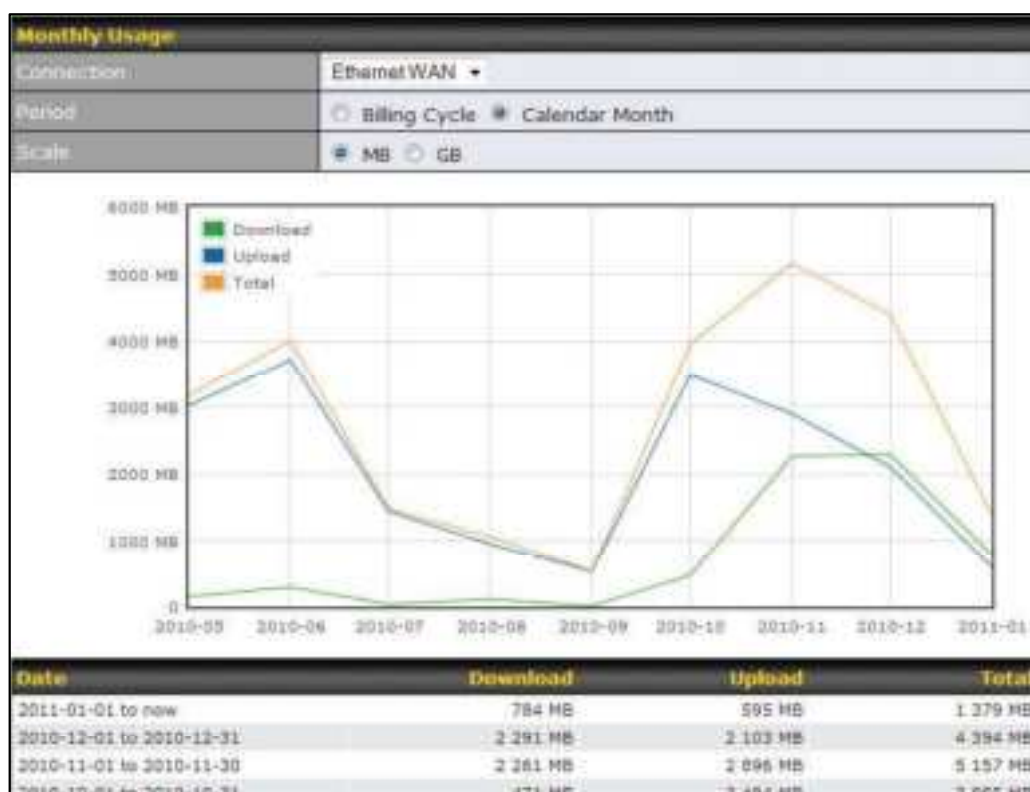
32.4 Monthly

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**).



All WAN Monthly Bandwidth Usage



Ethernet WAN Monthly Bandwidth Usage

Tip

By default, the scale of data size is in **MB**. 1GB equals 1024MB.

Appendix A. Restoration of Factory Defaults

To restore the factory default settings on a Pepwave router, follow the steps below:

1. Locate the reset button on the front or back panel of the Pepwave router.
2. With a paperclip, press the reset button and hold it for at least 10 seconds, until the unit reboots itself.

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

Important Note

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

In CB this product trade mark only PEPWAVE Brand ,



FCC 15.21:

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

RF exposure warning:

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

IC Warning:

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Informations concernant l'exposition aux fréquences radio (RF)

Cet équipement est conforme avec l'exposition aux radiations IC définies pour un environnement noncontrôlé.

Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

Cet émetteur ne doit pas être co-localisées ou opérant en conjonction avec une autre antenne ou transmetteur.

Les utilisateurs finaux et les installateurs doivent être informés des instructions d'installation de l'antenne et des conditions de fonctionnement de l'émetteur afin de satisfaire à la conformité d'exposition RF.

This radio transmitter IC: 20682-P1930LITER6 has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio 20682-P1930LITER6 a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

antenna type: Omni-directional

antenna gain: 5.33