

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

Phase 2 SA Lifetime This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.

| WAN Connection Priority | |
|-------------------------|---------------|
| Priority | WAN Selection |
| 1 | WAN 1 |
| 2 | ----- |

WAN Connection Priority

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

11.2 GRE Tunnel

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

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

| GRE Tunnel Profiles | Remote Networks |
|--|-----------------|
| No GRE profile defined | |
| <input type="button" value="New Profile"/> | |

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

GRE Tunnel Profile
✕

| Name | <input style="width: 90%;" type="text"/> | | | | | |
|--|---|---------|-------------|--|--|---|
| Active | <input checked="" type="checkbox"/> | | | | | |
| Remote GRE IP Address | <input style="width: 90%;" type="text"/> | | | | | |
| Tunnel Local IP Address | <input style="width: 90%;" type="text"/> | | | | | |
| Tunnel Remote IP Address | <input style="width: 90%;" type="text"/> | | | | | |
| Tunnel Subnet Mask | <input checked="" type="radio"/> Auto <input type="radio"/> <input style="width: 80%;" type="text" value="255.255.255.0 (/24)"/> | | | | | |
| Connection | WAN ▼ | | | | | |
| Remote Networks | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Network</th> <th style="width: 50%;">Subnet Mask</th> </tr> </thead> <tbody> <tr> <td><input style="width: 90%;" type="text"/></td> <td>255.255.255.0 (/24) ▼</td> </tr> </tbody> </table> | Network | Subnet Mask | <input style="width: 90%;" type="text"/> | 255.255.255.0 (/24) ▼ | + |
| Network | Subnet Mask | | | | | |
| <input style="width: 90%;" type="text"/> | 255.255.255.0 (/24) ▼ | | | | | |

Save
Cancel

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

12 OpenVPN

OpenVPN is a site to site VPN mode that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

To configure a OpenVPN, navigate to **Advanced > OpenVPN** and click the **New Profile**.

| OpenVPN Profile Settings | |
|------------------------------------|---|
| Name | This field is for specifying a name to represent this OpenVPN profile. |
| Active | When this box is checked, this OpenVPN connection profile will be enabled. Otherwise, it will be disabled. |
| OpenVPN Profile | Upload the OpenVPN configuration (.ovpn) file from your service provider. |
| Login Credential (Optional) | This option is an optional for you to enter the username and password to login for the OpenVPN connection if the profile need to login. |
| Connection | Select the appropriate WAN connection from the drop-down menu. |

13 Outbound Policy

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

Important Note

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

The settings for managing and load balancing outbound traffic are located at **Advanced > Outbound Policy**.

| Service | Algorithm | Source | Destination | Protocol / Port | |
|---|--------------------------|--------|-------------|-----------------|---|
| SpeedFusion VPN / OSPF / BGP / RIPv2 Routes | | | | | |
| ☰ HTTPS Persistence | Persistence (Src) (Auto) | Any | Any | TCP 443 | ✖ |
| Default | (Auto) | | | | |
| Add Rule | | | | | |

| Expert Mode |
|-------------|
| Enabled |

13.1 Adding Rules for Outbound Policy

The menu underneath enables you to define Outbound policy rules:

| Service | Algorithm | Source | Destination | Protocol / Port | |
|---|--------------------------|--------|-------------|-----------------|---|
| SpeedFusion VPN / OSPF / BGP / RIPv2 Routes | | | | | |
| ☰ HTTPS Persistence | Persistence (Src) (Auto) | Any | Any | TCP 443 | ✖ |
| Default | (Auto) | | | | |
| Add Rule | | | | | |

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

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

Edit Default Custom Rule
✕

| | |
|--|---|
| Default Rule ? | <input checked="" type="radio"/> Custom <input type="radio"/> Auto |
| Algorithm ? | Weighted Balance ▼ |
| Load Distribution Weight ? | <div style="margin-bottom: 5px;">WAN 1 10 ●</div> <div style="margin-bottom: 5px;">WAN 2 10 ●</div> <div style="margin-bottom: 5px;">WAN 3 10 ●</div> <div style="margin-bottom: 5px;">WAN 4 10 ●</div> <div style="margin-bottom: 5px;">WAN 5 10 ●</div> <div style="margin-bottom: 5px;">Mobile Internet 10 ●</div> |
| When No Connections are Available ? | <div style="border: 1px solid #ccc; padding: 2px;"> Drop the Traffic ▼ <div style="background-color: #fff; padding: 2px; margin-top: 2px;"> Drop the Traffic </div> <div style="background-color: #007bff; color: #fff; padding: 2px; margin-top: 2px;"> Use Any Available Connections </div> </div> |

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

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

Add a New Custom Rule
✕

| | | | | | | | | | | | | | | | | | | | |
|-----------------------------------|---|-----------------------|----|-----------------------|-------|----|-----------------------|-------|----|-----------------------|-------|----|-----------------------|-------|----|-----------------------|-----------------|----|-----------------------|
| Service Name | <input type="text"/> | | | | | | | | | | | | | | | | | | |
| Enable | <input checked="" type="checkbox"/> Always on ▾ | | | | | | | | | | | | | | | | | | |
| Source | Any ▾ | | | | | | | | | | | | | | | | | | |
| Destination | ? IP Network ▾ <input type="text"/> Mask: 255.255.255.0 (/24) ▾ | | | | | | | | | | | | | | | | | | |
| Protocol | ? Any ▾ ← :: Protocol Selection :: ▾ | | | | | | | | | | | | | | | | | | |
| Algorithm | ? Weighted Balance ▾ | | | | | | | | | | | | | | | | | | |
| Load Distribution Weight | ? <table style="width: 100%; border-collapse: collapse;"> <tr><td>WAN 1</td><td>10</td><td><input type="range"/></td></tr> <tr><td>WAN 2</td><td>10</td><td><input type="range"/></td></tr> <tr><td>WAN 3</td><td>10</td><td><input type="range"/></td></tr> <tr><td>WAN 4</td><td>10</td><td><input type="range"/></td></tr> <tr><td>WAN 5</td><td>10</td><td><input type="range"/></td></tr> <tr><td>Mobile Internet</td><td>10</td><td><input type="range"/></td></tr> </table> | WAN 1 | 10 | <input type="range"/> | WAN 2 | 10 | <input type="range"/> | WAN 3 | 10 | <input type="range"/> | WAN 4 | 10 | <input type="range"/> | WAN 5 | 10 | <input type="range"/> | Mobile Internet | 10 | <input type="range"/> |
| WAN 1 | 10 | <input type="range"/> | | | | | | | | | | | | | | | | | |
| WAN 2 | 10 | <input type="range"/> | | | | | | | | | | | | | | | | | |
| WAN 3 | 10 | <input type="range"/> | | | | | | | | | | | | | | | | | |
| WAN 4 | 10 | <input type="range"/> | | | | | | | | | | | | | | | | | |
| WAN 5 | 10 | <input type="range"/> | | | | | | | | | | | | | | | | | |
| Mobile Internet | 10 | <input type="range"/> | | | | | | | | | | | | | | | | | |
| When No Connections are Available | ? Drop the Traffic ▾ | | | | | | | | | | | | | | | | | | |

New Custom Rule Settings

| | | | | | | | | | | | | | | | |
|---------------------|--|--------|----------------------|-------------|--------------------|----------|---------------------------|-----------|---------------------------|--|-------------|--|-------------|--|--------------------------|
| Service Name | This setting specifies the name of the outbound traffic rule. | | | | | | | | | | | | | | |
| Enable | <p>This setting specifies whether the outbound traffic rule takes effect. When Enable is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When Enable is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule.</p> <p>Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.</p> | | | | | | | | | | | | | | |
| Source | <p>This setting specifies the source IP Address, IP Network, MAC Address or Grouped Network for traffic that matches the rule.</p> <div style="border: 1px solid gray; padding: 5px; width: fit-content;"> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Source</td><td>? Any ▾</td></tr> <tr><td>Destination</td><td>? Any</td></tr> <tr><td>Protocol</td><td>? IP Address</td></tr> <tr><td>Algorithm</td><td>? IP Network</td></tr> <tr><td></td><td>MAC Address</td></tr> <tr><td></td><td>Client Type</td></tr> <tr><td></td><td>Client's Associated SSID</td></tr> </table> </div> | Source | ? Any ▾ | Destination | ? Any | Protocol | ? IP Address | Algorithm | ? IP Network | | MAC Address | | Client Type | | Client's Associated SSID |
| Source | ? Any ▾ | | | | | | | | | | | | | | |
| Destination | ? Any | | | | | | | | | | | | | | |
| Protocol | ? IP Address | | | | | | | | | | | | | | |
| Algorithm | ? IP Network | | | | | | | | | | | | | | |
| | MAC Address | | | | | | | | | | | | | | |
| | Client Type | | | | | | | | | | | | | | |
| | Client's Associated SSID | | | | | | | | | | | | | | |
| Destination | This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, SpeedFusion VPN Profile or Grouped network for traffic that matches the rule. | | | | | | | | | | | | | | |

| | | |
|--------------------------|---|-----------------------------|
| Destination | ? | Any |
| Protocol | ? | Any |
| Algorithm | ? | IP Address |
| Load Distribution Weight | ? | IP Network |
| | | Domain Name |
| | | SpeedFusion Connect Protect |
| | | SpeedFusion VPN Profile |

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

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

Protocol and Port

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

- Any
- TCP
- UDP
- IP
- DSCP

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

Algorithm

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

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

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

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

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

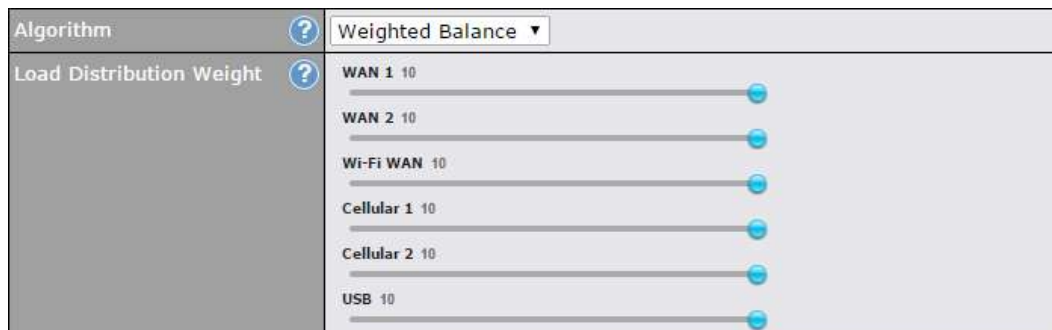
Load Distribution Weight

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

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

13.1.1 Algorithm: Weighted Balance

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



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

For example, with the following weight settings:

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

- USB: 10

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

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

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

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

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

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

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

13.1.2 Algorithm: Persistence

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

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

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

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

| | |
|--------------------------|---|
| Algorithm | Persistence |
| Persistence Mode | <input checked="" type="radio"/> By Source <input type="radio"/> By Destination |
| Load Distribution | <input type="radio"/> Auto <input checked="" type="radio"/> Custom |
| Load Distribution Weight | <p>WAN 1 10 </p> <p>WAN 2 10 </p> <p>Wi-Fi WAN 10 </p> <p>Cellular 1 10 </p> <p>Cellular 2 10 </p> <p>USB 10 </p> |

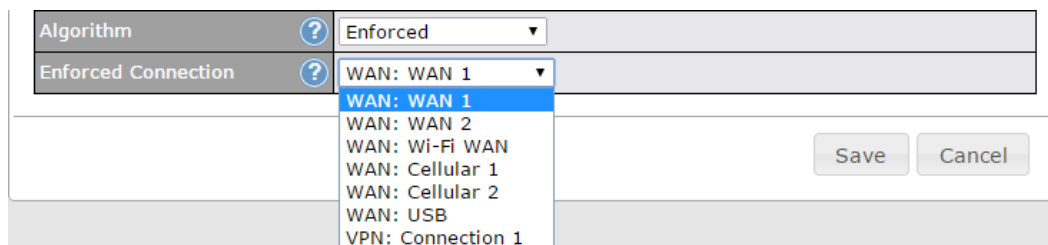
There are two persistent modes: **By Source** and **By Destination**.

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

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

13.1.3 Algorithm: Enforced

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



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

13.1.4 Algorithm: Priority

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

| | | |
|---|---------------------------------|------------|
| Algorithm | Priority | |
| Priority Order | Highest Priority | Not In Use |
| | WAN: WAN | |
| | WAN: Cellular 1 | |
| | WAN: Cellular 2 | |
| | WAN: USB | |
| | WAN: LAN 1 as WAN | |
| | WAN: GRE WAN 1 | |
| | WAN: GRE WAN 2 | |
| | WAN: OpenVPN WAN 1 | |
| | Lowest Priority | |
| When No Connections are Available | Drop the Traffic | |
| Terminate Sessions on Connection Recovery | <input type="checkbox"/> Enable | |

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

Tip

Configure multiple distribution rules to accommodate different kinds of services.

13.1.5 Algorithm: Overflow

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

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

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

13.1.6 Algorithm: Least Used

| | |
|------------|---|
| Algorithm | Least Used |
| Connection | <input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB |

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

13.1.7 Algorithm: Lowest Latency

| | |
|------------|---|
| Algorithm | Lowest Latency <small>Note: Use of Lowest Latency will incur additional network usage.</small> |
| Connection | <input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB |

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

Tip

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

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

13.1.8 Expert Mode

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

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

above the bar to override the SpeedFusion™ routes.

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

| Help | Close |
|---|-------|
| <p>This table allows you to fine tune how the outbound traffic should be distributed to the WAN connections.</p> | |
| <p>Click the <i>Add Rule</i> button to add a new rule. Click the <i>X</i> button to remove a rule. Drag a rule to promote or demote its precedence. A higher position of a rule signifies a higher precedence. You may change the default outbound policy behavior by clicking the <i>Default</i> link.</p> | |
| <p>If you require advanced control of PepVPN traffic, turn on Expert Mode.</p> | |

14 Port Forwarding

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

| Service | IP Address(es) | Server | Protocol |
|--|----------------|--------|----------|
| No Services Defined | | | |
| <input type="button" value="Add Service"/> | | | |

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

Port Forwarding
✕

| | |
|---|--|
| Enable | <input checked="" type="checkbox"/> |
| Service Name | <input type="text"/> |
| Protocol | TCP ▾ ← :: Protocol Selection :: ▾ |
| Port | Any Port ▾ |
| Inbound IP Address(es) (Require at least one IP address) ? | <div style="display: flex; justify-content: space-between; align-items: center;"> Connection / IP Address(es) All Clear </div> |
| | <input type="checkbox"/> WAN |
| | <input type="checkbox"/> Cellular |
| | <input type="checkbox"/> Wi-Fi WAN on 2.4 GHz |
| | <input type="checkbox"/> Wi-Fi WAN on 5 GHz |
| <input type="checkbox"/> SpeedFusion VPN | |
| Server IP Address ? | <input type="text"/> |

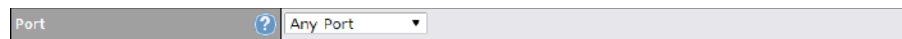
| Port Forwarding Settings | |
|--------------------------|--|
| Enable | This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule.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

Protocol

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

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

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

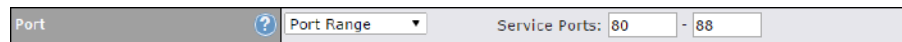


Any Port: all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.



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

Port



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



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

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

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

| | | | |
|--|--|--|---|
| | <input type="text" value="Port"/> | <input type="text" value="Range Mapping"/> | Service Ports: <input type="text" value="80"/> - <input type="text" value="88"/> Map to Ports: <input type="text" value="88"/> - <input type="text" value="96"/> |
| <p>Range Mapping: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the Servers setting.</p> | | | |
| Inbound IP Address(es) | This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed. | | |
| Server IP Address | This setting specifies the LAN IP address of the server that handles the requests for the service. | | |

14.1 UPnP / NAT-PMP Settings

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

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

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

UPnP / NAT-PMP Settings ?

| | |
|---------|---------------------------------|
| UPnP | <input type="checkbox"/> Enable |
| NAT-PMP | <input type="checkbox"/> Enable |

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

15 NAT Mappings

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

| LAN Clients | Inbound Mappings | Outbound Mappings | |
|------------------------------|------------------------------------|------------------------------|--|
| 192.168.1.23 | (WAN 1):10.88.3.158 (Interface IP) | Use <i>Interface IP</i> only | |
| Add NAT Rule | | | |

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

NAT Mappings ✕

| | | | | | | | | | | | |
|----------------------|---------------------------------|---|--|-----|---------------------------------|----------|----------------|----------------------|----------------|--------------------|----------------|
| LAN Client | ? | IP Address ▾ | | | | | | | | | |
| IP Address | | <input type="text"/> | | | | | | | | | |
| Inbound Mappings | ? | Connection / Inbound IP Address(es) <ul style="list-style-type: none"> <input type="checkbox"/> WAN <input type="checkbox"/> Cellular <input type="checkbox"/> Wi-Fi WAN on 2.4 GHz <input type="checkbox"/> Wi-Fi WAN on 5 GHz <input type="checkbox"/> SpeedFusion VPN | | | | | | | | | |
| Outbound Mappings | ? | Connection / Outbound IP Address <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>WAN</td> <td>192.168.52.152 (Interface IP) ▾</td> </tr> <tr> <td>Cellular</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN on 2.4 GHz</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN on 5 GHz</td> <td>Interface IP ▾</td> </tr> </table> | | WAN | 192.168.52.152 (Interface IP) ▾ | Cellular | Interface IP ▾ | Wi-Fi WAN on 2.4 GHz | Interface IP ▾ | Wi-Fi WAN on 5 GHz | Interface IP ▾ |
| WAN | 192.168.52.152 (Interface IP) ▾ | | | | | | | | | | |
| Cellular | Interface IP ▾ | | | | | | | | | | |
| Wi-Fi WAN on 2.4 GHz | Interface IP ▾ | | | | | | | | | | |
| Wi-Fi WAN on 5 GHz | Interface IP ▾ | | | | | | | | | | |

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

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

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

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

Important Note

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

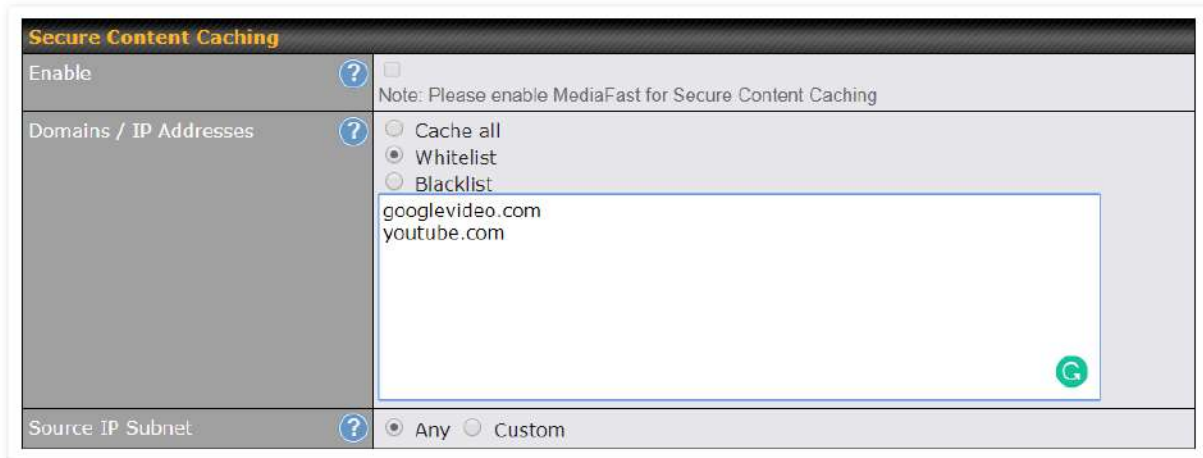
16 Media Fast

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

16.1 Setting Up MediaFast Content Caching

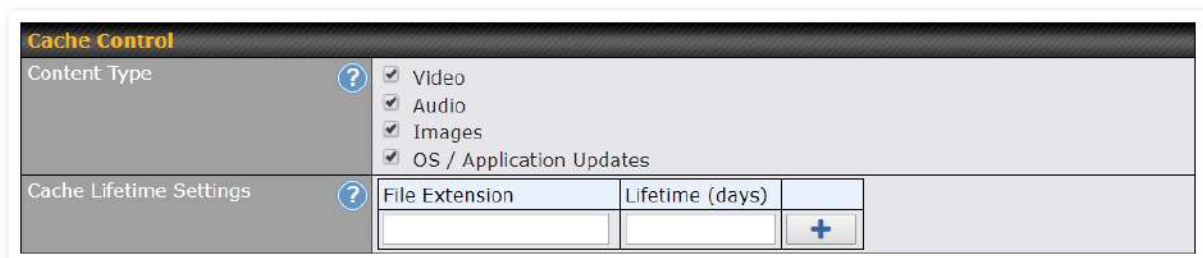
To access MediaFast content caching settings, select **Advanced > Cache Control**

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



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

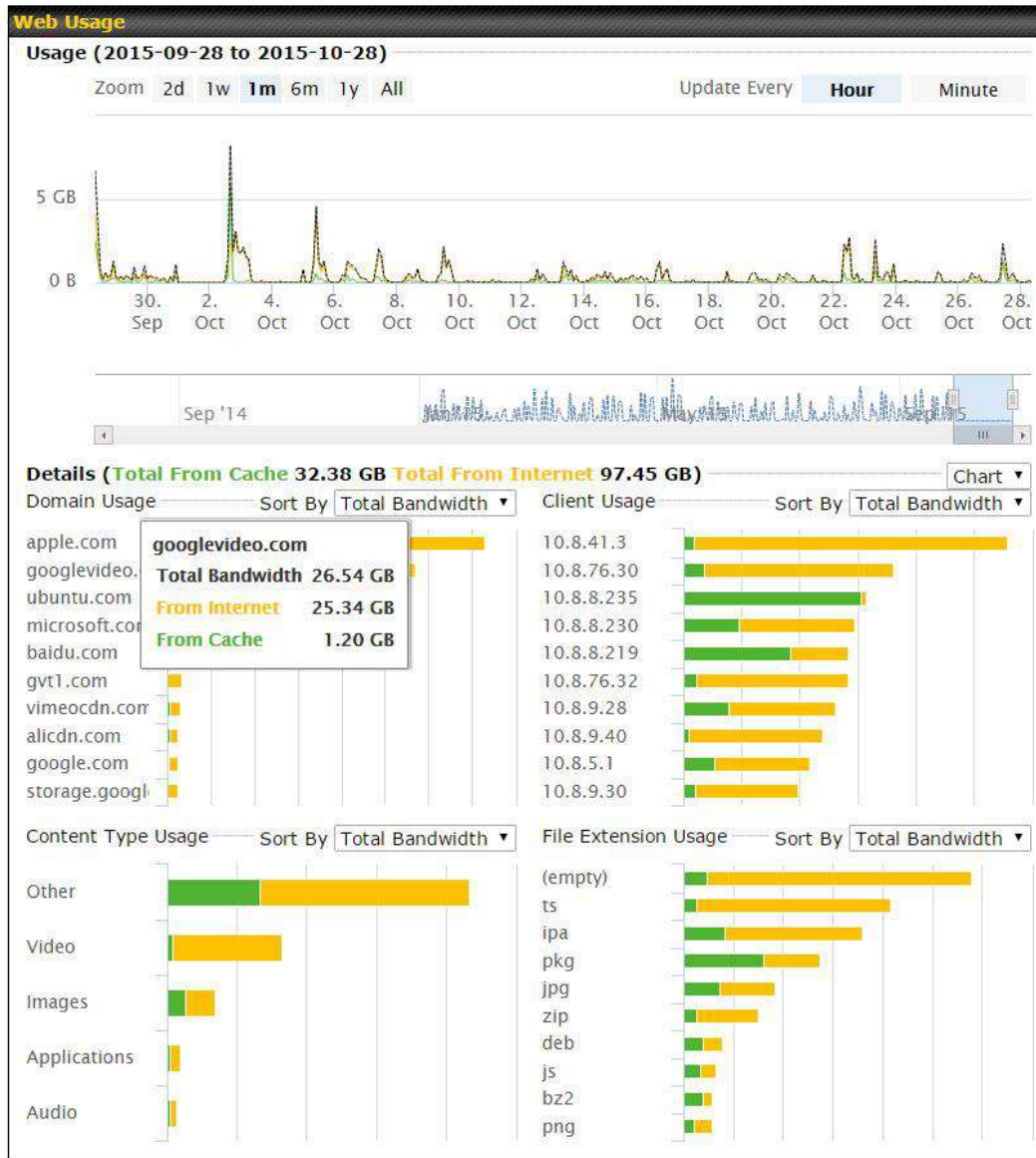
*See <https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/>



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

16.2 Viewing MediaFast Statistics

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



16.3 Prefetch Schedule

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

| Prefetch Schedule | | | | | | | | | |
|-------------------|-------------|---------------|---------------|---------------|--------|---------------|---------|--|--|
| Name | Status | Next Run Time | Last Run Time | Last Duration | Result | Last Download | Actions | | |
| ▶ Course Progress | Downloading | 04-11 06:00 | 04-09 02:03 | - | | 0 B | | | |
| ▶ National Geog | Ready | 04-11 00:00 | 04-09 00:00 | 00:01 | | 4.98 kB | | | |
| ▶ Syllabus | Downloading | 04-11 06:00 | 04-09 06:00 | - | | 0 B | | | |
| ▶ Vimeo | Ready | 04-11 00:00 | 04-09 02:03 | 00:01 | | 115.91 kB | | | |
| ▶ ted | Ready | 04-11 00:00 | 04-09 00:00 | 00:01 | | 62.26 kB | | | |

[New Schedule](#)

| Tools | |
|---------------------------------|----------------------------------|
| Clear Web Cache | Clear Statistics |

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

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

New Schedule

| | |
|-----------------|---|
| Name (optional) | <input type="text"/> |
| Active | <input checked="" type="checkbox"/> |
| URL | <input type="text" value="URL"/> <input type="button" value="+"/> |
| Depth | 2 levels <input type="button" value="Default"/> |
| Time Period | From 00:00 to 01:00 |
| Repeat | Everyday |
| Bandwidth Limit | 0 Gbps (0: Unlimited) |

Simply provide the requested information to create your schedule.

Clear Web Cache

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

Clear Statistics

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

17 Edge Computing

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

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

17.1 Configuring the ContentHub

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

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

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

| ContentHub | | | | | | |
|--|--------|-------------------------------------|--------------|--------------|--------|---------|
| Enable | | <input checked="" type="checkbox"/> | | | | |
| <input type="button" value="Save"/> | | | | | | |
| Schedule | | | | | | |
| Websites | Source | Next Update | Last Updated | Elapsed Time | Status | Actions |
| No Schedule | | | | | | |
| <input type="button" value="New Website"/> | | | | | | |

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

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

17.2 Configure a website for ContentHub

This option allows you to sync a website to the Pepwave router. This website will then be published with the specified domain from the router itself and makes the content available to the client via the HTTP/HTTPS protocol.

Only FTP sync is supported for this type of ContentHub content.

The content should be uploaded to an FTP server before you sync it with ContentHub.

Click **New Website** and a window with the following configuration options will appear:

Schedule
✕

| | |
|-----------------|--|
| Active | <input checked="" type="checkbox"/> |
| Type | <input checked="" type="radio"/> Website <input type="radio"/> Application |
| Protocol | HTTP ▾ |
| Domain/Path | http:// <input type="text"/> |
| Source | ftp ▾ :// <input type="text"/> Username: <input type="text"/> Password: <input type="password"/> |
| Period | Everyday ▾ From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾ |
| Bandwidth Limit | 0 <input type="text"/> Gbps ▾ (0: Unlimited) |

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


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



| Websites | Source | Next Update | Last Updated | Elapsed Time | Status | Actions |
|-------------------|--------------------------|-------------|--------------|--------------|--------|-----------------------------|
| http://mytest.com | ftp://10.8.76.254/web... | - | - | - | | + [edit] [delete] |
| /(root) | ftp://10.8.76.254/web... | | | | | ↓ [refresh] [edit] [delete] |

New Website

The content will be synced regularly according to the time set in the **Period** that was configured earlier.

If you want to activate the sync manually, you can click the “” icon. The “Status” column will display the sync progress. When the sync is completed, a summary will be displayed, as shown in the screenshot below:



| Websites | Source | Next Update | Last Updated | Elapsed Time | Status | Actions |
|-------------------|--------------------------|-------------|--------------|--------------|--------|-----------------------------|
| http://mytest.com | ftp://10.8.76.254/web... | - | 05-23 03:41 | 00:00:11 | ✓ | + [edit] [delete] |
| /(root) | ftp://10.8.76.254/web... | | | | | ↓ [refresh] [edit] [delete] |

New Website

Status details Close
 Completed
 +1 / 0 / -0 files

To access the content, open a browser in the MFA’s client and enter the domain details that were configured earlier (such as <http://mytest.com>).

17.3 Configure an application for ContentHub

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

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

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

PEPWAVE Dashboard SpeedFusion Cloud Network Advanced AP System Status Apply Changes

System

- Admin Security
- Firmware
- Time
- Schedule
- Email Notification
- Event Log
- SNMP
- InControl
- Configuration
- Feature Add-ons
- Reboot

Tools

- Ping
- Traceroute
- Wake-on-LAN
- WAN Analysis
- Storage Manager
- Package Manager

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

Package List Update All

| | |
|--|--|
| Node.js Version: 6.9.2 (17178) Size: 8.99 MB Date: Fri Feb 24 07:45:28 UTC 2017 | |
| Python Version: 2.7.12 (17178) Size: 20.29 MB Date: Fri Feb 24 07:45:28 UTC 2017 | |
| Ruby Version: 2.3.3 (17178) Size: 31.44 MB Date: Fri Feb 24 07:45:30 UTC 2017 | |

After installing the framework, change the "Type" to "Application" and configure the website.

Schedule ✕

| | |
|-----------------|--|
| Active | <input checked="" type="checkbox"/> |
| Type | <input type="radio"/> Website <input checked="" type="radio"/> Application |
| Protocol | HTTP |
| Domain | http:// |
| Method | <input checked="" type="radio"/> Sync <input type="radio"/> File Upload |
| Source | ftp :// Username: Password: |
| Period | Everyday From 00:00 to 01:00 |
| Bandwidth Limit | 0 Gbps (0: Unlimited) |

Save & Apply Now Cancel

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

Application type content need to be packed as explained below:

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

18 Docker

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

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

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

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

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

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

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

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

For detailed configuration instructions, refer to our knowledge base:

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

19 KVM

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



The screenshot shows a configuration panel for KVM. At the top, the word 'KVM' is displayed in orange. Below it, there is a section with the label 'Enable' and a checked checkbox. A 'Save' button is located below the checkbox. At the bottom of the panel, there is a link that says 'Click [here](#) to open file manager'.

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


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


20 QoS

20.1 User Groups

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

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

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



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

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

20.2 Bandwidth Control

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

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

| Group Bandwidth Reservation | | | |
|-----------------------------|-------------------------------------|------------------|------------------|
| Enable | <input checked="" type="checkbox"/> | | |
| | Manager | Staff | Guest |
| Bandwidth % | 50% | 30% | 20% |
| WAN 1 | 500.0M/500.0M | 300.0M/300.0M | 200.0M/200.0M |
| WAN 2 | 500.0M/500.0M | 300.0M/300.0M | 200.0M/200.0M |

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

| Individual Bandwidth Limit | | | |
|-----------------------------|-------------------------------------|-----------------------------|--|
| Enable | <input checked="" type="checkbox"/> | | |
| User Bandwidth Limit | | Download | Upload |
| Manager | | Unlimited | Unlimited |
| Staff | | 0 <input type="text"/> Mbps | 0 <input type="text"/> Mbps (0: Unlimited) |
| Guest | | 0 <input type="text"/> Mbps | 0 <input type="text"/> Mbps (0: Unlimited) |

20.3 Application Queue

This section is to define the QoS Application Queue. You can set guaranteed bandwidth for a queue and assign it to applications.

| QoS Application Queue | |
|------------------------------------|--|
| No Application Queue Defined | |
| <input type="button" value="Add"/> | |

Click the Add button to create the QoS Application Queue.

Add Queue
✕

| | |
|---|--|
| Name | <input style="width: 90%;" type="text"/> |
| Bandwidth ? | <input type="checkbox"/> Upload <input style="width: 50px;" type="text"/> Mbps ▼ <input type="checkbox"/> Download <input style="width: 50px;" type="text"/> Mbps ▼ |
| Borrow Spare Bandwidth ? | <input type="checkbox"/> |

| Add Queue | |
|-------------------------------|---|
| Name | This setting specifies a name for the QoS Application Queue. |
| Bandwidth | Bandwidth to be reserved (for each WAN connection) for this queue. When WAN is congested, this bandwidth will remain available for applications assigned to this queue. |
| Borrow Spare Bandwidth | Enable this option if you want this queue to utilize WAN's unused bandwidth. |

20.4 Application

20.4.1 Application Prioritization

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


Application Prioritization
?

Apply same settings to all users
 Customize

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

| Application | Manager | Staff | Guest | |
|--------------------------------------|----------|----------|----------|---|
| All Supported Streaming Applications | ↑ High ▼ | ↑ High ▼ | ↑ High ▼ | ✕ |
| All Database Applications | ↑ High ▼ | ↑ High ▼ | ↑ High ▼ | ✕ |
| <input type="button" value="Add"/> | | | | |

20.4.2 Prioritization for Custom Applications

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

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

Add / Edit Application
✕

| | |
|-------------|---|
| Type | <input checked="" type="radio"/> Supported Applications <input type="radio"/> Custom Applications |
| Category | <input type="text" value="Email"/> |
| Application | <input type="text" value="All Email Protocols"/> |

20.4.3 DSL/Cable Optimization

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

DSL/Cable Optimization
?

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

20.4.4 SpeedFusion VPN Traffic Optimization

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

SpeedFusion VPN Traffic Optimization
?

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

21 Firewall

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

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

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

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

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

| Rule | Protocol | Source | Destination | Action | |
|---------|----------|--------|-------------|--------|--|
| Default | Any | Any | Any | ✔ | |

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

| Rule | Protocol | WAN | Source | Destination | Action | |
|---------|----------|-----|--------|-------------|--------|--|
| Default | Any | Any | Any | Any | ✔ | |

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

| Rule | Protocol | Source | Destination | Action | |
|---------|----------|--------|-------------|--------|--|
| Default | Any | Any | Any | ✔ | |

Intrusion Detection and DoS Prevention ?

| | |
|----------|----------------------------------|
| Disabled | <input type="button" value="⚙"/> |
|----------|----------------------------------|

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

| Rule | Service | WAN | Source | Action | |
|---------|---------|-----|--------|--------|--|
| Default | Any | Any | Any | ✔ | |

21.1 Access Rules

Outbound Firewall Rules

The outbound firewall settings are located at **Advanced > Firewall > Access 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 | ✔ | |

To enable or disable the Outbound Firewall to manage device local network traffic, click on the help icon and click [here](#), the screen will show below.

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

| Rule | Protocol | Source | Destination | Action | |
|--|----------|--------|-------------|--------|---|
| ⚠ Device local network traffic is now managed by Outbound Firewall Rules | | | | | |
| test | Any | | | Deny | ✖ |
| test1 | Any | | | Deny | ✖ |
| Default | Any | Any | Any | Allow | |

Add Rule

Note

To utilize the Outbound Firewall Rule to block the Peplink device from contacting InControl 2, may refer to the link below:
<https://forum.peplink.com/t/faq-prevent-device-reaching-incontrol-2/.63f48dfd466df34ab475f55/>

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

Add a New Outbound Firewall Rule

New Firewall Rule

| | |
|-----------------------|---|
| Rule Name | <input type="text"/> |
| Enable | <input checked="" type="checkbox"/> Always on |
| 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 |

Inbound Firewall Rules

Inbound firewall settings are located at **Advanced > Firewall > Access 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 | Allow | ✖ |
| Default | Any | Any | Any | Any | Allow | |

Add Rule

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

Add a New Inbound Firewall Rule
✕

New Firewall Rule

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

Internal Network Firewall Rules

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

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

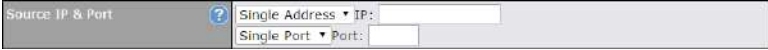
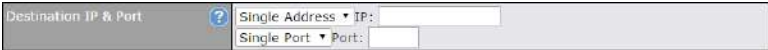
| Rule | Protocol | Source | Destination | Action | |
|----------------|----------|--------|-------------|-------------------------------------|-------------------------------------|
| <u>test</u> | Any | Any | Any | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <u>Default</u> | Any | Any | Any | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

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

Add a New Internal Network Firewall Rule
✕

New Firewall Rule

| | |
|---------------|--|
| Rule Name | <input type="text"/> |
| 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 |

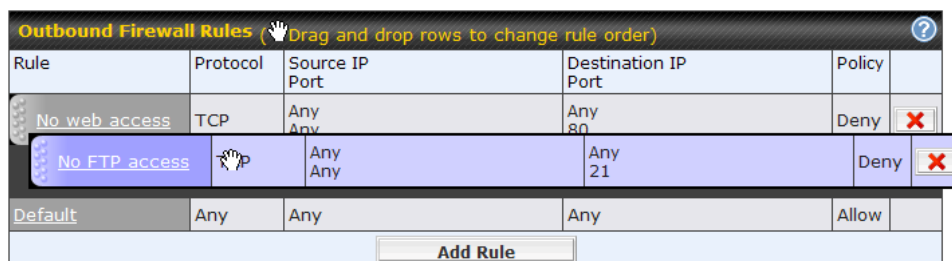
| Inbound / Outbound / Internal Network Firewall Settings | |
|---|--|
| Rule Name | This setting specifies a name for the firewall rule. |
| Enable | <p>This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by the Pepwave router based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Pepwave router will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p> |
| WAN Connection (Inbound) | Select the WAN connection that this firewall rule should apply to. |
| Protocol | <p>This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> • Any • TCP • UDP • ICMP • DSCP • IP <p>Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)</p> <p>After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remains manually modifiable.</p> |
| Source IP & Port | <p>This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the Source IP & Port setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the Source IP & Port settings.</p> |
| Destination IP & Port | <p>This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the Destination IP & Port setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the Destination IP & Port settings.</p> |

| | |
|-----------------------------|--|
| <p>Action</p> | <p>This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:</p> <ul style="list-style-type: none"> • Source IP & port • Destination IP & port <p>With the value of Allow for the Action setting, the matching traffic passes through the router (to be routed to the destination). If the value of the Action setting is set to Deny, the matching traffic does not pass through the router (and is discarded).</p> |
| <p>Event Logging</p> | <p>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page Status>Event Log. A sample message is as follows:</p> <p>Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80</p> <ul style="list-style-type: none"> • CONN: The connection where the log entry refers to • SRC: Source IP address • DST: Destination IP address • LEN: Packet length • PROTO: Protocol • SPT: Source port • DPT: Destination port |

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

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

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



To remove a rule, click the button.

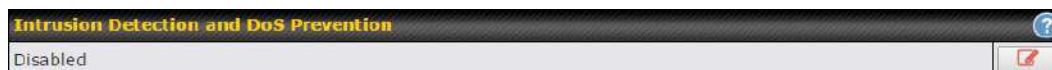
Rules are matched from top to bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match, the **Default** rule will be applied. By

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.

Intrusion Detection and DoS Prevention



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

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

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

Local Service Firewall Rules

For every WAN inbound traffic to local service, rules will be matched to take the defined action. The Local Service firewall settings are located at **Advanced > Firewall > Access Rules**.

| Local Service Firewall Rules <small>(Drag and drop rows by the left to change rule order)</small> | | | | | |
|--|---------|-----|--------|--------|--|
| Rule | Service | WAN | Source | Action | |
| Default | Any | Any | Any | | |
| <input type="button" value="Add Rule"/> | | | | | |

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

Local Service Firewall Rule
✕

| | |
|--|---|
| Rule Name | <input style="width: 90%;" type="text"/> |
| Enable | <input checked="" type="checkbox"/> |
| Service ? | <input style="width: 90%;" type="text" value="Any"/> ▾ |
| WAN Connection | <input style="width: 90%;" type="text" value="Any"/> ▾ |
| Source | <input style="width: 90%;" type="text" value="Any"/> ▾ |
| Action | <input checked="" type="radio"/> Allow <input type="radio"/> Deny |
| Event Logging | <input type="checkbox"/> |

| Local Service Firewall Settings | |
|---------------------------------|---|
| Rule Name | This setting specifies a name for the firewall rule. |
| Enable | <p>This setting specifies whether the firewall rule should take effect.</p> <p>If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule.</p> <p>If the box is not checked, the firewall rule does not take effect. The Peplink Balance 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> |
| Service | <p>This option allows you to define the supported local service to be matched.</p> <p>If Any is chosen, the firewall rule will match to all supported local services from the list.</p> <p>Via a drop-down menu, the following services can be specified:</p> <ul style="list-style-type: none"> • Any • SpeedFusion / PepVPN Handshake • SpeedFusion / PepVPN Data Port • Web Admin Access • DNS Server • SNMP Server • KVM Management Port • KVM VNC Port • FusionSIM Agent / Remote SIM Proxy |
| WAN Connection | Select the WAN connection that this firewall rule should apply to. |
| Source | This specifies the source IP address and IP Network to be matched for the firewall rule. |
| Action | 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

21.2 Content Blocking

Application Blocking ?

Please Select Application... +

Web Blocking ?

Preset Category
 High Adware Audio-Video File Hosting
 Moderate P2P/File sharing Pornography Update Sites
 Low
 Custom

Content Filtering Database Auto Update ?

Customized Domains ?
 +

Exempted Domains from Web Blocking ?
 +

Exempted User Groups ?

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

Exempted Subnets ?

| Network | Subnet Mask | |
|--|--|---|
| <input style="width: 95%;" type="text"/> | 255.255.255.0 (/24) v | + |

21.2.1 Application Blocking

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

21.2.2 Web Blocking

Defines website domain names to be blocked from LAN/PPTP/SpeedFusion VPN 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.

21.2.3 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.

21.2.4 Exempted User Groups

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

21.2.5 Exempted Subnets

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

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 | |
| No OSPF Area Defined. | | |
| Add | | |

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

| OSPF & RIPv2 Route Advertisement | | | | | | | | |
|----------------------------------|---------------------|--|-------------------|-------------|--|----------------------|---------------------|--|
| SpeedFusion VPN Route Isolation | | <input type="checkbox"/> Enable | | | | | | |
| Network Advertising | | <div style="border: 1px solid #ccc; padding: 2px;"> --- ▼ + </div> All LAN/VLAN networks will be advertised when no network advertising is chosen. | | | | | | |
| Static Route Advertising | | <input checked="" type="checkbox"/> Enable | | | | | | |
| | | <table border="1" style="width: 100%;"> <thead> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24)</td> <td style="text-align: right;">+</td> </tr> </tbody> </table> | Excluded Networks | Subnet Mask | | <input type="text"/> | 255.255.255.0 (/24) | + |
| Excluded Networks | Subnet Mask | | | | | | | |
| <input type="text"/> | 255.255.255.0 (/24) | + | | | | | | |
| Save | | | | | | | | |

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

| OSPF Settings | |
|-----------------------|--|
| Area ID | 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. |
| Link Type | Choose the type of network that this area will use. |
| Authentication | If an authentication method is used, select one from this drop-down menu. Available options are MD5 and Text . Authentication key(s) may be input next to the drop-down menu after selecting an authentication method. |
| Interfaces | 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 | <input type="text" value="None"/> |
| Interfaces | <input type="checkbox"/> Untagged LAN <input type="checkbox"/> V167 (192.168.167.1/24) <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 |

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

| OSPF & RIPv2 Route Advertisement | | | | | | | |
|-------------------------------------|---|-------------------|-------------|--|----------------------|---------------------|---|
| SpeedFusion VPN Route Isolation | <input type="checkbox"/> Enable | | | | | | |
| Network Advertising | <div style="border: 1px solid #ccc; padding: 2px;"> --- + </div> <small>All LAN/VLAN networks will be advertised when no network advertising is chosen.</small> | | | | | | |
| Static Route Advertising | <input checked="" type="checkbox"/> Enable <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Excluded Networks</th> <th style="width: 30%;">Subnet Mask</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24)</td> <td style="text-align: right;">+</td> </tr> </tbody> </table> | Excluded Networks | Subnet Mask | | <input type="text"/> | 255.255.255.0 (/24) | + |
| Excluded Networks | Subnet Mask | | | | | | |
| <input type="text"/> | 255.255.255.0 (/24) | + | | | | | |
| <input type="button" value="Save"/> | | | | | | | |

| OSPF & RIPv2 Route Advertisement | |
|--|--|
| SpeedFusion VPN Route Isolation | Isolate SpeedFusion VPN peers from each other. Received SpeedFusion VPN routes will not be forwarded to other SpeedFusion VPN peers to reduce bandwidth consumption.. |
| Network Advertising | Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default. |
| Static Route Advertising | 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 **Advanced** 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 | ✘ |
| <input type="button" value="Add"/> | | | |

Click the "✘" to delete a BGP profile.

Click "Add" to create a new BGP profile.

| BGP Profile | | | | | | |
|--------------------------------------|---|----------------------|----------------|----------------------|----------------------|----------------------------------|
| Profile Name | <input type="text"/> | | | | | |
| Enable | <input checked="" type="checkbox"/> | | | | | |
| Interface | Untagged LAN (192.:▼) | | | | | |
| Router ID | <input checked="" type="radio"/> LAN IP Address <input type="radio"/> Custom: <input type="text"/> | | | | | |
| Autonomous System | <input type="text"/> | | | | | |
| Neighbor ? | IP Address | Autonomous System | Multihop / TTL | Password | AS-Path Prepending | |
| | <input type="text"/> | <input type="text"/> | disable | <input type="text"/> | <input type="text"/> | <input type="button" value="+"/> |
| Hold Time ? | <input type="text" value="240"/> | | | | | |
| Next Hop Self ? | <input type="checkbox"/> | | | | | |
| iBGP Local Preference ? | <input type="text" value="100"/> | | | | | |
| BFD ? | <input type="checkbox"/> Enable | | | | | |

| BGP Profile | |
|----------------------------|--|
| Name | This field specifies the name that represents this profile. |
| Enable | When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled. |
| Interface | The interface in which the BGP neighbor is located. |
| Router ID | This field specifies the unique IP as the identifier of the local device running BGP. |
| Autonomous System | The Autonomous System Number (ASN) assigned to this profile. |
| Neighbor | BGP Neighbors and their details. |
| IP address | The IP address of the Neighbor. |
| Autonomous System | The Neighbor's ASN. |
| Multihop/TTL | 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. |
| Password | (Optional) Assign a password for MD5 authentication of BGP sessions. |
| AS-Path Prepending: | 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. |
| Hold Time | Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240 |
| Next Hop Self | Enable this option to advertise your own source address as the next hop when propagating routes. |
| iBGP Local Preference | This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100 |
| BFD | 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 | ? | --- <input type="button" value="+"/> | | | | | | |
| Static Route Advertising | ? | <input checked="" type="checkbox"/> Enable <table border="1"> <thead> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> <th><input type="button" value="+"/></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) <input type="button" value="v"/></td> <td></td> </tr> </tbody> </table> | Excluded Networks | Subnet Mask | <input type="button" value="+"/> | <input type="text"/> | 255.255.255.0 (/24) <input type="button" value="v"/> | |
| Excluded Networks | Subnet Mask | <input type="button" value="+"/> | | | | | | |
| <input type="text"/> | 255.255.255.0 (/24) <input type="button" value="v"/> | | | | | | | |
| Custom Route Advertising | ? | <table border="1"> <thead> <tr> <th>Networks</th> <th>Subnet Mask</th> <th><input type="button" value="+"/></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) <input type="button" value="v"/></td> <td></td> </tr> </tbody> </table> | Networks | Subnet Mask | <input type="button" value="+"/> | <input type="text"/> | 255.255.255.0 (/24) <input type="button" value="v"/> | |
| Networks | Subnet Mask | <input type="button" value="+"/> | | | | | | |
| <input type="text"/> | 255.255.255.0 (/24) <input type="button" value="v"/> | | | | | | | |
| Advertise OSPF Route | ? | <input type="checkbox"/> | | | | | | |
| Set Community | ? | <table border="1"> <thead> <tr> <th>Community</th> <th>Route Prefix</th> <th><input type="button" value="+"/></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> </tbody> </table> | Community | Route Prefix | <input type="button" value="+"/> | <input type="text"/> | <input type="text"/> | |
| Community | Route Prefix | <input type="button" value="+"/> | | | | | | |
| <input type="text"/> | <input type="text"/> | | | | | | | |

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

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 | Accept ▼ | | |
| Restricted Networks | Network | Subnet Mask | Exact Match |
| | | 255.255.255.0 (/24) ▼ | <input type="checkbox"/> |
| | | | + |

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 "Blocked Networks" will be rejected, routes not in the list will be accepted.

Restricted Networks / Blocked 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 | Accept ▼ | | |
| Restricted Networks | Network | Subnet Mask | Exact Match |
| | | 255.255.255.0 (/24) ▼ | <input type="checkbox"/> |
| Export to other BGP Profile | <input type="checkbox"/> | | |
| Export to OSPF | <input type="checkbox"/> | | |

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

| | |
|---|---|
| | <p>None: All BGP routes will be accepted.</p> <p>Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p>Reject: Routes in "Blocked Networks" will be rejected, routes not in the list will be accepted.</p> |
| Restricted Networks / Blocked Networks | <p>This field specifies the network(s) in the "route export" entry.</p> <p>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.</p> |
| Export to other BGP Profile | <p>When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.</p> |
| Export to OSPF | <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 **Advanced > Remote User Access** and choose the required VPN type.

| 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 | |
| Listen On | Connection / IP Address(es) <input type="checkbox"/> 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 | |
| Authentication | Local User Accounts ▼ | |
| User Accounts | <input type="text"/> Username | <input type="text"/> Password |
| | | + |
| <input type="button" value="Save"/> | | |

| Remote User Access Settings | | | | | |
|-----------------------------|--|----------|---|---------------|---|
| Enable | When this box is checked, this Remote User Access profile will be enabled. If it is left unchecked, it will be disabled. | | | | |
| VPN Type | <p>This field allows you to select the VPN type for the remote user access connection. The available options are:</p> <ul style="list-style-type: none"> L2TP with IPsec <table border="1"> <tr> <td>VPN Type</td> <td> <input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input type="radio"/> OpenVPN </td> </tr> <tr> <td>Preshared Key</td> <td> <input type="text"/> <input checked="" type="checkbox"/> Hide Characters </td> </tr> </table> <p>If L2TP with IPsec is selected, it may need to enter the pre-shared key for the remote user access.</p> <ul style="list-style-type: none"> PPTP | 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 |
| 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 | | | | |

| | |
|----------|---|
| VPN Type | <input type="radio"/> L2TP with IPsec <input checked="" type="radio"/> PPTP <input type="radio"/> OpenVPN |
|----------|---|

If PPTP selected, there is 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

- OpenVPN


| | |
|-----------------------------|---|
| VPN Type | <input type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input checked="" type="radio"/> OpenVPN <small>You can obtain the OpenVPN client profile from the status page.</small> |
| Connection Security Refresh | <input type="text" value="60"/> minute(s) |

If the OpenVPN is selected, the OpenVPN Client profile can be downloaded from the **Status > Device** page after the configuration has been saved.

| | |
|------------------------|--|
| OpenVPN Client Profile | <input type="button" value="Route all traffic"/> <input type="button" value="Split tunnel"/> |
|------------------------|--|

You have a choice between 2 different OpenVPN Client profiles:


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

| | |
|------------------------------------|---|
| Pre-shared Key | If L2TP with IPsec is selected in the VPN Type, enter the pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance. |
| Disabled Weak Ciphers | You may click the  button to show in the Pre-shared key and enable this option. When checked, weak ciphers such as 3DES will be disabled. Please note: Legacy and Android devices may not able to connect. |
| Connection Security Refresh | If OpenVPN is selected in the VPN Type, this settings is for specifying the interval for refreshing the connection. |
| Listen On | This setting is for specifying the WAN IP addresses that allow remote user access. |
| Port | If OpenVPN is selected in the VPN Type, the Port setting specifies the port(s) that correspond to the service. |

Determine the method of authenticating remote users:

- **Local User Accounts**

| | | | |
|----------------|---------------------------------------|---------------------------------------|----------------------------------|
| Authentication | Local User Accounts ▼ | | |
| User Accounts | <input type="text" value="Username"/> | <input type="text" value="Password"/> | <input type="button" value="X"/> |
| | <input type="text" value=""/> | <input type="text" value=""/> | <input type="button" value="X"/> |

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**

| | |
|-------------------------|---|
| Authentication | LDAP Server ▼ |
| Authentication Protocol | MS-CHAP v2 ▼ |
| LDAP Server | <input type="text"/> Port <input type="text" value="389"/> <input type="checkbox"/> Use DN/Password to bind to LDAP Server |
| Base DN | <input type="text"/> |
| Base Filter | <input type="text"/> |

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

• **Radius Server**

| | |
|-------------------------|--|
| Authentication Protocol | MS-CHAP v2 ▼ |
| | You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles |
| Authentication Host | <input type="text"/> |
| Authentication Port | <input type="text" value="1812"/> |
| Authentication Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters |
| | You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles |
| Accounting Host | <input type="text"/> |
| Accounting Port | <input type="text" value="1813"/> |
| Accounting Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters |
| Source Network Address | Untagged LAN ▼ |

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

• **Active Diretory**

| | |
|-------------------|---|
| Authentication | Active Directory ▼ |
| Server IP Address | <input type="text"/> |
| Server Hostname | <input type="text"/> |
| Domain | <input type="text"/> |
| Custom Workgroup | ((Optional) <input type="text"/>) |
| Admin Username | <input type="text"/> |
| Admin Password | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters |

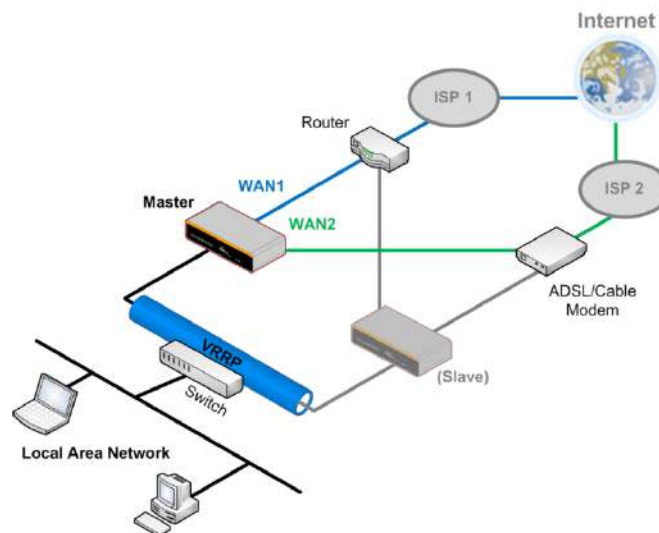
Enter the matching Active Directory details to allow for Active Directory server authentication.

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 Peplink 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

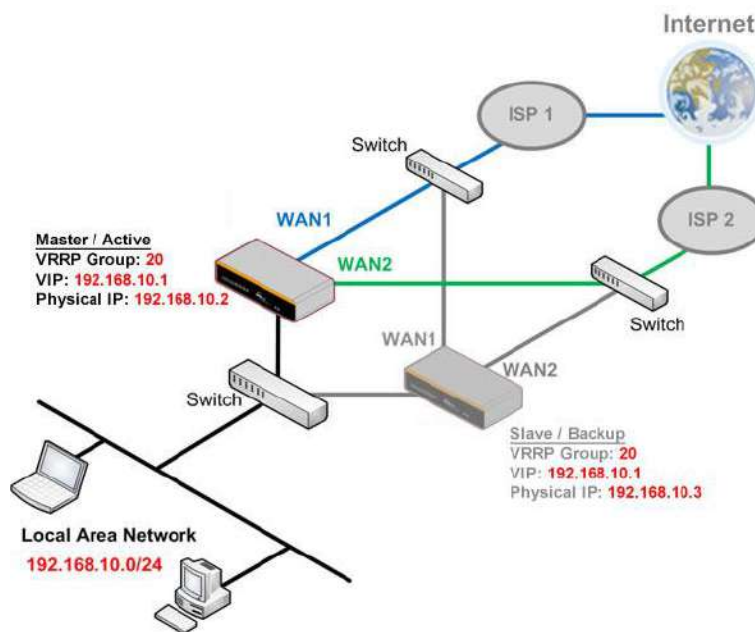
| High Availability | |
|-------------------------------------|---|
| Enable | <input checked="" type="checkbox"/> |
| Group Number | <input type="text"/> |
| Preferred Role | <input type="radio"/> Master <input checked="" type="radio"/> Slave |
| Configuration Sync. | <input type="checkbox"/> Master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

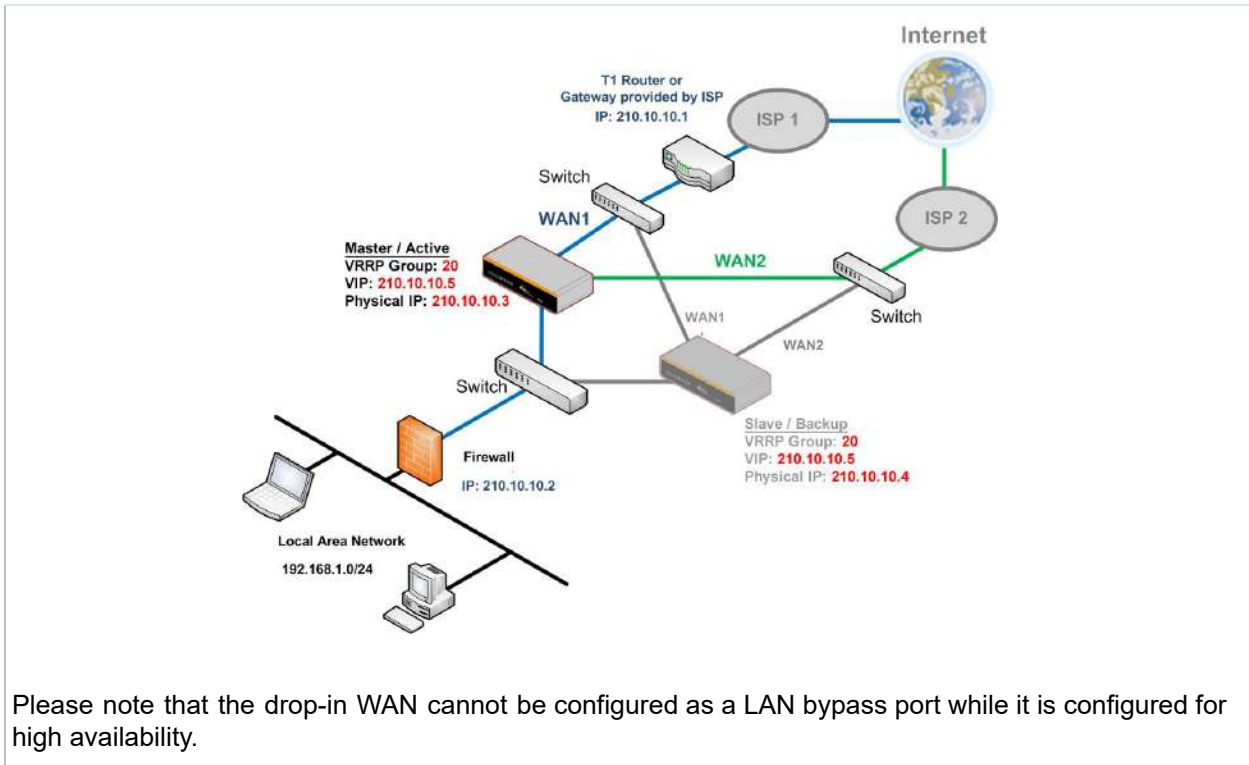
| | |
|--|--|
| Administration IP must be under the same network. | |
| LAN Administration IP | This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN. |
| Subnet Mask | This setting specifies the subnet mask of the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

Important Note

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



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



24.2 RADIUS Server

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

| Authentication Server | Host | Port |
|--|------|------|
| No server profiles defined | | |
| <input type="button" value="New Profile"/> | | |

| Accounting Server | Host | Port |
|--|------|------|
| No server profiles defined | | |
| <input type="button" value="New Profile"/> | | |

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

Authentication Server ✕

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

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

Accounting Server
✕

| | |
|--------|---|
| Name | <input style="width: 90%;" type="text"/> |
| Host | <input style="width: 90%;" type="text"/> |
| Port | <input style="width: 90%;" type="text" value="1813"/> |
| Secret | <input style="width: 90%;" type="password"/> <input checked="" type="checkbox"/> Hide Characters |

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

24.3 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 | |
| <input type="button" value="Add Certificate"/> | |

| Wi-Fi WAN CA Certificate | |
|--|--|
| No Certificates defined | |
| <input type="button" value="Add Certificate"/> | |

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

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

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

24.4 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 | |
|----------------------------------|---|
| SMTP Forwarding | When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting Enable . |
| Web Proxy Forwarding | When this option is enabled, all outgoing connections destined for the proxy server specified in Web Proxy Interception Settings will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting Enable . |
| DNS Forwarding | When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down. |
| Custom Service Forwarding | When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number. |

24.4.1 SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP's SMTP server. All outgoing SMTP connections are blocked except those connecting to the ISP's. Pepwave routers support intercepting and redirecting all outgoing SMTP connections (destined for TCP port 25) via a WAN connection to the WAN's corresponding SMTP server.

SMTP Forwarding Setup ?

SMTP Forwarding Enable

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

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

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

Note

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

24.4.2 Web Proxy Forwarding

Web Proxy Forwarding Setup ?

Web Proxy Forwarding Enable

Web Proxy Interception Settings

Proxy Server IP Address Port
(Current settings in users' browser)

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

When this feature is enabled, the Pepwave router will intercept all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings**, choose a WAN connection with reference to the outbound policy, and then forward them to the specified web proxy server and port number. Redirected server settings for each WAN can be set here. If forwarding is disabled for a WAN, web proxy connections for the WAN will be simply forwarded to the connection's original destination.

24.4.3 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.

24.4.4 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"/> |
| | | | + |

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.

24.5 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 <input checked="" type="checkbox"/> Define custom signal ports 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 <input type="checkbox"/> Define custom control ports |
| TFTP | <input checked="" type="checkbox"/> Enable |
| IPsec NAT-T | <input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Define custom ports 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> <input checked="" type="checkbox"/> Route IPsec Site-to-Site VPN 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 | |
|-----------------------------|--|
| SIP | <p>Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Pepwave router can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in NAT mode. Such passthrough support is always enabled, and there are two modes for selection: Standard Mode and Compatibility Mode. If your SIP server's signal port number is non-standard, you can check the box Define custom signal ports and input the port numbers to the text boxes.</p> |
| H.323 | <p>With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Pepwave router.</p> |
| FTP | <p>FTP sessions consist of two TCP connections; one for control and one for data. In a multi-WAN situation, they must be routed to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Pepwave router monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, you can check Define custom control ports and enter the port numbers in the text boxes.</p> |
| TFTP | <p>The Pepwave router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select Enable if you want to enable TFTP passthrough support.</p> |

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.

24.6 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 | 9500 ▼ |
| 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.

24.7 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 > Misc. Settings > 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="text"/> |
| GPS Report Format | <input checked="" type="radio"/> NMEA <input type="radio"/> TAIP | | | |
| NMEA Sentence Type | <input checked="" type="checkbox"/> GPRMC <input type="checkbox"/> GPGGA <input type="checkbox"/> GPVTG <input type="checkbox"/> GPGSA <input type="checkbox"/> GPGSV | | | |
| Vehicle ID | <input type="checkbox"/>  | | | |

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

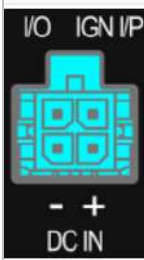
24.8 Ignition Sensing

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

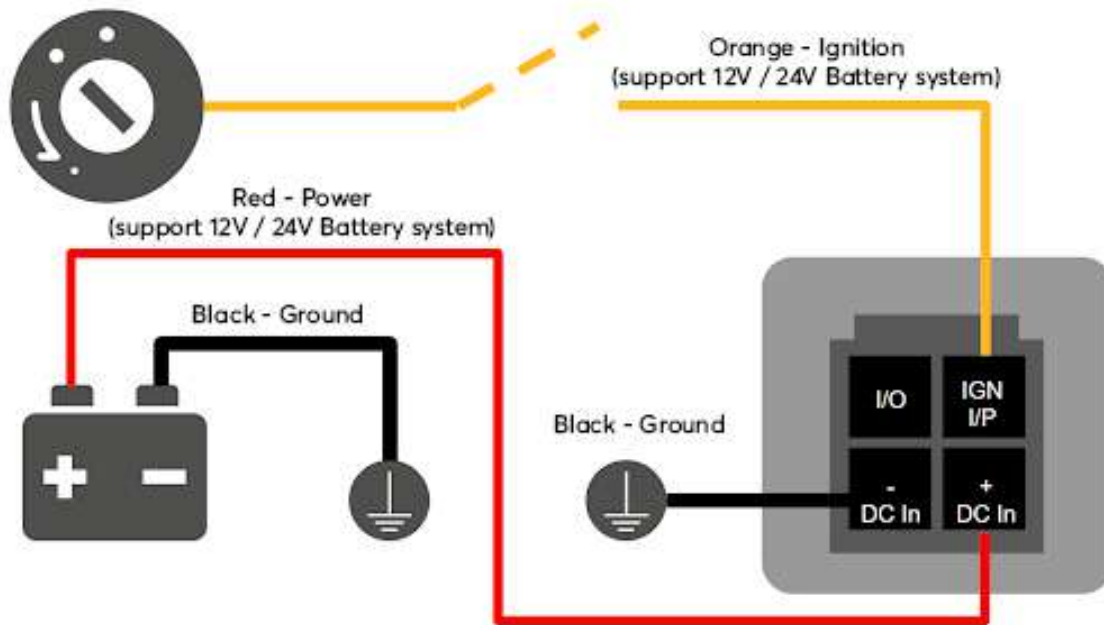
This feature allows the cellular router to start up or shut down when the engine of that vehicle is started or turned off.

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.

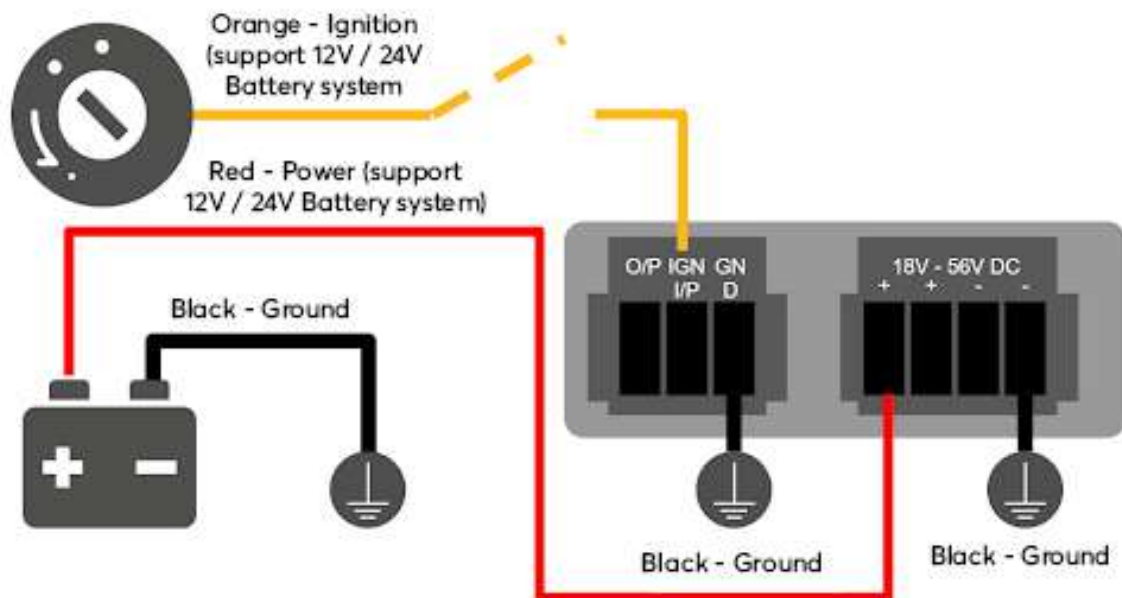
Ignition Sensing installation

| | 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) | Red |
| <p>* Currently not functional; will be used for additional features in future firmware. ** Connecting IGN I/P is optional and is needed only if the Ignition Sensing feature is configured.</p> | | |

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 > Misc. Settings > 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.

24.9 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, BR1 Pro CAT-20/5G, 700 HW3, HD2/4, Transit

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

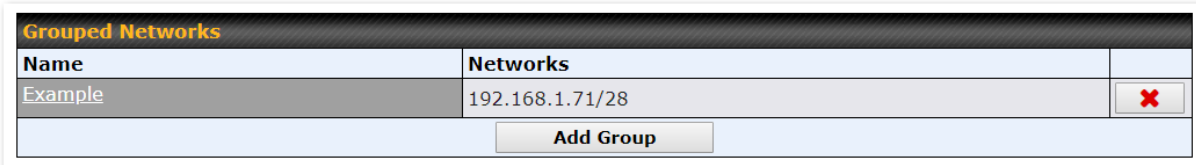
| NTP Server | |
|------------|--------------------------|
| Enable | <input type="checkbox"/> |

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

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

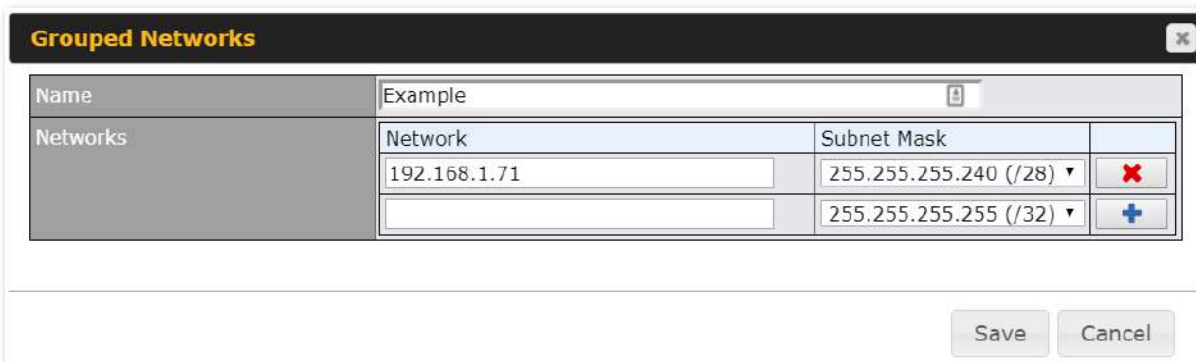
24.10 Grouped Networks

Advanced > Misc. Settings > 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) ▾ | + |

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

24.11 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 | <input type="checkbox"/> |
| Remote SIM Host | <input type="text"/> |

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

Remote SIM Host

192.168.1.10 ✖

| Remote SIM Management | Server | Slot |
|---|--------|------|
| No Remote SIM Defined. | | |
| <input type="button" value="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"/> (Confirm) |

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

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


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 | 234567 8901234567 |
| Tool | SMS |

| SMS | | | Refresh |
|--------------------|--|--|---------|
| Jun 21, 2017 18:00 | <p>Hi, Thank you, your self password is verified - you can change this when you first login at there as an</p> | | |
| May 06, 2017 12:23 | <p>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: http://mobile.energysource.com</p> | | |
| Mar 15, 2017 10:03 | <p>From: Home Hello, There is planned maintenance at the Berkeley area PG&E area this week. If your service is affected, you can get updates here: http://pge.com</p> | | |
| Mar 06, 2017 14:50 | <p>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: http://mobile.energysource.com</p> | | |
| Dec 28, 2016 09:53 | <p>From: Home Hi, we hope your appreciation is rewarded with your offer. And we remind you, this offer applied to your first 6 bills. Your monthly earnings change will start to be applied on your next 6 bills.</p> | | |
| Dec 06, 2016 13:09 | <p>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: http://mobile.energysource.com</p> | | |
| Nov 08, 2016 11:29 | <p>From: Home Hello, There is planned maintenance at the Berkeley area PG&E area this week. If your service is affected, you can get updates here: http://pge.com</p> | | |
| Sep 07, 2016 17:05 | <p>From: Home Read more details regarding our studies on wireless performance. You can find a PDF report on that your website here: http://www.peplink.com</p> | | |

24.13 UDP Relay

You may define the UDP relay by clicking the **Advanced > Misc Settings > UDP Relay**. You can click  to enable the UDP relay to relay UDP Broadcast or Multicast traffic for LAN/VLAN/SpeedFusion VPN.

Click “New UDP Relay Rule” to define the relay rule.

| Name | Port / Multicast Address | Source Network | Destination Network |
|------------------------------------|--------------------------|----------------|---------------------|
| No UDP relay rules defined | | | |
| New UDP Relay Rule | | | |

| UDP Relay | |
|----------------------------|--|
| Name | This field is for specifying a name to represent this profile. |
| Port | This feid is to enter the specific port number for the UDP relay |
| Multicast | If Multicast is not selected, it will broadcast relay rule. If Multicast is selected, you may need to enter a valid multicast address. |
| Secure Network | Select the specific connection as a source network to where the device is to relay UDP Broadcast packets. |
| Destination Network | You may select the specific connection from the drop-down list or may custom combination network as a destination network that receives the UDP packet relays. |

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.

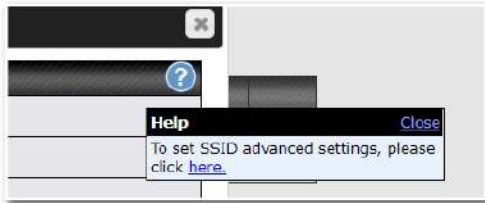
| AP Controller | |
|---------------|---|
| AP Management | <input checked="" type="checkbox"/> Integrated AP <input checked="" type="checkbox"/> External AP |
| Sync. Method | As soon as possible ▾ |
| Permitted AP | <input checked="" type="radio"/> Any <input type="radio"/> Approved List |

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

25.2 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"/> |
| Schedule | Always on ▼ |
| VLAN | Untagged LAN ▼ |
| Broadcast SSID | <input checked="" type="checkbox"/> |
| Data Rate | <input checked="" type="radio"/> Auto <input type="radio"/> Fixed <input type="radio"/> Minimum |
| Multicast Filter | <input type="checkbox"/> |
| Multicast Rate | MCS24/MCS16/MCS8/MCS0/6M ▼ |
| IGMP Snooping | <input type="checkbox"/> |
| Layer 2 Isolation | <input type="checkbox"/> |
| Maximum number of clients | 2.4 GHz: <input type="text" value="Unlimited"/> 5 GHz: <input type="text" value="Unlimited"/> |
| Band Steering | <input type="checkbox"/> Disable ▼ |

| SSID Settings | |
|-------------------------------------|---|
| SSID | This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients. |
| Schedule | Click the drop-down menu to apply a time schedule to this interface |
| VLAN | This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is 0 , which means VLAN tagging is disabled (instead of tagged with zero). |
| Broadcast SSID | This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default. |
| Data Rate ^A | Select Auto to allow the Pepwave router to set the data rate automatically, or select Fixed and choose a rate from the displayed drop-down menu. |
| Multicast Filter^A | This setting enables the filtering of multicast network traffic to the wireless SSID. |

| | |
|--|---|
| Multicast Rate^A | This setting specifies the transmit rate to be used for sending multicast network traffic. The selected Protocol and Channel Bonding settings will affect the rate options and values available here. |
| IGMP Snooping^A | To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option. |
| Layer 2 Isolation^A | Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to the upper communication layer(s). By default, the setting is disabled. |
| Maximum Number of Clients^A | Indicate the maximum number of clients that should be able to connect to each frequency. |
| Band Steering^A | To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency. Choose between: Force - Clients capable of 5 GHz operation are only offered with 5 GHz frequency. Prefer - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered. Disable - Default |

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

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

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

- **WPA/WPA2 – Enterprise**

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.

The screenshot shows a configuration interface for 'Access Control Settings'. It features two main sections: 'Restricted Mode' with a dropdown menu currently showing 'Deny all except listed', and 'MAC Address List' which is an empty text input field with a blue question mark icon to its left.

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

| RADIUS Settings | | |
|-----------------------|--|---|
| | Primary | Secondary |
| | You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles | |
| Authentication Host | <input type="text"/> | <input type="text"/> |
| Authentication Port | <input type="text" value="1812"/> | <input type="text" value="1812"/> |
| Authentication Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters |
| | You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles | |
| Accounting Host | <input type="text"/> | <input type="text"/> |
| Accounting Port | <input type="text" value="1813"/> | <input type="text" value="1813"/> |
| Accounting Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters |
| NAS-Identifier | <input type="text" value="Device Name"/> | |

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

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

| Firewall Settings | |
|-------------------|---|
| Firewall Mode | <div style="border: 1px solid #ccc; padding: 2px;"> Disable ▾ Disable Flexible - Allow all except... Lockdown - Block all except... </div> |

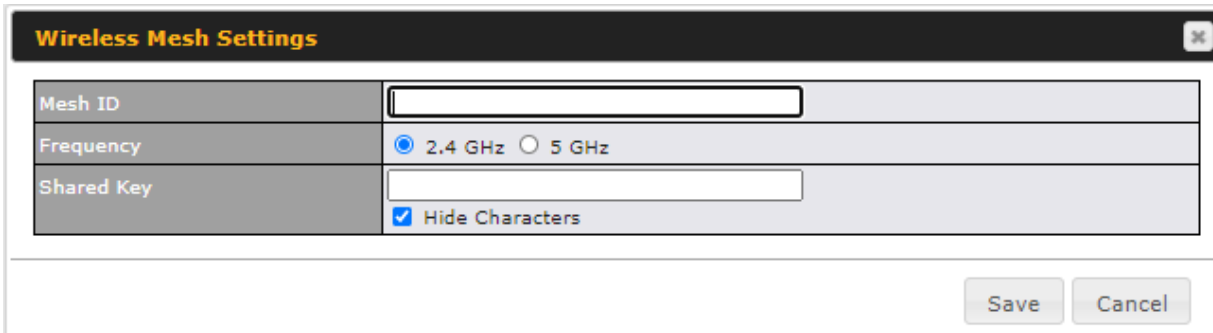
| Firewall Settings | |
|----------------------------|---|
| Firewall Mode | <p>The settings allow administrators to control access to the SSID based on Firewall Rules.</p> <p>Available options are Disable, Lockdown - Block all except... and Flexible -Allow all except...</p> |
| Firewall Exceptions |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

25.3 Wireless Mesh



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 | Enter a name to represent the Mesh profile. |
| Frequency | Select the 2.4GHz or 5GHz frequency to be used. |
| Shared Key | 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. Click Hide / Show Characters to toggle visibility. |

25.4 Settings

To configure the AP settings, navigating to **AP > Settings** :

| AP Settings | |
|----------------------------------|--|
| SSID | <input type="checkbox"/> 2.4 GHz <input checked="" type="checkbox"/> 5 GHz <input checked="" type="checkbox"/> PEPWAVE_A712 |
| Operating Country | United States |
| Protocol | 2.4 GHz: 802.11n 5 GHz: 802.11n/ac <small>Integrated AP supports 802.11n/ac only</small> |
| Channel Width | Auto |
| Channel | Auto <input type="button" value="Edit"/> Channels: 1 6 11 |
| Auto Channel Update | Daily at: <input type="button" value="Clear"/> <input type="button" value="All"/> <input type="checkbox"/> 00:00 <input type="checkbox"/> 01:00 <input type="checkbox"/> 02:00 <input checked="" type="checkbox"/> 03:00 <input type="checkbox"/> 04:00 <input type="checkbox"/> 05:00 <input type="checkbox"/> 06:00 <input type="checkbox"/> 07:00 <input type="checkbox"/> 08:00 <input type="checkbox"/> 09:00 <input type="checkbox"/> 10:00 <input type="checkbox"/> 11:00 <input type="checkbox"/> 12:00 <input type="checkbox"/> 13:00 <input type="checkbox"/> 14:00 <input type="checkbox"/> 15:00 <input type="checkbox"/> 16:00 <input type="checkbox"/> 17:00 <input type="checkbox"/> 18:00 <input type="checkbox"/> 19:00 <input type="checkbox"/> 20:00 <input type="checkbox"/> 21:00 <input type="checkbox"/> 22:00 <input type="checkbox"/> 23:00 <input checked="" type="checkbox"/> Wait until no active client associated |
| Output Power | Max <input type="checkbox"/> Boost |
| Client Signal Strength Threshold | Disabled |
| Maximum number of clients | Unlimited |
| Discover Nearby Networks | <input checked="" type="checkbox"/> <small>Note: Feature will be automatically turned on with Auto Channel / Dynamic Output Power</small> |
| Beacon Rate | 1 Mbps |
| Beacon Interval | 100 ms |
| DTIM | 1 |
| RTS Threshold | 0 |
| Fragmentation Threshold | 0 (0: Disable) |
| Distance / Time Converter | <input type="text" value="4050"/> m <small>Note: Input distance for recommended values</small> |
| Slot Time | <input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="9"/> μ s |
| ACK Timeout | <input type="text" value="48"/> μ s |

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

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

| | |
|---|---|
| Client Signal Strength Threshold | This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts. |
| Max number of Clients | This field determines the maximum clients that can be connected to APs under this profile. |
| Management VLAN ID | This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is 0 by default, meaning that no VLAN tagging will be applied. Note: change this value with caution as alterations may result in loss of connection to the AP controller. |
| Discover Nearby Networks^A | This option is to turn on and off to scan the nearby the AP. Note: Feature will be automatically turned on with Auto Channel / Dynamic Output Power |
| Beacon Rate^A | This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, and 11Mbps . |
| Beacon Interval^A | This drop-down menu provides the option to set the time between each beacon send. Available options are 100ms, 250ms, and 500ms . |
| DTIM^A | This field provides the option to set the frequency for beacon to include delivery traffic indication message (DTIM). The interval unit is measured in milliseconds. |
| RTS Threshold^A | This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature. |
| Fragmentation Threshold^A | Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation. |
| Distance/Time Converter^A | Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended. |
| Slot Time^A | This field provides the option to modify the unit wait time before it transmits. The default value is 9µs . |
| ACK Timeout^A | This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is 48µs . |

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

Important Note

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

Integrated AP

Wi-Fi Operating Mode ? WAN WAN + AP AP

The device with integrated AP can operate under the Wi-Fi Operating Mode, and the default setting is **WAN + AP** mode:

Note: This option is available for selected devices only (HD2/HD4 and HD2/HD4 MBX).

| Integrated AP | |
|-----------------|--|
| WAN | <p>In this mode, all Wi-Fi will operate as Wi-Fi WAN and no integrated Wi-Fi AP will be operated on this device.</p> <p>If Wi-Fi Operating mode is choosing WAN, The status indicated by the front panel LED is as follows:</p> <ul style="list-style-type: none"> - Wi-Fi 1 is Green if Wi-Fi WAN 1 is enabled. - Wi-Fi 2 is Green if Wi-Fi WAN 2 is enabled. |
| WAN + AP | <p>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.</p> <p>If Wi-Fi Operating mode is choosing WAN + AP, The status indicated by the front panel LED is as follows:</p> <ul style="list-style-type: none"> - Wi-Fi 1 is Green if WI-FI WAN is enabled. - Wi-Fi 2 is Green if Wi-Fi AP is ON. |
| AP | <p>In this mode, all Wi-Fi functions as integrated Wi-Fi AP. All Wi-Fi WANs will be forced to go offline.</p> <p>If Wi-Fi Operating mode is choosing AP, The status indicated by the front panel LED is as follows:</p> <ul style="list-style-type: none"> - W-Fi 1 is Green, if there is any Wireless SSID is selected 2.4GHz. - W-Fi 2 is Green, if there is any Wireless SSID is selected 5GHz. |

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 | <input type="text" value="443"/> |
| HTTP to HTTPS Redirection | <input checked="" type="checkbox"/> |
| Admin Username | <input type="text" value="admin"/> |
| Admin Password | <input type="password" value="....."/> <input type="button" value="Generate"/> <input checked="" type="checkbox"/> Hide Characters |

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

| AP Time Settings | |
|------------------|--|
| Time Zone | <input checked="" type="radio"/> Follow controller time zone selection <input type="radio"/> (GMT-11:00) Midway Island ▼ |
| Time Server | <input checked="" type="radio"/> Follow controller NTP server selection <input type="radio"/> <input type="text"/> |

This allows users to configure AP Time Settings (both Timezone and NTP) in AP Controller.

| AP Time Settings | |
|--------------------|--|
| Time Zone | This field is to select the time zone for the AP controller. |
| Time Server | This field is to select the time server for the AP controller. |

| Controller Management Settings | |
|--------------------------------|--------------------------|
| Manage Unreachable Action | <input type="checkbox"/> |

This settings is to allow user to manage external AP's controller unreachable action. When **Manage Unreachable Action** is checked, there will have 2 options which are "**None**" and "**Radio Off**".

| AP Controller Settings | |
|------------------------|--------------------------|
| Client Load Balancing | <input type="checkbox"/> |

This is an option to enable client load balancing for AP Controller. When the option is enabled, it is trying to balance the station count on APs within the same profile.

Some Pepwave models displays a screen similar to the one shown below, navigating to **AP > Settings**:

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

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

| 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 |

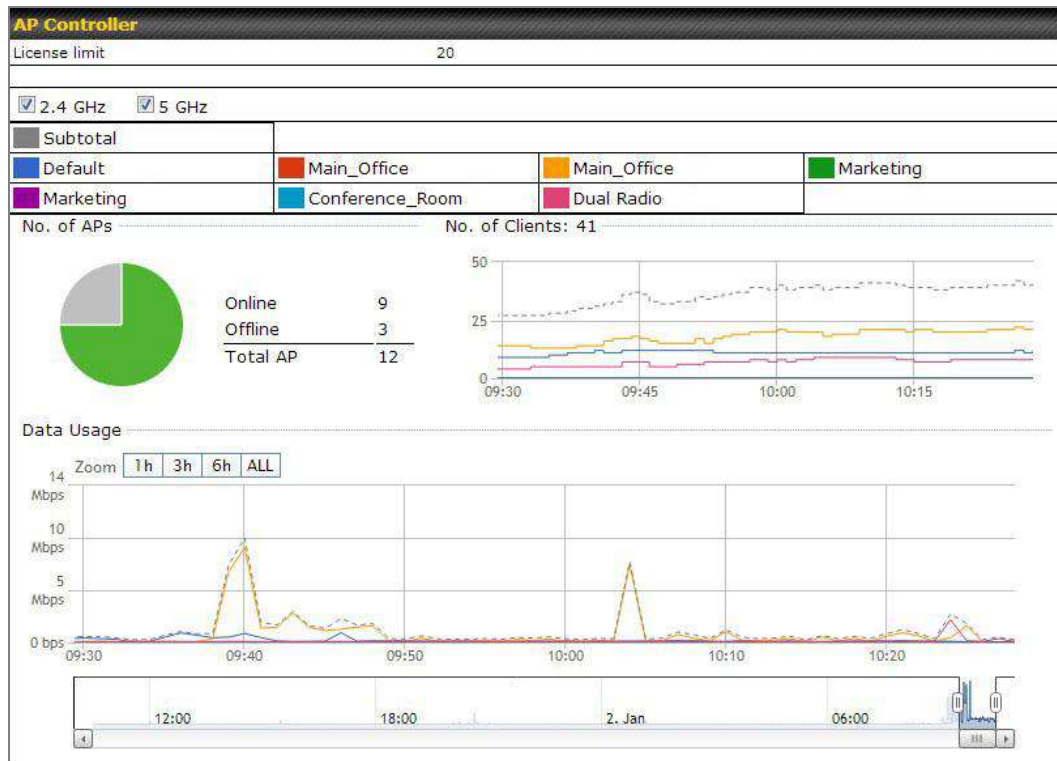
| Wi-Fi AP Settings | |
|-------------------|--|
| Protocol | This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are 802.11ng and 802.11na . By default, 802.11ng is selected. |

| | |
|--------------------------------------|--|
| Channel | This option allows you to select which 802.11 RF channel will be used. Channel 1 (2.412 GHz) is selected by default. |
| Channel Width | Auto (20/40 MHz) and 20 MHz are available. The default setting is Auto (20/40 MHz) , which allows both widths to be used simultaneously. |
| Output Power | This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – Max, High, Mid, and Low . The actual output power will be bound by the regulatory limits of the selected country. |
| Beacon Rate^A | This option is for setting the transmit bit rate for sending a beacon. By default, 1Mbps is selected. |
| Beacon Interval^A | This option is for setting the time interval between each beacon. By default, 100ms is selected. |
| DITM^A | This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to 1 ms . |
| Slot Time^A | This field is for specifying the wait time before the Router transmits a packet. By default, this field is set to 9 μs . |
| ACK Time^A | This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 μs . |
| Frame Aggreaction^A | This option allows you to enable frame aggregation to increase transmission throughput. |
| Guard Interval^A | This setting allows choosing a short or long guard period interval for your transmissions. |

26 AP Controller Status

26.1 Info

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



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

given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time.

Data Usage

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

| Events | | View Alerts |
|----------------|--|-----------------------------|
| Jan 2 11:01:11 | AP One 300M: Client 54:EA: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.

AP Time Settings

| | |
|-------------|---|
| Time Zone | <input checked="" type="radio"/> Follow controller time zone selection <input type="radio"/> (GMT-11:00) Midway Island |
| Time Server | <input checked="" type="radio"/> Follow controller NTP server selection <input type="radio"/> |

This allow user to configure AP Time Settings (both Timezone and NTP) in AP Controller.

AP Time Settings

| | |
|--------------------|--|
| Time Zone | This field is to select the time zone for the AP controller. |
| Time Server | This field is to select the time server for the AP controller. |

Controller Management Settings

Manage Unreachable Action

This settings is to allow user to manage external AP's controller unreachable action. When **Manage Unreachable Action** is checked, there will have 2 options which are "None" and "Radio Off".

AP Controller Settings

Client Load Balancing

This is an option to enable client load balancing for AP Controller. When the option is enabled, it is trying to balance the station count on APs within the same profile.

26.2 Access Point

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

Managed APs

| <input type="checkbox"/> | Name | IP Address | MAC | Location | Firmware | Radio Config. | Config. Sync. | |
|--------------------------|--------------------|------------|-----|----------|----------|---------------|---------------|--|
| <input type="checkbox"/> | MAX-BR1-85F4/29... | (Local) | - | - | - | | | |

Remove Offline Units Reboot Set Firmware

Managed APs

Managed APs

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

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

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

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

Close

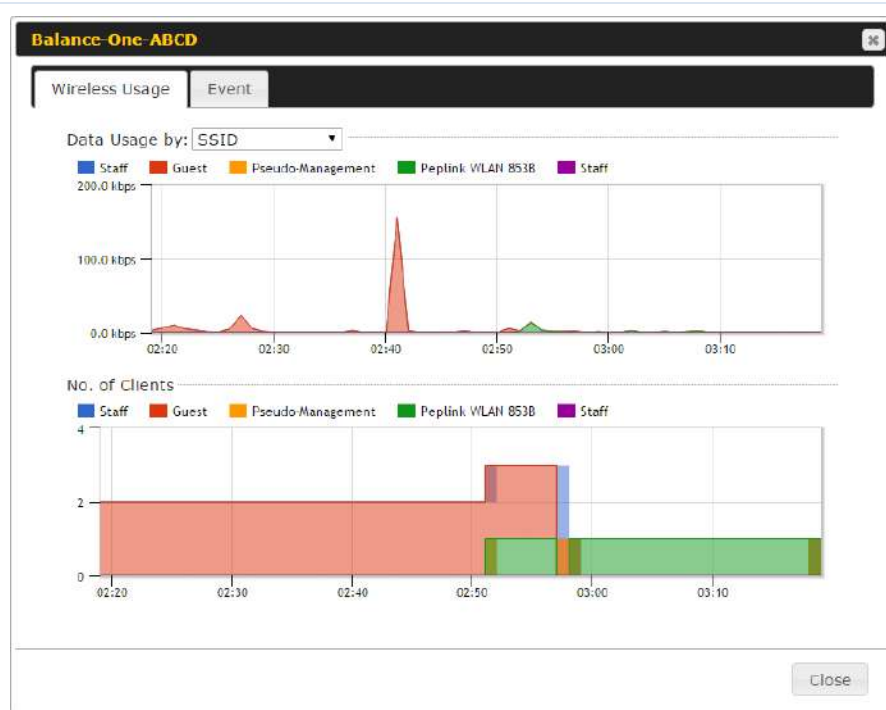
Click the icon to configure each client

| AP Details | |
|-----------------------------------|---|
| Serial Number | 1111-2222-3333 |
| MAC Address | 00:1A:DD:BD:73:E0 |
| Product Name | Pepwave AP Pro Duo |
| Name | <input type="text"/> |
| Location | <input type="text"/> |
| 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) 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.

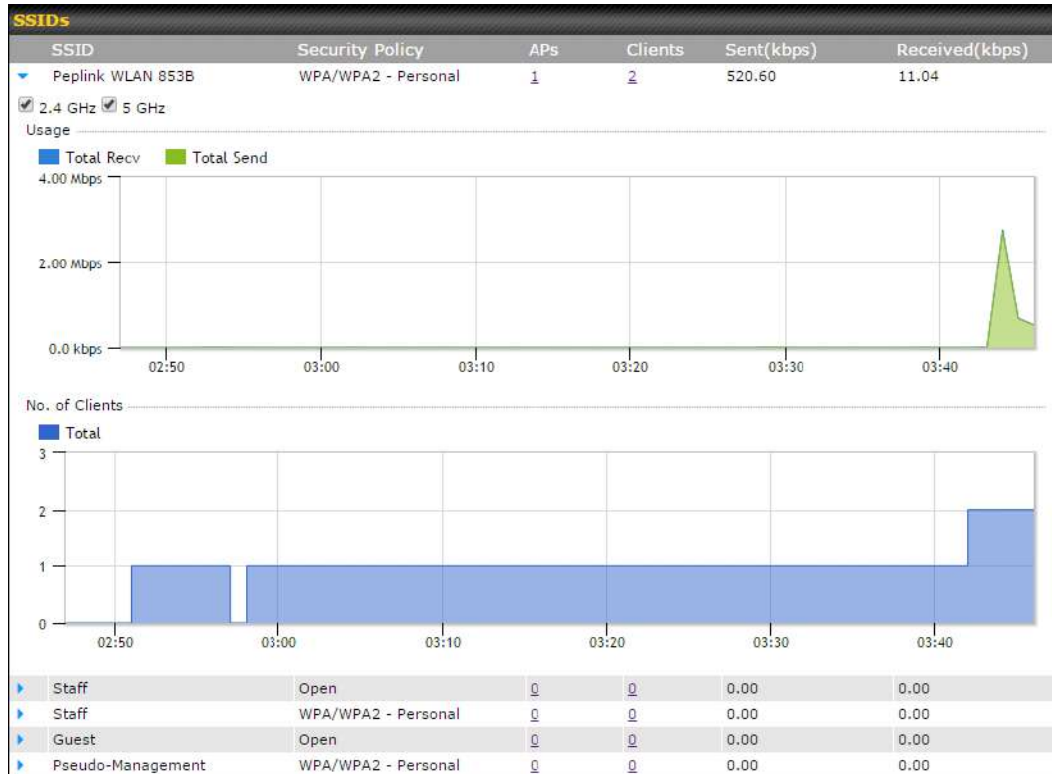
Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:

The "Event Information" window displays a list of events with the following columns: Time, Client MAC Address, and Action. The events are as follows:

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

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

Search Filter

| | |
|------------------------------|--|
| Search Key | Client MAC Address / SSID / AP Serial Number |
| Maximum Result (1-256) | 50 |
| Show Associated Clients Only | <input type="checkbox"/> |
| Search Result | |

Search

Wireless Clients

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

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

| Client | Upload | Download |
|----------------|--------|----------|
| No information | | |

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

Client C0:EE:FB:20:13:36

| Information | |
|---------------------------|---------------------|
| Status | Associated |
| Access Point | 1111-2222-3333 |
| SSID | Peplink WLAN 853B |
| IP Address | 192.168.1.34 |
| Duration | 00:27:31 |
| Usage (Upload / Download) | 141.28 MB / 4.35 MB |
| RSSI | -48 |
| Rate (Upload / Download) | 150M / 48M |
| Type | 802.11na |

■ Download ■ Upload

| SSID | AP | From | To | Upload | Download |
|-------------------|----------------|-----------------|-----------------|-----------|----------|
| Peplink WLAN 853B | 192C-1835-642F | Nov 23 03:43:04 | - | 141.28 MB | 4.35 MB |
| Peplink WLAN 853B | 192C-1835-642F | Nov 23 02:58:36 | Nov 23 03:47:52 | 173.7 KB | 94.2 KB |
| Peplink WLAN 853B | 192C-1835-642F | Nov 23 02:52:15 | Nov 23 02:58:15 | 105.9 KB | 62.5 KB |

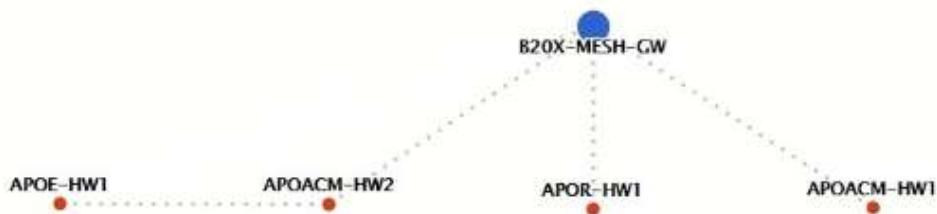
Close

26.5 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



26.6 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"/> hh:mm to <input type="text"/> hh:mm |
| Alerts only | <input type="checkbox"/> |
| <input type="button" value="Search"/> | |

| 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. 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 | | |

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

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 ? | |
|---|---|
| Device Name | MAX-BR1- hostname: max-br1 ⚙️ This configuration is being managed by InControl . |
| Admin User Name | <input type="text" value="admin"/> |
| Admin Password | <input type="password" value="••••••••"/> |
| Confirm Admin Password | <input type="password" value="••••••••"/> |
| Read-only User Name | <input type="text" value="user"/> |
| Read-only Password | <input type="password"/> |
| Confirm Read-only Password | <input type="password"/> |
| Web Session Timeout | 4 Hours 0 Minutes |
| Authentication Method | <input checked="" type="radio"/> Local Account <input type="radio"/> RADIUS <input type="radio"/> TACACS+ |
| CLI SSH & Console | <input checked="" type="checkbox"/> Enable |
| CLI SSH Access | LAN Only ▼ |
| CLI SSH Port | <input type="text" value="8822"/> |
| CLI SSH Access Public Key | Admin User: (Disabled) configure Read-only User: (Disabled) configure |
| Security | HTTP / HTTPS ▼ <input checked="" type="checkbox"/> Redirect HTTP to HTTPS |
| Web Admin Access | HTTP: LAN / WAN HTTPS: LAN / WAN ▼ |
| Web Admin Port | HTTP: <input type="text" value="80"/> HTTPS: <input type="text" value="443"/> |

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

| WAN Connection Access Settings | | | | | | | | | | | | | | | | | | | | | | |
|---|---|-----------------------------|-----|-------|------------------------------|--|--|-----------------------------------|--|--|---|--|--|---|--|--|-------------------------------------|--|--|--|--|--|
| Allowed Source IP Subnets | ? <input checked="" type="radio"/> Any <input type="radio"/> Allow access from the following IP subnets only | | | | | | | | | | | | | | | | | | | | | |
| Allowed WAN IP Address(es) | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Connection / IP Address(es)</th> <th style="text-align: center;">All</th> <th style="text-align: center;">Clear</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/> WAN</td><td></td><td></td></tr> <tr><td><input type="checkbox"/> Cellular</td><td></td><td></td></tr> <tr><td><input type="checkbox"/> Wi-Fi WAN on 2.4 GHz</td><td></td><td></td></tr> <tr><td><input type="checkbox"/> Wi-Fi WAN on 5 GHz</td><td></td><td></td></tr> <tr><td><input type="checkbox"/> VLAN WAN 1</td><td></td><td></td></tr> <tr><td><input type="checkbox"/> OpenVPN WAN 1</td><td></td><td></td></tr> </tbody> </table> | Connection / IP Address(es) | All | Clear | <input type="checkbox"/> WAN | | | <input type="checkbox"/> Cellular | | | <input type="checkbox"/> Wi-Fi WAN on 2.4 GHz | | | <input type="checkbox"/> Wi-Fi WAN on 5 GHz | | | <input type="checkbox"/> VLAN WAN 1 | | | <input type="checkbox"/> OpenVPN WAN 1 | | |
| Connection / IP Address(es) | All | Clear | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> WAN | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Cellular | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Wi-Fi WAN on 2.4 GHz | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Wi-Fi WAN on 5 GHz | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> VLAN WAN 1 | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> OpenVPN WAN 1 | | | | | | | | | | | | | | | | | | | | | | |

| Admin Settings | |
|--------------------|--|
| Device Name | This field allows you to define a name for this Pepwave router. By default, Device Name is set as MAX_XXXX , where XXXX refers to the last 4 digits of |

| | | | | | | | | | | | | | | | | | | | |
|-----------------------------------|--|-----------------------|---|-------------------------|------------|---------------------|----------------------|---------------------|------|-----------------------|--|-----------------|----------------------|-----------------|------|-------------------|--|------------------------|-----------|
| | the unit's serial number. | | | | | | | | | | | | | | | | | | |
| Admin User Name | Admin User Name is set as <i>admin</i> by default, but can be changed, if desired. | | | | | | | | | | | | | | | | | | |
| Admin Password | This field allows you to specify a new administrator password. | | | | | | | | | | | | | | | | | | |
| Confirm Admin Password | This field allows you to verify and confirm the new administrator password. | | | | | | | | | | | | | | | | | | |
| Read-only User Name | Read-only User Name is set as <i>user</i> by default, but can be changed, if desired. | | | | | | | | | | | | | | | | | | |
| Read-only Password | This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled. | | | | | | | | | | | | | | | | | | |
| Confirm Read-only Password | This field allows you to verify and confirm the new user password. | | | | | | | | | | | | | | | | | | |
| Web Session Timeout | This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to 4 hours . | | | | | | | | | | | | | | | | | | |
| Authentication Method | <p>With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.</p> <p>Available options:</p> <ul style="list-style-type: none"> Local Account RADIUS <table border="1"> <tr> <td>Authentication Method</td> <td><input type="radio"/> Local Account <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+</td> </tr> <tr> <td>Authentication Protocol</td> <td>MS-CHAP v2</td> </tr> <tr> <td>Authentication Host</td> <td><input type="text"/></td> </tr> <tr> <td>Authentication Port</td> <td>1812</td> </tr> <tr> <td>Authentication Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Accounting Host</td> <td><input type="text"/></td> </tr> <tr> <td>Accounting Port</td> <td>1813</td> </tr> <tr> <td>Accounting Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Authentication Timeout</td> <td>3 seconds</td> </tr> </table> <p>Authentication This specifies the authentication protocol used.</p> | Authentication Method | <input type="radio"/> Local Account <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ | Authentication Protocol | MS-CHAP v2 | Authentication Host | <input type="text"/> | Authentication Port | 1812 | Authentication Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | Accounting Host | <input type="text"/> | Accounting Port | 1813 | Accounting Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | Authentication Timeout | 3 seconds |
| Authentication Method | <input type="radio"/> Local Account <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ | | | | | | | | | | | | | | | | | | |
| Authentication Protocol | MS-CHAP v2 | | | | | | | | | | | | | | | | | | |
| Authentication Host | <input type="text"/> | | | | | | | | | | | | | | | | | | |
| Authentication Port | 1812 | | | | | | | | | | | | | | | | | | |
| Authentication Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | | | | | |
| Accounting Host | <input type="text"/> | | | | | | | | | | | | | | | | | | |
| Accounting Port | 1813 | | | | | | | | | | | | | | | | | | |
| Accounting Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | | | | | |
| Authentication Timeout | 3 seconds | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | |
|-------------------------------|---|-----------------------|---|------------------------------|--|-------------------------------|--|------------------------------|--|------------------------|--|------------------------|--|--------------------------|--|-------------------------------|---|
| | <table border="1"> <tr> <td>Protocol</td> <td>Available options are MS-CHAP v2 and PAP.</td> </tr> <tr> <td>Authentication Host</td> <td>This specifies the IP address or hostname of the RADIUS server host.</td> </tr> <tr> <td>Authentication Port</td> <td>This setting specifies the UDP destination port for authentication requests.</td> </tr> <tr> <td>Authentication Secret</td> <td>This field is for entering the secret key for accessing the RADIUS server.</td> </tr> <tr> <td>Accounting Host</td> <td>This specifies the IP address or hostname of the RADIUS server host.</td> </tr> <tr> <td>Accounting Port</td> <td>This setting specifies the UDP destination port for accounting requests.</td> </tr> <tr> <td>Accounting Secret</td> <td>This field is for entering the secret key for accessing the accounting server.</td> </tr> <tr> <td>Authentication Timeout</td> <td>This option specifies the time value for authentication timeout</td> </tr> </table> | Protocol | Available options are MS-CHAP v2 and PAP . | Authentication Host | This specifies the IP address or hostname of the RADIUS server host. | Authentication Port | This setting specifies the UDP destination port for authentication requests. | Authentication Secret | This field is for entering the secret key for accessing the RADIUS server. | Accounting Host | This specifies the IP address or hostname of the RADIUS server host. | Accounting Port | This setting specifies the UDP destination port for accounting requests. | Accounting Secret | This field is for entering the secret key for accessing the accounting server. | Authentication Timeout | This option specifies the time value for authentication timeout |
| Protocol | Available options are MS-CHAP v2 and PAP . | | | | | | | | | | | | | | | | |
| Authentication Host | This specifies the IP address or hostname of the RADIUS server host. | | | | | | | | | | | | | | | | |
| Authentication Port | This setting specifies the UDP destination port for authentication requests. | | | | | | | | | | | | | | | | |
| Authentication Secret | This field is for entering the secret key for accessing the RADIUS server. | | | | | | | | | | | | | | | | |
| Accounting Host | This specifies the IP address or hostname of the RADIUS server host. | | | | | | | | | | | | | | | | |
| Accounting Port | This setting specifies the UDP destination port for accounting requests. | | | | | | | | | | | | | | | | |
| Accounting Secret | This field is for entering the secret key for accessing the accounting server. | | | | | | | | | | | | | | | | |
| Authentication Timeout | This option specifies the time value for authentication timeout | | | | | | | | | | | | | | | | |
| | <ul style="list-style-type: none"> TACACS+ <table border="1"> <tr> <td>Authentication Method</td> <td><input type="radio"/> Local Account <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+</td> </tr> <tr> <td>TACACS+ Server</td> <td><input type="text"/></td> </tr> <tr> <td>TACACS+ Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>TACACS+ Server Timeout</td> <td><input type="text" value="3"/> seconds</td> </tr> </table> | Authentication Method | <input type="radio"/> Local Account <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+ | TACACS+ Server | <input type="text"/> | TACACS+ Server Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | TACACS+ Server Timeout | <input type="text" value="3"/> seconds | | | | | | | | |
| Authentication Method | <input type="radio"/> Local Account <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+ | | | | | | | | | | | | | | | | |
| TACACS+ Server | <input type="text"/> | | | | | | | | | | | | | | | | |
| TACACS+ Server Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | | | |
| TACACS+ Server Timeout | <input type="text" value="3"/> seconds | | | | | | | | | | | | | | | | |
| | <table border="1"> <tr> <td>TACACS+ Server</td> <td>This specifies the access address of the external TACACS+ server.</td> </tr> <tr> <td>TACACS+ Server Secret</td> <td>This field is for entering the secret key for accessing the RADIUS server.</td> </tr> <tr> <td>TACACS+ Server Timeout</td> <td>This option specifies the time value for TACACS+ timeout</td> </tr> </table> | TACACS+ Server | This specifies the access address of the external TACACS+ server. | TACACS+ Server Secret | This field is for entering the secret key for accessing the RADIUS server. | TACACS+ Server Timeout | This option specifies the time value for TACACS+ timeout | | | | | | | | | | |
| TACACS+ Server | This specifies the access address of the external TACACS+ server. | | | | | | | | | | | | | | | | |
| TACACS+ Server Secret | This field is for entering the secret key for accessing the RADIUS server. | | | | | | | | | | | | | | | | |
| TACACS+ Server Timeout | This option specifies the time value for TACACS+ timeout | | | | | | | | | | | | | | | | |
| CLI SSH & Console | The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to Section 30.5 . | | | | | | | | | | | | | | | | |
| CLI SSH Access | This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only. | | | | | | | | | | | | | | | | |

| | |
|----------------------------------|--|
| CLI SSH Port | This field determines the port on which clients can access CLI SSH. |
| CLI SSH Access Public Key | This field is for entering the Public Key for Admin Users and Read-only Users to access CLI SSH. |
| Security | <p>This option is for specifying the protocol(s) through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/HTTPS <p>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.</p> |
| Web Admin Access | <p>This option is for specifying the network interfaces through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> • LAN only • LAN/WAN <p>If LAN/WAN is chosen, the WAN Connection Access Settings form will be displayed.</p> |
| Web Admin Port | This field is for specifying the port number on which the web admin interface can be accessed. |

WAN Connection Access Settings

| | |
|----------------------------------|--|
| Allowed Source IP Subnets | <p>This field allows you to restrict web admin access only from defined IP subnets.</p> <ul style="list-style-type: none"> • Any - Allow web admin accesses to be from anywhere, without IP address restriction. • Allow access from the following IP subnets only - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath: |
|----------------------------------|--|

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

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

- 192.168.0.0/24
- 10.8.0.0/16

Allowed WAN IP Address(es)

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

28.2 Firmware

Web admin interface : automatically check for updates

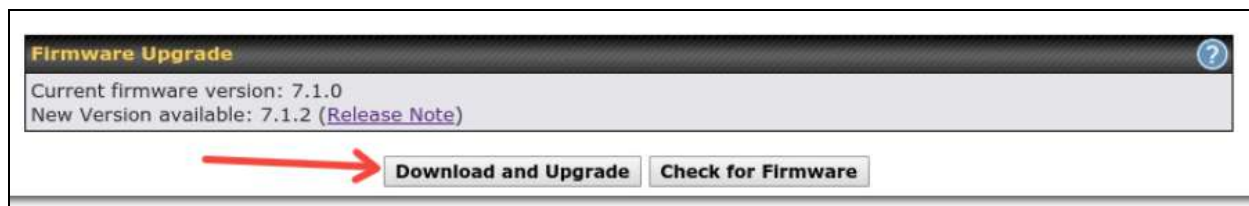
Upgrading firmware can be done in one of three ways.

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**.

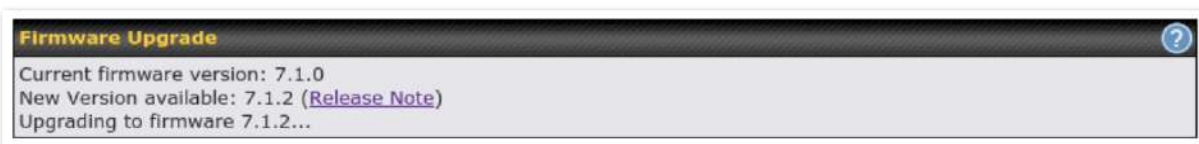


If an update is found the buttons will change to allow you to **Download and Update** the firmware.



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.



| Product | Hardware Revision | Firmware Version | Download Link | Release Notes | User Manual |
|--------------|-------------------|------------------|--------------------------|---------------------|---------------------|
| Balance 1350 | HW2 | 7.1.2 | Download | PDF | PDF |
| Balance 1350 | HW1 | 6.3.4 | Download | PDF | PDF |
| Balance 20 | HW1-6 | 7.1.2 | Download | PDF | PDF |
| Balance 210 | HW4 | 7.1.2 | Download | PDF | PDF |

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

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

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

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

Firmware Upgrade

It may take up to 8 minutes.



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

The InControl method

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

28.3 Time

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

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

| | |
|--------------------|---|
| Time Sync | <p>This field allows to select your time sync mode, the available options are:</p> <ul style="list-style-type: none"> • Time Server • GPS • GPS with Time Server as fallback |
| 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**

| Name | Time | Used by |
|---|------|---------|
| No schedule profiles defined. | | |
| <input type="button" value="New Schedule"/> | | |

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

Edit schedule profile ✕

Schedule Settings

| | |
|----------|--|
| Enable | <input checked="" type="checkbox"/> <small>The schedule function of those associated features will be lost if profile is disabled.</small> |
| Name | <input type="text" value="Weekdays Only"/> |
| Schedule | <input type="text" value="Weekdays only"/> |
| Used by | <small>You may go to supported feature settings page and set this profile as scheduler.</small> |

Schedule Map

| | Midnight | 4am | 8am | Noon | 4pm | 8pm |
|-----------|----------|-----|-----|------|-----|-----|
| Sunday | x | x | x | x | x | x |
| Monday | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Tuesday | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Wednesday | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Thursday | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Friday | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Saturday | x | x | x | x | x | x |

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

28.5 Email Notification

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

| Email Notification Setup ? | |
|---|--|
| Email Notification | <input checked="" type="checkbox"/> Enable |
| SMTP Server | smtp.mycompany.com <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 staff@mycompany.com ➤ |

| Email Notification Settings | |
|-----------------------------|---|
| Email Notification | This setting specifies whether or not to enable email notification. If Enable is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If Enable is not checked, email notification is disabled and the Pepwave router will not send email messages. |

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

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

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

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

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

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

Test 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"/> |
| Source Network Address | Untagged LAN ▼ |
| Push Events to Mobile Devices | |
| Push Events | <input type="checkbox"/> |
| URL Logging | |
| Enable | <input type="checkbox"/> |
| Session Logging | |
| Enable | <input type="checkbox"/> |
| <input type="button" value="Save"/> | |

| Event Log Settings | |
|-------------------------------|--|
| Remote Syslog | This setting specifies whether or not to log events at the specified remote syslog server. |
| Remote Syslog Host | This setting specifies the IP address or hostname of the remote syslog server. |
| Source Network Address | Via drop-down list, you may choose the LAN interface for Event Log, URL Logging, Sessions Logging and RADIUS. |
| Push Events | The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature. |
| URL Logging | This setting is to enable event logging at the specified log server. |
| URL Logging Host | This setting specifies the IP address or hostname of the URL log server. |

Session Logging This setting is to enable event logging at the specified log server.

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



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

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

SNMP Device This field shows the router name defined at **System > Admin Security**.

| Name | |
|-----------------------------------|--|
| SNMP Port | This option specifies the port which SNMP will use. The default port is 161 . |
| SNMPv1 | This option allows you to enable SNMP version 1. |
| SNMPv2 | This option allows you to enable SNMP version 2. |
| SNMPv3 | This option allows you to enable SNMP version 3. |
| SNMP Trap | This option allows you to enable SNMP Trap. If enabled, the following entry fields will appear. |
| SNMP Trap Community | This setting specifies the SNMP Trap community name. |
| SNMP Trap Server | Enter the IP address of the SNMP Trap server. |
| SNMP Trap Port | This option specifies the port which the SNMP Trap server will use. The default port is 162 . |
| SNMP Trap Server Heartbeat | 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 | <input type="text" value="My Company"/> |
| Allowed Network | <input type="text" value="192.168.1.25"/> / <input type="text" value="255.255.255.0 (/24)"/> ▾ |

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

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

SNMPv3 User
✕

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

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

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*

| SMS Control | |
|-------------|--------------------------|
| Enable | <input type="checkbox"/> |

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="text"/> <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 type="button" value="+"/></td> </tr> </tbody> </table> | Phone Number | | <input type="text"/> | <input type="button" value="+"/> |
| Phone Number | | | | | |
| <input type="text"/> | <input type="button" value="+"/> | | | | |

| SMS Control Settings | |
|----------------------|---|
| Enable | Click the checkbox to enable the SMS Control. |
| Password | This setting sets the password for authentication - maximum of 32 characters, which cannot include semicolon (;). |
| White List | 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 type="button" value="InControl"/> <input type="checkbox"/> Restricted to Status Reporting Only |
| Privately Host InControl | <input checked="" type="checkbox"/> |
| InControl Host | Primary: <input type="text"/> Backup: <input type="text"/> <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.

Restore Configuration to Factory Settings ?

Download Active Configurations ?

Upload Configurations ?

| | |
|---------------------------------------|--|
| Configuration File | <input type="button" value="Browse_"/> No file selected. |
| <input type="button" value="Upload"/> | |

Upload Configurations from High Availability Pair ?

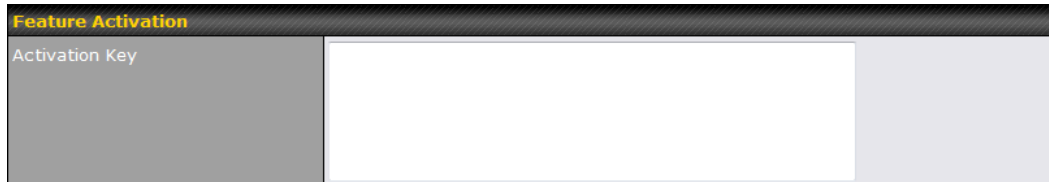
| | |
|---------------------------------------|--|
| Configuration File | <input type="button" value="Browse_"/> No file selected. |
| <input type="button" value="Upload"/> | |

| Configuration | |
|---------------------------------|--|
| Restore Configuration to | The Restore Factory Settings button is to reset the configuration to factory default settings. After clicking the button, you will need to click the Apply |

| | |
|--|---|
| Factory Settings | Click Changes button on the top right corner to make the settings effective. |
| Download Active Configurations | Click Download to backup the current active settings. |
| Upload Configurations | To restore or change settings based on a configuration file, click Choose File to locate the configuration file on the local computer, and then click Upload . The new settings can then be applied by clicking the Apply Changes button on the page header, or you can cancel the procedure by pressing discard on the main page of the web admin interface. |
| Upload Configurations from High Availability Pair | In a high availability (HA) configuration, a Pepwave router can quickly load the configuration of its HA counterpart. To do so, click the Upload button. After loading the settings, configure the LAN IP address of the Pepwave router so that it is different from the HA counterpart. |

28.11 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**.

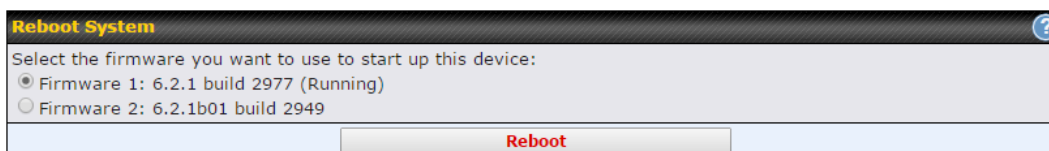


The screenshot shows a web form titled "Feature Activation". It contains a single input field labeled "Activation Key" which is currently empty.

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 form titled "Reboot System" with a help icon in the top right corner. The text reads "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 "Reboot" button.

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 <input type="range" value="5"/> |
| <input type="button" value="Start"/> <input type="button" value="Stop"/> | |

| 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**.

Traceroute

| | |
|-------------|---------------|
| Connection | WAN 1 |
| Destination | 64.233.189.99 |

Results

```

Traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 60 bytes packet size
 0 10.0.0.1 [10.0.0.1] <10.0.0.1> 0.100 ms 0.472 ms 0.287 ms
 1 10.0.0.254 [10.0.0.254] 0.019 ms 0.289 ms 0.498 ms
 2 10.0.0.254 [10.0.0.254] 0.019 ms 0.289 ms 0.498 ms
 3 10.0.0.1 [10.0.0.1] 0.075 ms 0.322 ms 0.560 ms
 4 10.0.0.2 [10.0.0.2] 0.082 ms 0.282 ms 0.289 ms
 5 10.0.0.254 [10.0.0.254] 0.284 ms 1.791.249.22 [10.0.0.254] 0.707 ms 1.083.00.254 [10.0.0.254] 0.472 ms
 6 192.75.48.129 [192.75.48.129] 0.688 ms 1.083.00.254 [1.083.00.254] 0.282 ms 0.282 ms
 7 209.128.1.158 [209.128.1.158] 0.201 ms 7.488 ms 7.488 ms
 8 209.176.0.244 [209.176.0.244] 0.811 ms 209.128.0.1 [209.128.0.1] 0.472 ms 192.75.48.129 [192.75.48.129] 0.282 ms
 9 209.128.0.228 [209.128.0.228] 0.238 ms 75.14.244.240 [75.14.244.240] 0.481 ms 209.128.0.228 [209.128.0.228] 0.478 ms
10 75.14.244.240 [75.14.244.240] 0.842 ms 75.128.48.129 [75.128.48.129] 0.877 ms 75.14.233.20 [75.14.233.20] 0.584 ms
11 75.14.233.20 [75.14.233.20] 0.584 ms 209.85.243.182 [209.85.243.182] 7.313 ms 209.85.243.30 [209.85.243.30] 0.484 ms
12 209.85.243.30 [209.85.243.30] 0.875 ms 209.85.243.182 [209.85.243.182] 0.888 ms 0.584 ms
13 209.85.243.182 [209.85.243.182] 0.882 ms 7.302 ms
14 64.233.189.99 [64.233.189.99] 0.170 ms 0.244 ms 0.202 ms
                    
```

Tip

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

29.3 Wake-on-LAN

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

Wake-on-LAN

| | | |
|--------------------|-------------------------------|-------------------------------------|
| Wake-on-LAN Target | 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”

29.4 WAN Analysis

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

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

WAN Performance Analysis

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

As a server

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

As a client

For the peer to initiate connection.

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

WAN Performance Analysis

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

Server Settings

| | |
|--|--|
| Status | <input checked="" type="checkbox"/> Listening (Control Port: 6000) |
| Control Port | <input type="text" value="6000"/> |
| <input type="button" value="Apply"/> <input type="button" value="Stop"/> | |

WAN Connection Status

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

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

WAN Performance Analysis

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

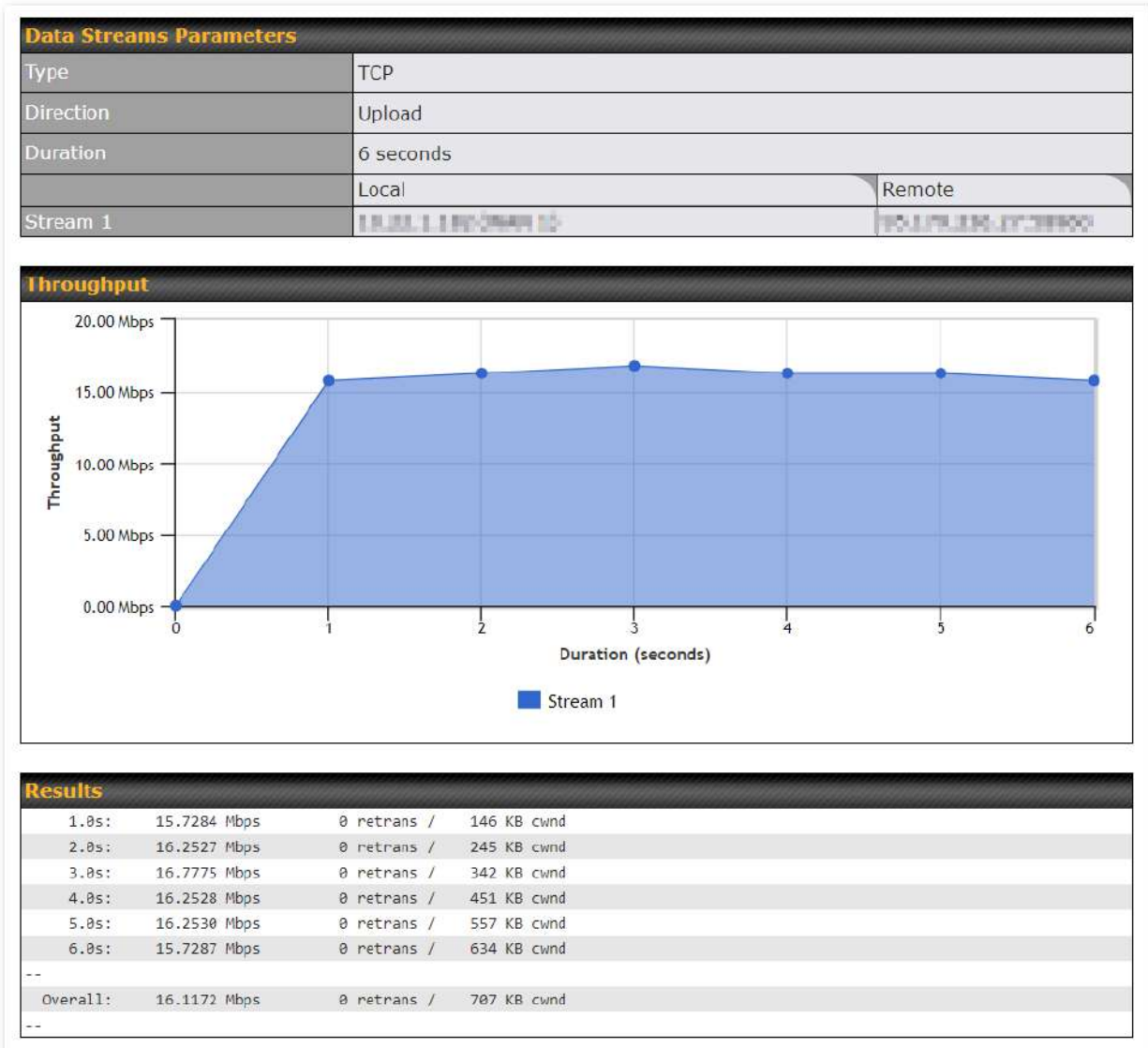
Client Settings

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

Data Streams

| Local WAN Connection | Remote IP Address |
|----------------------|----------------------|
| 1. -- Not Used -- | <input type="text"/> |
| 2. -- Not Used -- | <input type="text"/> |
| 3. -- Not Used -- | <input type="text"/> |
| 4. -- Not Used -- | <input type="text"/> |
| 5. -- Not Used -- | <input type="text"/> |
| 6. -- Not Used -- | <input type="text"/> |
| 7. -- Not Used -- | <input type="text"/> |
| 8. -- Not Used -- | <input type="text"/> |

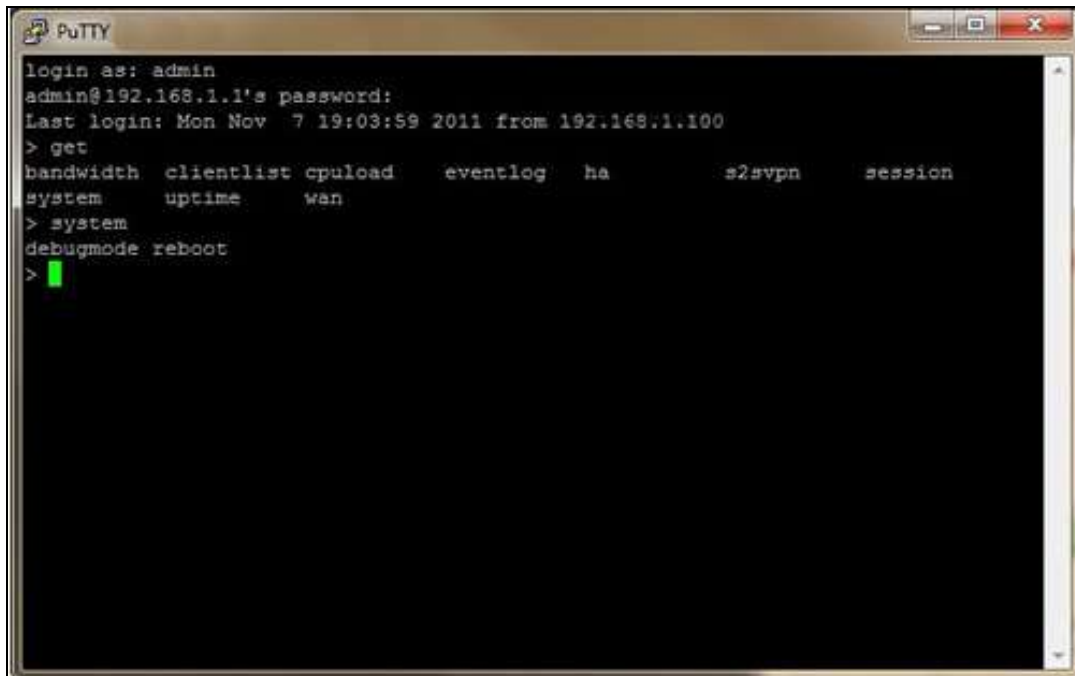
The test output will show the **Data Streams Parameters**, the **Throughput** as a graph, and the **Results**.



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

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.



```
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 | [REDACTED] |
| Model | Pepwave MAX BR1 Pro 5G |
| Product Code | [REDACTED] |
| Hardware Revision | 1 |
| Serial Number | [REDACTED] |
| Firmware | 8.3.0 build 5229 |
| SpeedFusion VPN Version | 9.2.0 |
| Host Name | [REDACTED] |
| Uptime | 2 minutes |
| System Time | Mon Feb 20 11:25:42 +08 2023 |
| GPS File | 2023-02-03 <input type="button" value="Download"/> |
| Diagnostic Report | Download |
| Remote Assistance | Turn On for <input type="text" value="7"/> days |
| MAC Address | |
| LAN | [REDACTED] |
| WAN | [REDACTED] |
| Wi-Fi WAN on 5 GHz | [REDACTED] |
| PepVPN NAT Mode | [REDACTED] |
| Legal | |

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

| | |
|--|---|
| Serial Number | This shows the serial number of this device. |
| Firmware | This shows the firmware version this device is currently running. |
| SpeedFusion VPN Version | This shows the current SpeedFusion VPN version. |
| Modem Support Version | This shows the modem support version. For a list of supported modems, click Modem Support List . |
| InControl Managed Configuration | InControl Managed Configurations (firmware, VLAN, Captive Portal, etcetera) |
| Host Name | The host name assigned to the Pepwave router appears here. |
| Uptime | This shows the length of time since the device has been rebooted. |
| System Time | This shows the current system time. |
| OpenVPN Client Profile | Link to download OpenVpn Client profile when this is enabled in Remote User Access |
| Diagnostic Report | The Download link is for exporting a diagnostic report file required for system investigation. |
| Remote Assistance | This option is to Turn on remote assistance with the time duration. |

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

30.2 GPS Data

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

GPS enabled models automatically store up to seven days of GPS location data in GPS eXchange format (GPX). To review this data using third-party applications, click **Status > Device** and then download your GPX file.

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

30.3 Active Sessions

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

| Overview | | Search | |
|--|------------------|-------------------|--|
| Session data captured within one minute. Refresh | | | |
| Service | Inbound Sessions | Outbound Sessions | |
| AIM/ICQ | 0 | 1 | |
| Bittorrent | 0 | 32 | |
| DNS | 0 | 51 | |
| Flash | 0 | 1 | |
| HTTPS | 0 | 76 | |
| Jabber | 0 | 5 | |
| MSN | 0 | 11 | |
| NTP | 0 | 4 | |
| QQ | 0 | 1 | |
| Remote Desktop | 0 | 3 | |
| SSH | 0 | 12 | |
| SSL | 0 | 64 | |
| XMPP | 0 | 4 | |
| Yahoo | 0 | 1 | |
| Interface | Inbound Sessions | Outbound Sessions | |
| WAN 1 | 0 | 176 | |
| WAN 2 | 0 | 32 | |
| Wi-Fi WAN | 0 | 51 | |
| Cellular 1 | 0 | 64 | |
| Cellular 2 | 0 | 0 | |
| USB | 0 | 0 | |
| Top Clients | | | |
| Client IP Address | Total Sessions | | |
| 10.9.66.66 | 1069 | | |
| 10.9.98.144 | 147 | | |
| 10.9.2.18 | 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"/> 1 WAN 1 <input type="checkbox"/> 2 WAN 2 <input type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> 1 Cellular 1 <input type="checkbox"/> 2 Cellular 2 <input type="checkbox"/> USB <input type="checkbox"/> VPN | | |

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 Online Clients Only 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 | |
| 192.168.50.12 | | max-hd2-██████ | 0 | 3 | ██████████ | | | |

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 Online Clients Only 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 | |
| 192.168.50.12 | | max-hd2-██████ | 0 | 0 | ██████████ | | | |

Scale: kbps Mbps


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

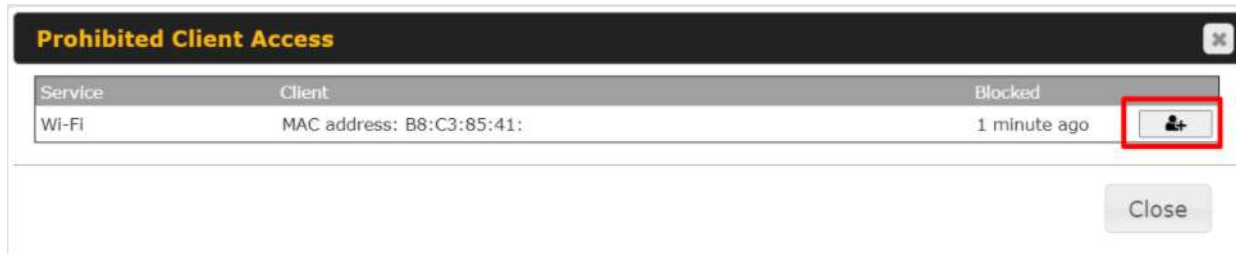
Filter Online Clients Only DHCP Clients Only

[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 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**.

| 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 |  |

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**.

30.6 OSPF & RIPv2

The table shows status of OSPF and RIPv2.

The screenshot shows the Peplink management interface. The 'Status' tab is selected, and the 'OSPF & RIPv2' section is expanded. A table displays the configuration for the 'PepVPN' area (0.0.0.0).

| Area | Remote Networks |
|-------------------|---|
| 0.0.0.0 PepVPN | 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 |

30.7 BGP

The table shows status of BGP

The screenshot shows the Peplink management interface. The 'Status' tab is selected, and the 'BGP' section is expanded. A table displays the configuration for BGP neighbors.

| Profile | Neighbor |
|---------|----------------|
| | No information |

30.8 SpeedFusion VPN

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

Details about SpeedFusion VPN connection peers appears as below:

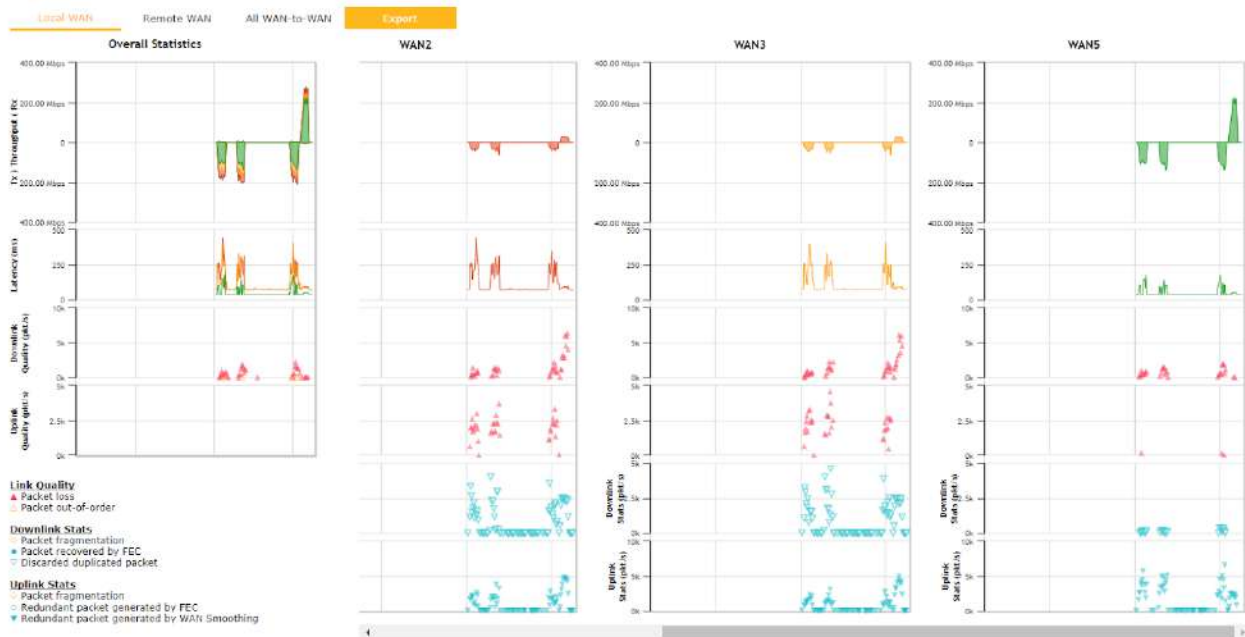
The screenshot shows the 'SpeedFusion VPN - Remote Peer' configuration page. It includes a search bar and a table listing remote peers.

| Remote Peer | Profile | Information |
|-----------------------------|---------------------------|-------------|
| FSH-B987 (FusionHub_SG) | FusionHub_SG (1) | [Redacted] |
| FSH-B987 (FusionHub_SG) | FusionHub_SG (2 - Tunn... | [Redacted] |
| SFC-SIN-H018 (SFC-SIN-H018) | SFH-SHARE-SIN | [Redacted] |

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

| SpeedFusion VPN - Remote Peer Show all profiles | | |
|--|--|---|
| Search <input type="text"/> | | |
| Remote Peer | Profile | Information |
| FSH-B987 (FusionHub_SG) | FusionHub_SG (1) | |
| WAN Cellular Wi-Fi WAN Total | Rx: < 1 kbps Tx: < 1 kbps Rx: < 1 kbps Tx: < 1 kbps | Loss rate: 0.0 pkt/s Latency: 11 ms Not available - WAN down Not available - WAN disabled Loss rate: 0.0 pkt/s |
| FSH-B987 (FusionHub_SG) | FusionHub_SG (2 - Tunn... | |
| SFC-SIN-H018 (SFC-SIN-H018) | SFH-SHARE-SIN | |

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:

SpeedFusion VPN Details ✕

Connection Information More information

| | |
|---------------|------------------|
| Profile | FusionHub_SG (1) |
| Remote ID | FusionHub_SG |
| Device Name | ██████████ |
| Serial Number | ██████████ |

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 | | | | |
| ■ WAN | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: 0.0 pkt/s Latency: 11 ms |
| ■ Cellular | Not available - WAN down | | | | |
| ■ Wi-Fi WAN | Not available - WAN disabled | | | | |
| Total | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: 0.0 pkt/s |

SpeedFusion VPN Test Configuration ?

| | | |
|-----------|--|---|
| Type | <input checked="" type="radio"/> TCP <input type="radio"/> UDP | <div style="border: 1px solid #ccc; padding: 5px; width: 40px; margin: auto;">Start</div> |
| Streams | 4 ▼ | |
| Direction | <input checked="" type="radio"/> Upload <input type="radio"/> Download | |
| Duration | 20 seconds (5 - 600) | |

SpeedFusion VPN Test Results

No information

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

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

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

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

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

The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15

minutes without any action.

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

| WAN Statistics | | | | | | | |
|--|---|--------------|----------------------|----------------|--|--|--|
| Remote Connections | <input checked="" type="checkbox"/> Show remote connections | | | | | | |
| WAN Label | <input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port | | | | | | |
| <input type="checkbox"/> BT | | | | | | | |
| <input checked="" type="checkbox"/> WAN | Rx: < 1 kbps | Tx: < 1 kbps | Loss rate: 0.0 pkt/s | Latency: 17 ms | | | |
| <input checked="" type="checkbox"/> Virgin Media | Not available - WAN disabled | | | | | | |

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

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

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

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

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

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

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

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

30.9 Event Log



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

30.9.1 Device Event Log




The screenshot shows the 'Device Event Log' interface. At the top, there are three tabs: 'Device', 'Firewall', and 'SpeedFusion VPN'. The 'Device' tab is selected. Below the tabs, the title 'Device Event Log' is displayed in orange, followed by a trash icon and a refresh icon. The main area contains a list of events with the following entries:

| Timestamp | Event Description |
|-----------------|--|
| Dec 30 10:43:07 | [Redacted] |
| Dec 29 16:59:31 | [Redacted] |
| Dec 29 16:57:13 | [Redacted] |
| Dec 29 16:56:47 | System: Time synchronization successful (0.pepwave.pool.ntp.org) |
| Dec 29 16:56:28 | SpeedFusion: SpeedFusion Cloud license expired |
| Dec 29 16:56:23 | System: Time synchronization successful (InControl) |
| Jan 01 08:03:50 | System: Wi-Fi AP Normal Mode |
| Jan 01 08:03:36 | [Redacted] |
| Jan 01 08:02:46 | System: Time synchronization fail |
| Jan 01 08:01:56 | System: Started up (8.3.0 build 5244) |
| Jan 01 08:01:50 | System: Started up (8.2.1 build 5195) |
| Jan 01 08:01:45 | System: Started up (8.3.0 build 5234) |
| Dec 29 16:23:11 | System: Reboot from Web |
| Dec 29 16:21:15 | [Redacted] |
| Dec 29 16:17:54 | [Redacted] |
| Dec 29 12:13:01 | [Redacted] |
| Dec 29 12:12:51 | [Redacted] |
| Dec 29 11:36:31 | [Redacted] |
| Dec 29 11:36:14 | [Redacted] |
| Dec 29 09:52:15 | [Redacted] |

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


30.9.2 Firewall Event log

| Time | Event |
|-----------------|---|
| Nov 15 02:48:07 | [82937.373922] Firewall: Denied PROTO=TCP SPT=55887 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1 |
| Nov 15 02:48:04 | [82934.377179] Firewall: Denied PROTO=TCP SPT=55887 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1 |
| Nov 15 02:47:07 | [82877.028738] Firewall: Denied PROTO=TCP SPT=55873 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1 |
| Nov 15 02:47:04 | [82874.033025] Firewall: Denied PROTO=TCP SPT=55873 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1 |
| Nov 15 02:46:07 | [82817.043526] Firewall: Denied PROTO=TCP SPT=55843 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1 |
| Nov 15 02:46:04 | [82814.047141] Firewall: Denied PROTO=TCP SPT=55843 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1 |

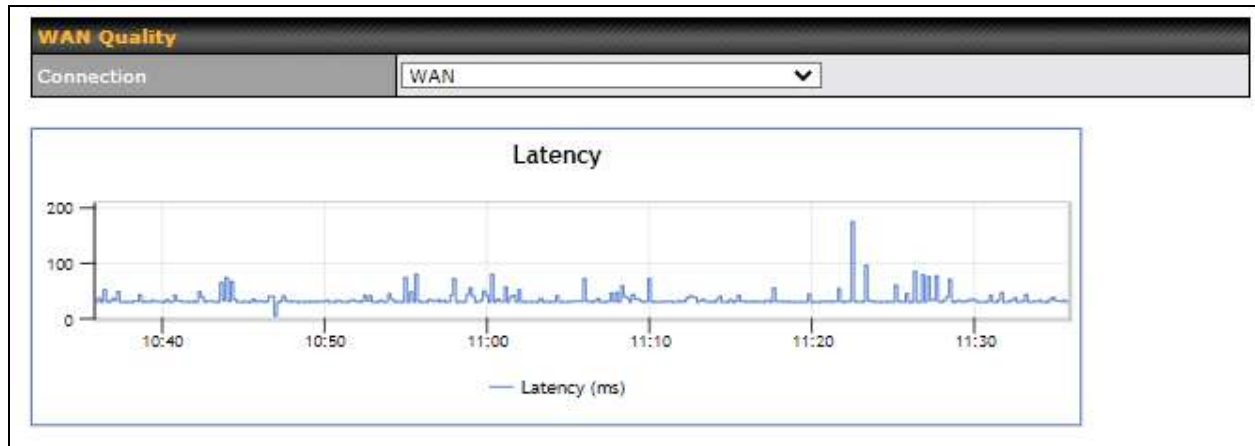
This section displays a list of events that have taken place within a firewall. Click the  button and the log will be refreshed.

30.9.3 SpeedFusion VPN Event log

| Time | Event |
|-----------------|---|
| Dec 29 16:57:17 | SpeedFusion: SFC-SIN-H018 |
| Dec 29 16:56:43 | SpeedFusion: SFH-SHARE-SIN failed to establish connection |
| Dec 29 16:56:42 | SpeedFusion: |
| Dec 29 16:56:38 | SpeedFusion: SFC-SIN-H018 failure detected (link) |
| Jan 01 08:04:00 | SpeedFusion: FusionHub_SG |
| Jan 01 08:03:53 | SpeedFusion: suite TLS_AES_256_GCM_SHA384 |
| Jan 01 08:03:51 | SpeedFusion: |
| Jan 01 08:03:48 | SpeedFusion: |
| Jan 01 08:03:43 | SpeedFusion: suite TLS_AES_256_GCM_SHA384 |

This section displays a list of events that have taken place within a SpeedFusion VPN connection. Click the  button and the log will be refreshed.

31 WAN Quality



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

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

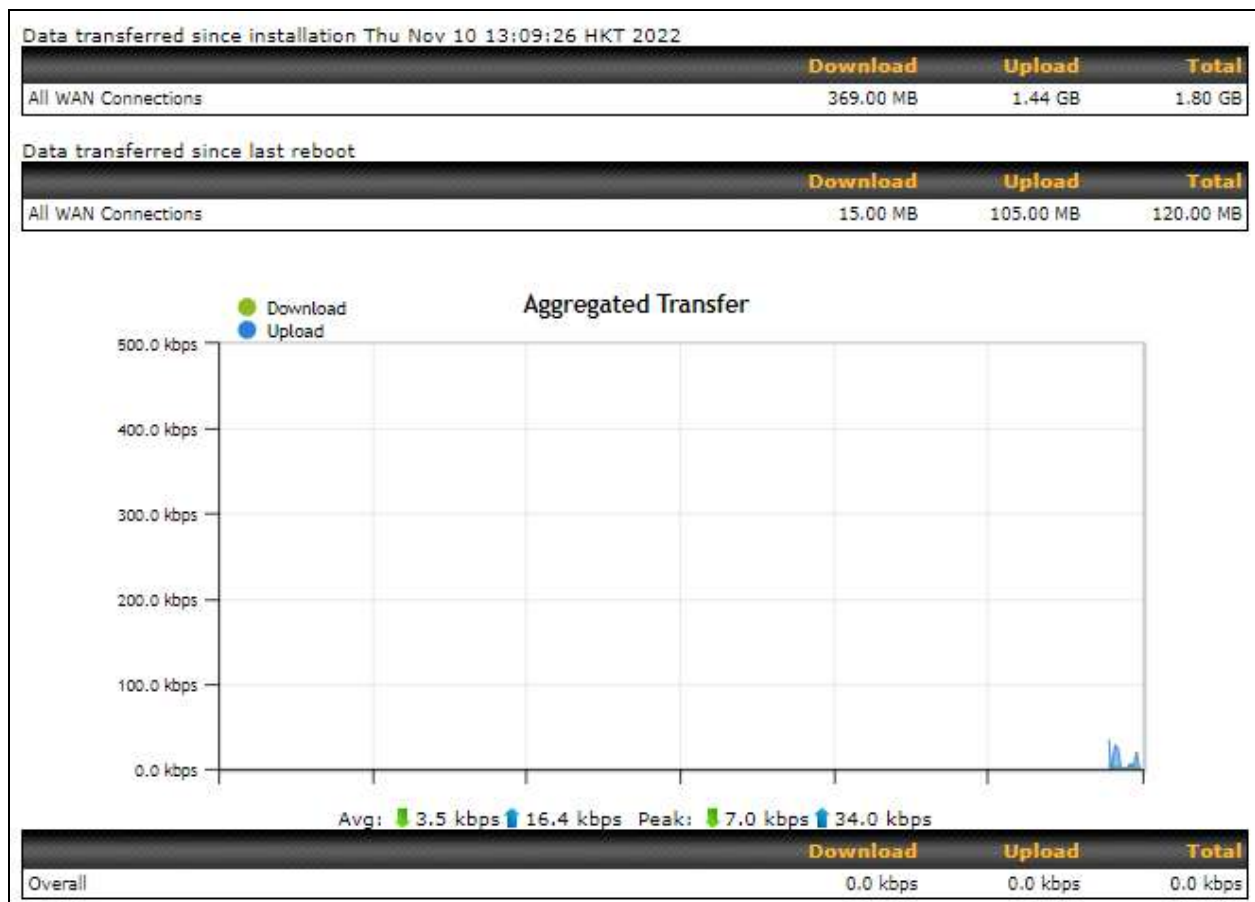
32 Usage Reports

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

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

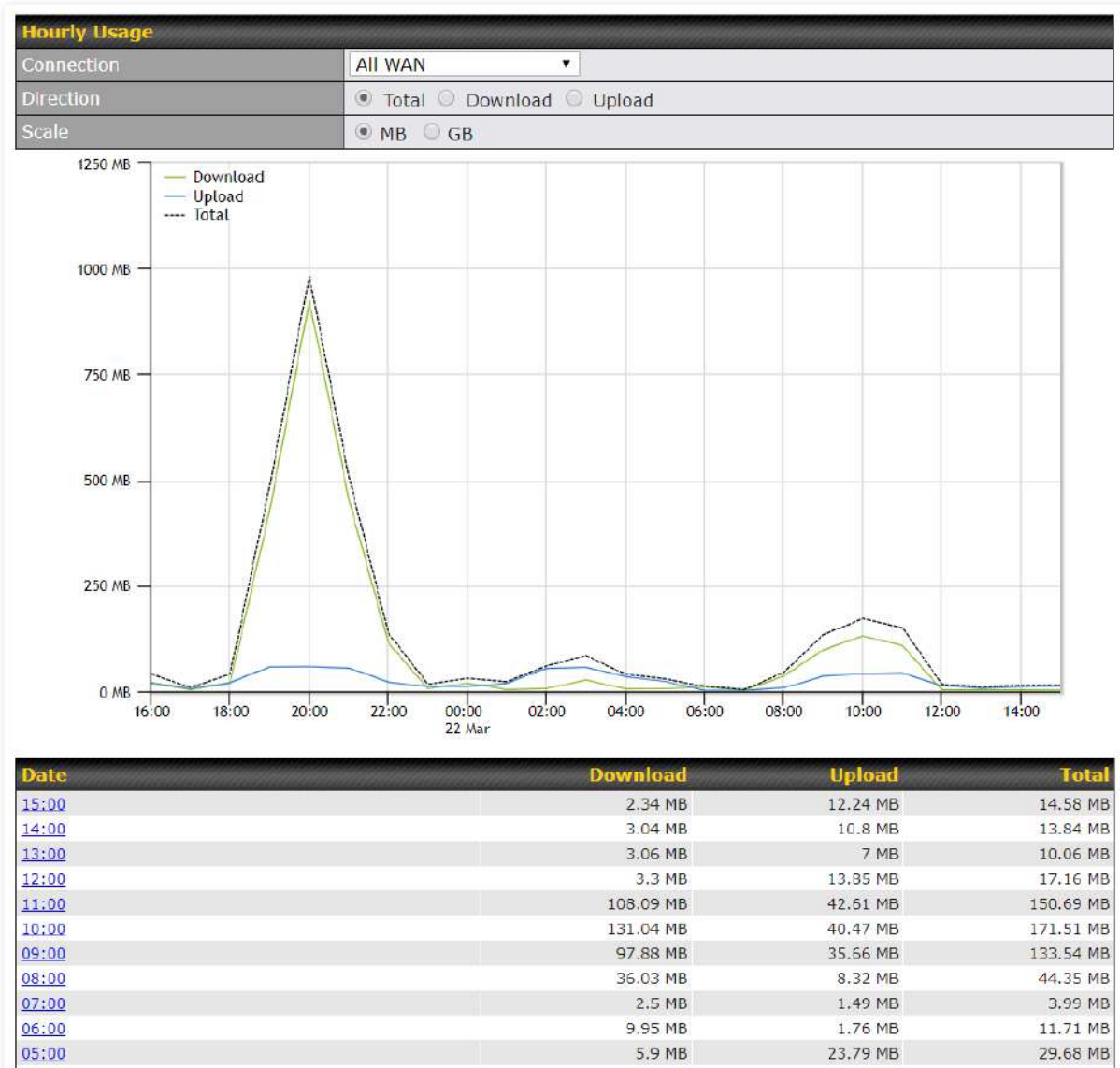
32.1 Real-Time

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



32.2 Hourly

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

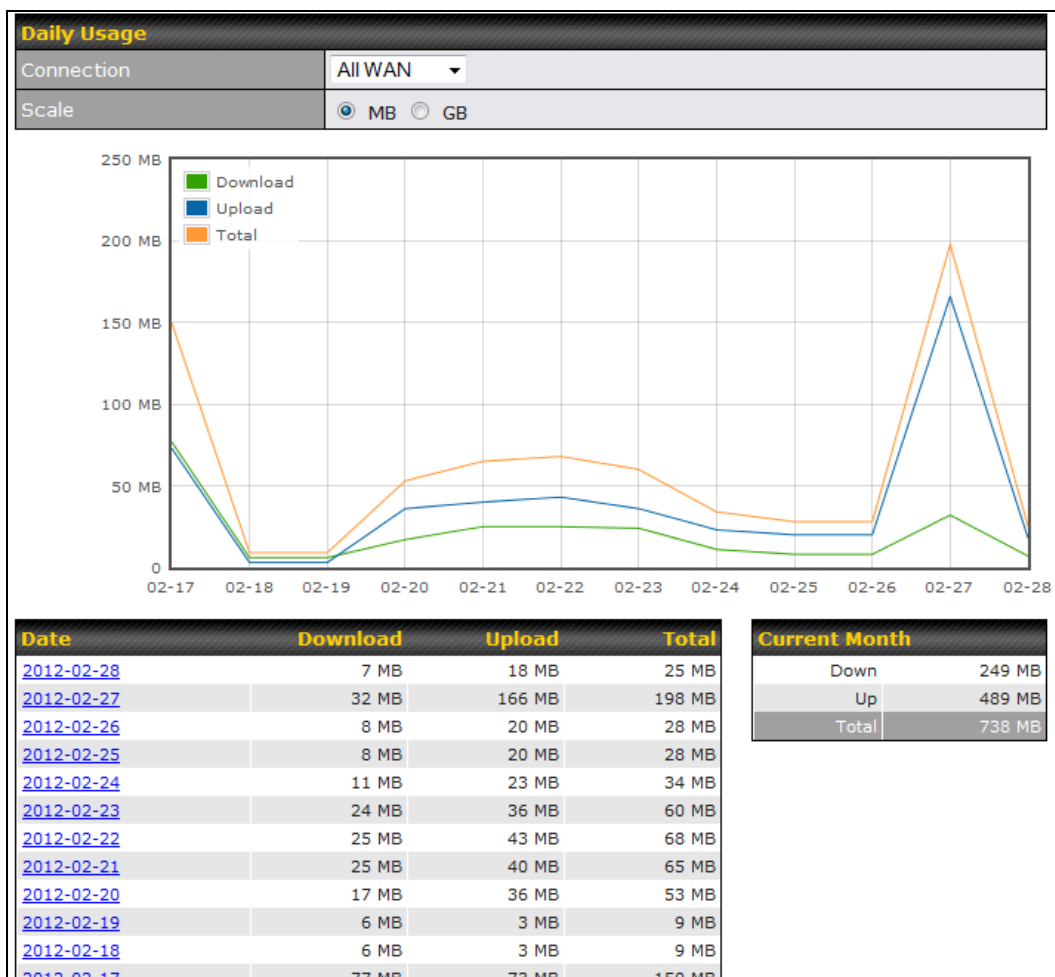


32.3 Daily

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

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

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

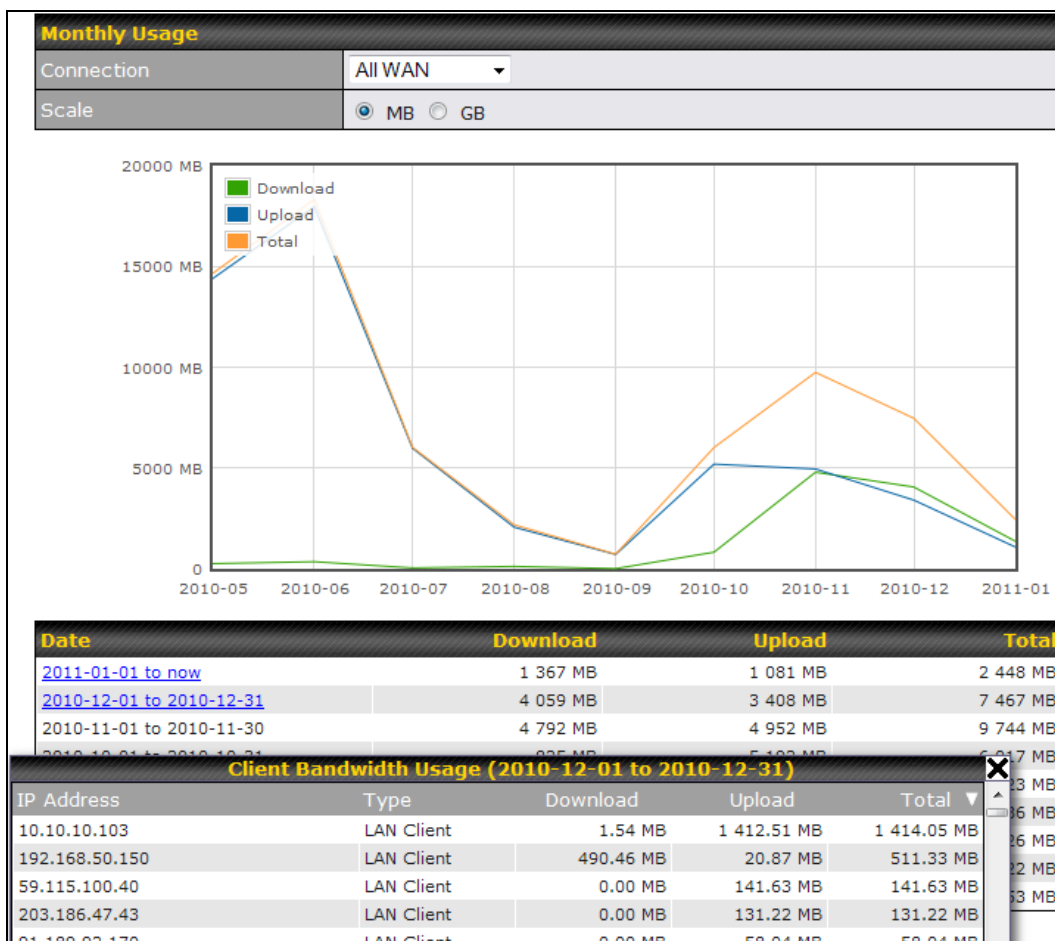


All WAN Daily Bandwidth Usage

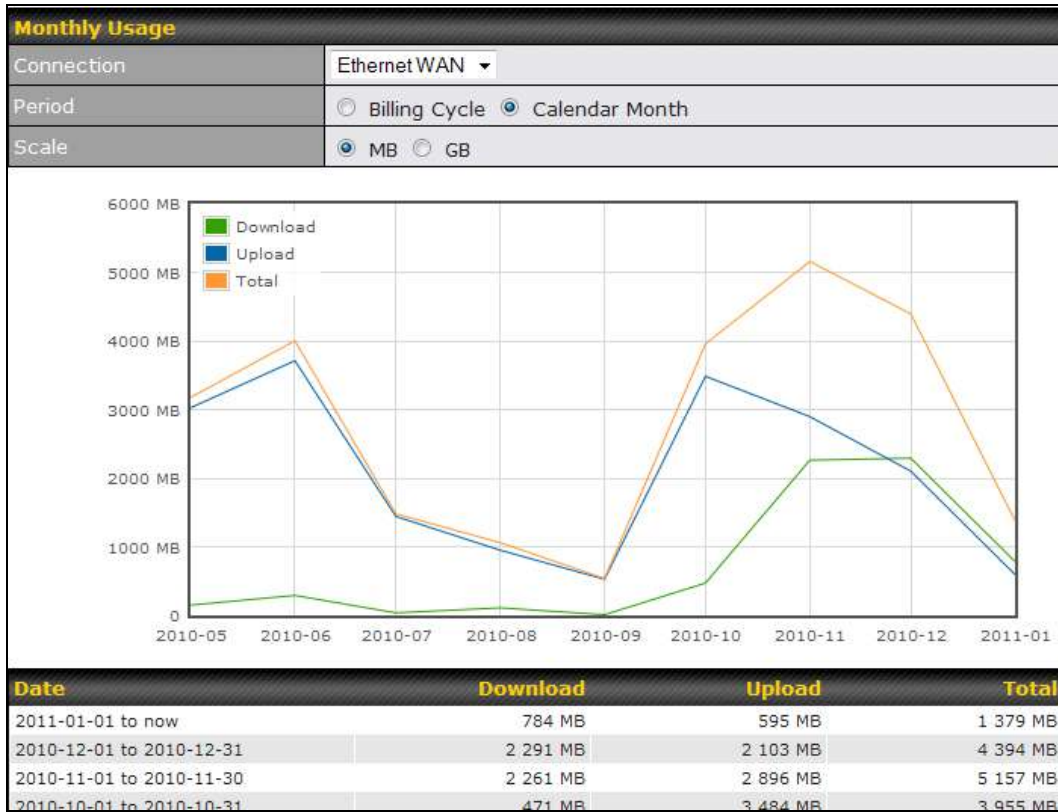
32.4 Monthly

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

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



All WAN Monthly Bandwidth Usage



Ethernet WAN Monthly Bandwidth Usage

Tip

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

Appendix A: Restoration of Factory Defaults

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

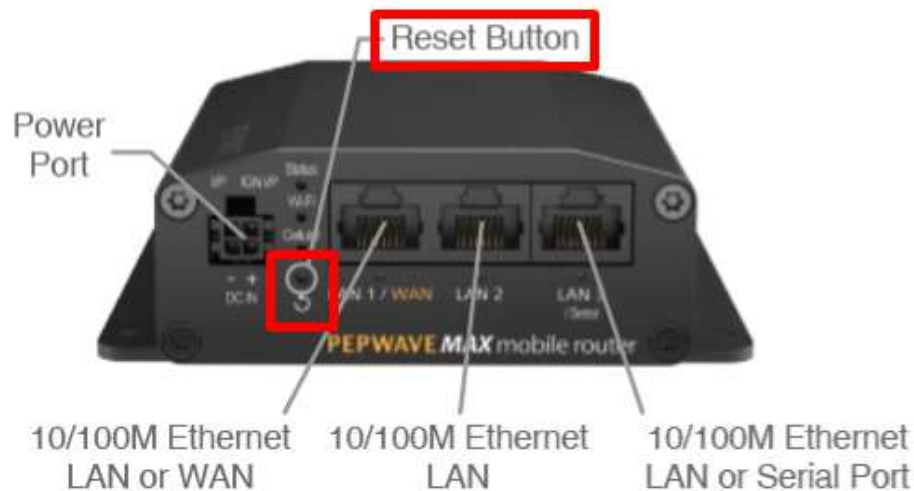
1. Locate the reset button on the front or back panel of the Pepwave router.
2. With a paperclip, press and keep the reset button pressed.

Hold for approximately 10 seconds for factory reset (Note: The LED status light shows in RED, until the status light off and release the button)

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:

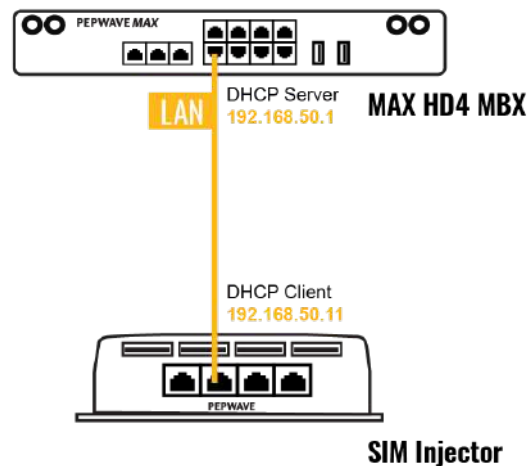
- **User:** admin
- **Password:** admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

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.

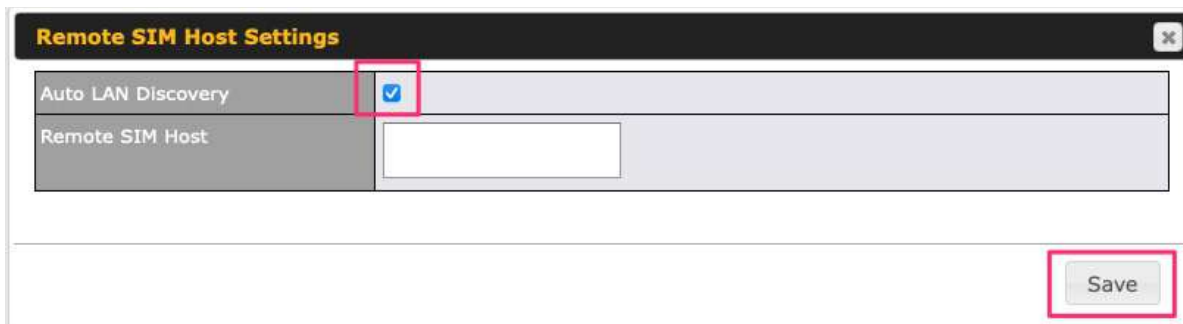
Configuring the Cellular Router

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**.



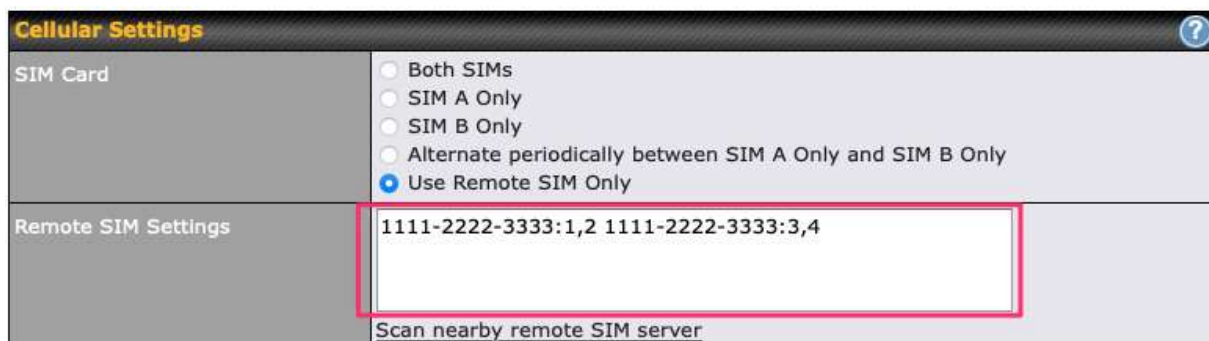
4. Enter configuration settings in **Remote SIM Settings** section. Click on **Scan nearby remote SIM server** to show the serial number(s) of the connected SIM Injector(s). Available configuration options for cellular interface are shown below:

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**.

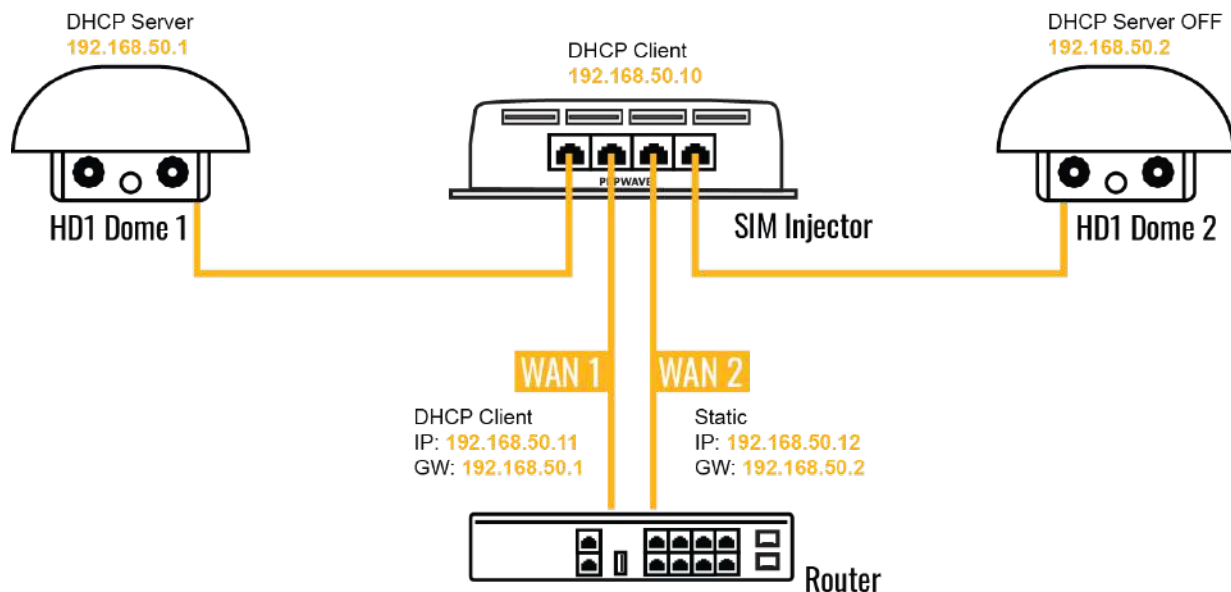
Step 3. (Optional) Custom SIM cards settings.

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 | <input checked="" type="checkbox"/> |
| Captive Portal | <input type="checkbox"/> |
| DHCP Server | |
| DHCP Server | <input type="checkbox"/> Enable |
| DHCP Server Logging | <input type="checkbox"/> |
| 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).

The screenshot shows the Peplink PEPWAVE web interface. The top navigation bar includes 'Dashboard', 'SpeedFusion Cloud', 'Network', 'Advanced', 'AP', 'System', and 'Status'. The left sidebar shows 'LAN' settings, with 'Port Settings' selected. The main content area displays the 'Port Settings' table:

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

Below the table is a 'Save' button. The 'Access' and 'Untagged LAN' cells in the table are highlighted with red boxes. The text 'Untagged LAN' is also displayed in red below the table.

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

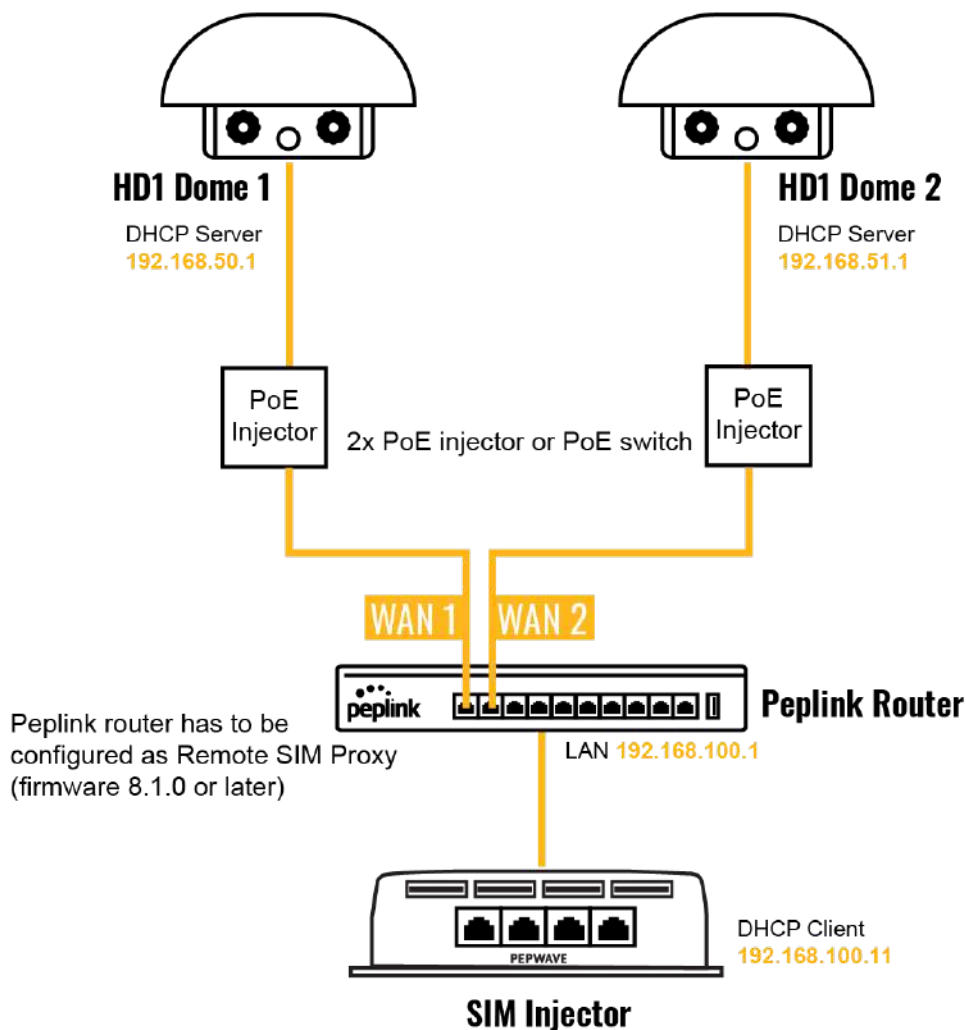
Configuration requirements for the main Router

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.

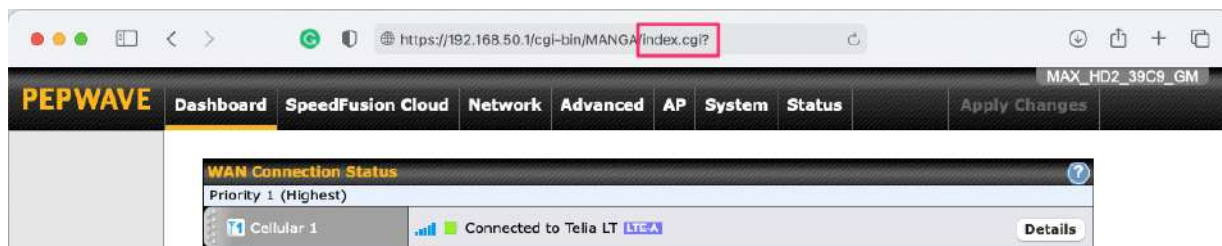
Main Router configuration

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**.

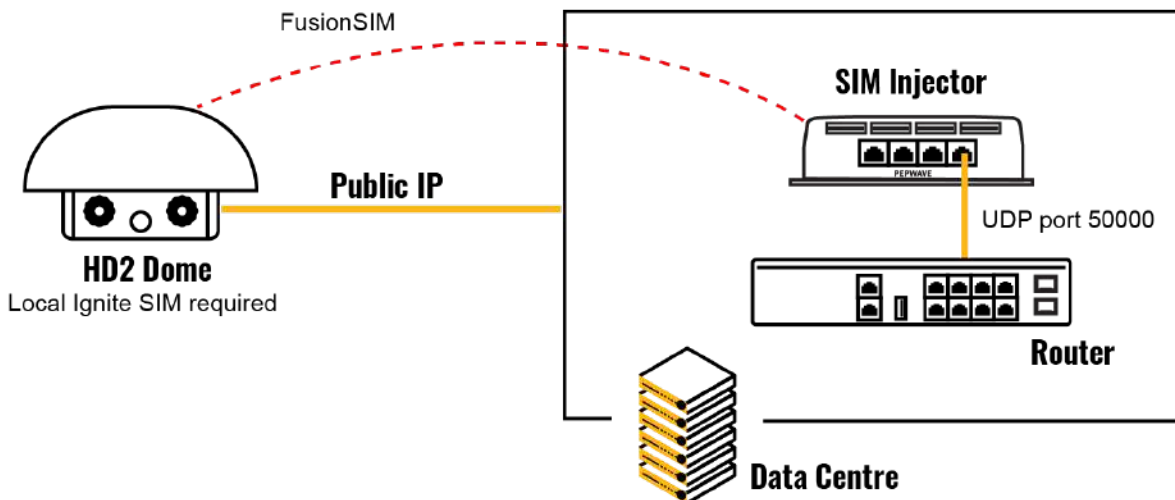
This will open the support.cgi page.



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).