




## 21.1 Outbound and Inbound Firewall Rules

### 21.1.2 Access Rules

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

| Outbound Firewall Rules ( Drag and drop rows by the left to change rule order) |          |        |             |   |   |  |
|--|----------|--------|-------------|---|---|--|
| Rule   | Protocol | Source | Destination | Action  |   |  |
| test   | Any      | Any    | Any         |  |  |  |
| Default  | Any      | Any    | Any         |  |   |  |
| Add Rule   |          |        |             |   |   |  |

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name

Enable

☒ Always on

Protocol

Any Protocol Selection Tool

Source IP & Port

Any Address

Destination IP & Port

Any Address

Action

☒ Allow ☐ Deny

Event Logging

☐ Enable

Save

Cancel

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

| Inbound Firewall Rules ( Drag and drop rows by the left to change rule order) |          |     |        |             |   |   |
|---|----------|-----|--------|-------------|---|---|
| Rule  | Protocol | WAN | Source | Destination | Action  |   |
| test  | Any      | Any | Any    | Any         |  |  |
| Default   | Any      | Any | Any    | Any         |  |   |
| Add Rule  |          |     |        |             |   |   |

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

Add a New Inbound Firewall Rule

### New Firewall Rule

|                       |   |
|-----------------------|---|
| Rule Name             |   |
| 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

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

| Internal Network Firewall Rules ( Drag and drop rows by the left to change rule order) |          |        |             |        |  |
|--|----------|--------|-------------|--------|--|
| Rule   | Protocol | Source | Destination | Action |  |
| test   | Any      | Any    | Any         |        |  |
| Default  | Any      | Any    | Any         |        |  |
| Add Rule   |          |        |             |        |  |

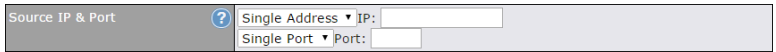
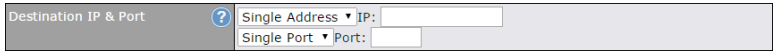
Click **Add Rule** to display the following window:

Add a New Internal Network Firewall Rule

### New Firewall Rule

|               |   |
|---------------|---|
| Rule Name     |   |
| Enable        | <input checked="" type="checkbox"/> Always on                     |
| Protocol      | Any :: Protocol Selection ::                                      |
| Source        | Any Address   |
| Destination   | Any Address   |
| Action        | <input checked="" type="radio"/> Allow <input type="radio"/> Deny |
| Event Logging | <input type="checkbox"/> Enable                                   |

Save
Cancel

| Inbound / Outbound / Internal Network Firewall Settings |  |
|---|--|
| <b>Rule Name</b>  | This setting specifies a name for the firewall rule.   |
| <b>Enable</b>   | <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>  |
| <b>WAN Connection (Inbound)</b>                         | Select the WAN connection that this firewall rule should apply to.   |
| <b>Protocol</b>   | <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"> <li>• Any</li> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• DSCP</li> <li>• IP</li> </ul> <p>Alternatively, the <b>Protocol Selection Tool</b> 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 <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remains manually modifiable.</p> |
| <b>Source IP &amp; Port</b>                             | <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 <b>Source IP &amp; Port</b> setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Source IP &amp; Port</b> settings.</p>   |
| <b>Destination IP &amp; Port</b>                        | <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 <b>Destination IP &amp; Port</b> setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Destination IP &amp; Port</b> settings.</p>  |
| <b>Action</b>   | This setting specifies the action to be taken by the router upon encountering traffic  |

that matches the both of the following:

- Source IP & port
- Destination IP & port

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).

### Event Logging

This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows:



Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1  
DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80

- **CONN:** The connection where the log entry refers to
- **SRC:** Source IP address
- **DST:** Destination IP address
- **LEN:** Packet length
- **PROTO:** Protocol
- **SPT:** Source port
- **DPT:** Destination port

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

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

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

| Outbound Firewall Rules ( Drag and drop rows to change rule order) |          |                |                     |        |   |
|--|----------|----------------|---------------------|--------|---|
| Rule   | Protocol | Source IP Port | Destination IP Port | Policy |   |
| No web access  | TCP      | Any Any        | Any 80              | Deny   |  |
| No FTP access  |          | Any Any        | Any 21              | Deny   |  |
| Default  | Any      | Any            | Any                 | Allow  |   |
| Add Rule   |          |                |                     |        |   |

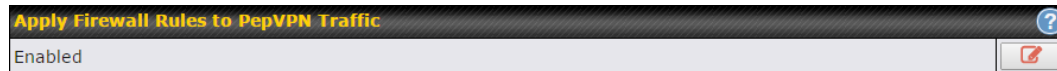
To remove a rule, click the  button.


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

### Tip

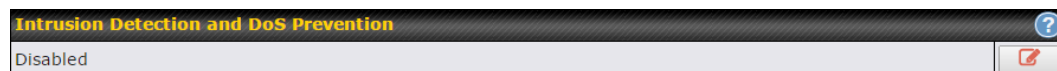
If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound Allow firewall rules will be required for inbound port forwarding and inbound NAT mapping rules. However, if the default inbound rule is set as **Deny**, a corresponding Allow firewall rule will be required.


## 21.1.3 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.

## 21.1.4 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
  - o NMAP FIN/URG/PSH
  - o Xmas tree
  - o Another Xmas tree
  - o Null scan
  - o SYN/RST
  - o SYN/FIN
- SYN flood prevention
- Ping flood attack prevention

## 21.2 Content Blocking

**Application Blocking**
?

Please Select Application...
+

**Web Blocking**
?

Preset Category

☐ High
☐ Moderate
☐ Low
☒ Custom

☐ Abortion
☐ Alcohol
☐ Dating
☐ Entertainment
☐ Gambling
☐ Instant Messaging
☐ Lingerie
☐ Nudity
☐ Phishing
☐ Radio
☐ Search Engines
☐ Sports
☐ Update Sites
☐ Viruses
☐ Webmail

☐ Adware
☐ Anti-Spyware
☐ Drugs
☐ File Hosting
☐ Games
☐ Job Search/Employment
☐ Malware
☐ News/Media
☐ Pornography
☐ Remote Access
☐ Sexuality Education
☐ Spyware
☐ Vacation
☐ Weapons
☐ WebTV

☐ Aggressive
☐ Chatroom
☐ Ecommerce/Shopping
☐ P2P/File sharing
☐ Hacking
☐ Kids Time Wasting
☐ Manga/Anime/Webcomic
☐ Auctions
☐ Proxy/Anonymizer
☐ Ringtones
☐ Social Networking
☐ Tobacco
☐ Violence
☐ Weather

Customized Domains

cbs.com
+

Exempted Domains from Web Blocking
+

**Exempted User Groups**
?

Manager
☐ Exempt

Staff
☐ Exempt

Guest
☐ Exempt

**Exempted Subnets**
?

Network
Subnet Mask

+

**URL Logging**

Enable
☐

Log Server Host
Port:

### 21.2.2 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.

### 21.2.3 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.

#### 21.2.4 Customized Domains

Enter an appropriate website address, and the Pepwave MAX 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 Pepwave MAX will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

#### 21.2.5 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.

#### 21.2.6 Exempted Subnets

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

#### 21.2.7 URL Logging



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

## 22 Routing Protocols


### 22.1 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         |  |
| <a href="#">Add</a> |                |   |

| PepVPN OSPF Area |   |
|------------------|---|
| 0.0.0.0          |  |

| RIPv2             |  |
|-------------------|--|
| No RIPv2 Defined. |  |

| OSPF             |  |
|------------------|--|
| <b>Router ID</b> | This field determines the ID of the router. By default, this is specified as the WAN IP address. If you want to specify your own ID, enter it into the <b>Custom</b> field.  |
| <b>Area</b>      | This is an overview of the OSPF areas that you have defined. Clicking on the name under Area allows you to configure the connection. To define a new area, click Add. To delete an existing area, click on the  . |



**OSPF settings**

|                |   |
|----------------|---|
| Area ID        | 0.0.0.0   |
| Link Type      | <input checked="" type="radio"/> Broadcast <input type="radio"/> Point-to-Point   |
| Authentication | None ▼  |
| Interfaces     | <input type="checkbox"/> Untagged LAN<br><input type="checkbox"/> V167 (192.168.167.1/24)<br><input type="checkbox"/> WAN 1<br><input type="checkbox"/> WAN 2<br><input type="checkbox"/> WAN 3<br><input type="checkbox"/> WAN 4<br><input type="checkbox"/> WAN 5<br><input checked="" type="checkbox"/> PepVPN |

Save
Cancel

| OSPF Settings         |  |
|-----------------------|--|
| <b>Area ID</b>        | Assign a name to be applied to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore them.   |
| <b>Link Type</b>      | Choose the type of network that this area will use.  |
| <b>Authentication</b> | If an authentication method is used, select one from this drop-down menu. Available options are <b>MD5</b> and <b>Text</b> . Authentication key(s) may be input next to the drop-down menu after selecting an authentication method. |
| <b>Interfaces</b>     | Select the interface(s) that this area will use to listen to and deliver OSPF packets.   |

To access RIPv2 settings, click on .

**RIPv2 settings**

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

Save
Cancel

| RIPv2 Settings        |  |
|-----------------------|--|
| <b>Authentication</b> | If an authentication method is used, select one from this drop-down menu. Available options are <b>MD5</b> and <b>Text</b> . Authentication key(s) may be input next to the drop-down menu after selecting an authentication method. |
| <b>Interfaces</b>     | Select the interface(s) that this area will use to listen to and deliver RIPv2 packets.  |

| OSPF & RIPv2 Route Advertisement |   |  |  |
|----------------------------------|---|--|--|
| PepVPN Route Isolation           | ? | <input type="checkbox"/> Enable            |  |
| Network Advertising              | ? | ---  | +<br>All LAN/VLAN networks will be advertised when no network advertising is chosen. |
| Static Route Advertising         | ? | <input checked="" type="checkbox"/> Enable |  |
|                                  |   | Excluded Networks                          | Subnet Mask  |
|                                  |   | <input type="text"/>                       | 255.255.255.0 (/24) +  |
| Save                             |   |  |  |

| OSPF & RIPv2 Route Advertisement |  |
|----------------------------------|--|
| <b>PepVPN Route Isolation</b>    | Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption..                               |
| <b>Network Advertising</b>       | Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.   |
| <b>Static Route Advertising</b>  | Enabling OSPF & RIPv2 Route Advertising allows it to advertise LAN static routes over OSPF & RIPv2. Static routes on the Excluded Networks table will not be advertised. |

## 22.2 BGP

Click the **Network** tab along the top bar, and then click the **BGP** item on the sidebar to configure BGP.

| BGP    | AS    | Neighbors   |   |
|--------|-------|-------------|---|
| Uplink | 64520 | 172.16.51.1 | ✖ |
| Add    |       |             |   |

Click the "✖" to delete a BGP profile.

Click "Add" to create a new BGP profile.

**BGP Profile**
✕

| BGP Profile  |  |  |                |  |  |   |
|--|--|--|----------------|--|--|---|
| Profile Name   | <input style="width: 90%;" type="text"/>   |  |                |  |  |   |
| Enable   | <input checked="" type="checkbox"/>  |  |                |  |  |   |
| Interface  | <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">WAN <span style="margin-left: 10px;">▼</span></div> |  |                |  |  |   |
| Router ID  | <input checked="" type="radio"/> WAN IP Address<br><input type="radio"/> Custom: <input style="width: 100px;" type="text"/>                |  |                |  |  |   |
| Autonomous System  | <input style="width: 90%;" type="text"/>   |  |                |  |  |   |
| Neighbor <span style="float: right;">?</span>              | IP Address   | Autonomous System                        | Multihop / TTL | Password                                 | AS-Path Prepending                       |   |
|  | <input style="width: 90%;" type="text"/>   | <input style="width: 90%;" type="text"/> | disable        | <input style="width: 90%;" type="text"/> | <input style="width: 90%;" type="text"/> | + |
| Hold Time <span style="float: right;">?</span>             | <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">240</div>   |  |                |  |  |   |
| Next Hop Self <span style="float: right;">?</span>         | <input type="checkbox"/>   |  |                |  |  |   |
| iBGP Local Preference <span style="float: right;">?</span> | <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">100</div>   |  |                |  |  |   |
| BFD <span style="float: right;">?</span>                   | <input type="checkbox"/> Enable  |  |                |  |  |   |

| BGP                        |  |
|----------------------------|--|
| <b>Name</b>                | This field specifies the name that represents this profile.  |
| <b>Enable</b>              | When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.  |
| <b>Interface</b>           | The interface in which the BGP neighbor is located.  |
| <b>Autonomous System</b>   | The Autonomous System Number (ASN) assigned to this profile.   |
| <b>Neighbor</b>            | BGP Neighbors and their details.   |
| <b>IP address</b>          | The IP address of the Neighbor.  |
| <b>Autonomous System</b>   | The Neighbor's ASN.  |
| <b>Multihop/TTL</b>        | This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255. |
| <b>Password</b>            | (Optional) Assign a password for MD5 authentication of BGP sessions.   |
| <b>AS-Path Prepending:</b> | AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received routes.  |

|                              |   |
|------------------------------|---|
| <b>Hold Time</b>             | Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled.<br>The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively.<br>Default: 240   |
| <b>Next Hop Self</b>         | Enable this option to advertise your own source address as the next hop when propagating routes.  |
| <b>iBGP Local Preference</b> | This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively.<br>Default: 100  |
| <b>BFD</b>                   | Enable this option to add Bidirectional Forwarding Detection for path failure. All directly connected Neighbors that use the same physical interface share the same BFD settings. All multihop Neighbors share the same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled. |

| Route Advertisement      |   |   |                                  |
|--------------------------|---|---|----------------------------------|
| Network Advertising      | ? | <div>---</div> <div>+</div>   |                                  |
| Static Route Advertising | ? | <input checked="" type="checkbox"/> Enable  |                                  |
|                          |   | Excluded Networks   | Subnet Mask                      |
|                          |   | <div></div>   | 255.255.255.0 (/24) <div>+</div> |
| Custom Route Advertising | ? | <div>Networks</div> <div>Subnet Mask</div> <div><div></div></div> <div>255.255.255.0 (/24) <div>+</div></div> |                                  |
| Advertise OSPF Route     | ? | <input type="checkbox"/>  |                                  |
| Set Community            | ? | Community   | Route Prefix                     |
|                          |   | <div></div>   | <div></div> <div>+</div>         |

|                                 |   |
|---------------------------------|---|
| <b>Network Advertising</b>      | Select the Networks that will be advertised to the BGP Neighbor.  |
| <b>Static Route Advertising</b> | Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised. |
| <b>Custom Route Advertising</b> | Additional routes to be advertised to the BGP Neighbor.   |
| <b>Advertise OSPF Route</b>     | When this box is checked, every learnt OSPF route will be advertised.   |
| <b>Set Community</b>            | Assign a prefix to a Community.<br><br>Community:   |

Two numbers in new-format.  
e.g. 65000:21344

Well-known communities:  
no-export 65535:65281  
no-advertise 65535:65282  
no-export-subconfed 65535:65283  
no-peer 65535:65284

Route Prefix:  
Comma separated networks.  
e.g. 172.168.1.0/24,192.168.1.0/28

| Route Import        |  |                       |                          |                                  |
|---------------------|--|-----------------------|--------------------------|----------------------------------|
| Filter Mode         | <input type="button" value="?"/> <div>Accept ▼</div> |                       |                          |                                  |
| Restricted Networks | Network  | Subnet Mask           | Exact Match              |                                  |
|                     |  | 255.255.255.0 (/24) ▼ | <input type="checkbox"/> | <input type="button" value="+"/> |

#### Filter Mode

This field allows for the selection of the filter mode for route import.

**None:** All BGP routes will be accepted.

**Accept:** Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.

**Reject:** Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.

#### Restricted Networks

This field specifies the network(s) in the "route import" entry.

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

Otherwise, routes within the Networks and Subnets will be filtered.

| Route Export                |   |                       |                          |                                  |
|-----------------------------|---|-----------------------|--------------------------|----------------------------------|
| Filter Mode                 | <input type="button" value="?"/> <div>Accept ▼</div>      |                       |                          |                                  |
| Restricted Networks         | Network   | Subnet Mask           | Exact Match              |                                  |
|                             |   | 255.255.255.0 (/24) ▼ | <input type="checkbox"/> | <input type="button" value="+"/> |
| Export to other BGP Profile | <input type="button" value="?"/> <input type="checkbox"/> |                       |                          |                                  |
| Export to OSPF              | <input type="button" value="?"/> <input type="checkbox"/> |                       |                          |                                  |

#### Filter Mode

This field allows for the selection of the filter mode for route export.

**None:** All BGP routes will be accepted.

**Accept:** Routes in "Restricted Networks" will be accepted, routes not in the list will


|                                    |   |
|------------------------------------|---|
|                                    | <p>be rejected.</p> <p><b>Reject:</b> Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.</p>  |
| <b>Restricted Networks</b>         | <p>This field specifies the network(s) in the "route export" entry.</p> <p><b>Exact Match:</b> When this box is checked, only routes with the same Network and Subnet Mask will be filtered.</p> <p>Otherwise, routes within the Networks and Subnets will be filtered.</p> |
| <b>Export to other BGP Profile</b> | <p>When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.</p>  |
| <b>Export to OSPF</b>              | <p>When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.</p>   |

## 23 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 Pepwave 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.

### 23.1 L2TP with IPsec

| Remote User Access Settings |   |
|-----------------------------|---|
| Enable                      | <input checked="" type="checkbox"/>   |
| VPN Type                    | <input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input type="radio"/> OpenVPN |
| Preshared Key               | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters                                  |

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

Continue to configure the authentication method.

### 23.2 OpenVPN

| Remote User Access Settings |   |
|-----------------------------|---|
| Enable                      | <input checked="" type="checkbox"/>   |
| VPN Type                    | <input type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input checked="" type="radio"/> OpenVPN<br>You can obtain the OpenVPN client profile from the <a href="#">status page</a> . |

Select OpenVPN and continue to configure the authentication method.

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

|                        |  |
|------------------------|--|
| OpenVPN Client Profile | <a href="#">Route all traffic</a>   <a href="#">Split tunnel</a> |
|------------------------|--|

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.

## 23.3 PPTP

| Remote User Access Settings |   |
|-----------------------------|---|
| Enable                      | <input checked="" type="checkbox"/>   |
| VPN Type                    | <input type="radio"/> L2TP with IPsec <input checked="" type="radio"/> PPTP <input type="radio"/> 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.

## 23.4 Authentication Methods

|                    |                                  |          |                   |
|--------------------|----------------------------------|----------|-------------------|
| Connect to Network | <a href="#">?</a> Untagged LAN ▾ |          |                   |
| Authentication     | Local User Accounts ▾            |          |                   |
| User Accounts      | <a href="#">?</a> Username       | Password | <a href="#">+</a> |

| Authentication Method     |   |
|---------------------------|---|
| <b>Connect to Network</b> | Select the VLAN network for remote users to enable remote user access on. |
| <b>Authentication</b>     | 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 <input type="text" value="389"/> <input type="button" value="Default"/> |
|                    | <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 <input type="text" value="1812"/> <input type="button" value="Default"/> |
| Auth Server Secret       | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters                           |
| Accounting Server        | <input type="text"/> Port <input type="text" value="1813"/> <input type="button" value="Default"/> |
| Accounting Server Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters                           |

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"/> <input checked="" type="checkbox"/> Hide Characters                           |

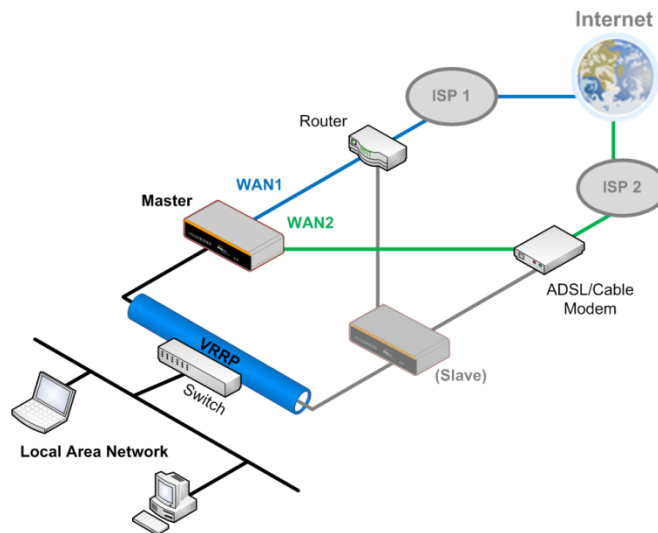
Enter the matching Active Directory details to allow for Active Directory server authentication.

## 24 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).

### 24.1 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

| High Availability                |   |
|----------------------------------|---|
| Enable                           | <input checked="" type="checkbox"/>                                 |
| Group Number                     | <input type="text"/>  |
| Preferred Role                   | <input checked="" type="radio"/> Master <input type="radio"/> Slave |
| Resume Master Role Upon Recovery | <input checked="" type="checkbox"/>                                 |
| Virtual IP Address               | <input type="text"/>  |
| LAN Administration IP Address    | 192.168.86.1  |
| Subnet Mask                      | 255.255.255.0   |

Interface for Slave Router

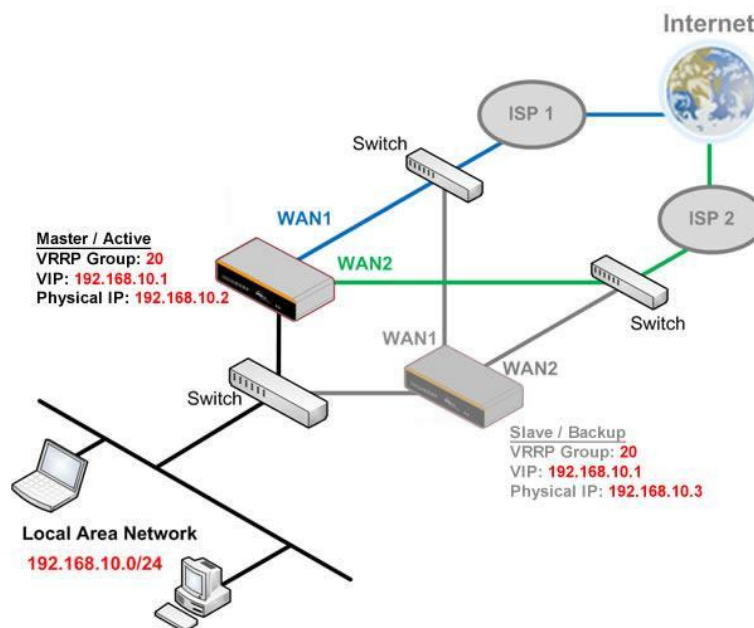
| High Availability                   |   |
|-------------------------------------|---|
| Enable                              | <input checked="" type="checkbox"/>                                 |
| Group Number                        | <input type="text"/>  |
| Preferred Role                      | <input type="radio"/> Master <input checked="" type="radio"/> Slave |
| Configuration Sync.                 | <input type="checkbox"/> Master Serial Number: <input type="text"/> |
| Establish Connections in Slave Role | <input type="checkbox"/>  |
| Virtual IP Address                  | <input type="text"/>  |
| LAN Administration IP Address       | 192.168.86.1  |
| Subnet Mask                         | 255.255.255.0   |

| High Availability                       |  |
|---|--|
| <b>Enable</b>                           | Checking this box specifies that the Pepwave router is part of a high availability configuration.  |
| <b>Group Number</b>                     | 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 <b>Group Number</b> value.   |
| <b>Preferred Role</b>                   | 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.   |
| <b>Resume Master Role Upon Recovery</b> | This option is displayed when <b>Master</b> mode is selected in <b>Preferred Role</b> . If this option is enabled, once the device has recovered from an outage, it will take over and resume its <b>Master</b> role from the slave unit.  |
| <b>Configuration Sync.</b>              | This option is displayed when <b>Slave</b> mode is selected in <b>Preferred Role</b> . If this option is enabled and the <b>Master Serial Number</b> entered matches with the actual master unit's, the master unit will automatically transfer the configuration to this unit. Please make sure the <b>LAN IP Address</b> and the <b>Subnet Mask</b> fields are set correctly in the LAN settings page. You can refer to the <b>Event Log</b> for the configuration synchronization status. |
| <b>Master Serial Number</b>             | If <b>Configuration Sync.</b> is checked, the serial number of the master unit is required here for the feature to work properly.  |
| <b>Virtual IP</b>                       | The HA pair must share the same <b>Virtual IP</b> . The <b>Virtual IP</b> and the <b>LAN</b>   |

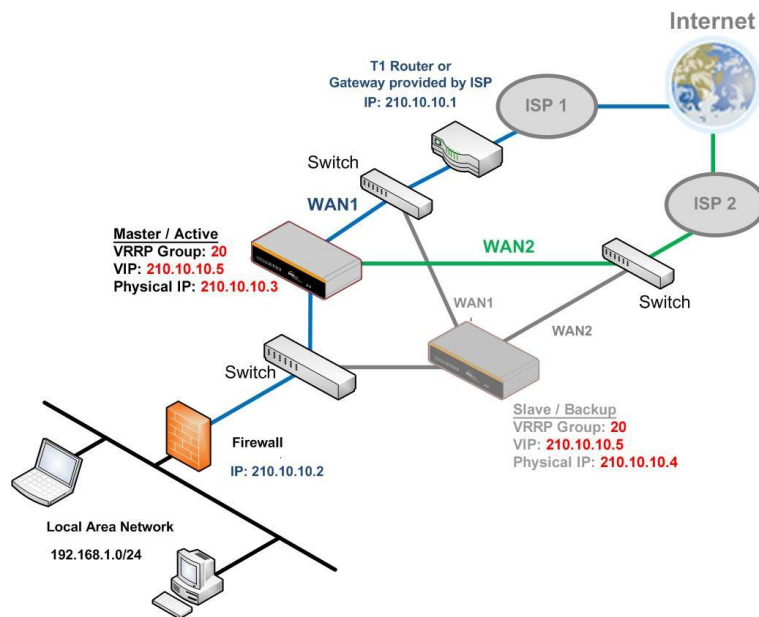
|  |  |
|--|--|
| <b>Administration IP</b> must be under the same network. |  |
| <b>LAN Administration IP</b>                             | This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN. |
| <b>Subnet Mask</b>                                       | 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.

## 24.2 Certificate Manager

| Certificate                      |                               |  |
|----------------------------------|-------------------------------|--|
| SpeedFusion/IPsec VPN            | 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          |                               |  |
| <button>Add Certificate</button> |                               |  |
| Wi-Fi WAN CA Certificate         |                               |  |
| No Certificates defined          |                               |  |
| <button>Add Certificate</button> |                               |  |

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/>

## 24.3 Service Forwarding

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

| SMTP Forwarding Setup                            |                                 |
|--|---------------------------------|
| SMTP Forwarding                                  | <input type="checkbox"/> Enable |
| Web Proxy Forwarding Setup                       |                                 |
| Web Proxy Forwarding                             | <input type="checkbox"/> Enable |
| DNS Forwarding Setup                             |                                 |
| Forward Outgoing DNS Requests to Local DNS Proxy | <input type="checkbox"/> Enable |
| Custom Service Forwarding Setup                  |                                 |
| Custom Service Forwarding                        | <input type="checkbox"/> Enable |

| Service Forwarding               |   |
|----------------------------------|---|
| <b>SMTP Forwarding</b>           | 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 <b>Enable</b> .  |
| <b>Web Proxy Forwarding</b>      | When this option is enabled, all outgoing connections destined for the proxy server specified in <b>Web Proxy Interception Settings</b> 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 <b>Enable</b> .  |
| <b>DNS Forwarding</b>            | 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. |
| <b>Custom Service Forwarding</b> | 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.   |

### 24.3.2 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       |                          | <input checked="" type="checkbox"/> 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**).

### 24.3.3 Web Proxy Forwarding

| Web Proxy Forwarding Setup      |  |   |
|---------------------------------|--|---|
| Web Proxy Forwarding            |  | <input checked="" type="checkbox"/> Enable  |
| Web Proxy Interception Settings |  |   |
| Proxy Server                    | IP Address <input type="text"/> Port <input type="text"/><br><small>(Current settings in users' browser)</small> |   |
| 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.

### 24.3.4 DNS Forwarding

| DNS Forwarding Setup                             |                                 |
|--|---------------------------------|
| Forward Outgoing DNS Requests to Local DNS Proxy | <input type="checkbox"/> Enable |

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

### 24.3.5 Custom Service Forwarding

| Custom Service Forwarding Setup |  |                      |   |
|---------------------------------|--|----------------------|---|
| Custom Service Forwarding       | <input checked="" type="checkbox"/> Enable |                      |   |
| Settings                        | TCP Port                                   | Server IP Address    | Server Port   |
|                                 | <input type="text"/>                       | <input type="text"/> | <input type="text"/> <input type="button" value="+"/> |

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.



## 24.4 Service Passthrough

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

| Service Passthrough Support |  |
|-----------------------------|--|
| SIP                         | <input checked="" type="radio"/> Standard Mode <input type="radio"/> Compatibility Mode<br><input checked="" type="checkbox"/> Define custom signal ports<br>1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>   |
| H.323                       | <input checked="" type="checkbox"/> Enable   |
| FTP                         | <input checked="" type="checkbox"/> Enable<br><input type="checkbox"/> Define custom control ports   |
| TFTP                        | <input checked="" type="checkbox"/> Enable   |
| IPsec NAT-T                 | <input checked="" type="checkbox"/> Enable<br><input checked="" type="checkbox"/> Define custom ports<br>1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/><br><input checked="" type="checkbox"/> Route IPsec Site-to-Site VPN<br>via <input type="text" value="WAN 1"/> |

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 |  |
|-----------------------------|--|
| <b>SIP</b>                  | 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: <b>Standard Mode</b> and <b>Compatibility Mode</b> . If your SIP server's signal port number is non-standard, you can check the box <b>Define custom signal ports</b> and input the port numbers to the text boxes. |
| <b>H.323</b>                | With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Pepwave router.  |
| <b>FTP</b>                  | 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 <b>Define custom control ports</b> and enter the port numbers in the text boxes.                                      |
| <b>TFTP</b>                 | The Pepwave router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select <b>Enable</b> 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.

## 24.5 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   | <input checked="" type="radio"/> Any <input type="radio"/> 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="checkbox"/> |
| 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.

## 24.6 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             | <input checked="" type="checkbox"/>   |                      |          |                     |                                  |
| Server             | Server IP Address / Host Name   | Port                 | Protocol | Report Interval (s) |                                  |
|                    | <input type="text"/>  | <input type="text"/> | UDP ▾    | 1                   | <input type="button" value="+"/> |
| GPS Report Format  | <input checked="" type="radio"/> NMEA <input type="radio"/> TAIP  |                      |          |                     |                                  |
| NMEA Sentence Type | <input checked="" type="checkbox"/> GPRMC<br><input type="checkbox"/> GPGGA<br><input type="checkbox"/> GPVTG<br><input type="checkbox"/> GPGSA<br><input type="checkbox"/> GPGSV |                      |          |                     |                                  |
| Vehicle ID         | <input type="text"/> <input <input="" type="checkbox" value="?"/>   |                      |          |                     |                                  |

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


## 24.7 Ignition Sensing

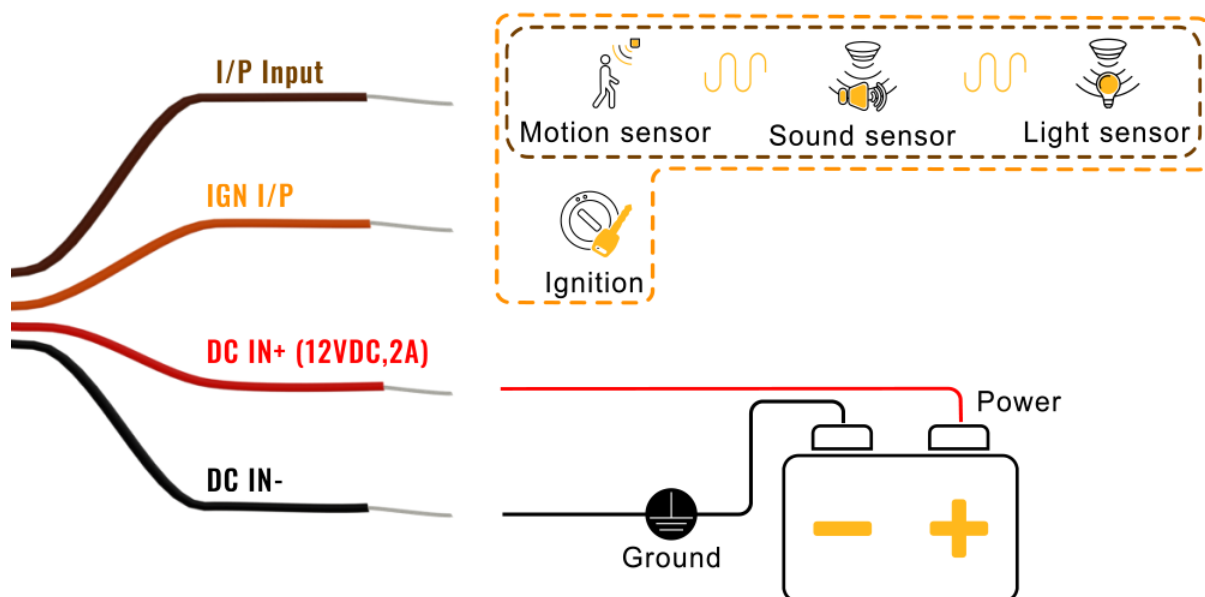
Ignition Sensing detects the ignition signal status of a vehicle it is installed in.

This feature allows the cellular router to start up or shut down when the engine of that vehicle is started or turned off.

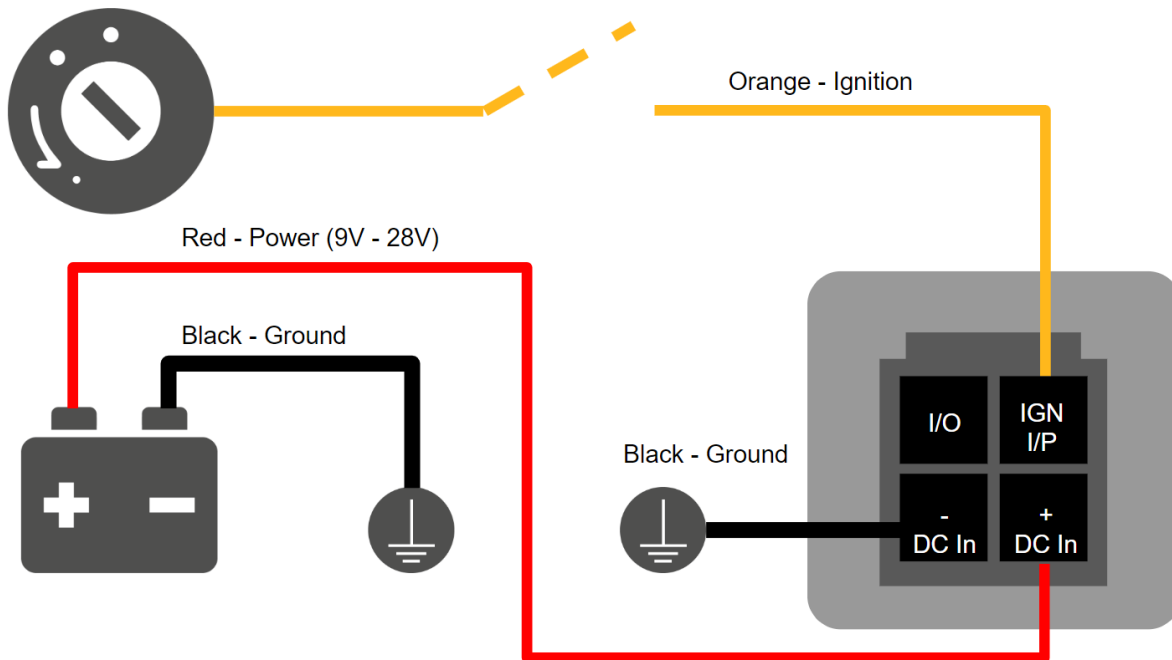
The time delay setting between ignition off and power down of the router is a configurable setting, which allows the router to stay on for a period of time after the engine of a vehicle is turned off.

### Ignition Sensing installation

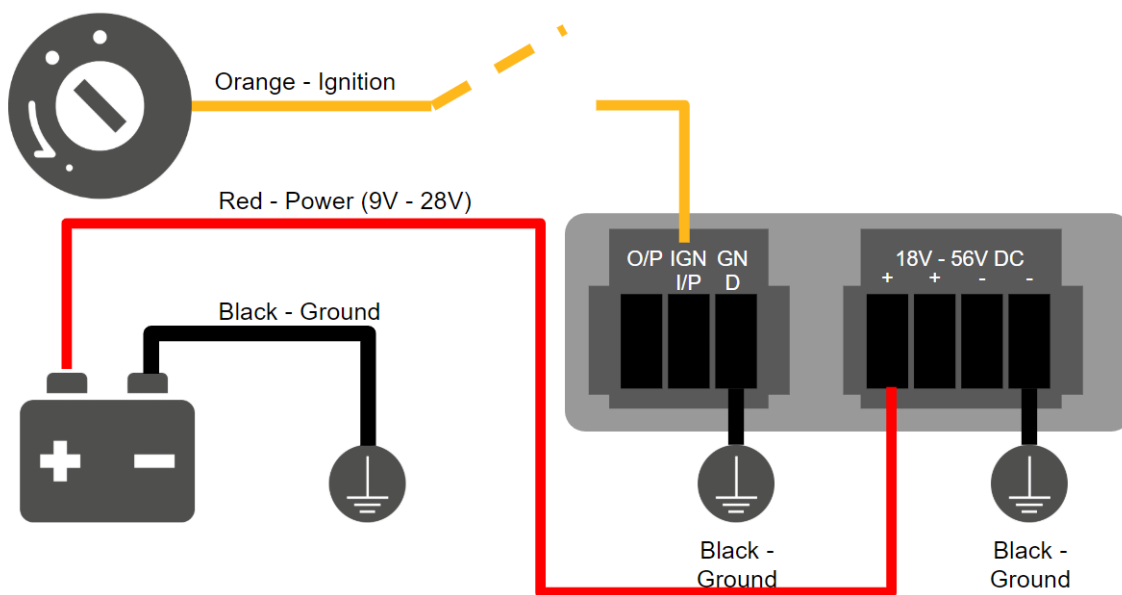
| Function  |  | Colour Wire |
|---|--|-------------|
|   | I/O optional*  | Brown       |
|   | IGN I/P connected to positive feed on the ignition .             | Orange      |
|   | DC IN - connected to permanent negative feed (ground)            | Black       |
|   | DC IN + connected to permanent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



### Connectivity diagram for devices with 4-pin connector



### Connectivity diagram for devices with terminal block connection



## GPIO Menu

**Note:** This feature is applicable for certain models that come with a GPIO interface.

Ignition Sensing options can be found in **Advanced > GPIO**.

The configurable option for Ignition Input is **Delay**; the time in seconds that 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        |

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

Digital Input - the connection supports input sensing; it reads the external input and determines 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).

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

**Note:** The Digital Output state (on/off) upon rebooting the device may vary depending on the model, eg. MAX BR1 MK2 = Persistent; MAX Transit Mini with ContentHub = Reset to default, etc.

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



## 24.8 NTP Server

Pepwave routers can now serve as a local NTP server. Upon start up, it is now able to provide connected devices with the accurate time, precise UTC from either an external NTP server or via GPS and ensuring that connected devices always receive the correct time.

Compatible with: BR1 ENT, 700 HW3, HD2/4, Transit

NTP Server setting can be found via: **Advanced>Misc. Settings>NTP Server**


| NTP Server |                          |
|------------|--------------------------|
| Enable     | <input type="checkbox"/> |

Time Settings can be found at **System>Time>Time Settings**





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

## 24.9 Grouped Networks

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

| Grouped Networks                         |                 |   |
|--|-----------------|---|
| Name                                     | Networks        |   |
| Example                                  | 192.168.1.71/28 |  |
| <input type="button" value="Add Group"/> |                 |   |

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

| Grouped Networks  |   |                         |   |
|--|---|-------------------------|---|
| Name   | Example  |                         |   |
| Networks   | Network   | Subnet Mask             |   |
|  | 192.168.1.71  | 255.255.255.240 (/28) ▼ |  |
|  |   | 255.255.255.255 (/32) ▼ |  |
| <input type="button" value="Save"/> <input type="button" value="Cancel"/>                            |   |                         |   |

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

## 24.10 Remote SIM Management

The Remote SIM management is accessible via **Advanced > Misc Settings > Remote SIM Management**. By default, this feature is disabled.

Please note that a limited number of Pepwave routers support the SIM Injector, may refer to the link: <https://www.peplink.com/products/sim-injector/> or Appendix B for more details on FusionSIM Manual.

Remote SIM Host

Remote SIM is disabled

### Remote SIM Host Settings

Remote SIM Host Settings

Auto LAN Discovery

☐

Remote SIM Host

Save

| Remote SIM Host Settings    |   |
|-----------------------------|---|
| <b>Active LAN Discovery</b> | Check this box to enable Auto LAN discovery of the remote SIM server..  |
| <b>Remote SIM Host</b>      | Enter the public IP address of the SIM Injector. If you enter IP addresses here, it is not necessary to tick the “ <b>Auto LAN Discovery</b> ” box above. |

Remote SIM Host

192.168.1.10

Remote SIM Management

Server

Slot

No Remote SIM Defined.

Add Remote SIM

You may define the Remote SIM information by clicking the “**Add Remote SIM**”. Here, you can enable **Data Roaming** and **custom APN** for your SIM cards.

### Add Remote SIM

| Remote SIM                                      |   |
|---|---|
| SIM Server                                      | <input type="text" value="New SIM Server..."/>  |
| SIM Server - Serial Number                      | <input type="text"/>  |
| SIM Server - Name                               | <input type="text" value="Optional"/>   |
| SIM Slot  | <input type="text" value="1"/>  |
| SIM Slot - Name                                 | <input type="text" value="Optional"/>   |
| Data Roaming                                    | <input type="checkbox"/>  |
| Operator Settings (for LTE/HSPA/EDGE/GPRS only) | <input checked="" type="radio"/> Auto <input type="radio"/> Custom Mobile Operator Settings |
| SIM PIN (Optional)                              | <input type="text"/> <input type="text" value="(Confirm)"/>                                 |

Save

### Add Remote SIM Settings

|  |  |
|--|--|
| <b>SIM Server</b>                                      | Add a new SIM Server   |
| <b>SIM Server - Serial Number</b>                      | Enter the serial number of SIM Server  |
| <b>SIM Server - Name</b>                               | This optional field allows you define a name for the SIM Server  |
| <b>SIM Slot</b>  | Click the drop-down menu and choose which SIM slot you want to connect.  |
| <b>SIM Slot - Name</b>                                 | This optional field allows you define a name for the SIM slot.   |
| <b>Data Roaming</b>                                    | Enables data roaming on this particular SIM card.  |
| <b>Operator Settings (for LTE/HSPA/EDGE/GPRS Only)</b> | <p>This setting allows you to configure the APN settings of your connection. If <b>Auto</b> is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making a connection, you may select <b>Custom</b> to enter your carrier's APN, Username and Password settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto.</p> |

## 24.11 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           | 7240207400000000 |
| 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           | 856195002108538                             |
| 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           | 856195002108538                             |
| 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       | <b>PCX</b><br>As of May 27th<br>Account Balance: \$ 0.00<br>Amount Unbilled<br>Voice Calls: 0 minutes<br>Video Calls: 0 minutes<br>SMS (Roaming): 0<br>SMS (Within Network): 0<br>MMS (Roaming):0<br>MMS (Within Network): 0<br>Data Usage: 7384KB<br>(For reference only, please refer to bill)                           |  |
| Aug 8 , 2013 14:51 | <b>PCX</b><br>iPhone & Android users need to make sure "PCX" is entered as the APN under "Settings" > "Mobile network setting" for web browsing and mobile data service. Other handset models will receive handset settings via SMS shortly (PIN: 1234) (Consumer Service Hotline: 1000 / Business Customer Hotline 10088) |  |

## SMS

The SMS option allows you to read SMS (text) messages that have been sent to the SIM in your Pepwave router.

| SIM Status     |                  |
|----------------|------------------|
| WAN Connection | Cellular         |
| SIM Card       | 1                |
| IMSI           | 214061 100040000 |
| Tool           | SMS              |

| SMS                |   | Refresh |
|--------------------|---|---------|
| Jun 21, 2017 18:00 | <b>Hi</b><br>Thanks you, your web page can't be visited - you can change this when you first login at there as an...  |         |
| May 06, 2017 12:23 | <b>Hi</b><br>Hi From 3: Your new bill is ready to view. Go to your PG&E account on your desktop or on a mobile phone click here: <a href="http://mobile.energysource.com">http://mobile.energysource.com</a>                |         |
| Mar 15, 2017 10:03 | <b>From 3</b><br>Hello, There is planned maintenance in the Southern Calif PG&E area this week. If your service is affected, you can get updates here: <a href="http://pgae.com">http://pgae.com</a>                        |         |
| Mar 06, 2017 14:50 | <b>Hi</b><br>Hi From 3: Your new bill is ready to view. Go to your PG&E account on your desktop or on a mobile phone click here: <a href="http://mobile.energysource.com">http://mobile.energysource.com</a>                |         |
| Dec 28, 2016 09:53 | <b>From 3</b><br>Hi, we hope your appreciation to receive half-price offer and to remind you, this offer applied to your first 10 bills. Your monthly electricity charge will revert to full price on your next bill. Thank |         |
| Dec 06, 2016 13:09 | <b>Hi</b><br>Hi From 3: Your new bill is ready to view. Go to your PG&E account on your desktop or on a mobile phone click here: <a href="http://mobile.energysource.com">http://mobile.energysource.com</a>                |         |
| Nov 08, 2016 11:29 | <b>From 3</b><br>Hello, There is planned maintenance in the Southern Calif PG&E area this week. If your service is affected, you can get updates here: <a href="http://pgae.com">http://pgae.com</a>                        |         |
| Sep 07, 2016 17:05 | <b>From 3</b><br>Hello there, please appreciate our studies on electricity usage and how it can help in PG&E area to help your electricity bill. Electricity Usage Only   |         |

## 25 AP

### 25.1 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 | <input checked="" type="checkbox"/> Integrated AP <input checked="" type="checkbox"/> External AP |
| Sync. Method  | As soon as possible ▼   |
| Permitted AP  | <input checked="" type="radio"/> Any <input type="radio"/> Approved List                          |

| AP Controller        |   |
|----------------------|---|
| <b>AP Management</b> | 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, <b>CAPWAP Access Controller addresses</b> (field 138), will be added to the DHCP server. A local DNS record, <b>AP Controller</b> , will be added to the local DNS proxy. |
| <b>Sync Method</b>   | <ul style="list-style-type: none"> <li>As soon as possible</li> <li>Progressively</li> <li>One at a time</li> </ul>   |
| <b>Permitted AP</b>  | Access points to manage can be specified here. If <b>Any</b> is selected, the AP controller will manage any AP that reports to it. If <b>Approved List</b> is selected, only APs with serial numbers listed in the provided text box will be managed.   |

### 25.2 Wireless SSID

| SSID                               | Security Policy |
|------------------------------------|-----------------|
| No SSID Defined                    |                 |
| <input type="button" value="Add"/> |                 |

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 show a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).



**SSID**

**SSID Settings**

|                           |  |
|---------------------------|--|
| SSID                      | <input type="text"/>   |
| Enable                    | <input checked="" type="checkbox"/>  |
| VLAN                      | Untagged LAN ▼   |
| Broadcast SSID            | <input checked="" type="checkbox"/>  |
| Data Rate                 | <input checked="" type="radio"/> Auto <input type="radio"/> Fixed                            |
| Multicast Filter          | <input type="checkbox"/>   |
| Multicast Rate            | MCS0/6M ▼  |
| IGMP Snooping             | <input type="checkbox"/>   |
| Layer 2 Isolation         | <input type="checkbox"/>   |
| Maximum number of clients | 2.4 GHz: <input type="text" value="0"/> 5 GHz: <input type="text" value="0"/> (0: Unlimited) |

**Security Settings**

|                 |                        |
|-----------------|------------------------|
| Security Policy | Open (No Encryption) ▼ |
|-----------------|------------------------|

**Access Control Settings**


|                 |        |
|-----------------|--------|
| Restricted Mode | None ▼ |
|-----------------|--------|

| SSID Settings |   |
|---------------|---|
| <b>SSID</b>   | This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.   |
| <b>Enable</b> | Click the drop-down menu to apply a time schedule to this interface   |
| <b>VLAN</b>   | 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 <b>0</b> , which means VLAN tagging is disabled (instead of tagged with zero). |



|                                       |  |
|---------------------------------------|--|
| <b>Broadcast SSID</b>                 | This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. <b>Broadcast SSID</b> is enabled by default.   |
| <b>Data Rate</b> <sup>A</sup>         | Select <b>Auto</b> to allow the Pepwave router to set the data rate automatically, or select <b>Fixed</b> and choose a rate from the displayed drop-down menu.   |
| <b>Multicast Filter</b> <sup>A</sup>  | This setting enables the filtering of multicast network traffic to the wireless SSID.  |
| <b>Multicast Rate</b> <sup>A</sup>    | This setting specifies the transmit rate to be used for sending multicast network traffic. The selected <b>Protocol</b> and <b>Channel Bonding</b> settings will affect the rate options and values available here.  |
| <b>IGMP Snooping</b> <sup>A</sup>     | To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.  |
| <b>DHCP Option 82</b> <sup>A</sup>    | 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.   |
| <b>Layer 2 Isolation</b> <sup>A</sup> | <b>Layer 2</b> refers to the second layer in the ISO Open System Interconnect model.<br>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 the upper communication layer(s). By default, the setting is disabled. |
| <b>Maximum Number of Clients</b>      | Indicate the maximum number of clients that should be able to connect to each frequency.   |

<sup>A</sup> - Advanced feature. Click the  button on the top right-hand corner to activate.

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

| Security Settings      |   |
|------------------------|---|
| <b>Security Policy</b> | <p>This setting configures the wireless authentication and encryption methods. Available options :</p> <ul style="list-style-type: none"> <li>• <b>Open</b> (No Encryption)</li> <li>• <b>Enhanced Open</b> (OWE)</li> <li>• <b>WPA3 -Personal</b> (AES:CCMP)</li> <li>• <b>WPA2/WPA3 -Personal</b> (AES:CCMP)</li> <li>• <b>WPA2 -Personal</b> (AES:CCMP)</li> <li>• <b>WPA2 – Enterprise</b></li> </ul> |

- **WPA/WPA2 - Personal** (TKIP/AES: CCMP)
- **WPA/WPA2 – Enterprise**

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

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

**NOTE:**

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

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

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

| RADIUS Server Settings | Primary Server   | Secondary Server   |
|------------------------|--|--|
| Host                   | <div></div>  | <div></div>  |
| Secret                 | <div><input checked="" type="checkbox"/> Hide Characters</div> | <div><input checked="" type="checkbox"/> Hide Characters</div> |
| Authentication Port    | <div>1812</div> <b>Default</b>                                 | <div>1812</div> <b>Default</b>                                 |
| Accounting Port        | <div>1813</div> <b>Default</b>                                 | <div>1813</div> <b>Default</b>                                 |
| NAS-Identifier         | <div>Device Name ▼</div>                                       |  |

| RADIUS Server Settings     |  |
|----------------------------|--|
| <b>Host</b>                | Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.   |
| <b>Secret</b>              | Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.                                     |
| <b>Authentication Port</b> | In the field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter <b>1812</b> . |
| <b>Accounting Port</b>     | In the field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter <b>1813</b> .     |
| <b>NAS-Identifier</b>      | Choose between <b>Device Name</b> , <b>LAN MAC address</b> , <b>Device Serial Number</b> and <b>Custom Value</b>                           |

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

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

| Firewall Settings |   |
|-------------------|---|
| Firewall Mode     | <div> Disable ▼ <div> Disable Flexible - Allow all except... Lockdown - Block all except... </div> </div> |

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

## 25.3 Wireless Mesh

| Wireless Mesh                      | Frequency Band |
|------------------------------------|----------------|
| No Wireless Mesh Defined           |                |
| <input type="button" value="Add"/> |                |

Wireless Mesh Support is available on devices running 802.11ac (Wi-Fi 5) and above. Along with the AP Controller, mesh network extensions can be established, which can expand network coverage. Note that the Wireless Mesh settings need to match the Mesh ID and Shared Key of the other devices on the same selected frequency band.

To create a new Wireless Mesh profile, go to **AP > Wireless Mesh**, and click **Add**.

Wireless Mesh Settings

|            |  |
|------------|--|
| Mesh ID    | <input type="text"/>   |
| Frequency  | <input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz     |
| Shared Key | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters |

| Wireless Mesh Settings |   |
|------------------------|---|
| <b>Mesh ID</b>         | Enter a name to represent the Mesh profile.   |
| <b>Frequency</b>       | Select the 2.4GHz or 5GHz frequency to be used.   |
| <b>Shared Key</b>      | Enter the shared key in the text field. Please note that it needs to match the shared keys of the other APs in the Wireless Mesh settings.<br>Click <b>Hide / Show Characters</b> to toggle visibility. |

## 25.4 Settings

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

| AP Settings                      |   |
|----------------------------------|---|
| SSID                             | <input checked="" type="checkbox"/> 2.4 GHz <input checked="" type="checkbox"/> 5 GHz Integrated AP supports 2.4 GHz only.<br><input checked="" type="checkbox"/> Testing                                 |
| Operating Country                | United States   |
| Preferred Frequency              | <input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz<br>Integrated AP supports 2.4 GHz only.  |
|                                  | <div>2.4 GHz</div> <div>5 GHz</div>   |
| Protocol                         | <div>802.11ng</div> <div>802.11n/ac</div>   |
| Channel Width                    | <div>20 MHz</div> <div>Auto</div>   |
| Channel                          | <div>Auto</div> <div>Edit</div><br>Channels: 1 2 3 4 5 6 7 8 9 10 11 <div>Auto</div> <div>Edit</div><br>Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165 |
| Auto Channel Update              | <div>Daily at 03:00</div> <input checked="" type="checkbox"/> Wait until no active client associated <div>Daily at 03:00</div> <input checked="" type="checkbox"/> Wait until no active client associated |
| Output Power                     | <div>Fixed: Max</div> <input type="checkbox"/> Boost <div>Fixed: Max</div> <input type="checkbox"/> Boost   |
| Client Signal Strength Threshold | <div>0 -95 dBm (0: Unlimited)</div> <div>0 -95 dBm (0: Unlimited)</div>   |
| Maximum number of clients        | <div>0 (0: Unlimited)</div> <div>0 (0: Unlimited)</div>   |
| Management VLAN ID               | Untagged LAN (No VLAN)  |
| Operating Schedule               | Always on   |
| Beacon Rate                      | <div>1 Mbps</div> 6 Mbps will be used for 5 GHz radio   |
| Beacon Interval                  | 100 ms  |
| DTIM                             | <div>1</div> <div>Default</div>   |
| RTS Threshold                    | <div>0</div> <div>Default</div>   |
| Fragmentation Threshold          | <div>0 (0: Disable)</div> <div>Default</div>  |
| Distance / Time Converter        | <div>4050 m</div><br>Note: Input distance for recommended values  |
| Slot Time                        | <input type="radio"/> Auto <input checked="" type="radio"/> Custom 9 <div>μs</div> <div>Default</div>   |
| ACK Timeout                      | <div>48</div> <div>μs</div> <div>Default</div>  |
| Frame Aggregation                | <input type="checkbox"/>  |


### AP Settings

#### SSID

These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Pepwave MAX 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.

|   |   |
|---|---|
| <b>Operating Country</b>                            | <p>This drop-down menu specifies the national / regional regulations which the AP should follow.</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).</li> </ul> <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>   |
| <b>Preferred Frequency</b>                          | 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.  |
| <b>Protocol</b>                                     | This section displays the 2.4 GHz protocols your APs are using.   |
| <b>Channel Width</b>                                | 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.  |
| <b>Channel</b>                                      | 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 <b>Auto</b> is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.  |
| <b>Auto Channel Update</b>                          | Indicate the time of day at which update automatic channel selection.   |
| <b>Output Power<sup>A</sup></b>                     | <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 <b>Dynamic</b> settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance.</p> <p>The <b>Dynamic: Auto</b> setting will set the AP to do this automatically. Otherwise, the <b>Dynamic: Manual</b> setting will set the AP to dynamically adjust only if instructed to do so. If you have set <b>Dynamic:Manual</b>, you can go to <b>AP&gt;Toolbox&gt;Auto Power Adj.</b> to give your AP further instructions.</p> <p>If you click the <b>Boost</b> checkbox, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to increased interference.</p> |
| <b>Client Signal Strength Threshold<sup>A</sup></b> | This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.  |

|  |   |
|--|---|
| <b>Max number of Clients<sup>A</sup></b>   | This field determines the maximum clients that can be connected to APs under this profile.  |
| <b>Management VLAN ID</b>                  | This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is <b>0</b> by default, meaning that no VLAN tagging will be applied.<br>Note: change this value with caution as alterations may result in loss of connection to the AP controller. |
| <b>Operating Schedule</b>                  | Choose from the schedules that you have defined in <b>System&gt;Schedule</b> . Select the schedule for the integrated AP to follow from the drop-down menu.   |
| <b>Beacon Rate<sup>A</sup></b>             | This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are <b>1Mbps</b> , <b>2Mbps</b> , <b>5.5Mbps</b> , <b>6Mbps</b> , and <b>11Mbps</b> .  |
| <b>Beacon Interval<sup>A</sup></b>         | This drop-down menu provides the option to set the time between each beacon send. Available options are <b>100ms</b> , <b>250ms</b> , and <b>500ms</b> .  |
| <b>DTIM<sup>A</sup></b>                    | 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.  |
| <b>RTS Threshold<sup>A</sup></b>           | This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting <b>0</b> disables this feature.  |
| <b>Fragmentation Threshold<sup>A</sup></b> | Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.  |
| <b>Distance/Time Converter<sup>A</sup></b> | Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.   |
| <b>Slot Time<sup>A</sup></b>               | This field provides the option to modify the unit wait time before it transmits. The default value is <b>9μs</b> .  |
| <b>ACK Timeout<sup>A</sup></b>             | This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is <b>48μs</b> .   |
| <b>Frame Aggregation<sup>A</sup></b>       | With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.  |
| <b>Frame Length</b>                        | This field is only available when <b>Frame Aggregation</b> is enabled. It specifies the frame length for frame aggregation. By default, it is set to <b>50000</b> .   |

<sup>A</sup> - Advanced feature. Click the  button on the top right-hand corner to activate.

| Integrated AP        |  |
|----------------------|--|
| Wi-Fi Operating Mode | <input checked="" type="radio"/> WAN <input type="radio"/> WAN + AP <input type="radio"/> AP |

The device with integrated AP can operate under the Wi-Fi Operating Mode:

**Note:** This option is available only for HD2/HD4 and HD2/HD4 MBX.

| Integrated AP   |   |
|-----------------|---|
| <b>WAN</b>      | In this mode, all Wi-Fi will operate as Wi-Fi WAN. Since all device Wi-Fi are exhausted, no integrated Wi-Fi AP will be operated on this device.                                |
| <b>WAN + AP</b> | In this mode, some Wi-Fi will operate as Wi-Fi WAN. Some other Wi-Fi WANS will be forced offline and their Wi-Fi resources will be reserved for integrated Wi-Fi AP operations. |
| <b>AP</b>       | in this mode, all Wi-Fi functions as integrated Wi-Fi AP. All Wi-Fi WANS will be forced to go offline.  |

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

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

| Wi-Fi Radio Settings |  |
|----------------------|--|
| Operating Country    | United States ▼  |
| Wi-Fi Antenna        | <input type="radio"/> Internal <input checked="" type="radio"/> External |

| Wi-Fi AP Settings  |   |
|---|---|
| Protocol  | 802.11ng ▼  |
| Channel   | 1 (2.412 GHz) ▼   |
| Channel Width   | Auto ▼  |
| Output Power  | Max ▼ <input type="checkbox"/> Boost  |
| Beacon Rate   |  1Mbps ▼ |
| Beacon Interval   |  100ms ▼ |
| DTIM  |  1       |
| Slot Time   |  9 μs    |
| ACK Timeout   |  48 μs   |
| Frame Aggregation   | <input checked="" type="checkbox"/> Enable  |
| Guard Interval  | <input type="radio"/> Short <input type="radio"/> 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<sup>A</sup>

This option is for setting the transmit bit rate for sending a beacon. By default,

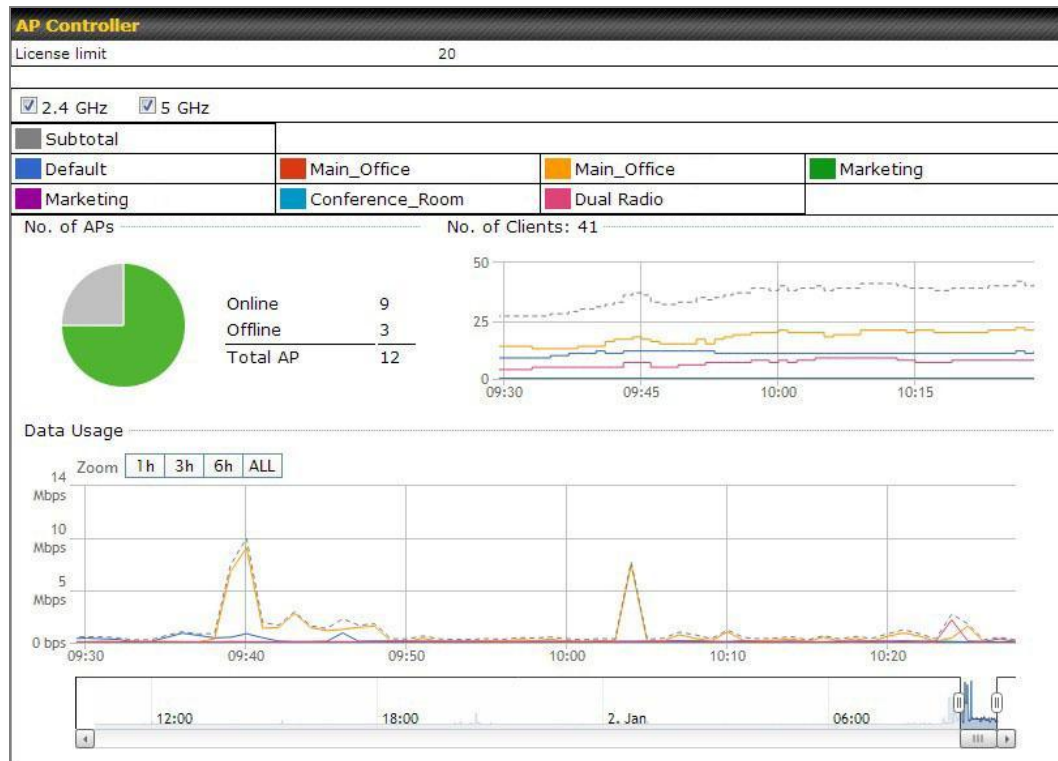
|                                      |   |
|--------------------------------------|---|
|                                      | <b>1Mbps</b> is selected.   |
| <b>Beacon Interval<sup>A</sup></b>   | This option is for setting the time interval between each beacon. By default, <b>100ms</b> is selected.   |
| <b>DTIM<sup>A</sup></b>              | 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 <b>1 ms</b> . |
| <b>Slot Time<sup>A</sup></b>         | This field is for specifying the wait time before the Router transmits a packet. By default, this field is set to <b>9 µs</b> .   |
| <b>ACK Timeout<sup>A</sup></b>       | This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to <b>48 µs</b> .                                |
| <b>Frame Aggregation<sup>A</sup></b> | This option allows you to enable frame aggregation to increase transmission throughput.   |
| <b>Guard Interval<sup>A</sup></b>    | This setting allows choosing a short or long guard period interval for your transmissions.  |

<sup>A</sup> - 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         |   |
|-----------------------|---|
| <b>License Limit</b>  | 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.  |
| <b>Frequency</b>      | Underneath, there are two check boxes labeled <b>2.4 Ghz</b> and <b>5 Ghz</b> . 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. |
| <b>SSID</b>           | 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.   |
| <b>No. of APs</b>     | This pie chart and table indicates how many APs are online and how many are offline.  |
| <b>No. of Clients</b> | 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:A8:2D:A0:D5 disassociated from Marketing_11a |             |
| Jan 2 11:00:42 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |             |
| Jan 2 11:00:38 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |             |
| Jan 2 11:00:36 | AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a      |             |
| Jan 2 11:00:20 | AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a |             |
| Jan 2 11:00:09 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |             |
| Jan 2 10:59:09 | AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a   |             |
| Jan 2 10:59:08 | Office Fiber 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:A8:2D:A0:D5 disassociated from Marketing_11a |             |
| Jan 2 10:58:03 | Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless       |             |
| Jan 2 10:57:47 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |             |
| Jan 2 10:57:19 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |             |
| Jan 2 10:57:09 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |             |
| Jan 2 10:56:48 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |             |
| Jan 2 10:56:39 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |             |
| Jan 2 10:56:19 | AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a    |             |
| Jan 2 10:56:09 | AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a    |             |
| Jan 2 10:55:42 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |             |
| Jan 2 10:55:29 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |             |
|                |  | More...     |

### 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="text"/>                     |
|                                | <input type="checkbox"/> Include Offline APs |
| Search Result                  |  |

| Managed APs                             |            |                   |          |          |         |               | Expand | Collapse |
|---|------------|-------------------|----------|----------|---------|---------------|--------|----------|
| Name                                    | IP Address | MAC               | Location | Firmware | Pack ID | Configuration |        |          |
| Default (8/9 online)                    |            |                   |          |          |         |               |        |          |
| <input type="checkbox"/> J100-AM1P-BC10 | 10.8.82.11 | 00:1A:DD:BD:73:E0 | -        | 3.5.2    | None    | ✓             | -      |          |


| Usage                           |   |             |                |           |           |           |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
|---------------------------------|---|-------------|----------------|-----------|-----------|-----------|--------|----------|-------------------|----------|----------|----------------|---------|----------|----------|-------------------|------------|----------|----------------|---------|---------|---------|-------------------|------------|----------|-----------|---------|---------|-----------|-------------------|------------|----------|----------------|---------|---------|-----------|-------------------|-----------|----------|----------------|---------|-----------|-----------|-------------------|-----------|----------|----------------|---------|---------|---------|-------------------|-----------|----------|----------------|----------|---------|---------|-------------------|-----------|----------|----------------|----------|---------|----------|-------------------|-----------|----------|-----------|----------|-----------|---------|-------------------|-------------|----------|----------------|-----------|----------|---------|-------------------|-------------|----------|-----------|-----------|----------|
| <b>AP Name/Serial Number</b>    | 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.   |             |                |           |           |           |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| <b>Online Status</b>            | This button toggles whether your search will include offline devices.   |             |                |           |           |           |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| <b>Managed Wireless Devices</b> | <p>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.</p> <p>You could also expand and collapse all groups by using the <input type="button" value="Expand"/> <input type="button" value="Collapse"/></p>  |             |                |           |           |           |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
|                                 | <p>On the right of the table, you will see the following icons:   </p>   |             |                |           |           |           |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
|                                 | <p>Click the  icon to see a usage table for each client:</p>   |             |                |           |           |           |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
|                                 | <div> <div>Client List</div> <table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Type</th> <th>Signal</th> <th>SSID</th> <th>Upload</th> <th>Download</th> </tr> </thead> <tbody> <tr><td>80:56:f2:98:75:ff</td><td>10.9.2.7</td><td>802.11ng</td><td>Excellent (37)</td><td>Balance</td><td>66.26 MB</td><td>36.26 MB</td></tr> <tr><td>c4:6a:b7:bf:d7:15</td><td>10.9.2.123</td><td>802.11ng</td><td>Excellent (42)</td><td>Balance</td><td>6.65 MB</td><td>2.26 MB</td></tr> <tr><td>70:56:81:1d:87:f3</td><td>10.9.2.102</td><td>802.11ng</td><td>Good (23)</td><td>Balance</td><td>1.86 MB</td><td>606.63 KB</td></tr> <tr><td>e0:63:e5:83:45:c8</td><td>10.9.2.101</td><td>802.11ng</td><td>Excellent (39)</td><td>Balance</td><td>3.42 MB</td><td>474.52 KB</td></tr> <tr><td>18:00:2d:3d:4e:7f</td><td>10.9.2.66</td><td>802.11ng</td><td>Excellent (25)</td><td>Balance</td><td>640.29 KB</td><td>443.57 KB</td></tr> <tr><td>14:5a:05:80:4f:40</td><td>10.9.2.76</td><td>802.11ng</td><td>Excellent (29)</td><td>Balance</td><td>2.24 KB</td><td>3.67 KB</td></tr> <tr><td>00:1a:dd:c5:4e:24</td><td>10.8.9.84</td><td>802.11ng</td><td>Excellent (29)</td><td>Wireless</td><td>9.86 MB</td><td>9.76 MB</td></tr> <tr><td>00:1a:dd:bb:29:ec</td><td>10.8.9.73</td><td>802.11ng</td><td>Excellent (25)</td><td>Wireless</td><td>9.36 MB</td><td>11.14 MB</td></tr> <tr><td>40:b0:fa:c3:26:2c</td><td>10.8.9.18</td><td>802.11ng</td><td>Good (23)</td><td>Wireless</td><td>118.05 MB</td><td>7.92 MB</td></tr> <tr><td>e4:25:e7:8a:d3:12</td><td>10.10.11.23</td><td>802.11ng</td><td>Excellent (35)</td><td>Marketing</td><td>74.78 MB</td><td>4.58 MB</td></tr> <tr><td>04:f7:e4:ef:68:05</td><td>10.10.11.71</td><td>802.11ng</td><td>Poor (12)</td><td>Marketing</td><td>84.84 KB</td><td>119.32 KB</td></tr> </tbody> </table> <div>Close</div> </div> | MAC Address | IP Address     | Type      | Signal    | SSID      | Upload | Download | 80:56:f2:98:75:ff | 10.9.2.7 | 802.11ng | Excellent (37) | Balance | 66.26 MB | 36.26 MB | c4:6a:b7:bf:d7:15 | 10.9.2.123 | 802.11ng | Excellent (42) | Balance | 6.65 MB | 2.26 MB | 70:56:81:1d:87:f3 | 10.9.2.102 | 802.11ng | Good (23) | Balance | 1.86 MB | 606.63 KB | e0:63:e5:83:45:c8 | 10.9.2.101 | 802.11ng | Excellent (39) | Balance | 3.42 MB | 474.52 KB | 18:00:2d:3d:4e:7f | 10.9.2.66 | 802.11ng | Excellent (25) | Balance | 640.29 KB | 443.57 KB | 14:5a:05:80:4f:40 | 10.9.2.76 | 802.11ng | Excellent (29) | Balance | 2.24 KB | 3.67 KB | 00:1a:dd:c5:4e:24 | 10.8.9.84 | 802.11ng | Excellent (29) | Wireless | 9.86 MB | 9.76 MB | 00:1a:dd:bb:29:ec | 10.8.9.73 | 802.11ng | Excellent (25) | Wireless | 9.36 MB | 11.14 MB | 40:b0:fa:c3:26:2c | 10.8.9.18 | 802.11ng | Good (23) | Wireless | 118.05 MB | 7.92 MB | e4:25:e7:8a:d3:12 | 10.10.11.23 | 802.11ng | Excellent (35) | Marketing | 74.78 MB | 4.58 MB | 04:f7:e4:ef:68:05 | 10.10.11.71 | 802.11ng | Poor (12) | Marketing | 84.84 KB |
| MAC Address                     | IP Address  | Type        | Signal         | SSID      | Upload    | Download  |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 80:56:f2:98:75:ff               | 10.9.2.7  | 802.11ng    | Excellent (37) | Balance   | 66.26 MB  | 36.26 MB  |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| c4:6a:b7:bf:d7:15               | 10.9.2.123  | 802.11ng    | Excellent (42) | Balance   | 6.65 MB   | 2.26 MB   |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 70:56:81:1d:87:f3               | 10.9.2.102  | 802.11ng    | Good (23)      | Balance   | 1.86 MB   | 606.63 KB |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| e0:63:e5:83:45:c8               | 10.9.2.101  | 802.11ng    | Excellent (39) | Balance   | 3.42 MB   | 474.52 KB |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 18:00:2d:3d:4e:7f               | 10.9.2.66   | 802.11ng    | Excellent (25) | Balance   | 640.29 KB | 443.57 KB |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 14:5a:05:80:4f:40               | 10.9.2.76   | 802.11ng    | Excellent (29) | Balance   | 2.24 KB   | 3.67 KB   |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 00:1a:dd:c5:4e:24               | 10.8.9.84   | 802.11ng    | Excellent (29) | Wireless  | 9.86 MB   | 9.76 MB   |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 00:1a:dd:bb:29:ec               | 10.8.9.73   | 802.11ng    | Excellent (25) | Wireless  | 9.36 MB   | 11.14 MB  |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 40:b0:fa:c3:26:2c               | 10.8.9.18   | 802.11ng    | Good (23)      | Wireless  | 118.05 MB | 7.92 MB   |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| e4:25:e7:8a:d3:12               | 10.10.11.23   | 802.11ng    | Excellent (35) | Marketing | 74.78 MB  | 4.58 MB   |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
| 04:f7:e4:ef:68:05               | 10.10.11.71   | 802.11ng    | Poor (12)      | Marketing | 84.84 KB  | 119.32 KB |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |
|                                 | Click the  icon to configure each client   |             |                |           |           |           |        |          |                   |          |          |                |         |          |          |                   |            |          |                |         |         |         |                   |            |          |           |         |         |           |                   |            |          |                |         |         |           |                   |           |          |                |         |           |           |                   |           |          |                |         |         |         |                   |           |          |                |          |         |         |                   |           |          |                |          |         |          |                   |           |          |           |          |           |         |                   |             |          |                |           |          |         |                   |             |          |           |           |          |

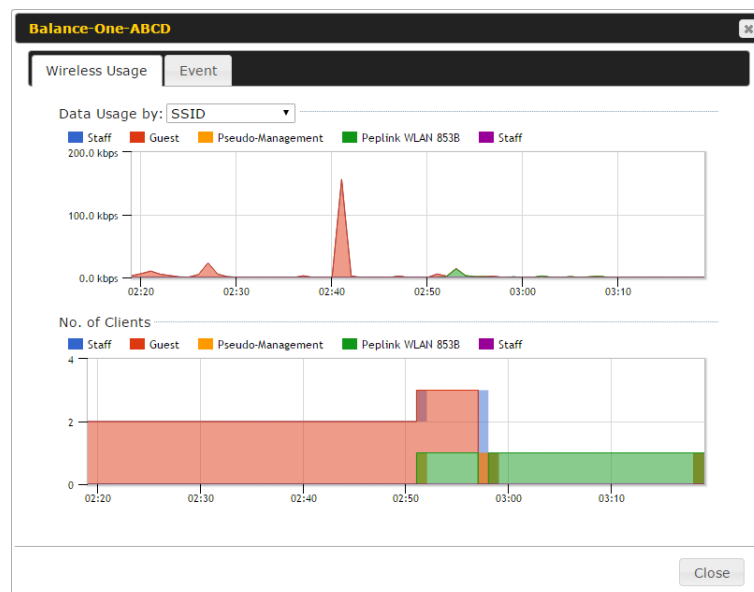
**AP Details**

|                                   |   |
|-----------------------------------|---|
| Serial Number                     | 1111-2222-3333  |
| MAC Address                       | 00:1A:DD:BD:73:E0   |
| Product Name                      | Pepwave AP Pro Duo  |
| Name                              |   |
| Location                          |   |
| Firmware Version                  | 3.5.2   |
| Firmware Pack                     | Default (None)  |
| AP Client Limit                   | <input checked="" type="radio"/> Follow AP Profile <input type="radio"/> Custom |
| 2.4 GHz SSID List                 | T4Open  |
| 5 GHz SSID List                   | T4Open  |
| Last config applied by controller | Mon Nov 23 11:25:03 HKT 2015  |
| Uptime                            | Wed Nov 11 15:00:27 HKT 2015  |
| Current Channel                   | 1 (2.4 GHz)<br>153 (5 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                   |

Close

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

Click the  icon to see a graph displaying usage:



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

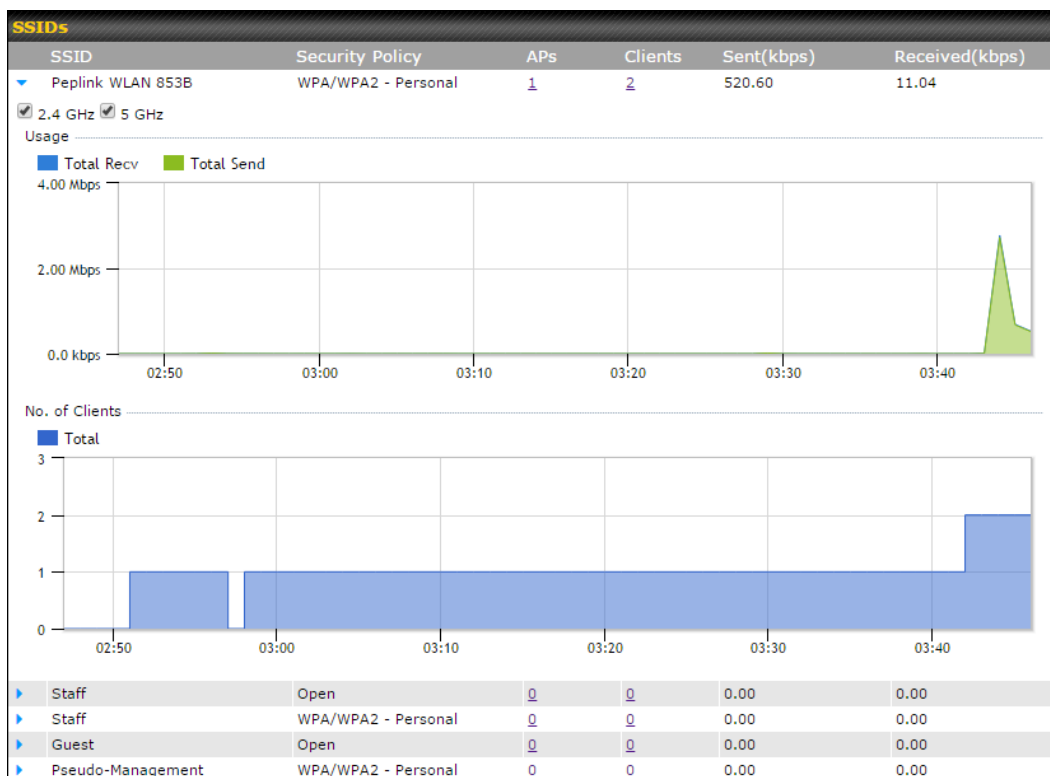
Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that

particular device:

| Event Information |  |
|-------------------|--|
| Events            |  |
| Jan 2 11:53:39    | Client 00:26:BB:08:AC:FD associated with Wireless_11a              |
| Jan 2 11:39:31    | Client 60:67:20:24:B6:4C disassociated from Marketing_11a          |
| Jan 2 11:16:55    | Client A8:BB:CF:E1:0F:1E disassociated from Balance_11a            |
| Jan 2 11:11:54    | Client A8:BB:CF:E1:0F:1E associated with Balance_11a               |
| Jan 2 11:10:45    | Client 60:67:20:24:B6:4C associated with Marketing_11a             |
| Jan 2 11:00:36    | Client 00:21:6A:35:59:A4 associated with Balance_11a               |
| Jan 2 11:00:20    | Client 60:67:20:24:B6:4C disassociated from Marketing_11a          |
| Jan 2 10:59:09    | Client 00:21:6A:35:59:A4 disassociated from Balance_11a            |
| Jan 2 10:42:28    | Client F4:B7:E2:16:35:E9 associated with Balance_11a               |
| Jan 2 10:29:12    | Client 84:7A:88:78:1E:4B associated with Balance_11a               |
| Jan 2 10:24:27    | Client 90:B9:31:0D:11:EC disassociated from Marketing_11a          |
| Jan 2 10:24:27    | Client 90:B9:31:0D:11:EC roamed to Marketing_11a at 2830-BFC8-D230 |
| Jan 2 10:13:22    | Client E8:8D:28:A8:43:93 associated with Balance_11a               |
| Jan 2 10:13:22    | Client E8:8D:28:A8:43:93 roamed to Balance_11a from 2830-BF7F-694C |
| Jan 2 10:07:52    | Client CC:3A:61:89:07:F3 associated with Wireless_11a              |
| Jan 2 10:04:35    | Client 60:67:20:24:B6:4C associated with Marketing_11a             |
| Jan 2 10:03:38    | Client 60:67:20:24:B6:4C disassociated from Marketing_11a          |
| Jan 2 09:58:27    | Client 00:26:BB:08:AC:FD disassociated from Wireless_11a           |
| Jan 2 09:52:46    | Client 00:26:BB:08:AC:FD associated with Wireless_11a              |
| Jan 2 09:20:26    | Client 8C:3A:E3:3F:17:62 associated with Balance_11a               |

## 26.3 Wireless SSID

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





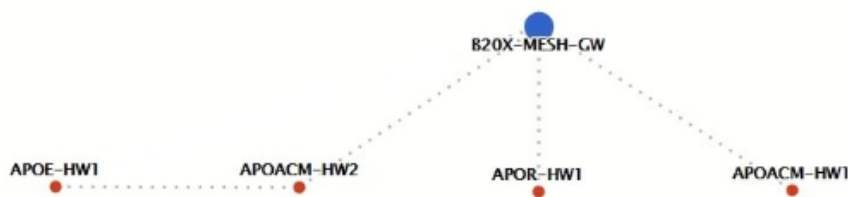
Click the blue arrow on any SSID to obtain more detailed usage information on each SSID.

## 26.4 Mesh / WDS

Mesh / WDS allows you to monitor the status of your wireless distribution system (WDS) or Mesh, and track activity by MAC address by navigating to **AP > Controller Status > Mesh / WDS**. This table shows the detailed information of each AP, including protocol, transmit rate (sent / received), signal strength, and duration.

| Mesh / WDS      |          |          |             |                |              |          |
|-----------------|----------|----------|-------------|----------------|--------------|----------|
| Type            | Peer MAC | Protocol | Rate (Send) | Rate (Receive) | Signal (dBm) | Duration |
| ▼ APOACM-HW1/   |          |          |             |                |              |          |
| Mesh ( )        |          | 802.11ac | 325M        | 650M           | -56          | 19:13:35 |
| ▼ APOACM-HW2/   |          |          |             |                |              |          |
| Mesh ( )        |          | 802.11ac | 650M        | 351M           | -63          | 00:49:20 |
| Mesh ( )        |          | 802.11ac | 390M        | 325M           | -67          | 01:35:09 |
| ▼ APOE-HW1/     |          |          |             |                |              |          |
| Mesh ( )        |          | 802.11ac | 58.5M       | 130M           | -69          | 00:45:22 |
| ▼ APOR-HW1/     |          |          |             |                |              |          |
| Mesh ( )        |          | 802.11ac | 325M        | 866.7M         | -53          | 19:14:44 |
| ▼ B20X-MESH-GW/ |          |          |             |                |              |          |
| Mesh ( )        |          | 802.11ac | 433M        | 650M           | -69          | 19:14:44 |
| Mesh ( )        |          | 802.11ac | 325M        | 390M           | -66          | 01:35:42 |
| Mesh ( )        |          | 802.11ac | 351M        | 650M           | -70          | 19:13:45 |
| Mesh ( )        |          | 802.11ac | 130M        | 117M           | -88          | 00:45:52 |

Network Graph







## 26.5 Wireless Client

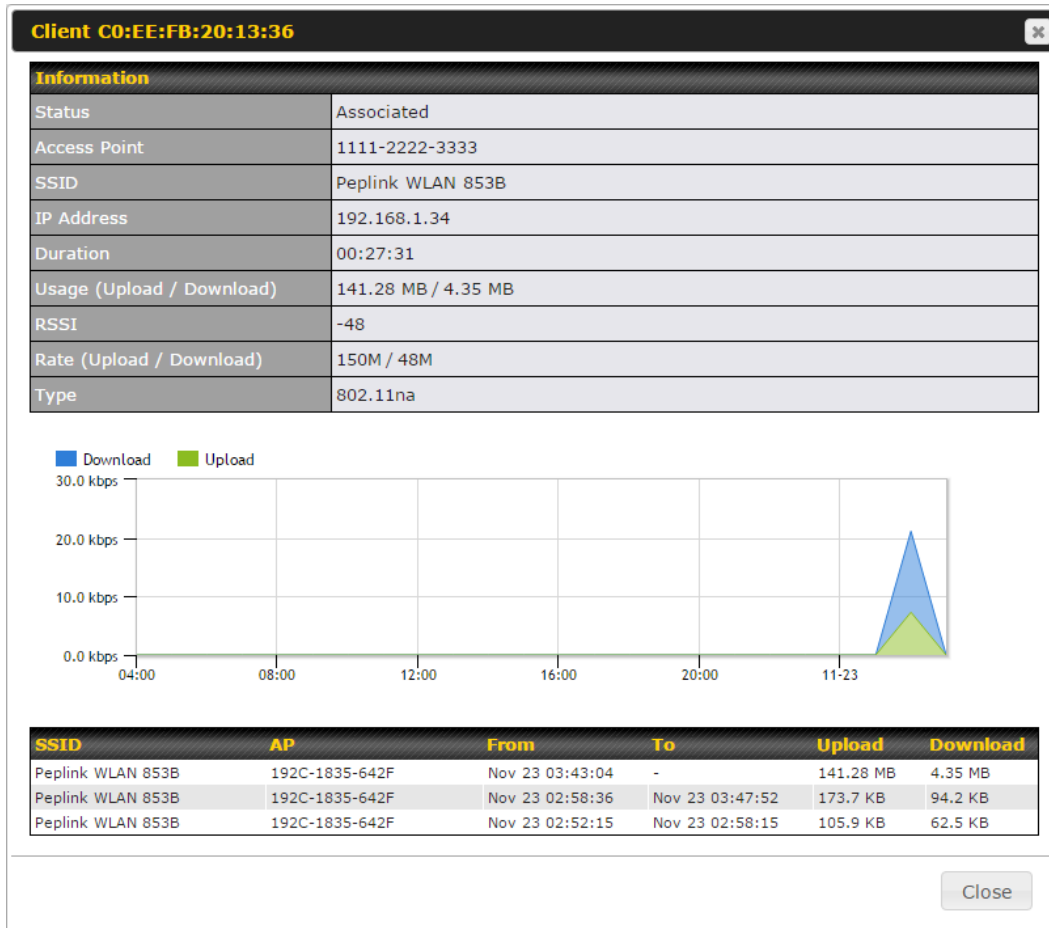
You can search for specific Wi-Fi users by navigating to **AP > Controller Status > Wireless Client**.

| Search Filter                         |                                 |  |
|---------------------------------------|---------------------------------|--|
| Client MAC / SSID / AP Serial Number  | <input type="text"/>            |  |
| Maximum Result (1-256)                | <input type="text" value="50"/> |  |
| Search Result                         |                                 |  |
| <input type="button" value="Search"/> |                                 |  |














| Top 10 Clients of last hour (Updated at 03:00) |         |          |   |
|--|---------|----------|---|
| Client MAC Address                             | Upload  | Download |   |
| C0:EE:FB:20:13:36                              | 53.5 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:





## 26.6 Nearby Device

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

| Suspected Rogue APs |                         |         |            |                |   |
|---------------------|-------------------------|---------|------------|----------------|---|
| BSSID               | SSID                    | Channel | Encryption | Last Seen      | Mark as   |
| 00:1A:DD:EC:25:22   | Wireless                | 11      | WPA2       | 10 hours ago   |       |
| 00:1A:DD:EC:25:23   | Accounting              | 11      | WPA2       | 10 hours ago   |       |
| 00:1A:DD:EC:25:24   | Marketing               | 11      | WPA2       | 11 hours ago   |       |
| 00:03:7F:00:00:00   | MYB1PUSH                | 1       | WPA & WPA2 | 11 minutes ago |       |
| 00:03:7F:00:00:01   | MYB1                    | 1       | WPA2       | 15 minutes ago |       |
| 00:1A:DD:B9:60:88   | PEPWAVE_CB7E            | 1       | WPA & WPA2 | 5 minutes ago  |       |
| 00:1A:DD:BB:09:C1   | Micro_S1_1              | 6       | WPA & WPA2 | 1 hour ago     |       |
| 00:1A:DD:BB:52:A8   | MAX HD2 Gobi            | 11      | WPA & WPA2 | 2 minutes ago  |       |
| 00:1A:DD:BF:75:81   | PEPLINK_05B5            | 4       | WPA & WPA2 | 1 minute ago   |       |
| 00:1A:DD:BF:75:82   | LK_05B5                 | 4       | WPA2       | 1 minute ago   |       |
| 00:1A:DD:BF:75:83   | LK_05B5_VLAN22          | 4       | WPA2       | 1 minute ago   |       |
| 00:1A:DD:C1:ED:E4   | dev_captive_portal_test | 1       | WPA & WPA2 | 3 minutes ago  |       |
| 00:1A:DD:C2:E4:C5   | PEPWAVE_7052            | 11      | WPA & WPA2 | 2 hours ago    |       |
| 00:1A:DD:C3:F1:64   | dev_captive_portal_test | 6       | WPA & WPA2 | 6 minutes ago  |       |
| 00:1A:DD:C4:DC:24   | ssid_test               | 8       | WPA & WPA2 | 2 minutes ago  |       |
| 00:1A:DD:C4:DC:25   | SSID New                | 8       | WPA & WPA2 | 2 minutes ago  |     |
| 00:1A:DD:C5:46:04   | Guest SSID              | 9       | WPA2       | 2 minutes ago  |   |
| 00:1A:DD:C5:47:04   | PEPWAVE_67B8            | 1       | WPA & WPA2 | 5 minutes ago  |   |
| 00:1A:DD:C5:4E:24   | G BR1 Portal            | 2       | WPA2       | 2 minutes ago  |   |
| 00:1A:DD:C6:9A:48   | ssid_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.

## 26.7 Event Log

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

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

| Events         |  | <a href="#">View Alerts</a> |
|----------------|--|-----------------------------|
| Jan 2 11:01:11 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |                             |
| Jan 2 11:00:42 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |                             |
| Jan 2 11:00:38 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |                             |
| Jan 2 11:00:36 | AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a      |                             |
| Jan 2 11:00:20 | AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a |                             |
| Jan 2 11:00:09 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |                             |
| Jan 2 10:59:09 | AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a   |                             |
| Jan 2 10:59:08 | Office Fiber 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:A8:2D:A0:D5 disassociated from Marketing_11a |                             |
| Jan 2 10:58:03 | Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless       |                             |
| Jan 2 10:57:47 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |                             |
| Jan 2 10:57:19 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |                             |
| Jan 2 10:57:09 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |                             |
| Jan 2 10:56:48 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |                             |
| Jan 2 10:56:39 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |                             |
| Jan 2 10:56:19 | AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a    |                             |
| Jan 2 10:56:09 | AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a    |                             |
| Jan 2 10:55:42 | AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a |                             |
| Jan 2 10:55:29 | AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a    |                             |
|                |  | <a href="#">More...</a>     |

## 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  |
| 1126   | 2013-08-26   |  |  |
| <a href="#">Check for Updates</a> <a href="#">Manual Upload</a> <a href="#">Default...</a> 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 hostname: mbx-345a<br>⚙️ This configuration is being managed by InControl. |
| 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<br><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           | <input checked="" type="radio"/> Any <input type="radio"/> Allow this network only |

Save

| Admin Settings                |  |
|-------------------------------|--|
| <b>Router Name</b>            | This field allows you to define a name for this Pepwave router. By default, <b>Router Name</b> is set as <b>MAX_XXXX</b> , where XXXX refers to the last 4 digits of the unit's serial number. |
| <b>Admin User Name</b>        | <b>Admin User Name</b> is set as <i>admin</i> by default, but can be changed, if desired.  |
| <b>Admin Password</b>         | This field allows you to specify a new administrator password.   |
| <b>Confirm Admin Password</b> | This field allows you to verify and confirm the new administrator password.  |
| <b>Read-only User Name</b>    | <b>Read-only User Name</b> is set as <i>user</i> by default, but can be changed, if desired.   |
| <b>User Password</b>          | This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.   |
| <b>Confirm User Password</b>  | This field allows you to verify and confirm the new user password.   |

|                                  |  |
|----------------------------------|--|
| <b>Web Session Timeout</b>       | 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 <b>4 hours</b> .  |
| <b>Authentication by RADIUS</b>  | 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. |
| <b>Auth Protocol</b>             | This specifies the authentication protocol used. Available options are <b>MS-CHAP v2</b> and <b>PAP</b> .  |
| <b>Auth Server</b>               | This specifies the access address and port of the external RADIUS server.  |
| <b>Auth Server Secret</b>        | This field is for entering the secret key for accessing the RADIUS server.   |
| <b>Auth Timeout</b>              | This option specifies the time value for authentication timeout.   |
| <b>Accounting Server</b>         | This specifies the access address and port of the external accounting server.  |
| <b>Accounting Server Secret</b>  | This field is for entering the secret key for accessing the accounting server.   |
| <b>Network Connection</b>        | This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.   |
| <b>CLI SSH</b>                   | The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to <b>Section 30.5</b> .  |
| <b>CLI SSH Access</b>            | This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.   |
| <b>CLI SSH Port</b>              | This field determines the port on which clients can access CLI SSH.  |
| <b>CLI SSH Access Public Key</b> | This field is for entering the Public Key for Admin Users and Read-only Users to access CLI SSH.   |
| <b>Security</b>                  | <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"> <li>• HTTP</li> <li>• HTTPS</li> <li>• HTTP/HTTPS</li> </ul>  |
| <b>Web Admin Port</b>            | This field is for specifying the port number on which the web admin interface can  |

|                         |   |
|-------------------------|---|
|                         | be accessed.  |
| <b>Web Admin Access</b> | <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"> <li>• LAN only</li> <li>• LAN/WAN</li> </ul> <p>If LAN/WAN is chosen, the <b>WAN Connection Access Settings</b> form will be displayed.</p> |

| LAN Connection Access Settings |  |
|--------------------------------|--|
| Allowed LAN Networks           | <input type="radio"/> Any <input checked="" type="radio"/> Allow this network only           Public (10) ▼ |

| LAN Connection Access Settings |   |
|--------------------------------|---|
| <b>Allowed LAN Networks</b>    | This field allows you to permit only specific networks or VLANs to access the Web UI. |

| WAN Connection Access Settings            |  |                             |     |       |   |  |  |                                |  |  |                                    |  |  |                                     |  |  |                                     |  |  |                              |  |  |
|---|--|-----------------------------|-----|-------|---|--|--|--------------------------------|--|--|------------------------------------|--|--|-------------------------------------|--|--|-------------------------------------|--|--|------------------------------|--|--|
| Allowed Source IP Subnets ?               | <input type="radio"/> Any <input checked="" type="radio"/> Allow access from the following IP subnets only<br><div></div>  |                             |     |       |   |  |  |                                |  |  |                                    |  |  |                                     |  |  |                                     |  |  |                              |  |  |
| Allowed WAN IP Address(es)                | <table border="1"> <thead> <tr> <th>Connection / IP Address(es)</th> <th>All</th> <th>Clear</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> WAN 1</td> <td><input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Wi-Fi WAN</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 1</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 2</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> USB</td> <td></td> <td></td> </tr> </tbody> </table> | Connection / IP Address(es) | All | Clear | <input checked="" type="checkbox"/> WAN 1 | <input checked="" type="checkbox"/> 10.88.3.158 (Interface IP) |  | <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 |  |  |
| Connection / IP Address(es)               | All  | Clear                       |     |       |   |  |  |                                |  |  |                                    |  |  |                                     |  |  |                                     |  |  |                              |  |  |
| <input checked="" type="checkbox"/> WAN 1 | <input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)   |                             |     |       |   |  |  |                                |  |  |                                    |  |  |                                     |  |  |                                     |  |  |                              |  |  |
| <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              |  |                             |     |       |   |  |  |                                |  |  |                                    |  |  |                                     |  |  |                                     |  |  |                              |  |  |

| WAN Connection Access Settings   |  |
|----------------------------------|--|
| <b>Allowed Source IP Subnets</b> | <p>This field allows you to restrict web admin access only from defined IP subnets.</p> <ul style="list-style-type: none"> <li>• <b>Any</b> - Allow web admin accesses to be from anywhere, without IP address restriction.</li> <li>• <b>Allow access from the following IP subnets only</b> - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:</li> </ul> <p>The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of <i>w.x.y.z/m</i>, where <i>w.x.y.z</i> is an IP address (e.g., 192.168.0.0), and <i>m</i> is the subnet mask in CIDR format, which is between 0 and</p> |



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

### 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**.

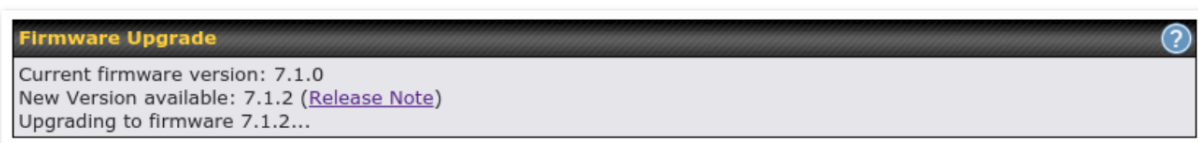


If an update is found the buttons will change to allow you to **Download and Update** the firmware.



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.**

### 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.

| Balance   |                   |                  |                          |                     |                     |  |
|---|-------------------|------------------|--------------------------|---------------------|---------------------|--|
| <div>Product <span>▼</span></div> <div>Search: <input type="text"/></div> |                   |                  |                          |                     |                     |  |
| Product   | Hardware Revision | Firmware Version | Download Link            | Release Notes       | User Manual         |  |
| Balance 1350  | HW2               | 7.1.2            | <a href="#">Download</a> | <a href="#">PDF</a> | <a href="#">PDF</a> |  |
| Balance 1350  | HW1               | 6.3.4            | <a href="#">Download</a> | <a href="#">PDF</a> | <a href="#">PDF</a> |  |
| Balance 20  | HW1-6             | 7.1.2            | <a href="#">Download</a> | <a href="#">PDF</a> | <a href="#">PDF</a> |  |
| Balance 210   | HW4               | 7.1.2            | <a href="#">Download</a> | <a href="#">PDF</a> | <a href="#">PDF</a> |  |

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

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

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

**Manual Firmware Upgrade**

Firmware Image
No file chosen

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.**

## 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

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▼
☐ Show all

Time Server

0.pepwave.pool.ntp.org

### 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**

| Schedule                |               |         |   |
|-------------------------|---------------|---------|---|
| Enabled                 |               |         |  |
| Name                    | Time          | Used by |   |
| <u>Weekdays Only</u>    | Weekdays only | -       |  |
| <div>New Schedule</div> |               |         |   |

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

[illegible]

## Edit Schedule Profile


## Enabling


Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.

|                     |   |
|---------------------|---|
| <b>Name</b>         | Enter your desired name for this particular schedule profile.   |
| <b>Schedule</b>     | 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. |
| <b>Schedule Map</b> | 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 Setup**


|                           |  |
|---------------------------|--|
| Email Notification        | <input checked="" type="checkbox"/> Enable   |
| SMTP Server               | smtp.mycompany.com<br><input checked="" type="checkbox"/> Require authentication   |
| Connection Security       | SSL/TLS ▼ (Note: any server certificate will be accepted)  |
| SMTP Port                 | 465  |
| SMTP User Name            | smtpuser   |
| SMTP Password             | *****  |
| Confirm SMTP Password     | *****  |
| Sender's Email Address    | admin@mycompany.com  |
| Recipient's Email Address | system@mycompany.com<br>staff@mycompany.com<br> |

Test Email Notification
Save

| Email Notification Settings |   |
|-----------------------------|---|
| <b>Email Notification</b>   | This setting specifies whether or not to enable email notification. If <b>Enable</b> is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If <b>Enable</b> is not checked, email notification is disabled and the Pepwave router will not send email messages. |
| <b>SMTP Server</b>          | This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check <b>Require authentication</b> .   |
| <b>Connection Security</b>  | This setting specifies via a drop-down menu one of the following valid Connection Security:   |

|                                  |  |
|----------------------------------|--|
|                                  | <ul style="list-style-type: none"> <li>• None</li> <li>• STARTTLS</li> <li>• SSL/TLS</li> </ul>  |
| <b>SMTP Port</b>                 | <p>This field is for specifying the SMTP port number. By default, this is set to <b>25</b>. If Connection Security is selected “<b>STARTTLS</b>”, the default port number will be set to <b>587</b>. If Connection Security is selected “<b>SSL/TLS</b>”, the default port number will be set to <b>465</b>.</p> <p>You may customize the port number by editing this field.</p> |
| <b>SMTP User Name / Password</b> | <p>This setting specifies the SMTP username and password while sending email. These options are shown only if <b>Require authentication</b> is checked in the <b>SMTP Server</b> setting.</p>  |
| <b>Confirm SMTP Password</b>     | <p>This field allows you to verify and confirm the new administrator password.</p>   |
| <b>Sender's Email Address</b>    | <p>This setting specifies the email address the Pepwave router will use to send reports.</p>   |
| <b>Recipient's Email Address</b> | <p>This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the enter key.</p>   |

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

| Test Email Notification   |   |
|---------------------------|---|
| SMTP Server               | smtp.mycompany.com                          |
| SMTP Port                 | 465   |
| SMTP UserName             | smtpuser                                    |
| Sender's Email Address    | admin@mycompany.com                         |
| Recipient's Email Address | system@mycompany.com<br>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.**  
(NOTE: Settings are not saved. To confirm the update, click 'Save' button.)

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

**Test Email Notification** **Save**

#### Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
[<-] 220 smtp.gmail.com ESMTP h11sm3907691pjj.46 - gsmt
-> EHLO balance.peplink.com
[<-] 250-smtp.gmail.com at your service, [14.192.209.255]
[<-] 250-SIZE 35882577
[<-] 250-8BITMIME
[<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
[<-] 250-ENHANCEDSTATUSCODES
[<-] 250-PIPELINING
[<-] 250-CHUNKING
[<-] 250 SMTPUTF8
-> AUTH PLAIN AGdwc2dhbjk0QGdtYVlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

## 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 type="checkbox"/>         |
| Remote Syslog Host                  | <input type="text"/>             |
| Port:                               | <input type="text" value="514"/> |

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

| URL Logging     |                                     |
|-----------------|-------------------------------------|
| Enable          | <input checked="" type="checkbox"/> |
| Log Server Host | <input type="text"/>                |
| Port:           | <input type="text" value="514"/>    |

| Session Logging |                                     |
|-----------------|-------------------------------------|
| Enable          | <input checked="" type="checkbox"/> |
| Log Server Host | <input type="text"/>                |
| Port:           | <input type="text" value="514"/>    |

| Event Log Settings        |  |
|---------------------------|--|
| <b>Remote Syslog</b>      | This setting specifies whether or not to log events at the specified remote syslog server.   |
| <b>Remote Syslog Host</b> | This setting specifies the IP address or hostname of the remote syslog server.   |
| <b>Push Events</b>        | 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. |
| <b>URL Logging</b>        | This setting is to enable event logging at the specified log server.   |
| <b>URL Logging Host</b>   | This setting specifies the IP address or hostname of the URL log server.   |
| <b>Session Logging</b>    | This setting is to enable event logging at the specified log server.   |



## Session Logging Host

This setting specifies the IP address or hostname of the Session log server.



For more information on the Router Utility, go to: [www.peplink.com/products/router-utility](http://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                    | MAX_TST_3D8B  |
| Location                            | <input type="text"/>  |
| SNMP Port                           | <input type="text" value="161"/> <input type="button" value="Default"/> |
| SNMPv1                              | <input type="checkbox"/> Enable   |
| SNMPv2c                             | <input type="checkbox"/> Enable   |
| SNMPv3                              | <input type="checkbox"/> Enable   |
| SNMP Trap                           | <input checked="" type="checkbox"/> Enable                              |
| SNMP Trap Community                 | <input type="text"/>  |
| SNMP Trap Server                    | <input type="text"/>  |
| SNMP Trap Port                      | <input type="text" value="162"/>  |
| SNMP Trap Server Heartbeat          | <input type="checkbox"/>  |
| <input type="button" value="Save"/> |   |

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

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

| SNMP Settings           |  |
|-------------------------|--|
| <b>SNMP Device Name</b> | This field shows the router name defined at <b>System&gt;Admin Security</b> .        |
| <b>SNMP Port</b>        | This option specifies the port which SNMP will use. The default port is <b>161</b> . |

|                                   |  |
|-----------------------------------|--|
| <b>SNMPv1</b>                     | This option allows you to enable SNMP version 1.   |
| <b>SNMPv2</b>                     | This option allows you to enable SNMP version 2.   |
| <b>SNMPv3</b>                     | This option allows you to enable SNMP version 3.   |
| <b>SNMP Trap</b>                  | This option allows you to enable SNMP Trap. If enabled, the following entry fields will appear.      |
| <b>SNMP Trap Community</b>        | This setting specifies the SNMP Trap community name.   |
| <b>SNMP Trap Server</b>           | Enter the IP address of the SNMP Trap server.  |
| <b>SNMP Trap Port</b>             | This option specifies the port which the SNMP Trap server will use. The default port is <b>162</b> . |
| <b>SNMP Trap Server Heartbeat</b> | This option allows you to enable and configure the heartbeat interval for the SNMP Trap server.      |

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

**SNMP Community**

|                 |              |                         |
|-----------------|--------------|-------------------------|
| Community Name  | My Company   |                         |
| Allowed Network | 192.168.1.25 | / 255.255.255.0 (/24) ▼ |

Save
Cancel

**SNMPv3 User**

|                |          |                 |
|----------------|----------|-----------------|
| User Name      | SNMPUser |                 |
| Authentication | SHA ▼    | password        |
| Privacy        | DES ▼    | privacypassword |

Save
Cancel

| SNMP Community Settings |   |
|-------------------------|---|
| <b>Community Name</b>   | 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:

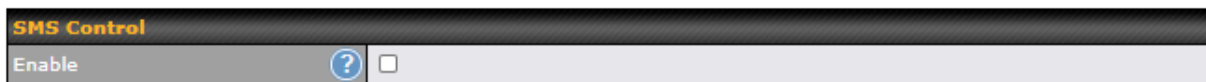
| SNMPv3 User Settings           |   |
|--------------------------------|---|
| <b>User Name</b>               | This setting specifies a user name to be used in SNMPv3.  |
| <b>Authentication Protocol</b> | <p>This setting specifies via a drop-down menu one of the following valid authentication protocols: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

## 28.8 SMS Control

SMS Control allows the user to control the device using SMS even if the modem does not have a data connection. The settings for configuring the SMS Control can be found at **System>SMS Control**.

Supported Models

- **Balance/MAX:** \*-LTE-E, \*-LTEA-W, \*-LTEA-P, \*-LTE-MX
- **EPX:** \*-LW\*, \*-LP\*



When this box is checked, the device will be allowed to take actions according to received commands via SMS.

Make sure your mobile plan supports SMS, and note that some plans may incur additional charges for this.

SMS Control can reboot devices and configure cellular settings over signalling channels, even if the modem does not have a data connection.

For details of supported SMS command sets, please refer to our [knowledge base](#).

| SMS Control          |   |              |  |                      |  |
|----------------------|---|--------------|--|----------------------|--|
| Enable               | <input checked="" type="checkbox"/>   |              |  |                      |  |
| Password             | <input type="password"/><br><input checked="" type="checkbox"/> Hide Characters   |              |  |                      |  |
| White List           | <table border="1"> <thead> <tr> <th>Phone Number</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input data-bbox="1339 514 1372 546" type="button" value="+"/></td> </tr> </tbody> </table> | Phone Number |  | <input type="text"/> | <input data-bbox="1339 514 1372 546" type="button" value="+"/> |
| Phone Number         |   |              |  |                      |  |
| <input type="text"/> | <input data-bbox="1339 514 1372 546" type="button" value="+"/>  |              |  |                      |  |

Save

| SMS Control Settings |   |
|----------------------|---|
| <b>Enable</b>        | Click the checkbox to enable the SMS Control.   |
| <b>Password</b>      | This setting sets the password for authentication - maximum of 32 characters, which cannot include semicolon (;).   |
| <b>White List</b>    | Optionally, you can add phone number(s) to the whitelist. Only matching phone numbers are allowed to issue SMS commands. Phone numbers must be in the E.164 International Phone Numbers format. |

## 28.9 InControl

| Controller Management Settings |  |
|--------------------------------|--|
| Controller                     | <input checked="" type="radio"/> InControl <input type="radio"/> Restricted to Status Reporting Only                           |
| Privately Host InControl       | <input checked="" type="checkbox"/>  |
| InControl Host                 | Primary: <input type="text"/><br>Backup: <input type="text"/><br><input type="checkbox"/> Fail over to InControl in the cloud. |

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.

Alternatively, you can also privately host InControl. Simply check the "Privately Host InControl" box and enter the IP Address of your InControl Host. If you have multiple hosts, you may enter the primary and backup IP addresses for the InControl Host and tick the "Fail over to InControl in the cloud" box. The device will connect to either the primary InControl Host or the secondary/backup ICA/IC2.

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.

## 28.10 Configuration

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

The image shows four screenshots of the Configuration page in the Pepwave web interface, separated by horizontal lines. Each screenshot has a dark header bar with a title and a help icon (question mark in a circle).

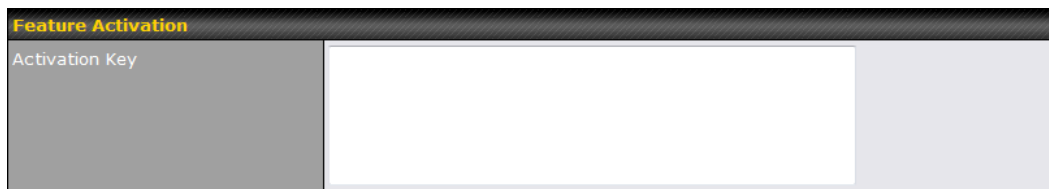
- Restore Configuration to Factory Settings:** The header is yellow. Below it is a light blue bar with a red button labeled "Restore Factory Settings".
- Download Active Configurations:** The header is yellow. Below it is a light blue bar with a grey button labeled "Download".
- Upload Configurations:** The header is yellow. Below it is a light blue bar with a "Configuration File" label, a "Browse..." button, and the text "No file selected.". At the bottom is a grey button labeled "Upload".
- Upload Configurations from High Availability Pair:** The header is yellow. Below it is a light blue bar with a "Configuration File" label, a "Browse..." button, and the text "No file selected.". At the bottom is a grey button labeled "Upload".

| Configuration                                    |   |
|--|---|
| <b>Restore Configuration to Factory Settings</b> | The <b>Restore Factory Settings</b> button is to reset the configuration to factory default settings. After clicking the button, you will need to click the <b>Apply Changes</b> button on the top right corner to make the settings effective.   |
| <b>Download Active Configurations</b>            | Click <b>Download</b> to backup the current active settings.  |
| <b>Upload Configurations</b>                     | To restore or change settings based on a configuration file, click <b>Choose File</b> to locate the configuration file on the local computer, and then click <b>Upload</b> . The new settings can then be applied by clicking the <b>Apply Changes</b> button on the page header, or you can cancel the procedure by pressing <b>discard</b> on the main page of the web admin interface. |
| <b>Upload Configurations</b>                     | In a high availability (HA) configuration, a Pepwave router can quickly load the configuration of its HA counterpart. To do so, click the <b>Upload</b> button. After loading   |

**from High Availability Pair** the settings, configure the LAN IP address of the Pepwave router so that it is different from the HA counterpart.

## 28.11 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**.

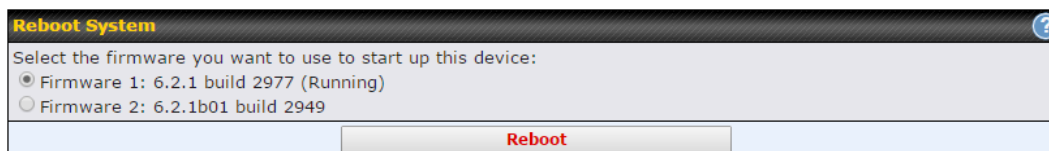


The screenshot shows a web interface titled "Feature Activation". It contains a label "Activation Key" next to a large, empty text input field for entering the activation key.

## 28.12 Reboot

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

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




The screenshot shows a web interface titled "Reboot System" with a help icon (question mark) in the top right corner. Below the title, it says "Select the firmware you want to use to start up this device:". There are two radio button options: "Firmware 1: 6.2.1 build 2977 (Running)" which is selected, and "Firmware 2: 6.2.1b01 build 2949". At the bottom of the form is a button labeled "Reboot" in red text.

## 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:

| Ping                  |   |
|-----------------------|---|
| Connection            | WAN 1 ▼   |
| Destination           | 10.10.10.1  |
| Packet Size           | 56  |
| Number of times       | Times 5  |
| <div>Start Stop</div> |   |

| Results   | Clear Log |
|---|-----------|
| PING 10.10.10.1 (10.10.10.1) from 10.88.3.158 56(84) bytes of data. |           |
| 64 bytes from 10.10.10.1: icmp_req=1 ttl=62 time=27.6 ms            |           |
| 64 bytes from 10.10.10.1: icmp_req=2 ttl=62 time=26.5 ms            |           |
| 64 bytes from 10.10.10.1: icmp_req=3 ttl=62 time=28.9 ms            |           |
| 64 bytes from 10.10.10.1: icmp_req=4 ttl=62 time=28.3 ms            |           |
| 64 bytes from 10.10.10.1: icmp_req=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 = 26.516/27.855/28.933/0.814 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**.

[illegible]

**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:



| PepVPN Throughput Test             |  |
|------------------------------------|--|
| Profile                            | NY Office ▾  |
| Type                               | <input checked="" type="radio"/> TCP <input type="radio"/> UDP         |
| Direction                          | <input checked="" type="radio"/> Upload <input type="radio"/> Download |
| Duration                           | 10 seconds (5 - 600)   |
| <input type="button" value="Go!"/> |  |
| Results                            |  |
| (Empty)                            |  |

## 29.4 Wake-on-LAN

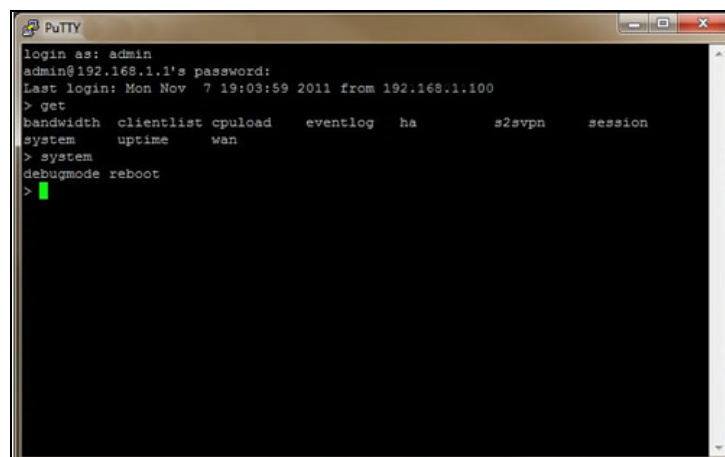
Peplink routers can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**

| Wake-on-LAN        |   |
|--------------------|---|
| Wake-on-LAN Target | Surf_SOHO (00:90:0B:36:3C:8C) ▾ <input type="button" value="Send"/> |

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.



```

PuTTY
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov 7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist  cpuload  eventlog  ha      s2svpn  session
system    uptime    wan
> system
debugmode reboot
>
  
```

## 30 Status

### 30.1 Device

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


| System Information              |   |
|---------------------------------|---|
| Device Name                     | MAX-HD2-7029                                |
| Model                           | Pepwave MAX HD2 Mini                        |
| Product Code                    | MAX-HD2-MINI-LTEA-P                         |
| Hardware Revision               | 1   |
| Serial Number                   |   |
| Firmware                        | 8.1.1 build 5033                            |
| PepVPN Version                  | 9.1.0                                       |
| Modem Support Version           | 1024 ( <a href="#">Modem Support List</a> ) |
| InControl Managed Configuration | Outbound Management                         |
| Host Name                       | max-hd2-7029                                |
| Uptime                          | 6 hours 36 minutes                          |
| System Time                     | Thu Jan 14 15:11:20 +08 2021                |
| Diagnostic Report               | <a href="#">Download</a>                    |

| MAC Address  |  |
|--------------|--|
| LAN          |  |
| WAN          |  |
| LAN 1 as WAN |  |

[Legal](#)

| System Information       |   |
|--------------------------|---|
| <b>Device Name</b>       | This is the name specified in the <b>Device Name</b> field located at <b>System&gt;Admin Security</b> . |
| <b>Model</b>             | This shows the model name and number of this device.  |
| <b>Product Code</b>      | If your model uses a product code, it will appear here.   |
| <b>Hardware Revision</b> | This shows the hardware version of this device.   |

|  |   |
|--|---|
| <b>Serial Number</b>                   | This shows the serial number of this device.  |
| <b>Firmware</b>                        | This shows the firmware version this device is currently running.                                       |
| <b>PepVPN Version</b>                  | This shows the current PepVPN version.  |
| <b>Modem Support Version</b>           | This shows the modem support version. For a list of supported modems, click <b>Modem Support List</b> . |
| <b>InControl Managed Configuration</b> | InControl Managed Configurations (firmware, VLAN, Captive Portal, etcetera)                             |
| <b>Host Name</b>                       | The host name assigned to the Pepwave router appears here.  |
| <b>Uptime</b>                          | This shows the length of time since the device has been rebooted.                                       |
| <b>System Time</b>                     | This shows the current system time.   |
| <b>OpenVPN Client Profile</b>          | Link to download OpenVpn Client profile when this is enabled in Remote User Access                      |
| <b>Diagnostic Report</b>               | The <b>Download</b> link is for exporting a diagnostic report file required for system investigation.   |
| <b>Remote Assistance</b>               | Click <b>Turn on</b> 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           |          |
| <b>MAC Address</b> |   | 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 |
|--------------------------------|------------------|-------------------|
| <a href="#">AIM/ICQ</a>        | 0                | 1                 |
| <a href="#">Bittorrent</a>     | 0                | 32                |
| <a href="#">DNS</a>            | 0                | 51                |
| <a href="#">Flash</a>          | 0                | 1                 |
| <a href="#">HTTPS</a>          | 0                | 76                |
| <a href="#">Jabber</a>         | 0                | 5                 |
| <a href="#">MSN</a>            | 0                | 11                |
| <a href="#">NTP</a>            | 0                | 4                 |
| <a href="#">QQ</a>             | 0                | 1                 |
| <a href="#">Remote Desktop</a> | 0                | 3                 |
| <a href="#">SSH</a>            | 0                | 12                |
| <a href="#">SSL</a>            | 0                | 64                |
| <a href="#">XMPP</a>           | 0                | 4                 |
| <a href="#">Yahoo</a>          | 0                | 1                 |

| Interface                  | Inbound Sessions | Outbound Sessions |
|----------------------------|------------------|-------------------|
| <a href="#">WAN 1</a>      | 0                | 176               |
| <a href="#">WAN 2</a>      | 0                | 32                |
| <a href="#">Wi-Fi WAN</a>  | 0                | 51                |
| <a href="#">Cellular 1</a> | 0                | 64                |
| <a href="#">Cellular 2</a> | 0                | 0                 |
| <a href="#">USB</a>        | 0                | 0                 |

**Top Clients**

| Client IP Address | Total Sessions |
|-------------------|----------------|
| 10.9.66.66        | 1069           |
| 10.9.98.144       | 147            |
| 10.9.2.18         | 63             |
| 10.9.66.14        | 56             |
| 10.9.2.26         | 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 ▾  | / 255.255.255.255 (/32) ▾ |
| Port               | Source or Destination ▾  |                           |
| Protocol / Service | TCP ▾  |                           |
| Interface          | <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> Wi-Fi WAN<br><input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB<br><input type="checkbox"/> VPN |                           |
| Search             |  |                           |

**Outbound**

| Protocol    | Source IP | Destination IP | Service | Interface | Idle Time |
|-------------|-----------|----------------|---------|-----------|-----------|
| No sessions |           |                |         |           |           |

Total searched results: 0

**Inbound**

| Protocol    | Source IP | Destination IP | Service | Interface | Idle Time |
|-------------|-----------|----------------|---------|-----------|-----------|
| No sessions |           |                |         |           |           |

Total searched results: 0

**Transit**


| Protocol    | Source IP | Destination IP | Service | Interface | Idle 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  |   | <input type="checkbox"/> Online Clients Only<br><input type="checkbox"/> DHCP Clients Only |                 |               |   |  |   |  |
|---|---|--|-----------------|---------------|---|--|---|--|
| Client List   |   |  |                 |               |   |  |   |  |
| IP Address ▲  | Type  | Name   | Download (kbps) | Upload (kbps) | MAC Address   | Network Name (SSID)  | Signal (dBm)  |  |
|  192.168.50.10 |  | LAPTOP-   | 32              | 85            |  | PEPWAVE_  |  -57 | <br> |
|  192.168.50.12 |  | max-hd2-  | 0               | 3             |  |  |   | <br> |

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.


In the client list table, there is a “Ban Client” feature which is used to disconnect the Wi-Fi and Remote User Access clients by clicking the  button on the right.

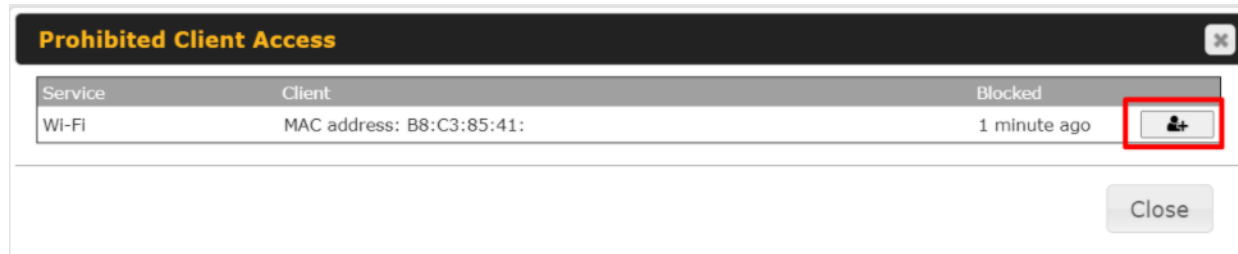
| Filter  |   | <input type="checkbox"/> Online Clients Only<br><input type="checkbox"/> DHCP Clients Only   |                 |               |   |  |   |  |
|---|---|--|-----------------|---------------|---|--|---|--|
| Client List   |   |  |                 |               |   |  |   |  |
| IP Address ▲  | Type  | Name   | Download (kbps) | Upload (kbps) | MAC Address   | Network Name (SSID)  | Signal (dBm)  |  |
|  192.168.50.10 |  | LAPTOP-   | 279             | 14            |  | PEPWAVE_  |  -52 | <br> |
|  192.168.50.12 |  | max-hd2-  | 0               | 0             |  |  |   | <br> |

Scale: ☒ kbps ☐ Mbps

There is a blocklist on the same page after you banned the Wi-Fi or Remote User Access clients.

| Filter   |      | <input type="checkbox"/> Online Clients Only<br><input type="checkbox"/> DHCP Clients Only |               |             |                     |              |  |  |
|--|------|--|---------------|-------------|---------------------|--------------|--|--|
| Access restriction in action, some clients are currently banned. |      |  |               |             |                     |              |  |  |
| Client List  |      |  |               |             |                     |              |  |  |
| IP Address ▲   | Name | Download (kbps)  | Upload (kbps) | MAC Address | Network Name (SSID) | Signal (dBm) |  |  |

You may also unblock the Wi-Fi or Remote User Access clients when the client devices need to reconnect the network by clicking  the button on the right.



## 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            | 10.9.30.1  |
| 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            | 10.9.30.1  |
| 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           | 11265    | 192.168.1.50     | NAT-PMP | TCP      | NAT-PMP 58      |  |
| 4500            | 3560     | 192.168.1.20     | UPnP    | TCP      | Application 013 |  |
| 5921            | 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 |  |
|                 |          |                  |         |          |                 | <button>Delete All</button>   |


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



Dashboard

Setup Wizard

Network

AP

System

Status

Apply Changes

Status

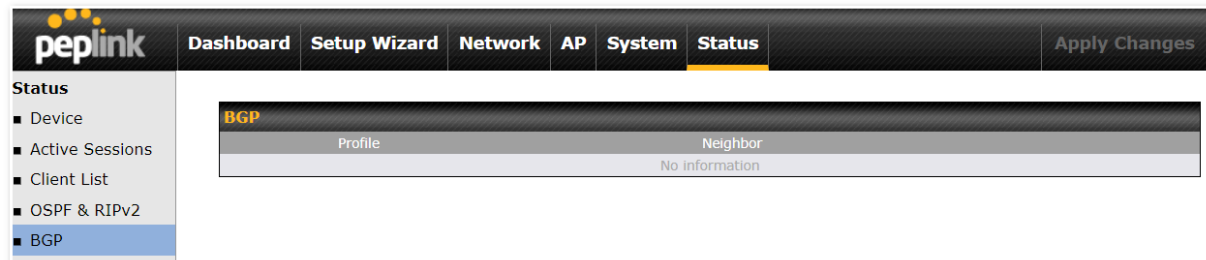
- Device
- Active Sessions
- Client List
- OSPF & RIPv2
- BGP

OSPF & RIPv2

| Area                                 | Remote Networks   |
|--------------------------------------|---|
| <div>0.0.0.0</div> <div>PepVPN</div> | 10.0.2.0/24 10.0.3.0/24 192.168.63.0/24 10.0.100.0/24 192.168.100.0/24 192.168.162.0/24 |

## 30.8 BGP

Shows status of BGP



The screenshot shows the Peplink web interface. The top navigation bar includes 'Dashboard', 'Setup Wizard', 'Network', 'AP', 'System', and 'Status' (which is highlighted). A sidebar on the left lists 'Status' with sub-items: 'Device', 'Active Sessions', 'Client List', 'OSPF & RIPv2', and 'BGP' (which is selected). The main content area is titled 'BGP' and shows a table with columns 'Profile' and 'Neighbor'. The table contains one row with the text 'No information'.

## 30.9 SpeedFusion Status

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

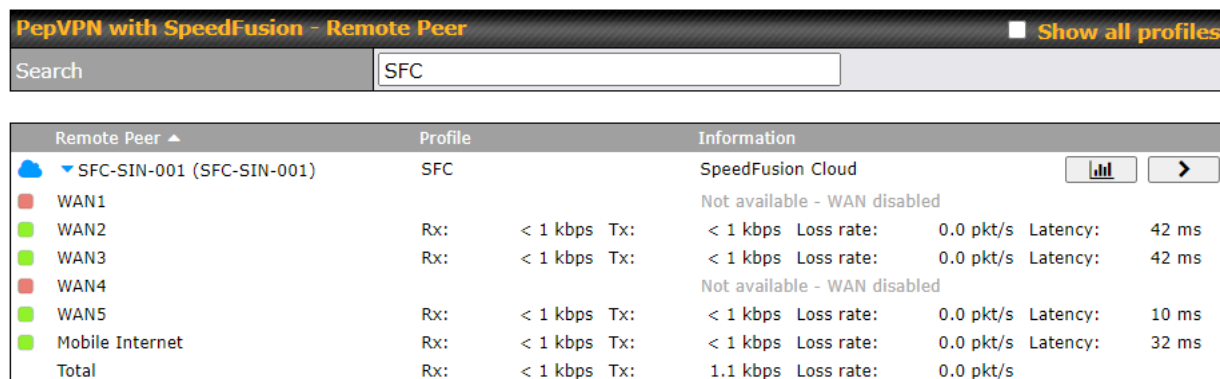
Details about SpeedFusion™ connection peers appears as below:



The screenshot shows the 'PepVPN with SpeedFusion - Remote Peer Details' page. It has a search bar and a 'Show disconnected profiles' checkbox. Below is a table with columns 'Remote Peer', 'Profile', and 'Information'.


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

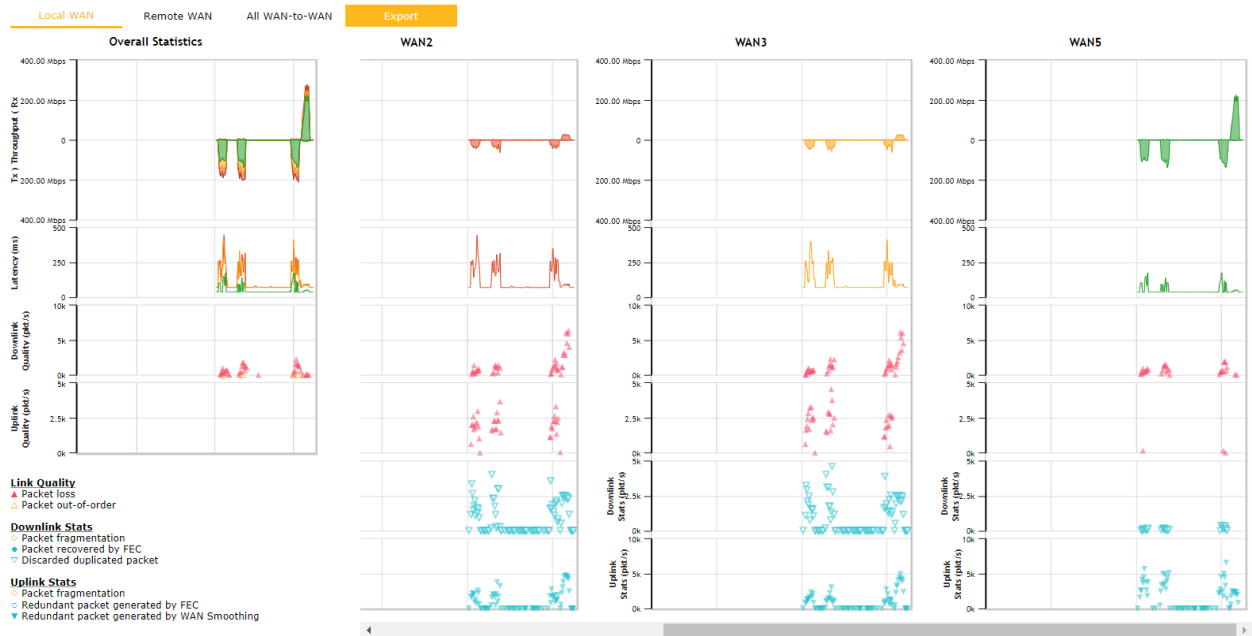
Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.




The screenshot shows the 'PepVPN with SpeedFusion - Remote Peer' page. It has a search bar with 'SFC' entered and a 'Show all profiles' checkbox. Below is a table with columns 'Remote Peer', 'Profile', and 'Information'.

| Remote Peer               | Profile                   | Information                         |
|---------------------------|---------------------------|-------------------------------------|
| SFC-SIN-001 (SFC-SIN-001) | SFC                       | SpeedFusion Cloud                   |
| WAN1                      |                           | Not available - WAN disabled        |
| WAN2                      | Rx: < 1 kbps Tx: < 1 kbps | Loss rate: 0.0 pkt/s Latency: 42 ms |
| WAN3                      | Rx: < 1 kbps Tx: < 1 kbps | Loss rate: 0.0 pkt/s Latency: 42 ms |
| WAN4                      |                           | Not available - WAN disabled        |
| WAN5                      | Rx: < 1 kbps Tx: < 1 kbps | Loss rate: 0.0 pkt/s Latency: 10 ms |
| Mobile Internet           | Rx: < 1 kbps Tx: < 1 kbps | Loss rate: 0.0 pkt/s Latency: 32 ms |
| Total                     | Rx: < 1 kbps Tx: 1.1 kbps | Loss rate: 0.0 pkt/s                |

Click the  button for a SpeedFusion 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 |                | More information |  |
|------------------------|----------------|------------------|--|
| Profile                | SFC            |                  |  |
| Remote ID              | SFC-SIN-001    |                  |  |
| Device Name            | SFC-SIN-001    |                  |  |
| Serial Number          | 1197-A047-2E3D |                  |  |

**WAN Statistics**


|   |   |          |     |          |                                     |
|---|---|----------|-----|----------|-------------------------------------|
| Remote Connections  | <input type="checkbox"/> Show remote connections                                    |          |     |          |                                     |
| WAN Label   | <input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port |          |     |          |                                     |
|  WAN1            | Not available - WAN disabled  |          |     |          |                                     |
|  WAN2            | Rx:   | < 1 kbps | Tx: | < 1 kbps | Loss rate: 0.0 pkt/s Latency: 43 ms |
|  WAN3            | Rx:   | < 1 kbps | Tx: | < 1 kbps | Loss rate: 0.0 pkt/s Latency: 44 ms |
|  WAN4            | Not available - WAN disabled  |          |     |          |                                     |
|  WAN5            | Rx:   | < 1 kbps | Tx: | < 1 kbps | Loss rate: 0.0 pkt/s Latency: 10 ms |
|  Mobile Internet | Rx:   | < 1 kbps | Tx: | < 1 kbps | Loss rate: 0.0 pkt/s Latency: 42 ms |
| Total   | Rx:   | < 1 kbps | Tx: | < 1 kbps | Loss rate: 0.0 pkt/s                |

**PepVPN Test Configuration**


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

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

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

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

## 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 14:28:29 | 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 11:47:28 | 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: 6000, max. streams: 8)          |
| Mar 19 14:05:30 | WAN: WAN 2 connected (10.22.1.165)   |
| 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 13:56:31 | WAN: WAN 2 connected (10.22.1.165)   |

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.

Data transferred since installation (Sun Oct 10 05:56:02 PST 2010)

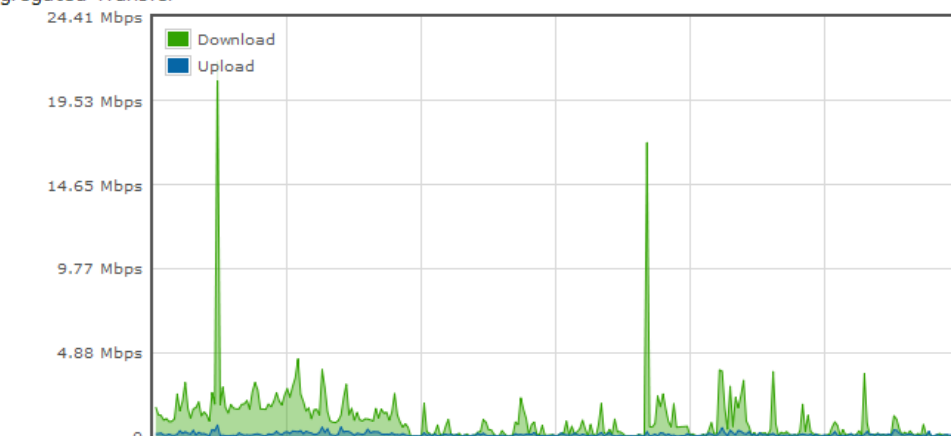
|                     | Download  | Upload   | Total     |
|---------------------|-----------|----------|-----------|
| All WAN Connections | 216.68 GB | 91.70 GB | 308.38 GB |

Data transferred since last reboot

[\[ Hide Details \]](#)

|                     | Download | Upload  | Total   |
|---------------------|----------|---------|---------|
| All WAN Connections | 0.74 GB  | 0.63 GB | 1.37 GB |
| WAN1                | 0.67 GB  | 0.61 GB | 1.28 GB |
| WAN2                | 0.07 GB  | 0.02 GB | 0.09 GB |

Aggregated Transfer



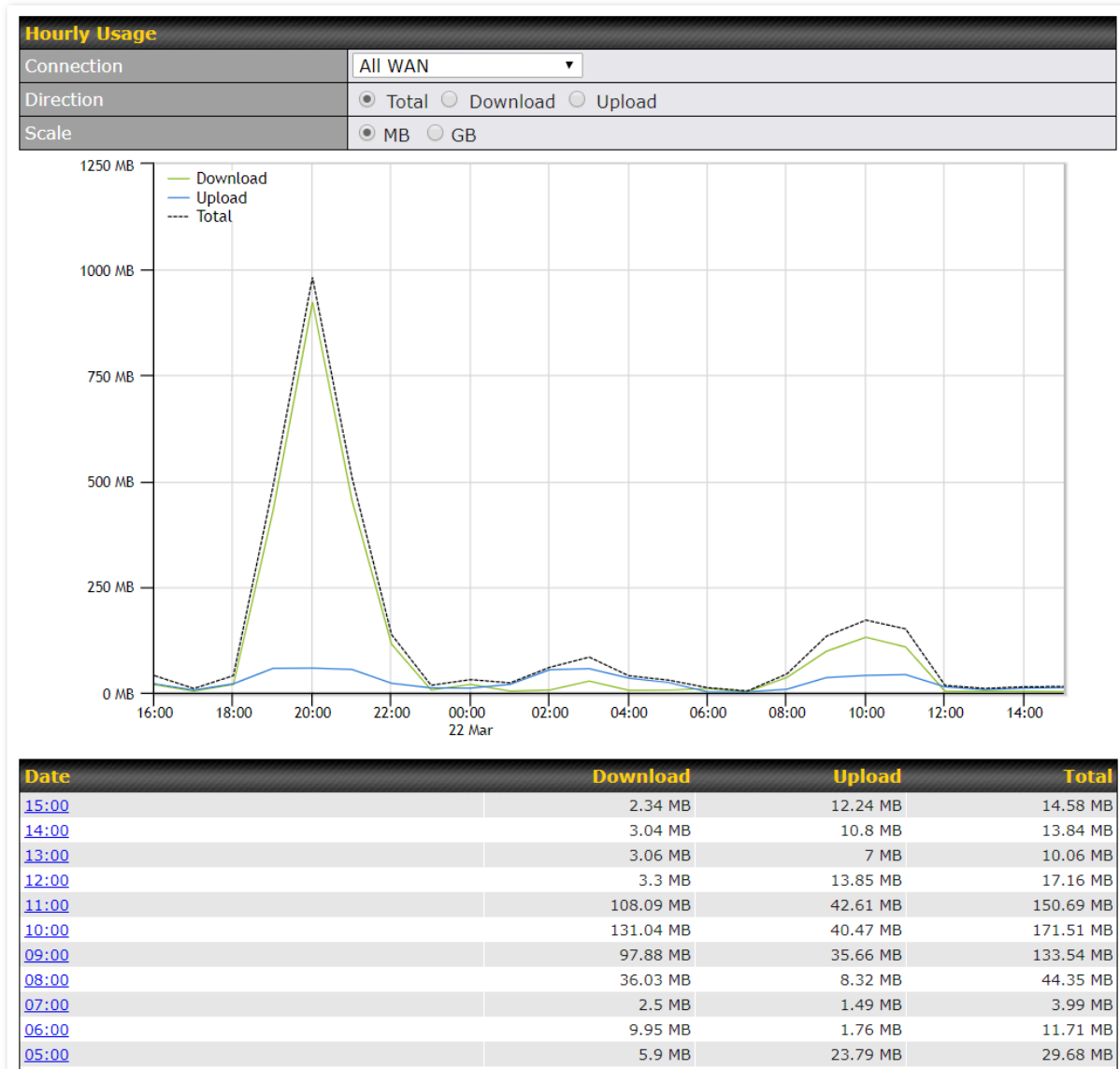
Avg: ↓ 0.99 Mbps ↑ 0.12 Mbps      Peak: ↓ 21.78 Mbps ↑ 0.67 Mbps

Stacked ☐

|         | Download | Upload  | Total    |
|---------|----------|---------|----------|
| Overall | 61 kbps  | 75 kbps | 136 kbps |

## 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.





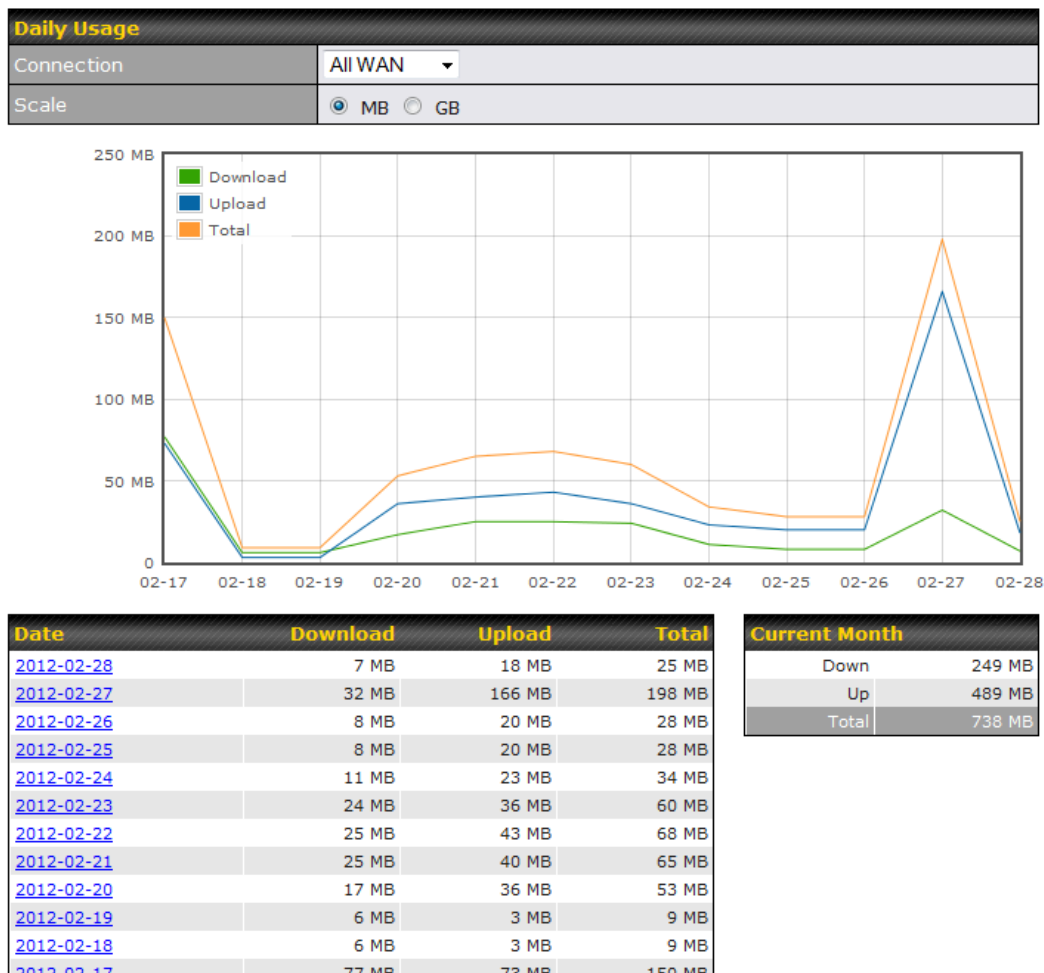
## 32.3 Daily

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**).

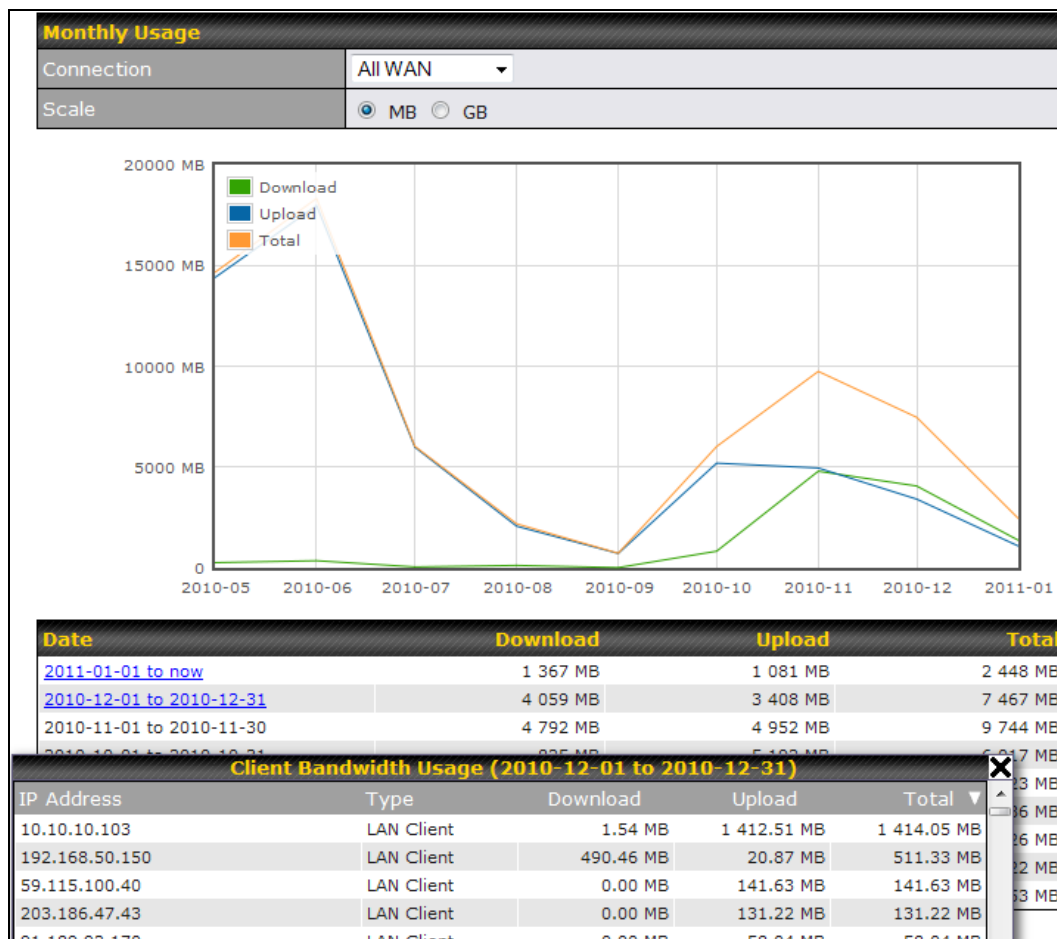


All WAN Daily Bandwidth Usage

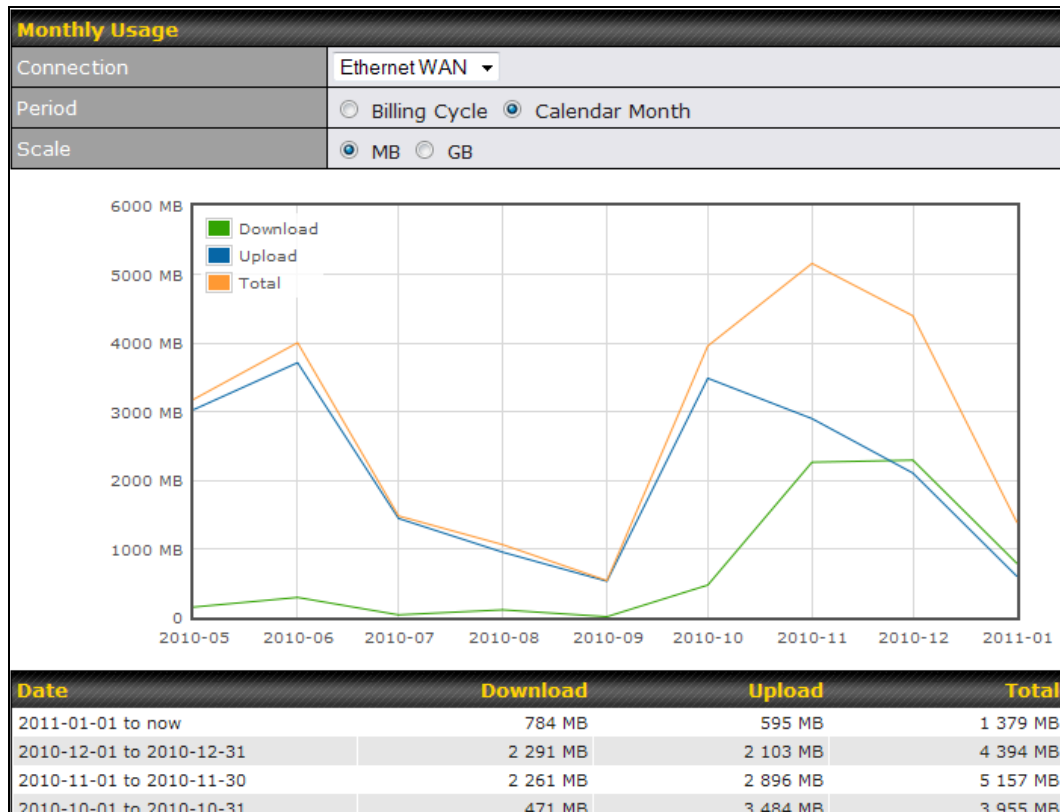
## 32.4 Monthly

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 and keep the reset button pressed.

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

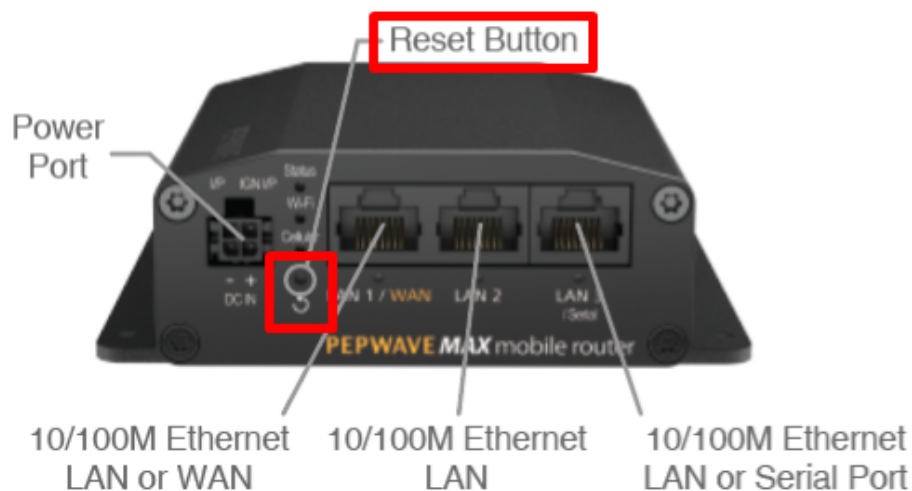
Hold for 5-10 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

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

After the Pepwave 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.



## Appendix B: FusionSIM Manual

Peplink has developed a unique technology called FusionSIM, which allows SIM cards to remotely link to a cellular router. This can be done via cloud or within the same physical network. There are a few key scenarios to fit certain applications.

The purpose of this manual is to provide an introduction on where to start and how to set up for the most common scenarios and uses.

### Requirements

1. A Cellular router that supports FusionSIM technology
2. SIM Injector
3. SIM card

Notes:

- Always check for the latest [Firmware version](#) for both the cellular router and the SIM Injector. You can also check for the latest Firmware version on the device's WEB configuration page.
- A list of products that support FusionSIM can be found on the SIM Injector [WEB page](#). Please check under the section **Supported models**.

### SIM Injector reset and login details

How to reset a SIM Injector:

- Hold the reset button for 5-10 seconds. Once the LED status light turns RED, the reset button can be released. SIM Injector will reboot and start with the factory default settings.

The default WEB login settings:

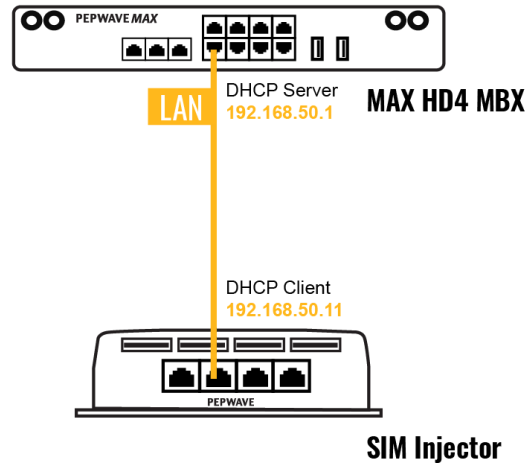
- **User:** admin
- **Password:** admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

Notes:

- The SIM Injector can be monitored via InControl 2. Configuration is not supported.

### Scenario 1: SIM Injector in LAN of Cellular Router

## Setup topology



This is the most basic scenario in which the SIM Injector is connected directly to the cellular router's LAN port via an ethernet cable. This allows for the cellular router to be positioned for the best possible signal. Meanwhile, the SIM cards can be conveniently located in other locations such as the office, passenger area, or the bridge of a ship. The SIM Injector allows for easily swapping SIM cards without needing to access a cellular router.

**IMPORTANT:** Cellular WAN will not fallback to the local SIM if it is configured to use the SIM Injector.

## Configuring the SIM Injector

1. Connect the SIM Injector to the LAN port of the cellular router.
2. Insert SIM cards into the SIM Injector. The SIM cards will be automatically detected.

**IMPORTANT:** SIM cards inserted into SIM Injector must not have a PIN code.

**Note 1:** The SIM Injector gets its IP address via DHCP and doesn't have a static IP address. To find it's address, please check the DHCP lease on the cellular router.

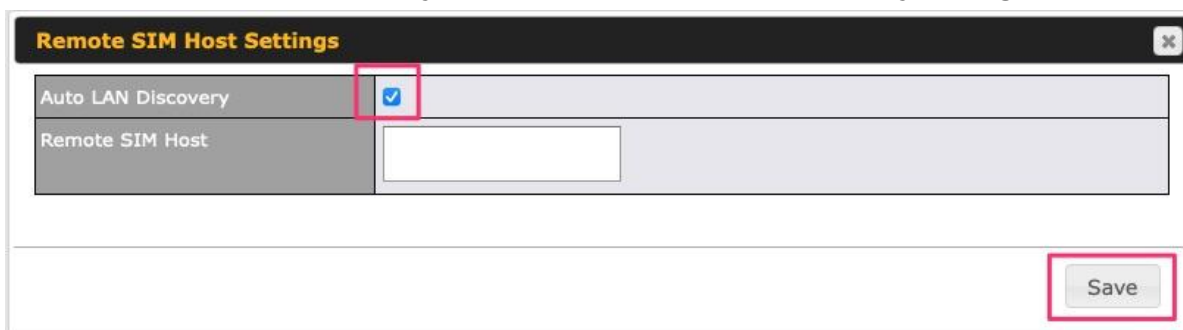
## Configuring the Cellular Router

**Step 1.** Enable the SIM Injector communication protocol.

- 1a. If you are using a Balance cellular router, go to the **Network** tab (top navigation bar).
- 1b. If you are using a MAX cellular router, go to the **Advanced** tab (top navigation bar).
2. Under **Misc. settings** (left navigation bar) find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.



4. Check the **Auto LAN discovery** checkbox and click **Save** and **Apply Changes**.



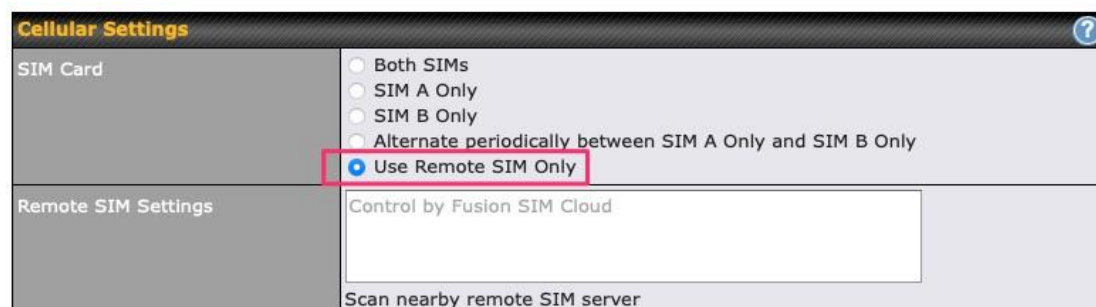
5. Click **Save** and then **Apply Changes**.

## Step 2. Enable RemoteSIM for the selected Cellular interface.

1. Go to **Network** (top navigation bar), then **WAN** (left navigation bar) and click **Details** for a selected cellular WAN. This will open the WAN Connection Settings page.



2. Scroll down to **Cellular settings**.
3. In the **SIM Card** section, select **Use Remote SIM Only**.



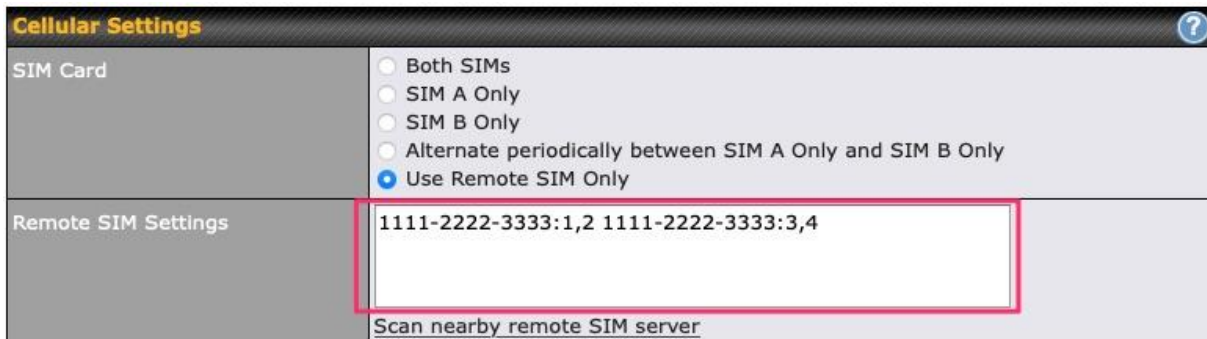
4. Enter configuration settings in **Remote SIM Settings** section. Click on **Scan nearby remote SIM server** to show the serial number(s) of the connected SIM Injector(s). Available configuration options for cellular interface are shown below:

A. Defining SIM Injector(s)

- Format: <S/N>
- Example 1: 1111-2222-3333
- Example 2: 1111-2222-3333 4444-5555-6666

B. Defining SIM Injector(s) SIM slot(s):

- Format: <S/N:slot number>
- Example 1: 1111-2222-3333:7,5 (the Cellular Interface will use SIM in slot 7, then 5)
- Example 2: 1111-2222-3333:1,2 1111-2222-3333:3,4 (the cellular Interface will use SIM in slot 1, then in 2 from the first SIM Injector, and then it will use 3 and 4 from the second SIM Injector).



Note: It is recommended to use different SIM slots for each cellular interface.

5. Click **Save** and **Apply Changes**.

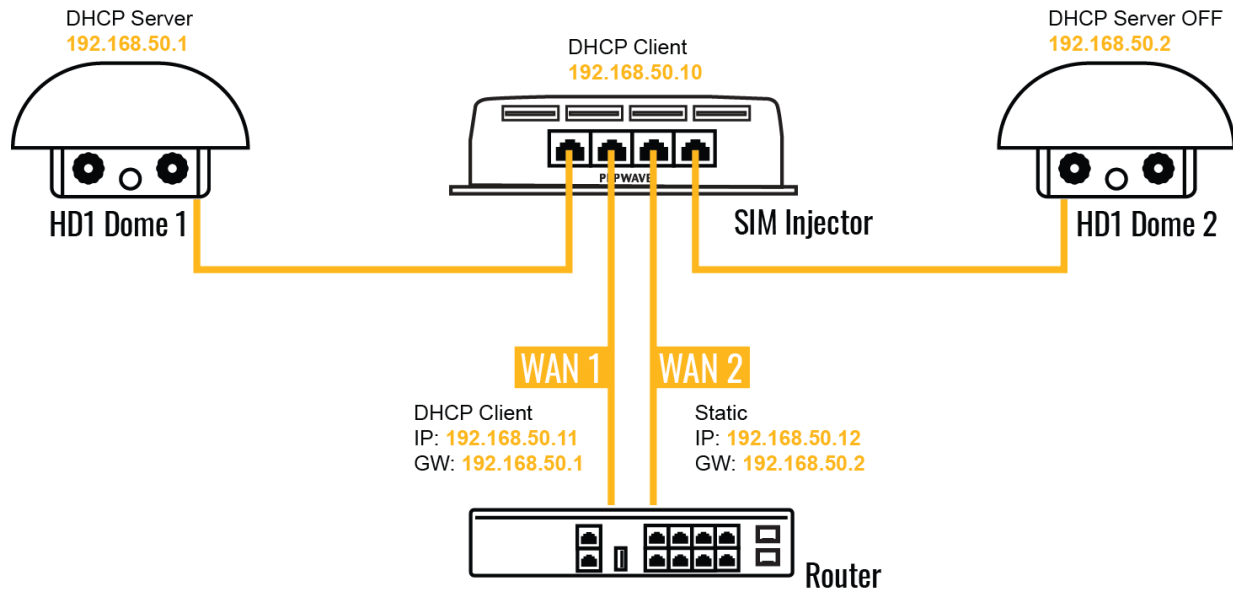
**Step 3.** (Optional) Custom SIM cards settings.

- 1a. For a Balance router, go to the **Network** (Top tab).
- 1b. For a MAX router, go to the **Advanced** (Top tab).
2. Under **Misc. settings** (Left-side tab) find **Remote SIM Management**.
3. Click on the **Add Remote SIM** button, fill in all the required info and click **Save**. This section allows defining custom requirements for a SIM card located in a certain SIM slot:
  - Enable/Disable roaming (by default roaming is disabled).
  - Add Custom mobile operator settings (APN, user name, password).
4. Repeat configuration for all SIM cards which need custom settings.
5. Click **Apply Changes** to take effect.

## Scenario 2: SIM Injector in WAN of main Router and multiple Cellular Routers



## Setup topology



In this scenario, each HD Dome creates a WAN connection to the main router. A single SIM Injector is used to provide SIM cards for each HD Dome. The HD Dome can be replaced with any Peplink cellular router supporting RemoteSIM technology.

**This scenario requires the completion of the configuration steps shown in Scenario 1 in addition to the configuration steps explained below.**

## Additional configurations for Cellular Routers

### Step 1. Disable the DHCP server.

- HD Dome 1 should act as a DHCP server.
- HD Dome 2 should be configured to have a static IP address with DHCP disabled.
- Both routers should be in the same subnet (e.g. 192.168.50.1 and 192.168.50.2).

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **Untagged LAN**. This will open up the LAN settings page.
2. Change the IP address to 192.168.50.2.
3. In the **DHCP Server** section, uncheck the checkbox to disable DHCP Server.
4. Click **Save** and **Apply Changes**.

## Step 2. Ethernet port configuration

The Ethernet port must be set to **ACCESS** mode for each HD Dome. To do this, dummy VLANs need to be created first.

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **New LAN**. This will open the settings page to create a dummy VLAN.
2. The image below shows the values that need to be changed to create a new VLAN:

**LAN**

**IP Settings**

IP Address: 192.168.10.1 255.255.255.0 (/24)

**Network Settings**

Name: VLAN10

VLAN ID: 10

Inter-VLAN routing: ☒

Captive Portal: ☐

**DHCP Server**

DHCP Server: ☒ Enable

DHCP Server Logging: ☐

IP Range: - 255.255.255.0 (/24)

**Note:** set different IP addresses for each HD dome (e.g. 192.168.10.1 and 192.168.10.2).

3. Click Save and **Apply Changes**.
4. Go to **Network** (Top tab), then **Port Settings** (Left-side tab).
5. Set the Port Type to **Access** and set VLAN to **Untagged LAN** (see picture below).

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

**LAN**

- Network Settings
- Port Settings**
- Captive Portal

**WAN**

Logout

**Port Settings**

|   | Name     | Enable                              | Speed | Advertise Speed                     | Port Type | VLAN         |
|---|----------|-------------------------------------|-------|-------------------------------------|-----------|--------------|
| 1 | LAN Port | <input checked="" type="checkbox"/> | Auto  | <input checked="" type="checkbox"/> | Access    | Untagged LAN |

Save

6. Click **Save** and **Apply Changes**.

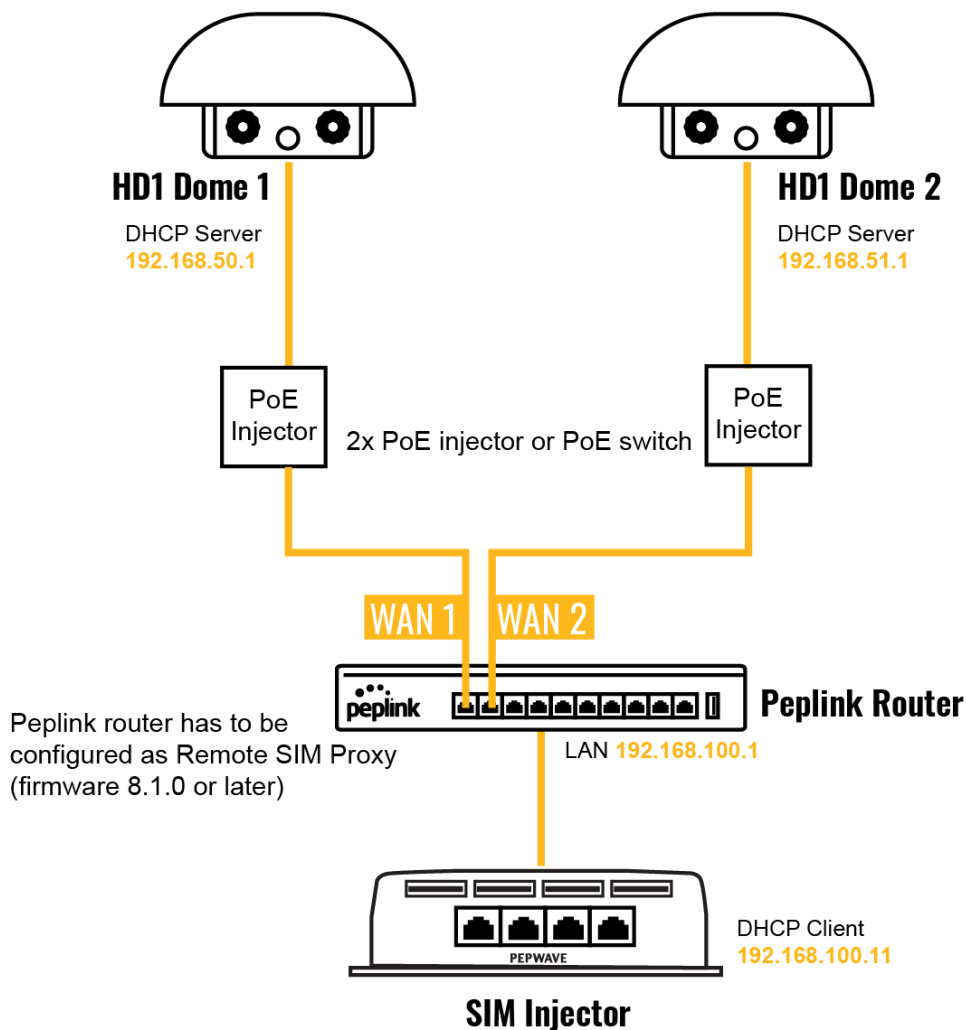
## Configuration requirements for the main Router

Requirements for the main router are:

- Configure **WAN 1** as a DHCP client.
- **WAN 1** will automatically get the Gateway IP address from HD Dome 1.
- Configure **WAN 2** as a Static IP and set it to 192.168.50.12.
- Configure **WAN 2** Gateway to 192.168.50.2. Same as the HD Dome 2's IP address.

## Scenario 3: SIM Injector in LAN of main Router and multiple Cellular Routers

### Setup topology



In this scenario, SIMs are provided to the HD Domes via the main router. In this example, the **Remote SIM Proxy** functionality needs to be enabled on the main router.

#### Notes:

- HD Dome can be replaced with any other cellular router that supports RemoteSIM.
- It is recommended to use Peplink [Balance series](#) or [X series](#) routers as the main router.

This scenario requires the completion of the configuration steps for the cellular router and the SIM Injector as in Scenario 1. The configuration for the main router is explained below.

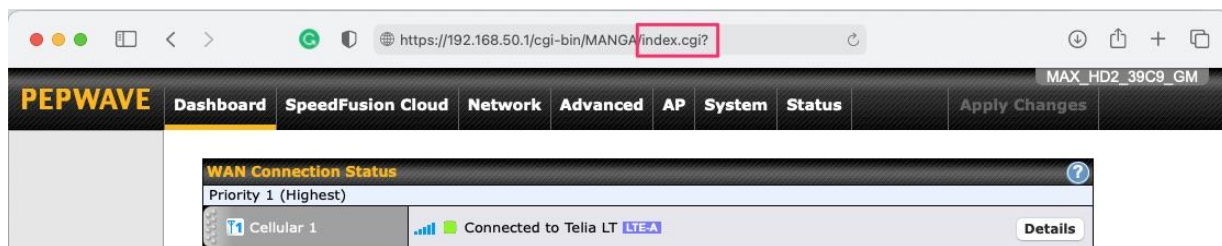
## Main Router configuration

**IMPORTANT:** Main router LAN side and Cellular Routers must be configured using different subnets, e.g. 192.168.**50**.1/24 and 192.168.**100**.1/24.

**Note:** please make sure the Peplink router is running Firmware 8.1.0 or above.

1. Open the main router WEB interface and change:  
From <IP address>/cgi-bin/MANGA/**index.cgi** to <IP address>/cgi-bin/MANGA/**support.cgi**.

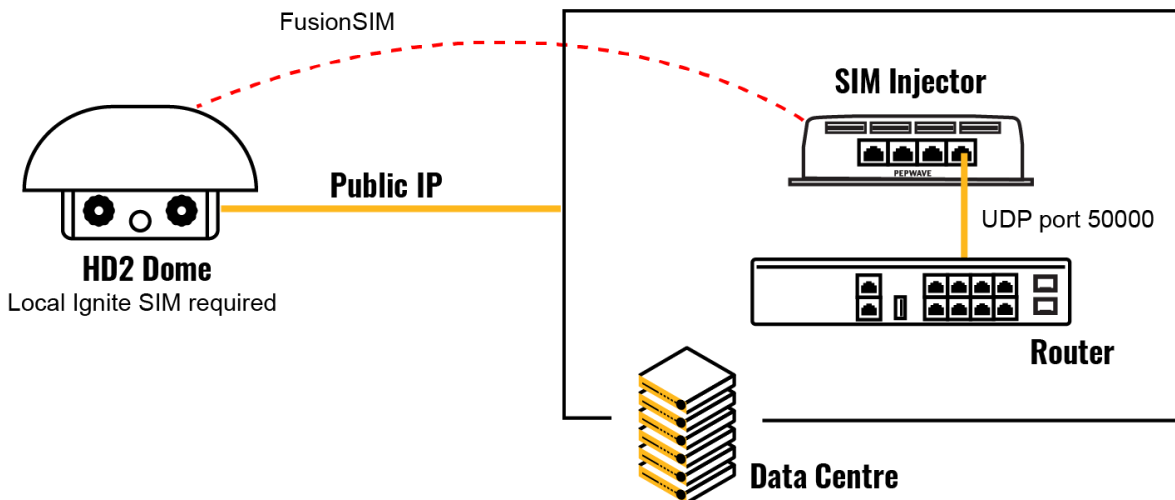
This will open the support.cgi page.



2. Scroll down to find **Remote SIM Proxy** and click on **[click to configure]** that is located next to it.
3. Check the **Enable** checkbox.
4. Click on **Save**.
5. Go back to the index.cgi page and click on **Apply Changes**.

## Scenario 4: SIM Injector in a remote location

### Setup topology



Requirements for installing a SIM Injector in a remote location:

- Cellular router communicates with the SIM Injector via UDP port 50000. Therefore this port must be reachable via public IP over the Internet.
- The one way latency between the cellular router and the SIM Injector should be **up to 250 ms**. A higher latency may lead to stability issues.
- The cellular router must have Internet connection to connect to the SIM Injector. It can be another Internet connection via Ethernet or Fiber if possible, or a secondary cellular interface with a local SIM (Ignite SIM).
- Due to its high latency, it is not recommended to use satellite WAN for connecting to a SIM Injector in remote locations.

**SIM Injector configuration is the same as in Scenario 1.**

### Cellular Router configuration

**Step 1.** Enable the SIM Injector communication protocol.

- 1a. For a Balance cellular router, go to the **Network** (Top tab).
- 1b. For a MAX cellular router, go to the **Advanced** (Top tab).

2. Under **Misc. settings** (Left-side tab), find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.
4. Enter the public IP of the SIM Injector and click **Save** and **Apply Changes**.

| Remote SIM Host Settings |                          |
|--------------------------|--------------------------|
| Auto LAN Discovery       | <input type="checkbox"/> |
| Remote SIM Host          | 84.199.92.62             |

**Notes:**

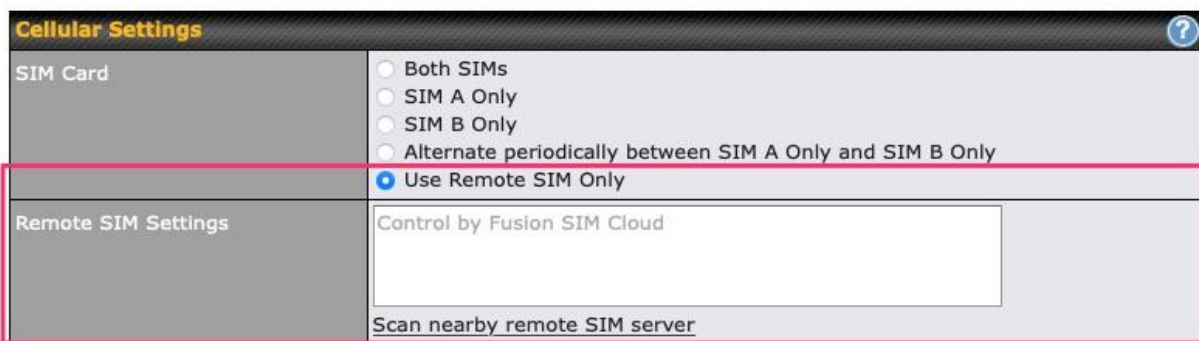
- **Do NOT check Auto LAN Discovery.**
- **Do NOT add a SIM Injector serial number to the Remote SIM Host field.**

**Step 2.** RemoteSIM and custom SIM card settings configurations are the same as in Scenario 1.

## How to check if a Pepwave Cellular Router supports Remote SIM

1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on any cellular WAN. This will open the WAN Connection Settings page.
2. Scroll down to **Cellular settings**.

If you can see the **Remote SIM Settings** section, then the cellular router supports Remote SIMs.

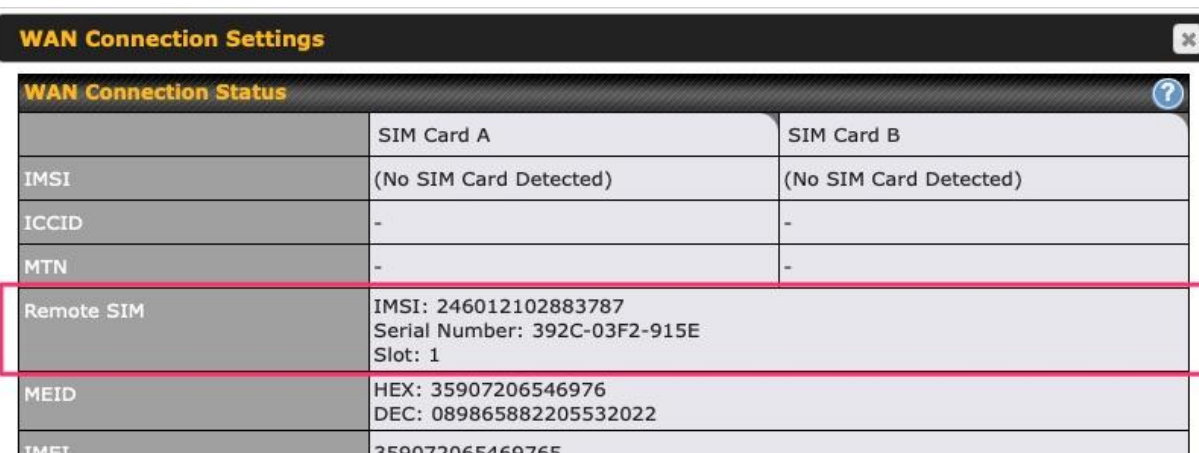


**Cellular Settings**

|                     |   |
|---------------------|---|
| SIM Card            | <input type="radio"/> Both SIMs<br><input type="radio"/> SIM A Only<br><input type="radio"/> SIM B Only<br><input type="radio"/> Alternate periodically between SIM A Only and SIM B Only<br><input checked="" type="radio"/> Use Remote SIM Only |
| Remote SIM Settings | Control by Fusion SIM Cloud<br><input type="text"/><br><a href="#">Scan nearby remote SIM server</a>  |

## Monitor the status of the Remote SIM

1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on the cellular WAN which was configured to use RemoteSIM.
2. Check the **WAN Connection Status** section. Within the cell WAN details, there is a section for **Remote SIM** (SIM card IMSI, SIM Injector serial number and SIM slot).



**WAN Connection Settings**

**WAN Connection Status**

|            | SIM Card A  | SIM Card B             |
|------------|---|------------------------|
| IMSI       | (No SIM Card Detected)  | (No SIM Card Detected) |
| ICCID      | -   | -                      |
| MTN        | -   | -                      |
| Remote SIM | IMSI: 246012102883787<br>Serial Number: 392C-03F2-915E<br>Slot: 1 |                        |
| MEID       | HEX: 35907206546976<br>DEC: 089865882205532022                    |                        |
| IMEI       | 359072065469765   |                        |



## Appendix C: Overview of ports used by Peplink SD-WAN routers and other Peplink services

| Default Port Number           | Usage   | Service                            | Inbound/Outbound    | Default Status |
|-------------------------------|---|------------------------------------|---------------------|----------------|
| UDP 5246                      | Data flow                                     | InControl                          | Outbound            | Enabled        |
| TCP 443                       | HTTPS service                                 | InControl                          | Outbound            | Enabled        |
| TCP 5246                      | Optional, used when TCP 443 is not responding | InControl                          | Outbound            | Enabled        |
| TCP 5246                      | Remote Web Admin                              | InControl Virtual Appliance        | Outbound            | Enabled        |
| TCP 4500                      | VPN Data (TCP Mode)                           | PepVPN / SpeedFusion               | Inbound / Outbound* | Disabled       |
| TCP 32015                     | VPN handshake                                 | PepVPN / SpeedFusion               | Inbound / Outbound* | Disabled       |
| UDP 4500                      | VPN Data                                      | PepVPN / SpeedFusion               | Inbound / Outbound* | Disabled       |
| UDP 32015 <sup>o</sup>        | VPN Data (alternative)                        | PepVPN / SpeedFusion               | Inbound / Outbound* | Disabled       |
| TCP/UDP 4500+N-1 <sup>^</sup> | VPN Sub-Tunnels Data                          | PepVPN / SpeedFusion               | Inbound / Outbound* | Disabled       |
| UDP 32015+N-1 <sup>^</sup>    | VPN Sub-Tunnels Data (alternative)            | PepVPN / SpeedFusion               | Inbound / Outbound* | Disabled       |
| UDP 4500                      | VPN Data                                      | IPsec                              | Inbound / Outbound* | Disabled       |
| UDP 500                       | VPN initiation                                | IPsec                              | Inbound / Outbound* | Disabled       |
| UDP 500                       | L2TP  | Remote User Access                 | Inbound             | Disabled       |
| UDP 1701                      | L2TP  | Remote User Access                 | Inbound             | Disabled       |
| UDP 4500                      | L2TP  | Remote User Access                 | Inbound             | Disabled       |
| UDP 1194                      | OpenVPN                                       | Remote User Access                 | Inbound             | Disabled       |
| IP 47                         | PPTP (GRE)                                    | Remote User Access                 | Inbound             | Disabled       |
| TCP 2222                      | Remote Assistance Direct connection           | Peplink Troubleshooting Assistance | Outbound            | Enabled        |
| TCP 80                        | HTTP traffic                                  | Web Admin                          | Inbound             | Enabled        |

|               |   |   |                     |                     |
|---------------|---|---|---------------------|---------------------|
|               |   | Interface access                          |                     |                     |
| TCP 443       | HTTPS traffic                             | Web Admin<br>Interface access<br>(secure) | Inbound             | Enabled             |
| TCP 8822      | SSH                                       | SSH                                       | Inbound             | Disabled            |
| UDP 161       | SNMP Get                                  | SNMP monitoring                           | Inbound             | Disabled            |
| UDP 162       | SNMP Trap                                 | SNMP monitoring                           | Outbound            | Disabled            |
| TCP, UDP 1812 | Radius Authentication                     | Radius                                    | Outbound            | Disabled            |
| TCP, UDP 1813 | Radius Accounting                         | Radius                                    | Outbound            | Disabled            |
| UDP 123       | Network Time Protocol                     | NTP                                       | Inbound<br>Outbound | Disabled<br>Enabled |
| TCP 60660     | Real-time location data in<br>NMEA format | GPS                                       | Outbound            | Disabled            |

#### Disclaimer:

- By default, only TCP 32015 and UDP 4500 are needed for PepVPN / SpeedFusion.
- Inbound / Outbound\* - Inbound = For Server mode; Outbound = For Client mode
- UDP 32015° - If IPsec VPN or L2TP/IPsec RUA is enabled, the UDP 4500 is occupied, so PepVPN / SpeedFusion will automatically switch to UDP 32015 as VPN data port .
- $UDP\ 32015+N-1^{\wedge}$  /  $TCP/UDP\ 4500+N-1^{\wedge}$  - When using Sub-Tunnels, multiple ports are in use (1 for each Sub-Tunnel profile).
- The default UDP data ports used when using (N number of Sub-Tunnel profiles) are:  
4500...4500+N-1, or (when port 4500 is in use by IPsec or L2TP/IPsec) 32015... 32015+N-1".

## Appendix D: Declaration

### FCC Requirements for Operation in the United States

#### Federal Communications Commission (FCC) Compliance Notice:

#### For MAX Transit Pro E / MAX Transit LTEA (FCC ID: U8G-P1835)

##### **FCC 15.21:**

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

##### **FCC 15.105**

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, it 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.

##### **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 provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

## ICES Statement

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

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

## RF exposure warning

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. 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 colocalisées ou opérant en conjonction avec une autre antenne ou transmetteur.

This radio transmitter IC: 20682-P1835 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.

|                     |                                |
|---------------------|--------------------------------|
| <b>Antenna Type</b> | WLAN: Omni-directional Antenna |
|---------------------|--------------------------------|

| <b>Antenna information</b>   |                 |                                  |
|------------------------------|-----------------|----------------------------------|
| <b>2400 MHz ~ 2483.5 MHz</b> | Peak Gain (dBi) | <Ant. 0>: 2.44<br><Ant. 1>: 2.44 |

|                     |                                |
|---------------------|--------------------------------|
| <b>Antenna Type</b> | WLAN: Omni-directional Antenna |
|---------------------|--------------------------------|

| <b>Antenna information</b> |                 |                                  |
|----------------------------|-----------------|----------------------------------|
| <b>5150 MHz ~ 5250 MHz</b> | Peak Gain (dBi) | <Ant. 0>: 4.10<br><Ant. 1>: 4.10 |
| <b>5250 MHz ~ 5350 MHz</b> | Peak Gain (dBi) | <Ant. 0>: 4.41<br><Ant. 1>: 4.41 |
| <b>5470 MHz ~ 5725 MHz</b> | Peak Gain (dBi) | <Ant. 0>: 4.41<br><Ant. 1>: 4.41 |

|                     |                                |
|---------------------|--------------------------------|
| <b>Antenna Type</b> | WLAN: Omni-directional Antenna |
|---------------------|--------------------------------|

| <b>Antenna information</b> |                 |                                  |
|----------------------------|-----------------|----------------------------------|
| <b>5725 MHz ~ 5850 MHz</b> | Peak Gain (dBi) | <Ant. 0>: 4.73<br><Ant. 1>: 4.73 |

Cet émetteur radio IC : 20682-P1835 a été approuvé par Innovation, Sciences et Développement économique Canada doit fonctionner avec les types d'antennes énumérés ci-dessous, avec le gain maximal admissible indiqué. Les types d'antenne non inclus dans cette liste qui ont un gain supérieur au gain maximum indiqué pour tout type répertorié sont strictement interdits pour une utilisation avec cet appareil.

|                            |                                   |                                  |
|----------------------------|-----------------------------------|----------------------------------|
| Type d'antenne             | WLAN: Omni-directionnelle Antenne |                                  |
| Informations sur l'antenne |                                   |                                  |
| 2400 MHz ~ 2483.5 MHz      | Gain de crête(dBi)                | <Ant. 0>: 2.44<br><Ant. 1>: 2.44 |

|                            |                                   |                                  |
|----------------------------|-----------------------------------|----------------------------------|
| Type d'antenne             | WLAN: Omni-directionnelle Antenne |                                  |
| Informations sur l'antenne |                                   |                                  |
| 5150 MHz ~ 5250 MHz        | Gain de crête(dBi)                | <Ant. 0>: 4.10<br><Ant. 1>: 4.10 |
| 5250 MHz ~ 5350 MHz        | Gain de crête(dBi)                | <Ant. 0>: 4.41<br><Ant. 1>: 4.41 |
| 5470 MHz ~ 5725 MHz        | Gain de crête(dBi)                | <Ant. 0>: 4.41<br><Ant. 1>: 4.41 |

|                            |                                   |                                  |
|----------------------------|-----------------------------------|----------------------------------|
| Type d'antenne             | WLAN: Omni-directionnelle Antenne |                                  |
| Informations sur l'antenne |                                   |                                  |
| 5725 MHz ~ 5850 MHz        | Gain de crête(dBi)                | <Ant. 0>: 4.73<br><Ant. 1>: 4.73 |

## **FCC Requirements for Operation in the United States**

### **Federal Communications Commission (FCC) Compliance Notice:**

#### **For MAX Transit Pro E (FCC ID: U8G-P1AX09)**

#### **Federal Communication Commission Interference Statement**

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

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, it 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

#### **Radiation Exposure Statement**

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

#### **Industry Canada Statement (MAX Transit Pro E, IC: 20682-P1AX09)**

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

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 ex-empts 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

(i) The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; (detachable antenna only) ; and

The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(iii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5725-5850 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

(iii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point.

### **Radiation Exposure Statement**

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

Cet appareil doit être installé et utilisé avec une distance minimale de 20cm entre l'émetteur et votre corps. Cet appareil et sa ou ses antennes ne doivent pas être co-localisés ou fonctionner en conjonction avec tout autre antenne ou transmetteur.



This radio transmitter IC: 20682-P1AX09 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.

WIFI Antenna type: Omni-directional  
 WIFI Antenna gain: 2.4GHz / 2.44 dBi  
 5150 ~ 5250 MHz / 4.10 dBi  
 5725 ~ 5850 MHz / 4.73 dBi

Cet émetteur radio IC : 20682-P1AX09 a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antennes répertoriés ci-dessous, avec le gain maximal autorisé indiqué. Les types d'antenne non inclus dans cette liste qui ont un gain supérieur au gain maximum indiqué pour tout type répertorié sont strictement interdits pour une utilisation avec cet appareil.

Type d'antenne WIFI : omnidirectionnelle  
 Gain de l'antenne Wi-Fi : 2.4 GHz / 2.44 dBi  
 5150 ~ 5250 MHz / 4.10 dBi  
 5725 ~ 5850 MHz / 4.73 dBi

## USB WAN Modem Port Specification

### MAX Series

|                      | MAX 700          | MAX HD2 /<br>MAX HD2<br>Media Fast | MAX HD2<br>Mini  | MAX HD2 /<br>HD4 MBX | MAX BR1<br>ENT<br>MAX BR1NT | MAX HD4 / MAX<br>HD4 Media Fast /<br>MediaFast 200 |
|----------------------|------------------|------------------------------------|------------------|----------------------|-----------------------------|--|
| <b>Output Rating</b> | <b>5V DC, 2A</b> | <b>5V DC, 2A</b>                   | <b>5V DC, 2A</b> | <b>5V DC, 0.5A</b>   | <b>5V DC, 2A</b>            | <b>5V DC, 2A</b>                                   |