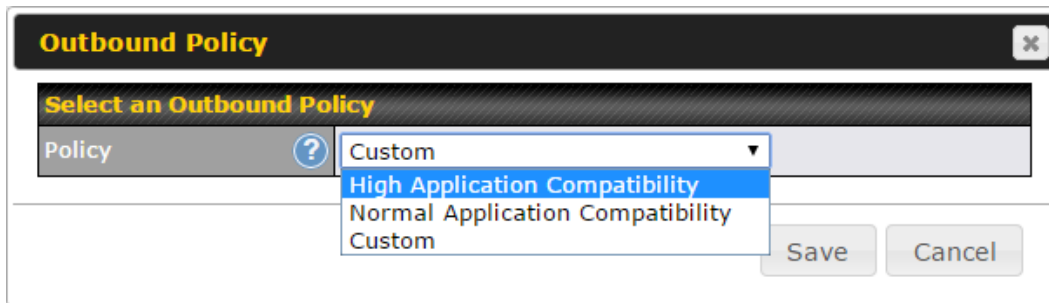


17.1 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at

Advanced>Outbound Policy> or **Advanced>PepVPN>Outbound Policy**. Click the  button beside the **Outbound Policy** box:



There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

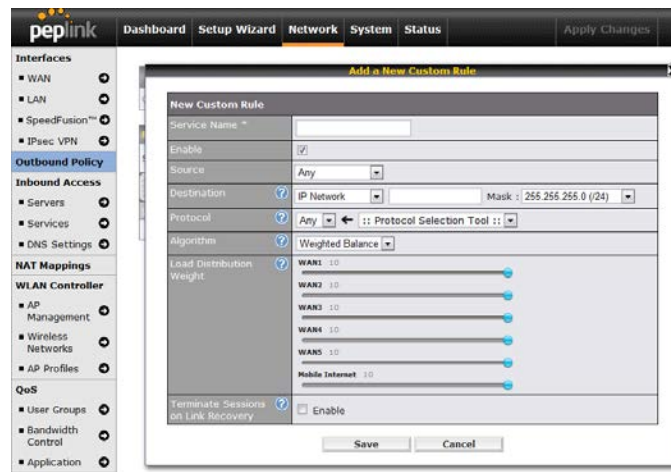
Note that some Pepwave routers provide only the **Send All Traffic To** setting here. See **Section 12.1** for details.

Outbound Policy Settings	
High Application Compatibility	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the highest application compatibility.
Normal Application Compatibility	Outbound traffic from a source LAN device to the same destination Internet IP address will be routed through the same WAN connection persistently, regardless of protocol. This option provides high compatibility to most applications, and users still benefit from WAN link load balancing when multiple Internet servers are accessed.
Custom	Outbound traffic behavior can be managed by defining rules in a custom rule table. A default rule can be defined for connections that cannot be matched with any of the rules.

The default policy is **Normal Application Compatibility**.

Tip

Want to know more about creating outbound rules? Visit our YouTube Channel for a video tutorial!



http://youtu.be/rKH4AS_bQnE

17.2 Adding Rules for Outbound Policy

The menu underneath enables you to define Outbound policy rules:

Rules (🖱️ Drag and drop rows by the left to change rule order) ?					
Service	Algorithm	Source	Destination	Protocol / Port	
 HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	
Default	(Auto)				
Add Rule					

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

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

Edit Default Custom Rule

Default Rule	☒ Custom ☐ Auto
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic Drop the Traffic Use Any Available Connections

Save
Cancel

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

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

Add a New Custom Rule

Service Name			
Enable	☒	Always on	
Source	Any		
Destination	IP Network		Mask: 255.255.255.0 (/24)
Protocol	Any	Protocol Selection	
Algorithm	Weighted Balance		
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10		
When No Connections are Available	Drop the Traffic		

Save
Cancel

New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	This setting specifies whether the outbound traffic rule takes effect. When Enable is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When Enable is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.
Source	This setting specifies the source IP Address, IP Network, MAC Address or Grouped Network for traffic that matches the rule. Source Destination Protocol Any Any IP Address IP Network MAC Address Grouped Network
Destination	This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, PepVPN Profile or Grouped network for traffic that matches the rule.

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

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

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

Protocol and Port

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

- Any
- TCP
- UDP
- IP
- DSCP

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

Algorithm

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

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

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

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

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

Load Distribution Weight

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

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

17.2.1 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**.

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

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

For example, with the following weight settings:

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

- USB: 10

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

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

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

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

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

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

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

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

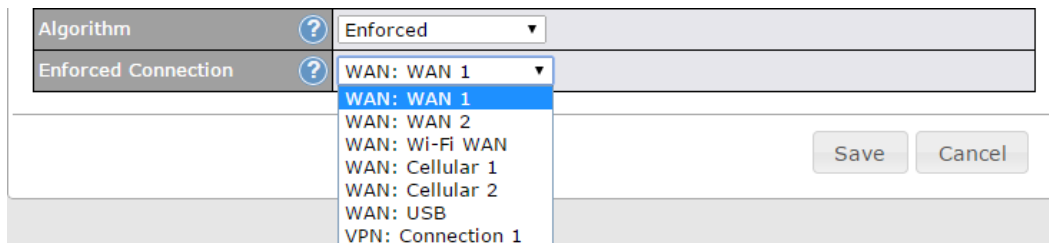
There are two persistent modes: **By Source** and **By Destination**.

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

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

17.2.3 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.

17.2.4 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	☐ Enable	

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

Tip

Configure multiple distribution rules to accommodate different kinds of services.

17.2.5 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.

17.2.6 Algorithm: Least Used

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

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

17.2.7 Algorithm: Lowest Latency

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

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

Tip

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

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

17.2.8 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

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

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

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

18 Port Forwarding

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

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

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

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

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

IP Protocol

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

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

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



The screenshot shows the 'Port' configuration interface. A dropdown menu is set to 'Any Port'. There is a help icon (question mark) to the left of the dropdown.

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.



The screenshot shows the 'Port' configuration interface. A dropdown menu is set to 'Single Port'. To the right, there is a text input field labeled 'Service Port:' with the value '80'. There is a help icon (question mark) to the left of the dropdown.

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.



The screenshot shows the 'Port' configuration interface. A dropdown menu is set to 'Port Range'. To the right, there is a text input field labeled 'Service Ports:' with the value '80 - 88'. There is a help icon (question mark) to the left of the dropdown.

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.



The screenshot shows the 'Port' configuration interface. A dropdown menu is set to 'Port Mapping'. To the right, there are two text input fields: 'Service Port:' with the value '80' and 'Map to Port:' with the value '88'. There is a help icon (question mark) to the left of the dropdown.

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.)



The screenshot shows the 'Port' configuration interface. A dropdown menu is set to 'Range Mapping'. To the right, there are two text input fields: 'Service Ports:' with the value '80 - 88' and 'Map to Ports:' with the value '88 - 96'. There is a help icon (question mark) to the left of the dropdown.

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

Port

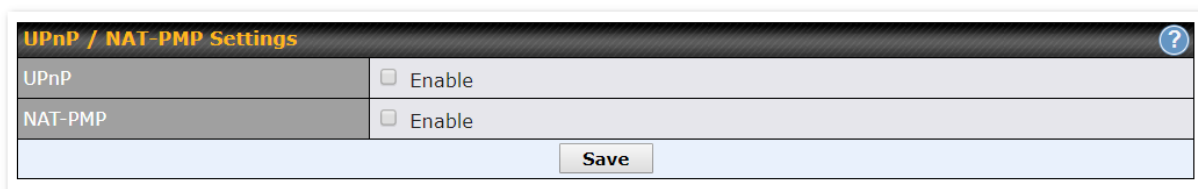
Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Server IP Address	This setting specifies the LAN IP address of the server that handles the requests for the service.

18.1 UPnP / NAT-PMP Settings

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

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

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



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

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

19 NAT Mappings

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

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

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

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

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

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

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

Important Note

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

20 QoS

20.1 User Groups

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

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

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

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

Add / Edit User Group

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

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

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

20.2 Bandwidth Control

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

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

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

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

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

20.3 Application

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

20.3.2 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
Category
Application

☒ Supported Applications
☐ Custom Applications

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

OK
Cancel

Add / Edit Application

Type

☐ Supported Applications
☒ Custom Applications

Application Name

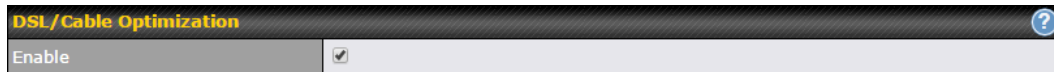
Scope / Protocol
TCP

Port
Single Port

OK
Cancel

20.3.3 DSL/Cable Optimization

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



21 Firewall

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

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

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

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

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

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

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

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

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

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

Intrusion Detection and DoS Prevention

Disabled
 

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

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

21.1 Outbound and Inbound Firewall Rules

21.1.1 Access Rules

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

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

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name

Enable

☒ Always on

Protocol

Any   Protocol Selection Tool

Source IP & Port

Any Address 

Destination IP & Port

Any Address 

Action

☒ Allow ☐ Deny 

Event Logging

☐ Enable 

Save

Cancel

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

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

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

Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☒
WAN Connection	Any
Protocol	Any :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save
Cancel

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

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

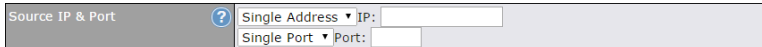
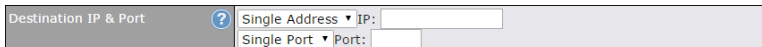
Click **Add Rule** to display the following window:

Add a New Internal Network Firewall Rule

New Firewall Rule

Rule Name	
Enable	☒ Always on
Protocol	Any :: Protocol Selection ::
Source	Any Address
Destination	Any Address
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save
Cancel

Inbound / Outbound / Internal Network Firewall Settings	
Rule Name	This setting specifies a name for the firewall rule.
Enable	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. Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: • Any • TCP • UDP • ICMP • DSCP • IP 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.
Source IP & Port	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:  In addition, a single port, or a range of ports, can be specified for the Source IP & Port settings.
Destination IP & Port	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:  In addition, a single port, or a range of ports, can be specified for the Destination IP & Port settings.
Action	This setting specifies the action to be taken by the router upon encountering traffic

that matches the both of the following:

- Source IP & port
- Destination IP & port

With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded).

Event Logging

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

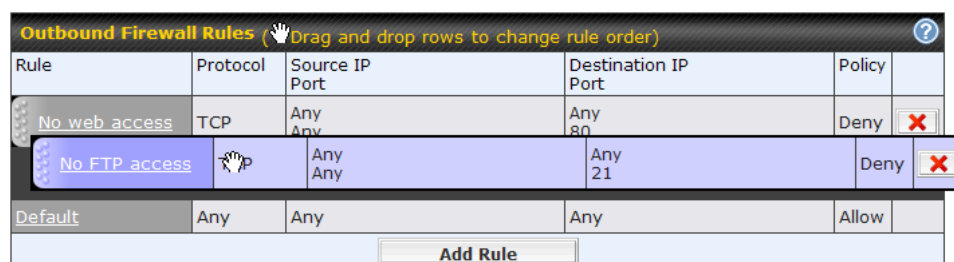
Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1
DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80

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

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

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

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



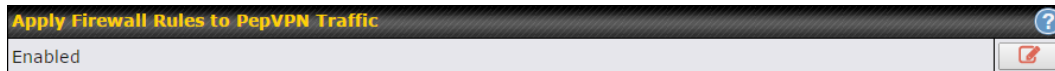
To remove a rule, click the button.

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

Tip

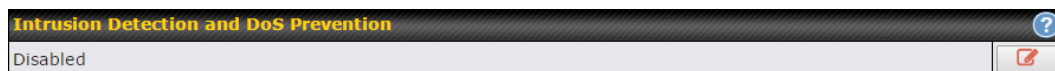
If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound Allow firewall rules will be required for inbound port forwarding and inbound NAT mapping rules. However, if the default inbound rule is set as **Deny**, a corresponding Allow firewall rule will be required.

21.1.2 Apply Firewall Rules to PepVpn Traffic



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

21.1.3 Intrusion Detection and DoS Prevention



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

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

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

21.2 Content Blocking

Application Blocking
?

Please Select Application...
+

Web Blocking
?

Preset Category

☐ High
☐ Moderate
☐ Low
☒ Custom

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

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

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

Customized Domains

cbs.com
+

Exempted Domains from Web Blocking
+

Exempted User Groups
?

Manager
☐ Exempt

Staff
☐ Exempt

Guest
☐ Exempt

Exempted Subnets
?

Network
Subnet Mask

255.255.255.0 (/24)
+

URL Logging

Enable
☐

Log Server Host
Port:

21.2.1 Application Blocking

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

21.2.2 Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access

except for those on the Exempted User Groups or Exempted Subnets defined below.

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

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

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

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.

21.2.6 URL Logging

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

22 Routing Protocols

22.1 OSPF & RIPv2

The Pepwave supports OSPF and RIPv2 dynamic routing protocols.

Click the **Advanced** tab from the top bar, and then click the **Routing Protocols > OSPF & RIPv2** item on the sidebar to reach the following menu:

OSPF		
Router ID	LAN IP Address	
Area	Interfaces	
0.0.0.0	PepVPN	
Add		
PepVPN OSPF Area		
0.0.0.0		
RIPv2		
No RIPv2 Defined.		

OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the 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	0.0.0.0
Link Type	☒ Broadcast ☐ Point-to-Point
Authentication	None ▾
Interfaces ?	☐ Untagged LAN ☐ V167 (192.168.167.1/24) ☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ WAN 5 ☒ PepVPN

Save

Cancel

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	None ▾
Interfaces	☐ Untagged LAN ☐ V167 (192.168.167.1/24) ☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ WAN 5

Save

Cancel

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

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

22.2 BGP

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

BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	
			

Click the "" to delete a BGP profile.

Click "**Add**" to create a new BGP profile.

BGP Profile
✕

BGP Profile						
Profile Name						
Enable	☒					
Interface	WAN ▼					
Router ID	☒ WAN IP Address ☐ Custom:					
Autonomous System						
Neighbor ?	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
			disable			+
Hold Time ?	240					
Next Hop Self ?	☐					
iBGP Local Preference ?	100					
BFD ?	☐ Enable					

BGP	
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.
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	?	--- +							
Static Route Advertising	?	☒ Enable <table border="1"> <thead> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td>255.255.255.0 (/24) ▾</td> <td> + </td> </tr> </tbody> </table>		Excluded Networks	Subnet Mask			255.255.255.0 (/24) ▾	+
Excluded Networks	Subnet Mask								
	255.255.255.0 (/24) ▾	+							
Custom Route Advertising	?	<table border="1"> <thead> <tr> <th>Networks</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td>255.255.255.0 (/24) ▾</td> <td> + </td> </tr> </tbody> </table>		Networks	Subnet Mask			255.255.255.0 (/24) ▾	+
Networks	Subnet Mask								
	255.255.255.0 (/24) ▾	+							
Advertise OSPF Route	?	☐							
Set Community	?	<table border="1"> <thead> <tr> <th>Community</th> <th>Route Prefix</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> + </td> </tr> </tbody> </table>		Community	Route Prefix				+
Community	Route Prefix								
		+							

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) ▼	☐	+

Filter Mode

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

None: All BGP routes will be accepted.

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

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

Restricted Networks

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

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

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

Route Export				
Filter Mode	? Accept ▼			
Restricted Networks	Network	Subnet Mask	Exact Match	
		255.255.255.0 (/24) ▼	☐	+
Export to other BGP Profile	? ☐			
Export to OSPF	? ☐			

Filter Mode

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

None: All BGP routes will be accepted.

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

	be rejected. Reject: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks	This field specifies the network(s) in the "route export" 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.
Export to other BGP Profile	When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.
Export to OSPF	When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.

23 Remote User Access

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

23.1 L2TP with IPsec

Remote User Access Settings	
Enable	☒
VPN Type	☒ L2TP with IPsec ☐ PPTP ☐ OpenVPN
Preshared Key	? ☒ Hide Characters

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

Continue to configure the authentication method.

23.2 OpenVPN

Remote User Access Settings	
Enable	☒
VPN Type	☐ L2TP with IPsec ☐ PPTP ☒ OpenVPN You can obtain the OpenVPN client profile from the status page

Select OpenVPN and continue to configure the authentication method.

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

OpenVPN Client Profile	Route all traffic 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.

23.3 PPTP

Remote User Access Settings	
Enable	☒
VPN Type	☐ L2TP with IPsec ☒ PPTP ☐ OpenVPN

No additional configuration required.

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

Continue to configure authentication method.

23.4 Authentication Methods

Connect to Network	Untagged LAN ▼		
Authentication	Local User Accounts ▼		
User Accounts	Username	Password	+

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

User accounts:

This setting allows you to define the Remote User Accounts.

Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

Note:

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

The password must be between 8 and 12 characters long.

LDAP Server:

Connect to Network	 Untagged LAN ▾
Authentication	LDAP Server ▾
LDAP Server	Port 389 Default
	☐ Use DN/Password to bind to LDAP Server
Base DN	
Base Filter	

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

Radius Server:

Authentication	RADIUS Server ▾
Auth Protocol	MS-CHAP v2 ▾
Auth Server	Port 1812 Default
Auth Server Secret	☒ Hide Characters
Accounting Server	Port 1813 Default
Accounting Server Secret	☒ Hide Characters

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

Active Directory:

Connect to Network	 Untagged LAN ▾
Authentication	Active Directory ▾
Server Hostname	
Domain	
Admin Username	
Admin Password	☒ Hide Characters

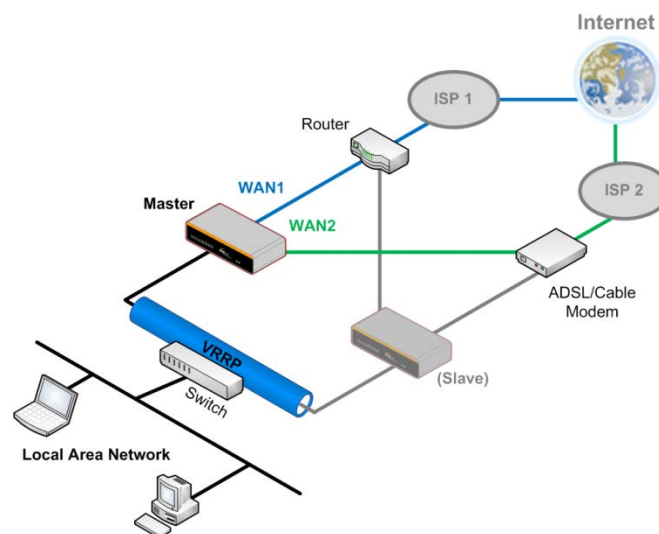
Enter the matching Active Directory details to allow for Active Directory server authentication.

24 Miscellaneous Settings

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

24.1 High Availability

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



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

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

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

configured LAN IP address.

- At a subsequent point when the master Pepwave router recovers, it will once again become active.

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

Interface for Master Router

High Availability	
Enable	☒
Group Number	
Preferred Role	☒ Master ☐ Slave
Resume Master Role Upon Recovery	☒
Virtual IP Address	
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

Interface for Slave Router

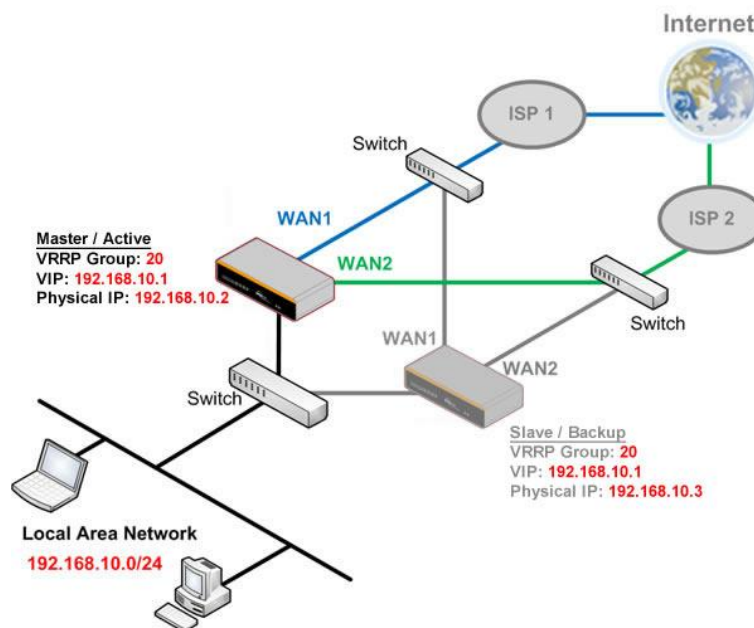
High Availability	
Enable	☒
Group Number	
Preferred Role	☐ Master ☒ Slave
Configuration Sync.	☐ Master Serial Number:
Establish Connections in Slave Role	☐
Virtual IP Address	
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

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

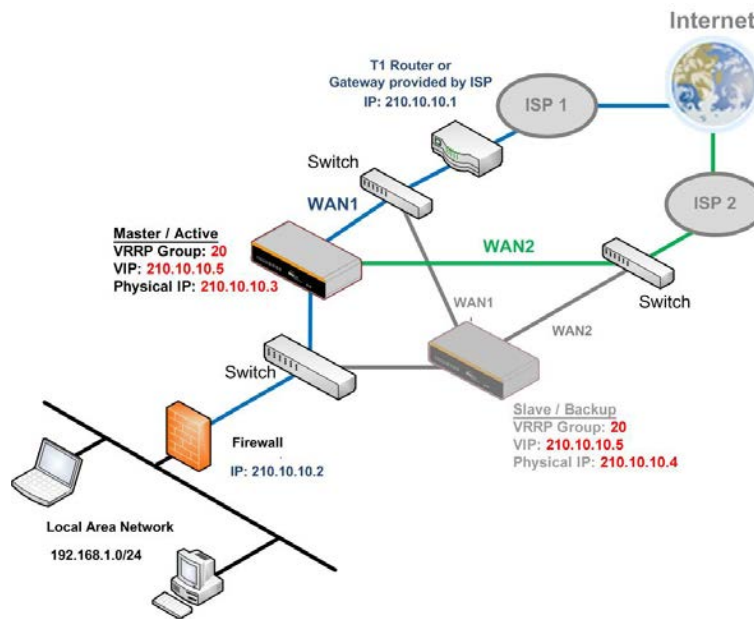
Administration IP must be under the same network.	
LAN Administration IP	This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN.
Subnet Mask	This setting specifies the subnet mask of the LAN.

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.



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

24.2 Certificate Manager

Certificate		
SpeedFusion/IPsec VPN	No Certificate	
Web Admin SSL	Default Certificate is in use	
Captive Portal SSL	Default Certificate is in use	
OpenVPN CA	Default Certificate is in use	
Wi-Fi WAN Client Certificate		
No Certificates defined		
<button>Add Certificate</button>		
Wi-Fi WAN CA Certificate		
No Certificates defined		
<button>Add Certificate</button>		

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

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

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

24.3 Service Forwarding

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

SMTP Forwarding Setup	
SMTP Forwarding	☐ Enable
Web Proxy Forwarding Setup	
Web Proxy Forwarding	☐ Enable
DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	☐ Enable
Custom Service Forwarding Setup	
Custom Service Forwarding	☐ 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.

24.3.1 SMTP Forwarding

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

SMTP Forwarding Setup			
SMTP Forwarding		☒ Enable	
Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	☐		
WAN 2	☐		
Wi-Fi WAN	☐		
Cellular 1	☐		
Cellular 2	☐		
USB	☐		

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

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

Note

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

24.3.2 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	☐	:
WAN 2	☐	:
Wi-Fi WAN	☐	:
Cellular 1	☐	:
Cellular 2	☐	:
USB	☐	:

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

24.3.3 DNS Forwarding

DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	☐ Enable

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

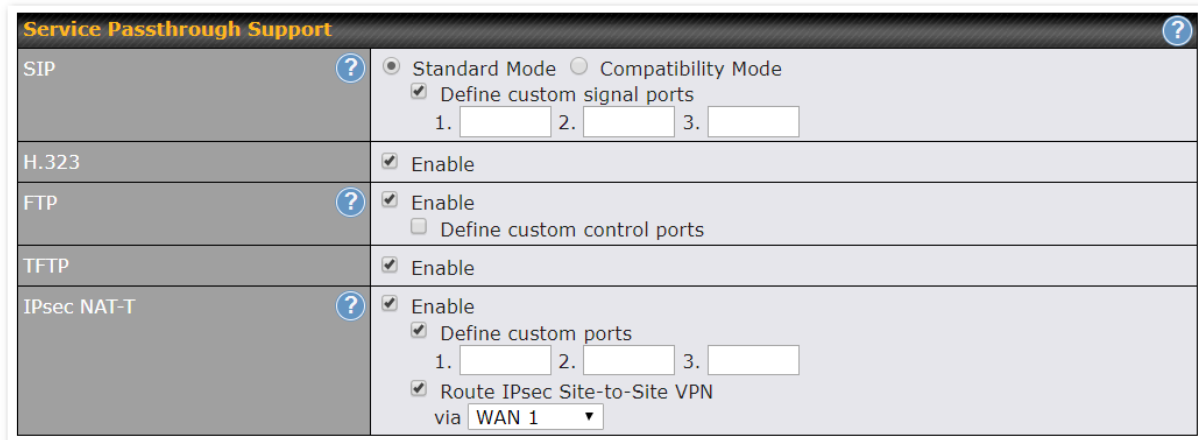
24.3.4 Custom Service Forwarding

Custom Service Forwarding Setup			
Custom Service Forwarding	☒ Enable		
Settings	TCP Port	Server IP Address	Server Port
			+

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

24.4 Service Passthrough

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



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

IPsec NAT-T

This field is for enabling the support of IPsec NAT-T passthrough. UDP ports 500, 4500, and 10000 are monitored by default. You may add more custom data ports that your IPsec system uses by checking **Define custom ports**. If the VPN contains IPsec site-to-site VPN traffic, check **Route IPsec Site-to-Site VPN** and choose the WAN connection to route the traffic to.

24.5 UART

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

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

Serial to Network	
Enable	☒
Allowed Source IP Subnets	☒ Any ☐ Allows access from the following IP subnets only
Web Console 	☐

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

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

Data Packing	
Packing Length	0 byte(s)
Delimiter	☐
Delimiter process	Do Nothing ▼
Force Transmit	0 ms

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

DB-9 Pepwave MAX Terminal Block

Pin 1 –

Pin 2 Rx (rated -+25V)

Pin 3 Tx (rated -+12V)

Pin 4 –

Pin 5 –

Pin 6 –

Pin 7 RTS

Pin 8 CTS

Pin 9 –

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

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

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

24.6 GPS Forwarding

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

GPS Forwarding					
Enable	☒				
Server	Server IP Address / Host Name	Port	Protocol	Report Interval (s)	
			UDP ▾	1	+
GPS Report Format	☒ NMEA ☐ TAIP				
NMEA Sentence Type	☒ GPRMC ☐ GPGGA ☐ GPVTG ☐ GPGSA ☐ GPGSV				
Vehicle ID	?				

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.

24.7 Ignition Sensing

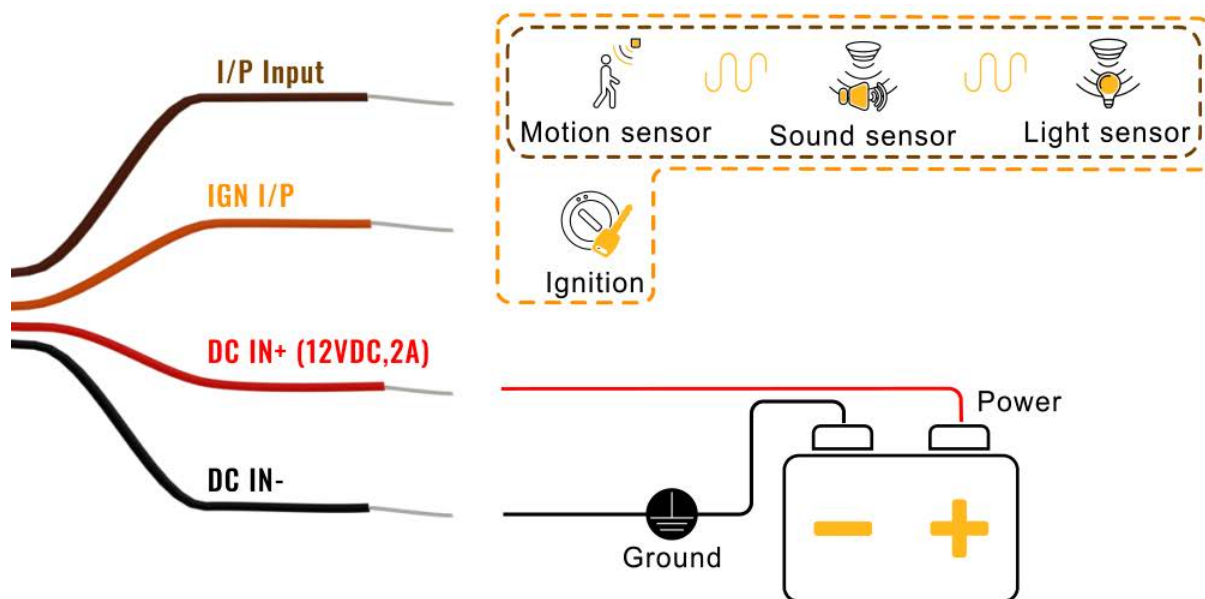
Ignition Sensing detects the ignition signal status of a vehicle it is installed in.

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

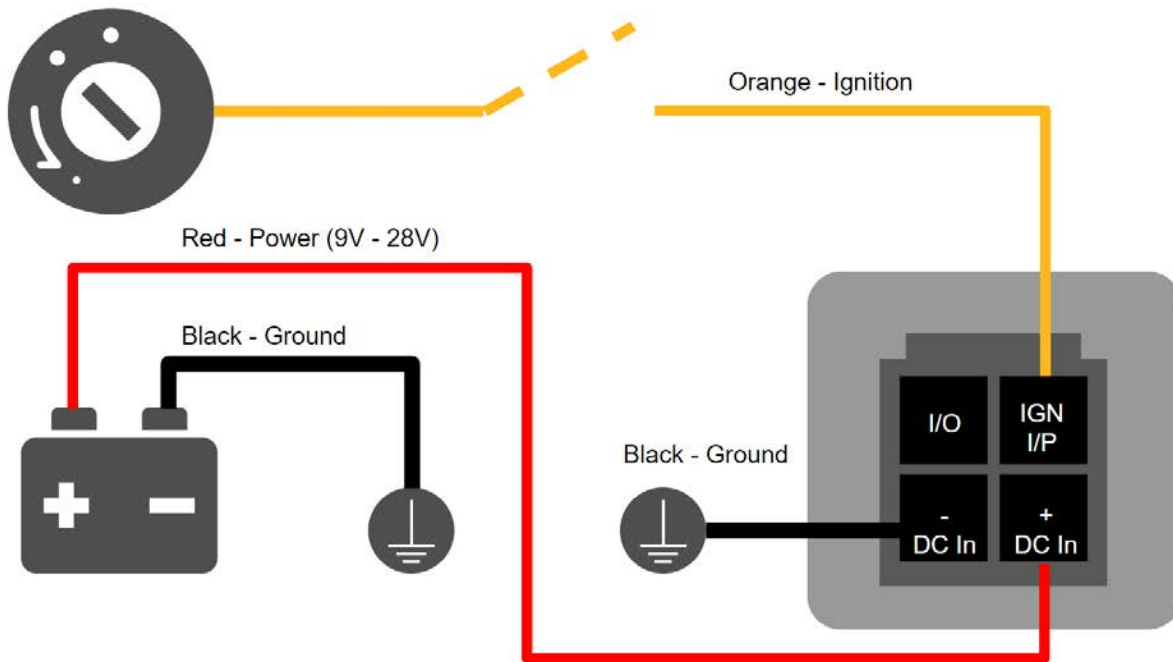
The time delay setting between ignition off and power down of the router is a configurable setting, which allows the router to stay on for a period of time after the engine of a vehicle is turned off.

Ignition Sensing installation

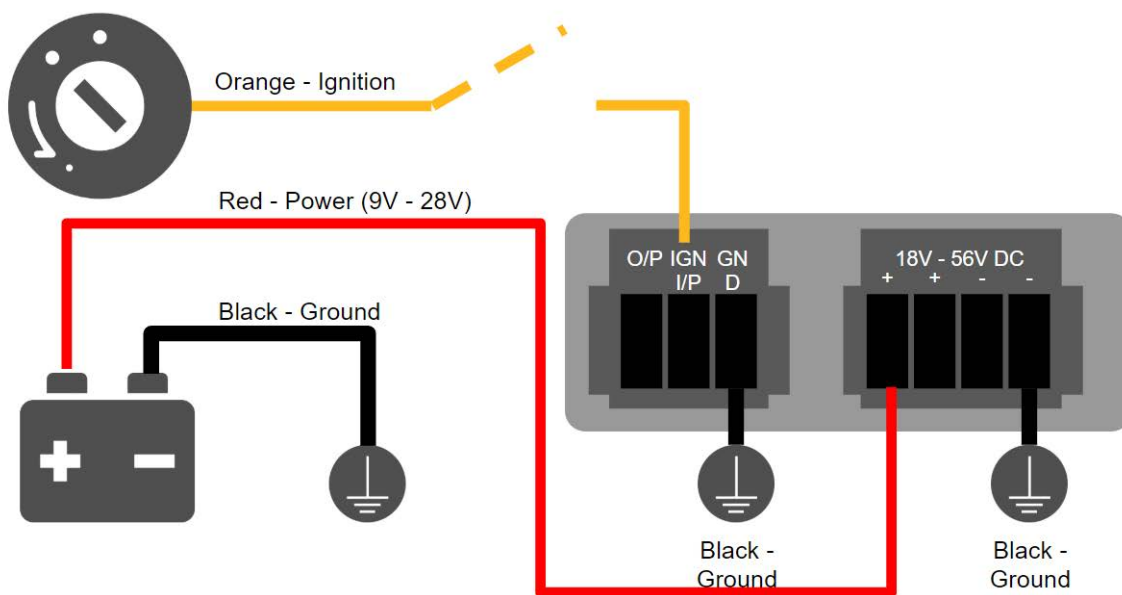
Function		Colour Wire
	I/O optional*	Brown
	IGN I/P connected to positive feed on the ignition .	Orange
	DC IN - connected to permanent negative feed (ground)	Black
	DC IN + connected to permanent positive feed (power 12VDC, 2A)).	Red
* Currently not functional; will be used for additional features in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



Connectivity diagram for devices with 4-pin connector



Connectivity diagram for devices with terminal block connection



GPIO Menu

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

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

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

IGN I/P	
Enable	☒
Type	Digital Input ▼
Mode	Ignition Sensing ▼
Delay	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	☒
Type	Digital Output ▼
Mode	WAN Status ▼

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

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

24.8 NTP Server

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

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

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

NTP Server	
Enable	☐

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

Time Settings	
Time Zone	(GMT) Casablanca ▼ ☐ Show all
Time Sync	Time Server ▼
Time Server	0.peplink.pool.ntp.org

24.9 Grouped Networks

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

Grouped Networks		
Name	Networks	
Example	192.168.1.71/28	
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) ▼	
Save Cancel			

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

24.10 Remote SIM Management

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

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

Remote SIM Host

Remote SIM is disabled

Remote SIM Host Settings

Remote SIM Host Settings

Auto LAN Discovery

☐

Remote SIM Host

Save

Remote SIM Host Settings	
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.

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	New SIM Server...
SIM Server - Serial Number	
SIM Server - Name	Optional
SIM Slot	1
SIM Slot - Name	Optional
Data Roaming	☐
Operator Settings (for LTE/HSPA/EDGE/GPRS only)	☒ Auto ☐ Custom Mobile Operator Settings
SIM PIN (Optional)	(Confirm)

Save

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 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.

24.11 SIM Toolkit

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

USSD

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

SIM Status	
WAN Connection	Cellular ▼
SIM Card	1
IMSI	724020400000000
Tool	USSD ▼

USSD	
USSD Code	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# Submit
Receive SMS	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# Submit
USSD Status	Request is sent successfully
Receive SMS	Get

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

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.

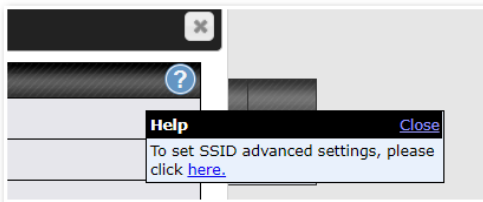
AP Controller			
AP Management	?	☒ Integrated AP	☒ External AP
Sync. Method	?	As soon as possible ▼	
Permitted AP	?	☒ Any ☐ Approved List	

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	- 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	
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	
Enable	☒
VLAN	Untagged LAN ▾
Broadcast SSID	☒
Data Rate	☒ Auto ☐ Fixed
Multicast Filter	☐
Multicast Rate	MCS0/6M ▾
IGMP Snooping	☐
Layer 2 Isolation	☐
Maximum number of clients	2.4 GHz: 0 5 GHz: 0 (0: Unlimited)

Security Settings

Security Policy	Open (No Encryption) ▾
-----------------	------------------------

Access Control Settings

Restricted Mode	None ▾
-----------------	--------

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Enable	Click the drop-down menu to apply a time schedule to this interface
VLAN	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is 0 , which means VLAN tagging is disabled (instead of tagged with zero).

Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate ^A	Select Auto to allow the Pepwave router to set the data rate automatically, or select Fixed and choose a rate from the displayed drop-down menu.
Multicast Filter ^A	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate ^A	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected Protocol and Channel Bonding settings will affect the rate options and values available here.
IGMP Snooping ^A	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
DHCP Option 82 ^A	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
Layer 2 Isolation ^A	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to the upper communication layer(s). By default, the setting is disabled.
Maximum Number of Clients	Indicate the maximum number of clients that should be able to connect to each frequency.

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

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Shared Key	 ☒ Hide Characters

Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options : • Open (No Encryption) • Enhanced Open (OWE) • WPA3 -Personal (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.

Access Control Settings	
Restricted Mode	Deny all except listed ▼
MAC Address List	?

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 Server Settings	Primary Server	Secondary Server
Host		
Secret	☒ Hide Characters	☒ Hide Characters
Authentication Port	1812 Default	1812 Default
Accounting Port	1813 Default	1813 Default
NAS-Identifier	Device Name ▼	

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

Guest Protect			
Block All Private IP	☐		
Custom Subnet	Network	Subnet Mask	
		255.255.255.0 (/24) ▼	+
Block Exception	Network	Subnet Mask	
		255.255.255.0 (/24) ▼	+

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	Disable ▼ Disable Flexible - Allow all except... Lockdown - Block all except...

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

25.3 Wireless Mesh

Wireless Mesh	Frequency Band
No Wireless Mesh Defined	
Add	

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

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

Wireless Mesh Settings

Mesh ID	
Frequency	☒ 2.4 GHz ☐ 5 GHz
Shared Key	☒ Hide Characters

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

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

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

AP Settings

SSID

These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Pepwave MAX does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.

Operating Country	This drop-down menu specifies the national / regional regulations which the AP should follow. • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). Note: Users are required to choose an option suitable to local laws and regulations. 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.
Preferred Frequency	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.
Protocol	This section displays the 2.4 GHz protocols your APs are using.
Channel Width	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.
Channel	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.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
Output Power^A	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. 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. 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.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.

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

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

Integrated AP

Wi-Fi Operating Mode
☒ WAN
☐ WAN + AP
☐ AP

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

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

Integrated AP	
WAN	In this mode, all Wi-Fi will operate as Wi-Fi WAN. Since all device Wi-Fi are exhausted, no integrated Wi-Fi AP will be operated on this device.
WAN + AP	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.
AP	in this mode, all Wi-Fi functions as integrated Wi-Fi AP. All Wi-Fi WANs will be forced to go offline.

Web Administration Settings (on External AP)

Enable	☒
Web Access Protocol	☐ HTTP ☒ HTTPS
Management Port	443
HTTP to HTTPS Redirection	☒
Admin Username	admin
Admin Password	25db591396e0 Generate

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

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

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

Wi-Fi Radio Settings	
Operating Country	United States ▼
Wi-Fi Antenna	☐ Internal ☒ External

Wi-Fi AP Settings 	
Protocol	802.11ng ▼
Channel	1 (2.412 GHz) ▼
Channel Width	Auto ▼
Output Power	Max ▼ ☐ Boost
Beacon Rate	 1Mbps ▼
Beacon Interval	 100ms ▼
DTIM	 1
Slot Time	 9 μs
ACK Timeout	 48 μs
Frame Aggregation	☒ Enable
Guard Interval	☐ Short ☐ Long

Wi-Fi Radio Settings

Operating Country

This option sets the country whose regulations the Pepwave router follows.

Wi-Fi Antenna

Choose from the router's internal or optional external antennas, if so equipped.

Important Note

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

Wi-Fi AP Settings

Protocol

This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, **802.11ng** is selected.

Channel

This option allows you to select which 802.11 RF channel will be used. **Channel 1 (2.412 GHz)** is selected by default.

Channel Width

Auto (20/40 MHz) and **20 MHz** are available. The default setting is **Auto (20/40 MHz)**, which allows both widths to be used simultaneously.

Output Power

This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country.

Beacon Rate^A

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

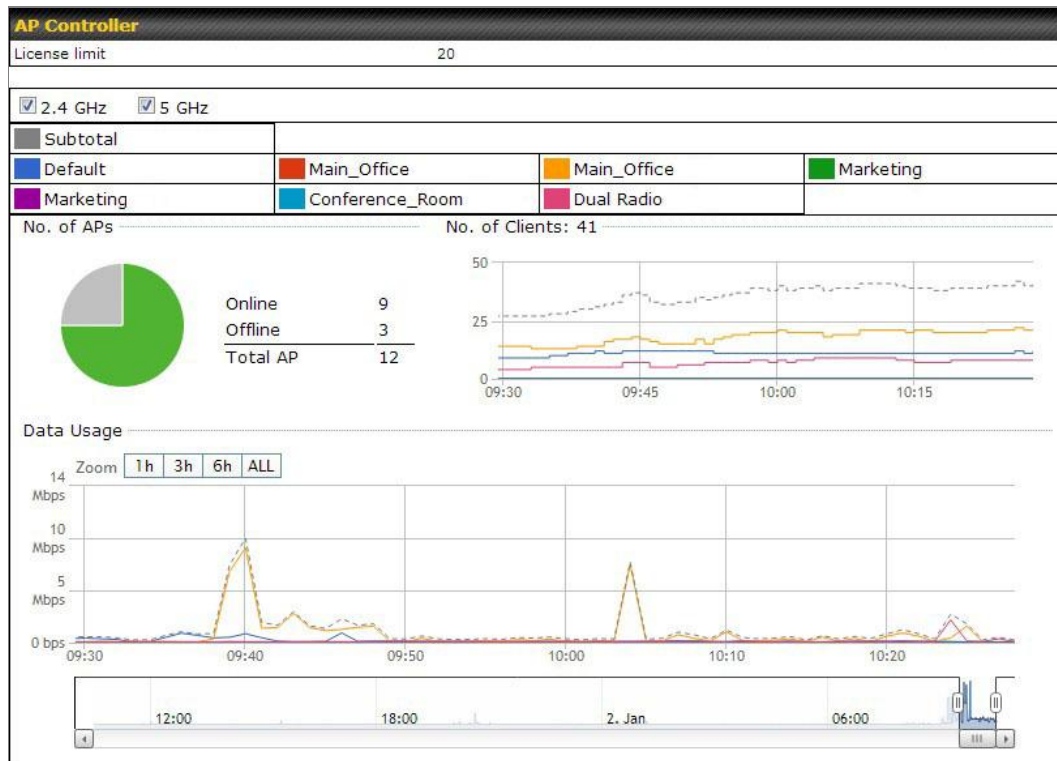
	1Mbps is selected.
Beacon Interval^A	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM^A	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to 1 ms .
Slot Time^A	This field is for specifying the wait time before the Router transmits a packet. By default, this field is set to 9 µs .
ACK Timeout^A	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 µs .
Frame Aggregation^A	This option allows you to enable frame aggregation to increase transmission throughput.
Guard Interval^A	This setting allows choosing a short or long guard period interval for your transmissions.

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

26 AP Controller Status

26.1 Info

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



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

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

Data Usage

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

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
		More...

Events

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

26.2 Access Point (Usage)

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

Search Filter	
AP Name / Serial Number / SSID	All
	☐ Include Offline APs
Search Result	

Managed APs							Expand	Collapse
Name	IP Address	MAC	Location	Firmware	Pack ID	Configuration		
Default (8/9 online)								
1000-AMT-1000	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None	✓	-	

Usage																																																																																					
AP Name/Serial Number	This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.																																																																																				
Online Status	This button toggles whether your search will include offline devices.																																																																																				
Managed Wireless Devices	This table shows the detailed information on each AP, including channel, number of clients, upload traffic, and download traffic. Click the blue arrows at the left of the table to expand and collapse information on each device group. You could also expand and collapse all groups by using the Expand Collapse buttons. 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 <table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Type</th> <th>Signal</th> <th>SSID</th> <th>Upload</th> <th>Download</th> </tr> </thead> <tbody> <tr> <td>80:56:f2:98:75:ff</td> <td>10.9.2.7</td> <td>802.11ng</td> <td>Excellent (37)</td> <td>Balance</td> <td>66.26 MB</td> <td>36.26 MB</td> </tr> <tr> <td>c4:6a:b7:bf:d7:15</td> <td>10.9.2.123</td> <td>802.11ng</td> <td>Excellent (42)</td> <td>Balance</td> <td>6.65 MB</td> <td>2.26 MB</td> </tr> <tr> <td>70:56:81:1d:87:f3</td> <td>10.9.2.102</td> <td>802.11ng</td> <td>Good (23)</td> <td>Balance</td> <td>1.86 MB</td> <td>606.63 KB</td> </tr> <tr> <td>e0:63:e5:83:45:c8</td> <td>10.9.2.101</td> <td>802.11ng</td> <td>Excellent (39)</td> <td>Balance</td> <td>3.42 MB</td> <td>474.52 KB</td> </tr> <tr> <td>18:00:2d:3d:4e:7f</td> <td>10.9.2.66</td> <td>802.11ng</td> <td>Excellent (25)</td> <td>Balance</td> <td>640.29 KB</td> <td>443.57 KB</td> </tr> <tr> <td>14:5a:05:80:4f:40</td> <td>10.9.2.76</td> <td>802.11ng</td> <td>Excellent (29)</td> <td>Balance</td> <td>2.24 KB</td> <td>3.67 KB</td> </tr> <tr> <td>00:1a:dd:c5:4e:24</td> <td>10.8.9.84</td> <td>802.11ng</td> <td>Excellent (29)</td> <td>Wireless</td> <td>9.86 MB</td> <td>9.76 MB</td> </tr> <tr> <td>00:1a:dd:bb:29:ec</td> <td>10.8.9.73</td> <td>802.11ng</td> <td>Excellent (25)</td> <td>Wireless</td> <td>9.36 MB</td> <td>11.14 MB</td> </tr> <tr> <td>40:b0:fa:c3:26:2c</td> <td>10.8.9.18</td> <td>802.11ng</td> <td>Good (23)</td> <td>Wireless</td> <td>118.05 MB</td> <td>7.92 MB</td> </tr> <tr> <td>e4:25:e7:8a:d3:12</td> <td>10.10.11.23</td> <td>802.11ng</td> <td>Excellent (35)</td> <td>Marketing</td> <td>74.78 MB</td> <td>4.58 MB</td> </tr> <tr> <td>04:f7:e4:ef:68:05</td> <td>10.10.11.71</td> <td>802.11ng</td> <td>Poor (12)</td> <td>Marketing</td> <td>84.84 KB</td> <td>119.32 KB</td> </tr> </tbody> </table> Close	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
	MAC Address	IP Address	Type	Signal	SSID	Upload	Download																																																																														
	80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB																																																																														
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB																																																																															
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB																																																																															
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB																																																																															
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB																																																																															
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB																																																																															
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB																																																																															
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB																																																																															
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB																																																																															
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB																																																																															
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB																																																																															
	Click the  icon to configure each client																																																																																				

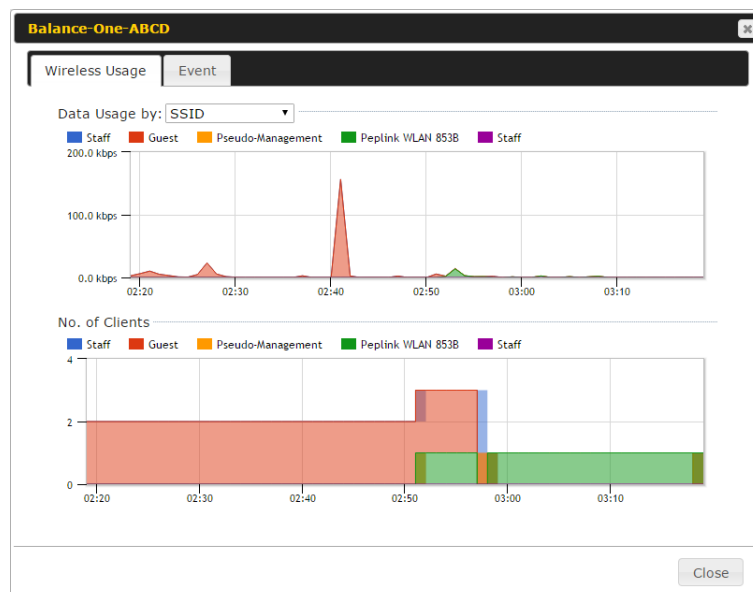
AP Details

Serial Number	1111-2222-3333		
MAC Address	00:1A:DD:BD:73:E0		
Product Name	Pepwave AP Pro Duo		
Name			
Location			
Firmware Version	3.5.2		
Firmware Pack	Default (None) ▼		
AP Client Limit	☒ Follow AP Profile ☐ 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.

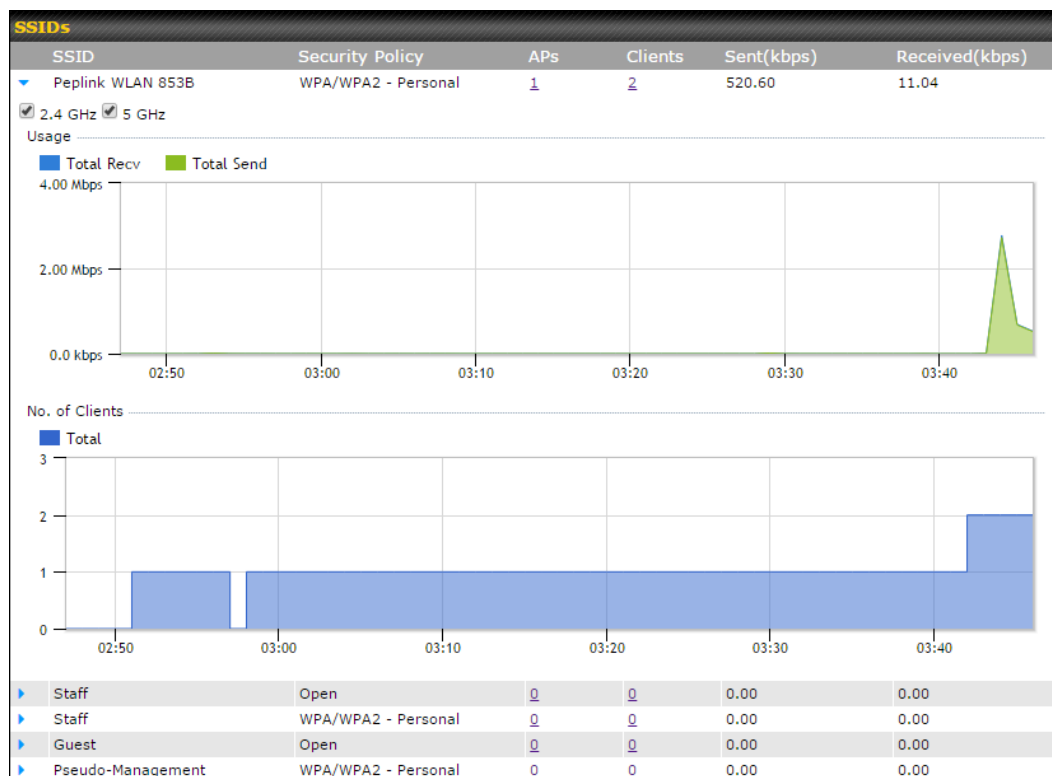
Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that

particular device:

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

26.3 Wireless SSID

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



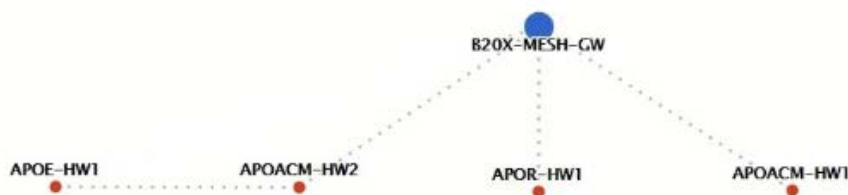
Click the blue arrow on any SSID to obtain more detailed usage information on each SSID.

26.4 Mesh / WDS

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

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

Network Graph



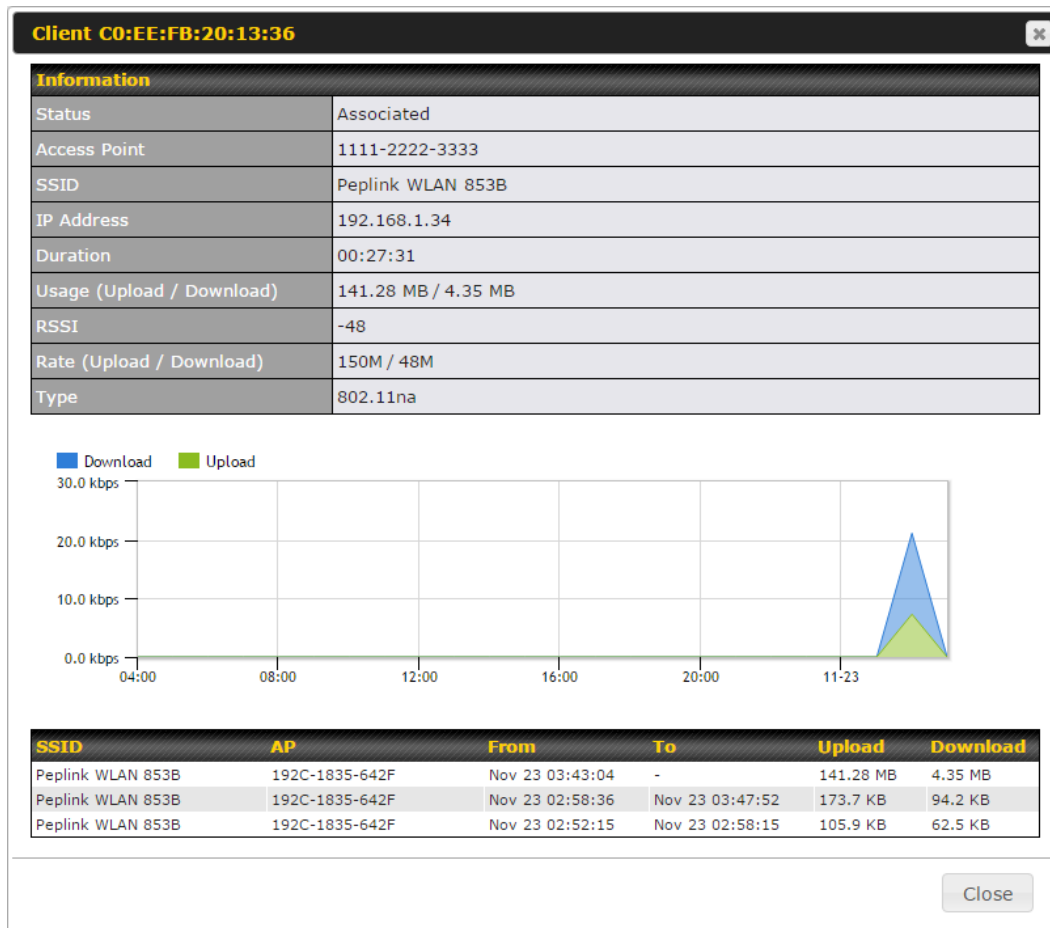
26.5 Wireless Client

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

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

Top 10 Clients of last hour (Updated at 03:00)			
Client MAC Address	Upload	Download	
C0:EE:FB:20:13:36	53.5 KB	101.4 KB	☆ 

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



26.6 Nearby Device

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

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

Suspected Rogue Devices

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

26.7 Event Log

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

Filter	
Search key	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name
Time	From hh:mm to hh:mm
Alerts only	☐
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		
Check for Updates Manual Upload Default... No default defined.			

Firmware Packs

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

28 System Settings

28.1 Admin Security

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

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

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

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

Admin Settings	
Router Name	MBX-345A hostname: mbx-345a ⚙️ This configuration is being managed by InControl .
Admin User Name	admin
Admin Password	••••••••
Confirm Admin Password	••••••••
Read-only User Name	DemoPep
User Password	••••••••
Confirm User Password	••••••~•
Web Session Timeout	4 Hours 0 Minutes
Authentication by RADIUS	☐ Enable
CLI SSH & Console	☐ Enable
Security	HTTP / HTTPS ☐ Redirect HTTP to HTTPS
Web Admin Access	HTTP: LAN Only HTTPS: LAN Only
Web Admin Port	HTTP: 80 HTTPS: 443 Default

LAN Connection Access Settings	
Allowed LAN Networks	☒ Any ☐ Allow this network only

Save

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

Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to 4 hours .
Authentication by RADIUS	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.
Auth Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.
Network Connection	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
CLI SSH	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to Section 30.5 .
CLI SSH 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	This option is for specifying the protocol(s) through which the web admin interface can be accessed: • HTTP • HTTPS • HTTP/HTTPS
Web Admin Port	This field is for specifying the port number on which the web admin interface can

	be accessed.
Web Admin Access	This option is for specifying the network interfaces through which the web admin interface can be accessed: • LAN only • LAN/WAN If LAN/WAN is chosen, the WAN Connection Access Settings form will be displayed.

LAN Connection Access Settings	
Allowed LAN Networks	☐ Any ☒ Allow this network only Public (10) ▼

LAN Connection Access Settings	
Allowed LAN Networks	This field allows you to permit only specific networks or VLANs to access the Web UI.

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

WAN Connection Access Settings	
Allowed Source IP Subnets	This field allows you to restrict web admin access only from defined IP subnets. • Any - Allow web admin accesses to be from anywhere, without IP address restriction. • Allow access from the following IP subnets only - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath: The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of <i>w.x.y.z/m</i>, where <i>w.x.y.z</i> is an IP address (e.g., 192.168.0.0), and <i>m</i> is the subnet mask in CIDR format, which is between 0 and

32 inclusively (For example, 192.168.0.0/24).

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

- 192.168.0.0/24
- 10.8.0.0/16

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

28.2 Firmware

Web admin interface : automatically check for updates

Upgrading firmware can be done in one of three ways.

Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

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

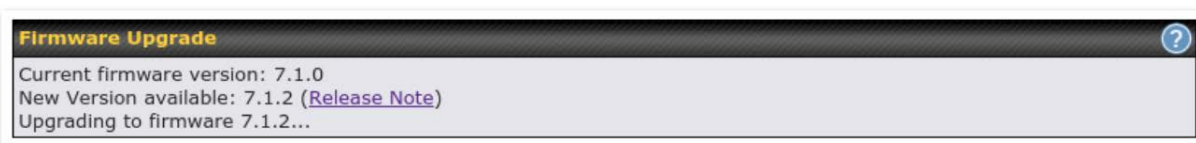


If an update is found the buttons will change to allow you to **Download and Update** the firmware.



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

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



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

Firmware Upgrade

It may take up to 8 minutes.



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

Web admin interface : install updates manually

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

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

Balance

Product

Search:

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.

Manual Firmware Upgrade
?

Firmware Image
No file chosen

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

Firmware Upgrade

It may take up to 8 minutes.



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

The InControl method

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

28.3 Time

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

Time Settings

Time Zone

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

Time Server

0.pepwave.pool.ntp.org

Time Settings

Time Zone

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

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	☒ Enable
SMTP Server	smtp.mycompany.com ☒ 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:

	• 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	☒ Enable
SMTP Server	 ☒ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	
SMTP Password	
Confirm SMTP Password	
Sender's Email Address	
Recipient's Email Address	

Test Email Notification **Save**

Test Result

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

28.6 Event Log

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

Send Events to Remote Syslog Server	
Remote Syslog	☐
Remote Syslog Host	
Port:	514

Push Events to Mobile Devices	
Push Events	☒

URL Logging	
Enable	☒
Log Server Host	
Port:	514

Session Logging	
Enable	☒
Log Server Host	
Port:	514

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

Session Logging Host

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



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

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	
SNMP Port	161 Default
SNMPv1	☐ Enable
SNMPv2c	☐ Enable
SNMPv3	☐ Enable
SNMP Trap	☒ Enable
SNMP Trap Community	
SNMP Trap Server	
SNMP Trap Port	162
SNMP Trap Server Heartbeat	☐
Save	

Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		
Add SNMP Community		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		
Add SNMP User		

SNMP Settings	
SNMP Device Name	This field shows the router name defined at System>Admin Security .
SNMP Port	This option specifies the port which SNMP will use. The default port is 161 .

SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.
SNMP Trap	This option allows you to enable SNMP Trap. If enabled, the following entry fields will appear.
SNMP Trap Community	This setting specifies the SNMP Trap community name.
SNMP Trap Server	Enter the IP address of the SNMP Trap server.
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	My Company	
Allowed Network	192.168.1.25	/ 255.255.255.0 (/24) ▼

Save
Cancel

SNMPv3 User

User Name	SNMPUser	
Authentication	SHA ▼	password
Privacy	DES ▼	privacypassword

Save
Cancel

SNMP Community Settings	
Community Name	This setting specifies the SNMP community name.

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

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

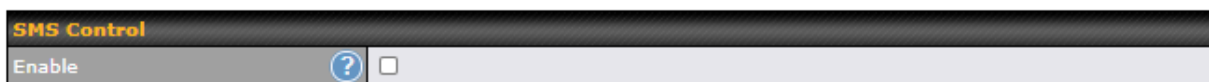
SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols: • NONE • MD5 • SHA When MD5 or SHA is selected, an entry field will appear for the password.
Privacy Protocol	This setting specifies via a drop-down menu one of the following valid privacy protocols: • 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*



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	☒				
Password	 ☒ Hide Characters				
White List	<table border="1"> <thead> <tr> <th>Phone Number</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td> + </td> </tr> </tbody> </table>	Phone Number			+
Phone Number					
	+				

Save

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	☒ InControl ☐ Restricted to Status Reporting Only
Privately Host InControl	☒
InControl Host	Primary: Backup: ☐ Fail over to InControl in the cloud.

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

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

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

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

28.10 Configuration

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

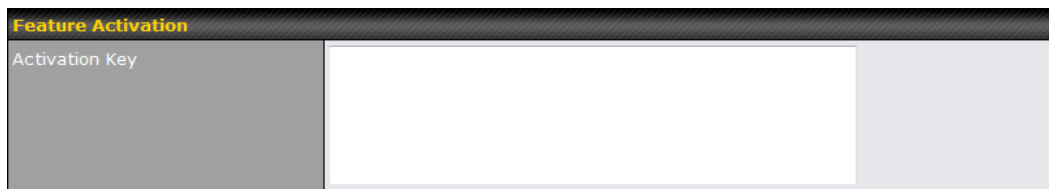
The image displays four sequential screenshots of the 'Configuration' page in the Pepwave web interface. Each screenshot shows a different section of the configuration menu, separated by horizontal lines. The first screenshot shows the 'Restore Configuration to Factory Settings' section with a 'Restore Factory Settings' button. The second screenshot shows the 'Download Active Configurations' section with a 'Download' button. The third screenshot shows the 'Upload Configurations' section with a 'Configuration File' input field, a 'Browse...' button, and an 'Upload' button. The fourth screenshot shows the 'Upload Configurations from High Availability Pair' section with a 'Configuration File' input field, a 'Browse...' button, and an 'Upload' button.

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

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

28.11 Feature Add-ons

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

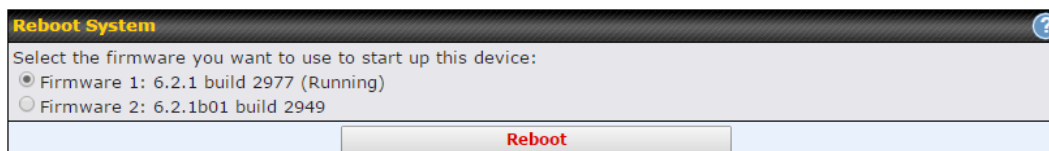


The screenshot shows a web interface titled "Feature Activation". It contains a label "Activation Key" followed by a large, empty text input field for entering the activation key.

28.12 Reboot

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

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



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

29 Tools

29.1 Ping

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

Ping	
Connection	WAN 1 ▼
Destination	10.10.10.1
Packet Size	56
Number of times	Times 5 <input type="range"/>

Results	Clear Log
PING 10.10.10.1 (10.10.10.1) from 10.88.3.158 56(84) bytes of data.	
64 bytes from 10.10.10.1: icmp_req=1 ttl=62 time=27.6 ms	
64 bytes from 10.10.10.1: icmp_req=2 ttl=62 time=26.5 ms	
64 bytes from 10.10.10.1: icmp_req=3 ttl=62 time=28.9 ms	
64 bytes from 10.10.10.1: icmp_req=4 ttl=62 time=28.3 ms	
64 bytes from 10.10.10.1: icmp_req=5 ttl=62 time=27.7 ms	

--- 10.10.10.1 ping statistics ---	
5 packets transmitted, 5 received, 0% packet loss, time 4005ms	
rtt min/avg/max/mdev = 26.516/27.855/28.933/0.814 ms	

Tip

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

29.2 Traceroute Test

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

[illegible]

Tip

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

29.3 PepVPN Test

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

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

PepVPN Throughput Test	
Profile	NY Office ▼
Type	☒ TCP ☐ UDP
Direction	☒ Upload ☐ Download
Duration	10 seconds (5 - 600)
Go!	
Results	
(Empty)	

29.4 Wake-on-LAN

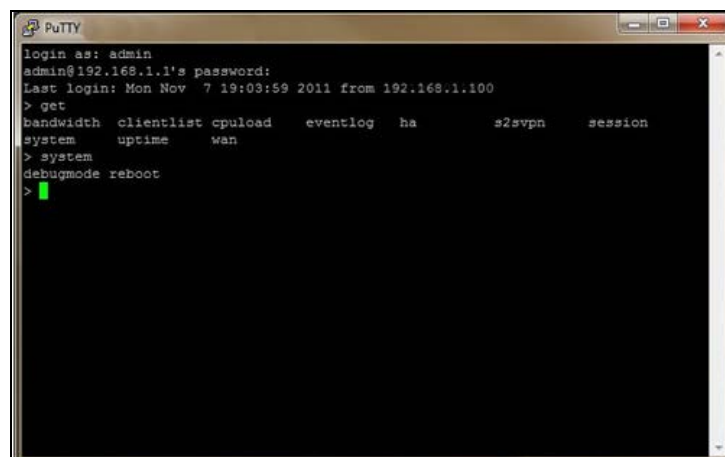
Peplink routers can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**

Wake-on-LAN	
Wake-on-LAN Target	Surf_SOHO (00:90:0B:36:3C:8C) ▼ Send

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

29.5 CLI (Command Line Interface Support)

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



```

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

30 Status

30.1 Device

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

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

MAC Address	
LAN	
WAN	
LAN 1 as WAN	

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

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

30.2 GPS Data

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

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

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

30.3 Active Sessions

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

Overview	Search
----------	--------

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

Service	Inbound Sessions	Outbound Sessions
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	☐ 1 WAN 1 ☐ 2 WAN 2 ☐ Wi-Fi WAN ☐ 1 Cellular 1 ☐ 2 Cellular 2 ☐ USB ☐ VPN	
Search		

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Transit

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

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

30.4 Client List

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

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

Filter		☐ 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.

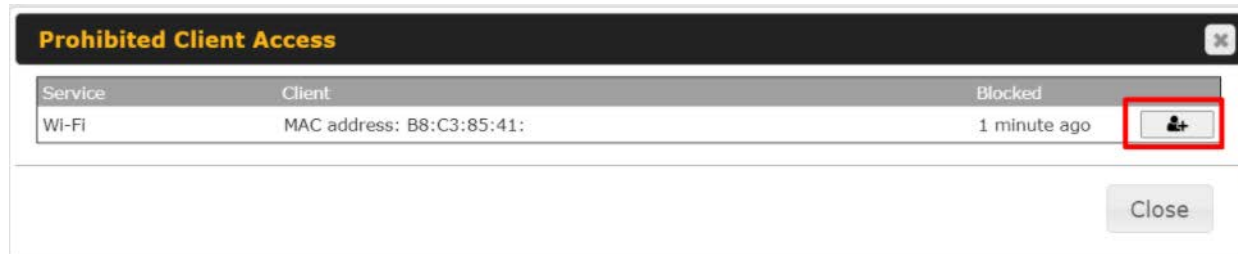
Filter		☐ Online Clients Only ☐ DHCP Clients Only						
Client List								
IP Address ▲	Type	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)	
 192.168.50.10		LAPTOP- 	279	14		PEPWAVE_ 	 -52	 
 192.168.50.12		max-hd2- 	0	0				 

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 WINS Client

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

WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4
Flush All	

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

WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4
Flush All	

30.6 UPnP / NAT-PMP

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

Forwarded Ports						
External	Internal	Internal Address	Type	Protocol	Description	
47453	3392	192.168.1.100	UPnP	UDP	Application 031	
35892	11265	192.168.1.50	NAT-PMP	TCP	NAT-PMP 58	
4500	3560	192.168.1.20	UPnP	TCP	Application 013	
5921	236	192.168.1.30	UPnP	TCP	Application 047	
22409	8943	192.168.1.70	NAT-PMP	UDP	NAT-PMP 97	
2388	27549	192.168.1.40	UPnP	TCP	Application 004	
						<button>Delete All</button>

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

Important Note

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

30.7 OSPF & RIPv2

Shows status of OSPF and RIPv2



Dashboard

Setup Wizard

Network

AP

System

Status

Apply Changes

Status

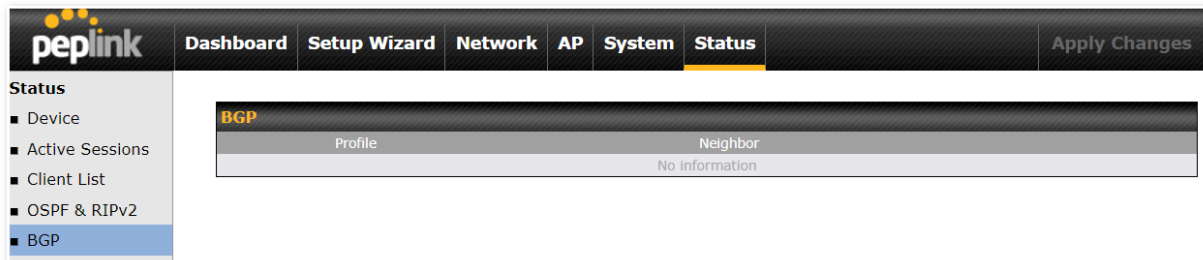
- Device
- Active Sessions
- Client List
- OSPF & RIPv2
- BGP

OSPF & RIPv2

Area	Remote Networks
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

30.8 BGP

Shows status of BGP



The screenshot shows the Peplink web interface. The top navigation bar includes 'Dashboard', 'Setup Wizard', 'Network', 'AP', 'System', and 'Status' (which is highlighted). Below the navigation bar, the 'Status' section is expanded, showing a sidebar with 'Device', 'Active Sessions', 'Client List', 'OSPF & RIPv2', and 'BGP' (which is selected). The main content area displays the 'BGP' status, which is currently 'No information'.

30.9 SpeedFusion Status

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

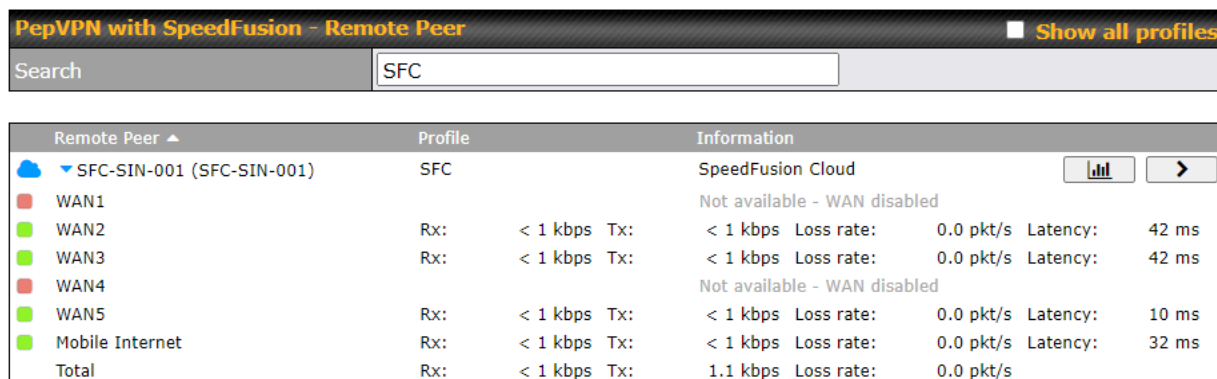
Details about SpeedFusion™ connection peers appears as below:



The screenshot shows the 'PepVPN with SpeedFusion - Remote Peer Details' page. It features a search bar and a 'Show disconnected profiles' checkbox. Below the search bar, there is a table with three columns: 'Remote Peer', 'Profile', and 'Information'. The table lists two remote peers: 'ADA0-FFFC-11F8' with profile 'FH' and IP '192.168.77.0/24', and '3ED2-8F63-1824' with profile '380-5 - NO NAT' and IP '192.168.3.0/24'. Each row has a status icon (a lock) and a 'Show disconnected profiles' checkbox.

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

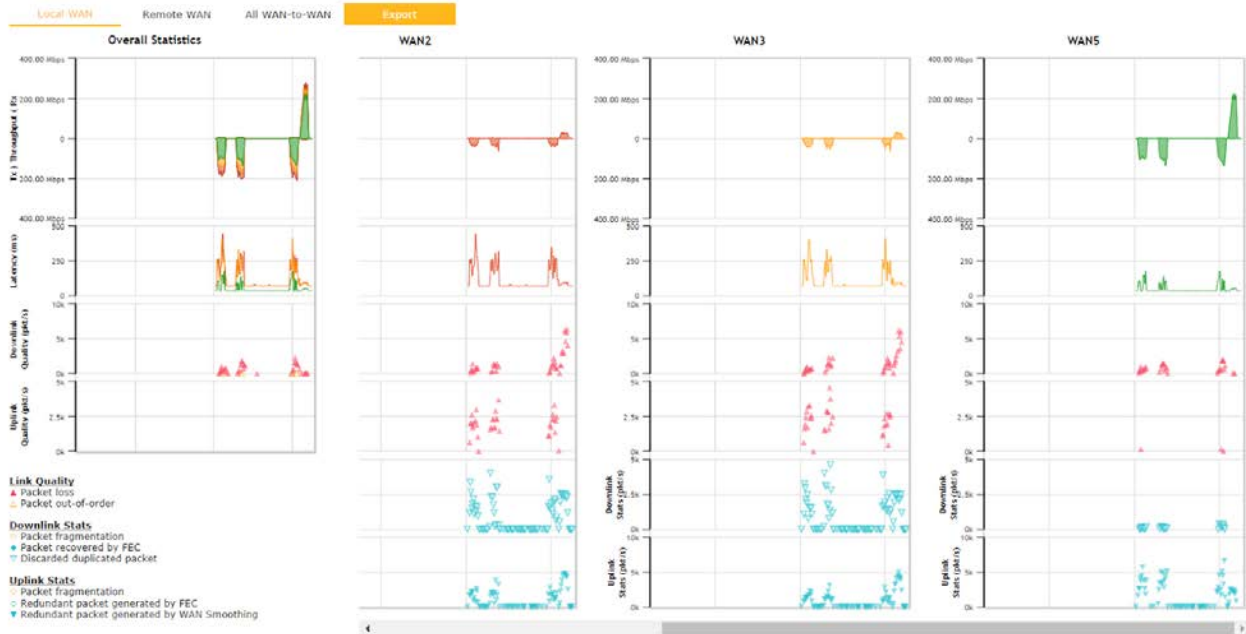
Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.

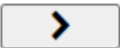


The screenshot shows the 'PepVPN with SpeedFusion - Remote Peer' page. It features a search bar and a 'Show all profiles' checkbox. Below the search bar, there is a table with three columns: 'Remote Peer', 'Profile', and 'Information'. The table lists a single remote peer: 'SFC-SIN-001 (SFC-SIN-001)' with profile 'SFC'. The 'Information' column shows 'SpeedFusion Cloud' and a list of WAN connections (WAN1, WAN2, WAN3, WAN4, WAN5, Mobile Internet, Total) with their respective status (Not available - WAN disabled) and performance metrics (Rx/Tx rate, Loss rate, Latency).

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

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



When pressing the  button, the following menu will appear:

PepVPN Details

Connection Information		More information
Profile	SFC	
Remote ID	SFC-SIN-001	
Device Name	SFC-SIN-001	
Serial Number	1197-A047-2E3D	

WAN Statistics

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

PepVPN Test Configuration

Type	TCP UDP		Start
Streams	4		
Direction	Upload Download		
Duration	20 seconds (5 - 600)		

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

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

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

30.10 Event Log

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

Device Event Log

Device Event Log

☒ Auto Refresh

Mar 22 14:29:44	System: Changes applied
Mar 22 14:28:29	System: Changes applied
Mar 22 14:00:26	WAN: Wi-Fi WAN connected to PEPLINK_1 (10.22.1.152)
Mar 22 11:47:45	Admin: DemoPep (10.22.1.160) login successful
Mar 22 11:47:28	Admin: admin (10.22.1.160) login failed
Mar 22 11:46:59	System: Changes applied
Mar 22 11:45:42	System: Changes applied
Mar 20 15:43:27	System: Changes applied
Mar 20 11:20:15	System: Changes applied
Mar 19 15:23:26	System: Changes applied
Mar 19 15:21:35	System: Changes applied
Mar 19 15:21:31	System: InControl has updated the configuration as InControl configuration updated
Mar 19 15:21:31	System: LAN Configuration has been updated by InControl
Mar 19 15:07:38	System: Changes applied
Mar 19 14:09:27	System: WAN Analysis server stopped
Mar 19 14:09:22	System: WAN Analysis server started (control port: 6000, max. streams: 8)
Mar 19 14:05:30	WAN: WAN 2 connected (10.22.1.165)
Mar 19 14:05:30	WAN: WAN 1 connected (10.22.1.151)
Mar 19 14:05:18	WAN: WAN 2 disconnected
Mar 19 14:05:18	WAN: WAN 1 disconnected
Mar 19 14:05:18	System: Changes applied
Mar 19 13:56:31	WAN: WAN 2 connected (10.22.1.165)

Clear Log

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

31 WAN Quality



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

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

32 Usage Reports

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

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

32.1 Real-Time

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

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

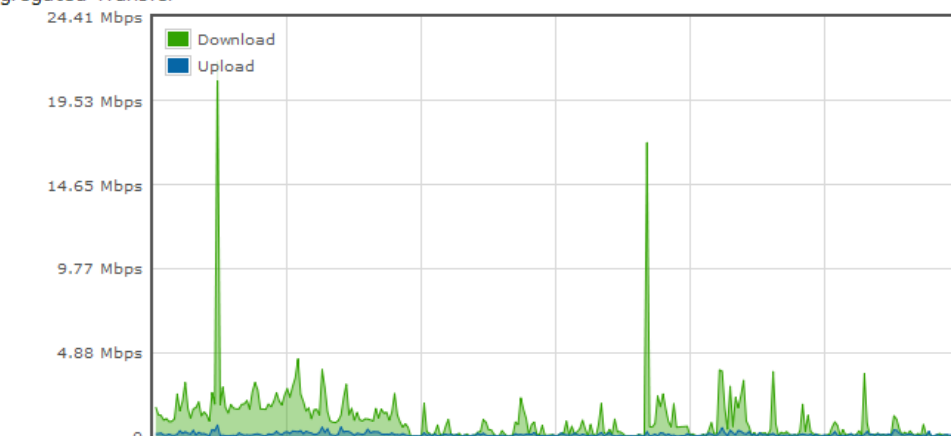
	Download	Upload	Total
All WAN Connections	216.68 GB	91.70 GB	308.38 GB

Data transferred since last reboot

[\[Hide Details \]](#)

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

Aggregated Transfer



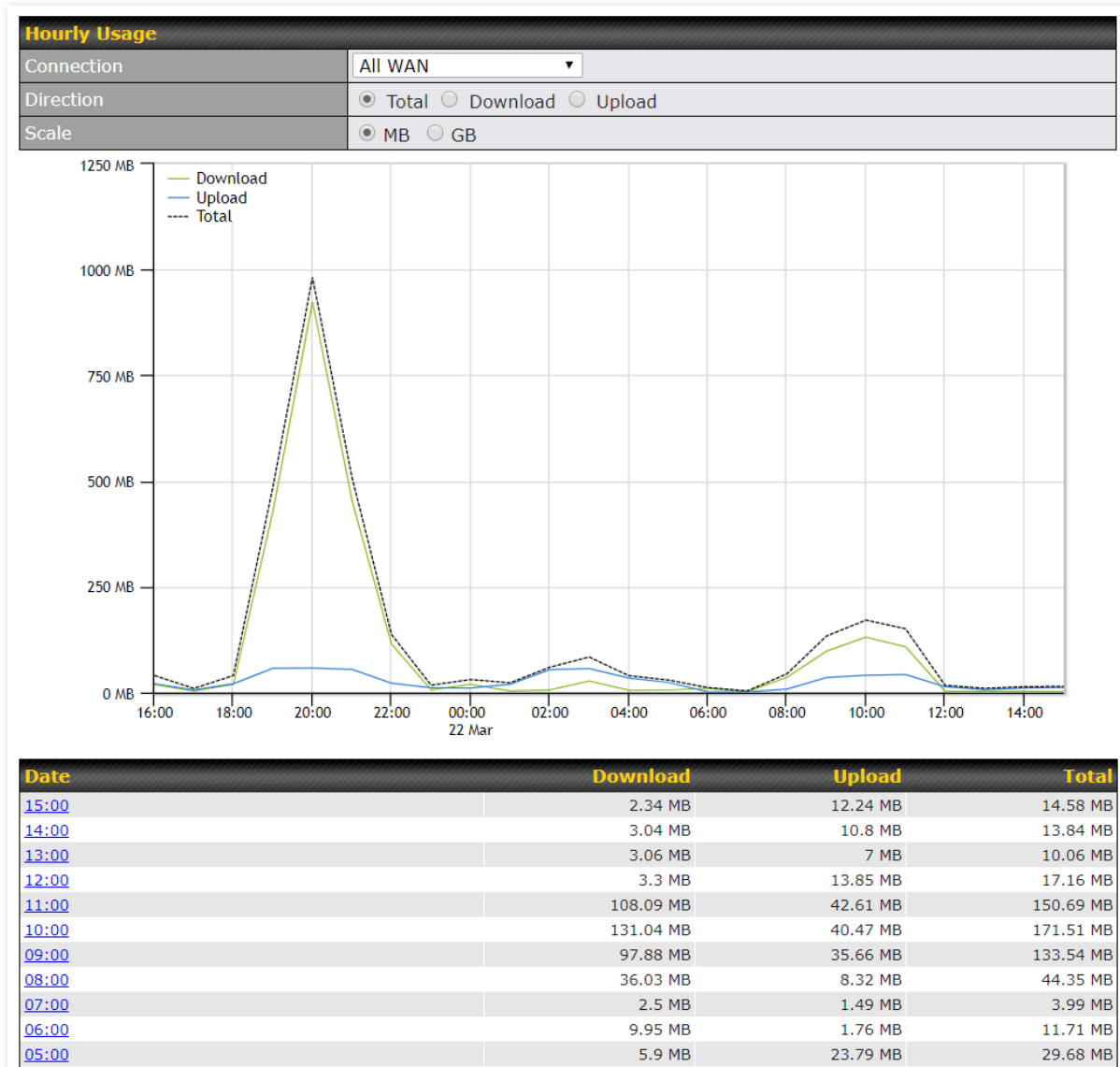
Avg: ↓ 0.99 Mbps ↑ 0.12 Mbps Peak: ↓ 21.78 Mbps ↑ 0.67 Mbps

Stacked ☐

	Download	Upload	Total
Overall	61 kbps	75 kbps	136 kbps

32.2 Hourly

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



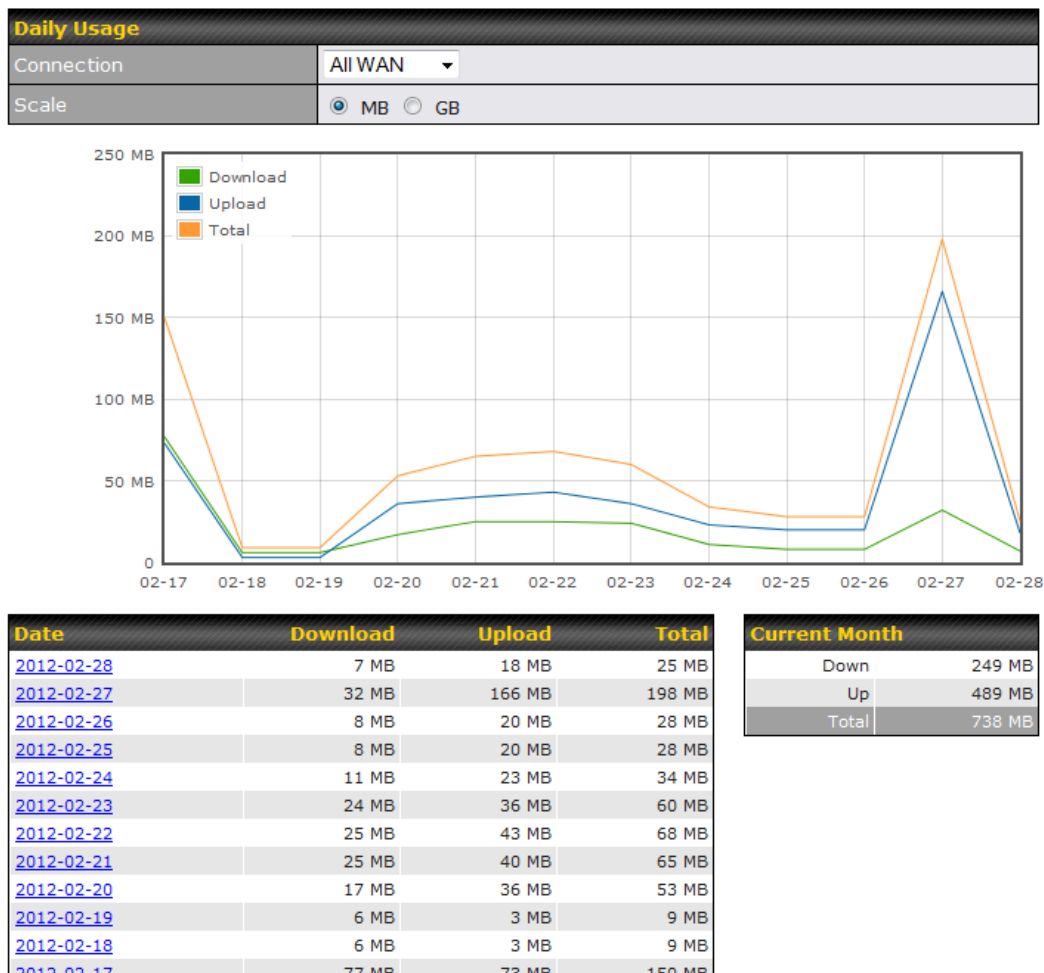
32.3 Daily

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

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

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection.

The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).

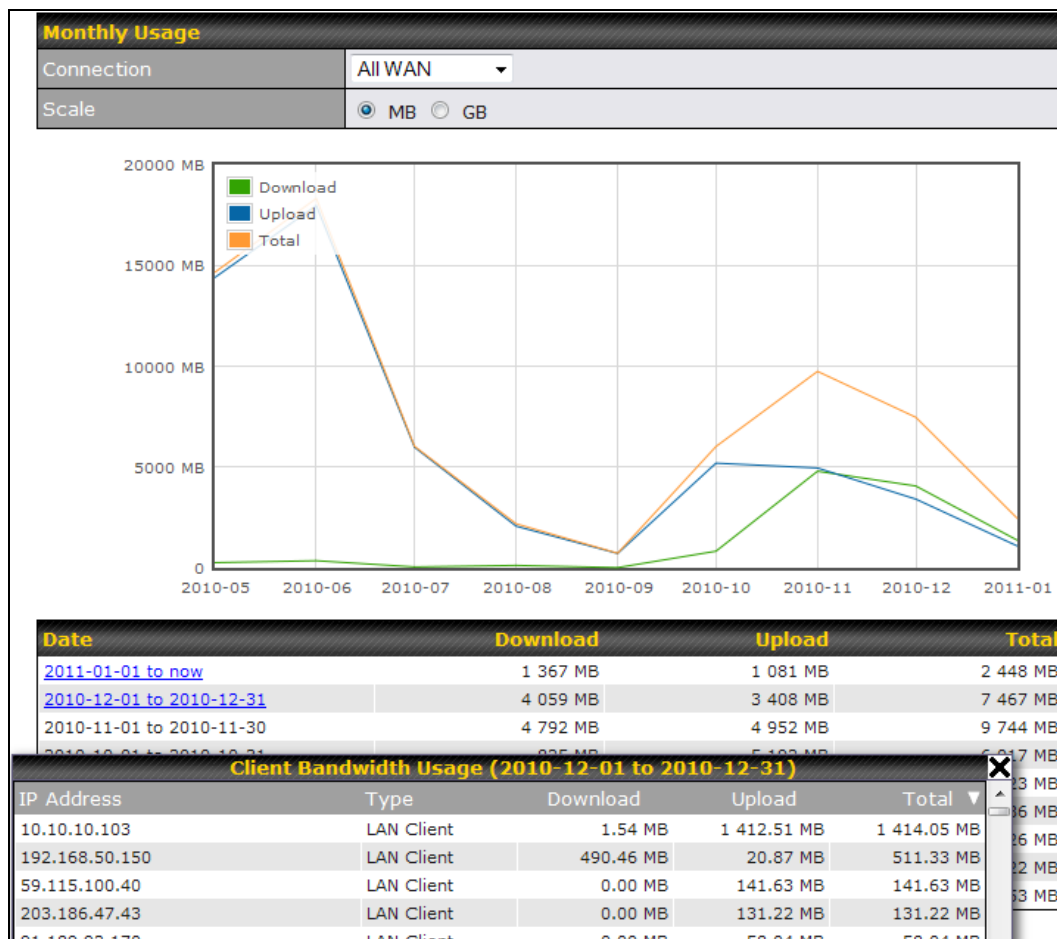


All WAN Daily Bandwidth Usage

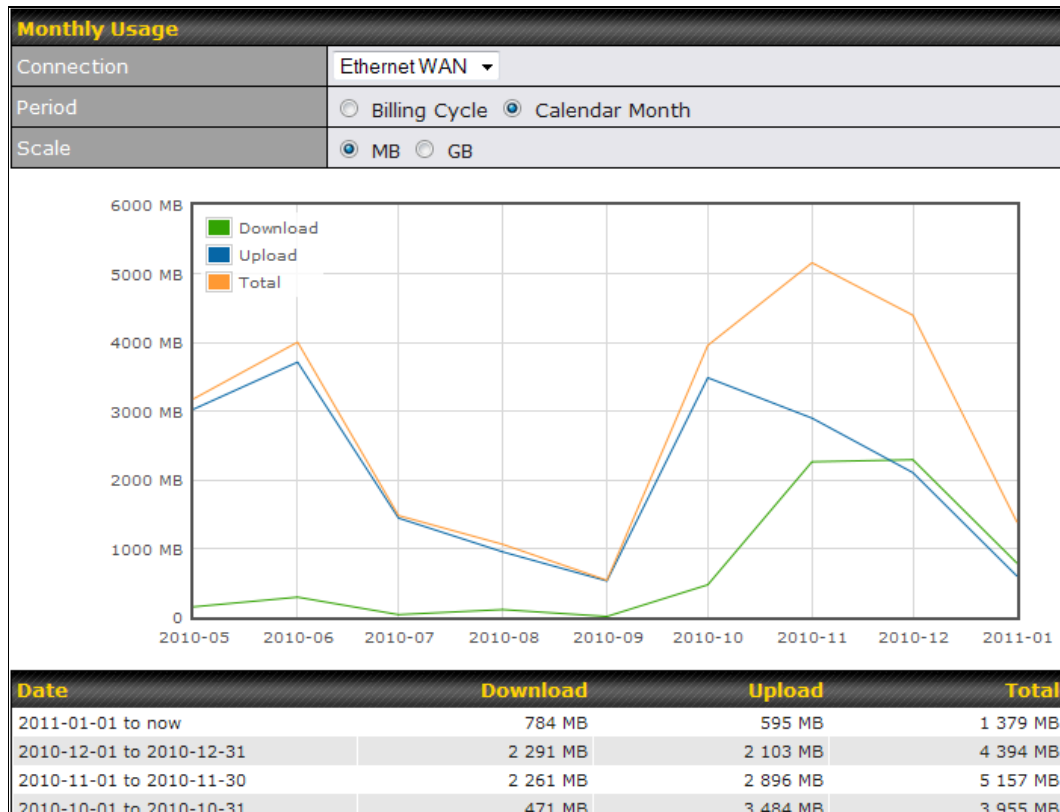
32.4 Monthly

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

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



All WAN Monthly Bandwidth Usage



Ethernet WAN Monthly Bandwidth Usage

Tip

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

Appendix A: Restoration of Factory Defaults

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

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

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

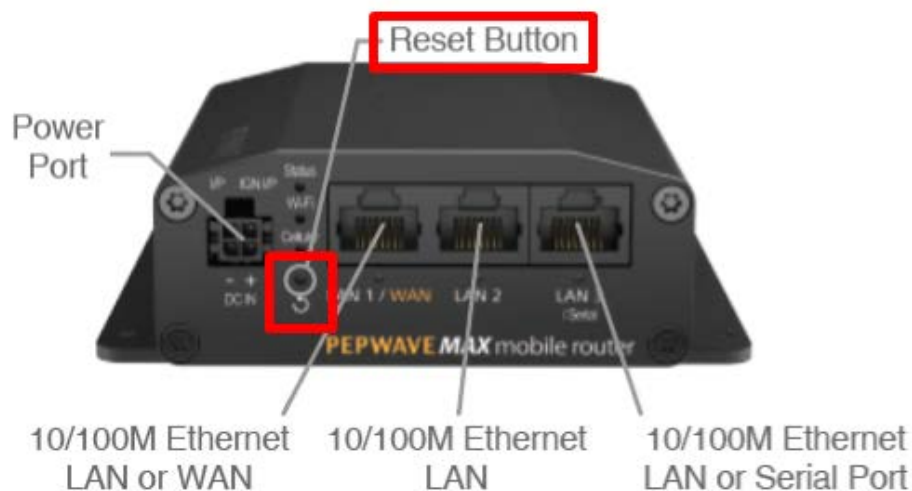
Hold for 5-10 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

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

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

Important Note

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



Appendix B: FusionSIM Manual

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

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

Requirements

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

Notes:

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

SIM Injector reset and login details

How to reset a SIM Injector:

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

The default WEB login settings:

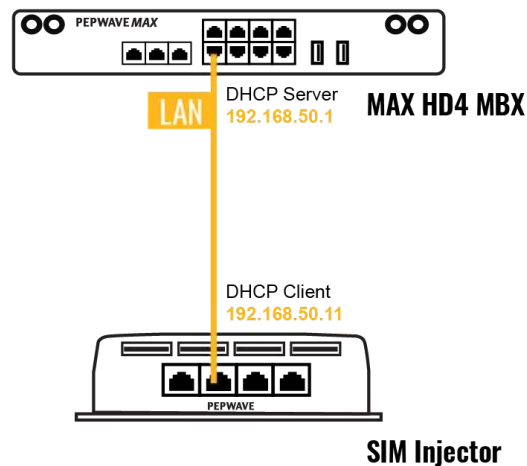
- **User:** admin
- **Password:** admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

Notes:

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

Scenario 1: SIM Injector in LAN of Cellular Router

Setup topology



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

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

Configuring the SIM Injector

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

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

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

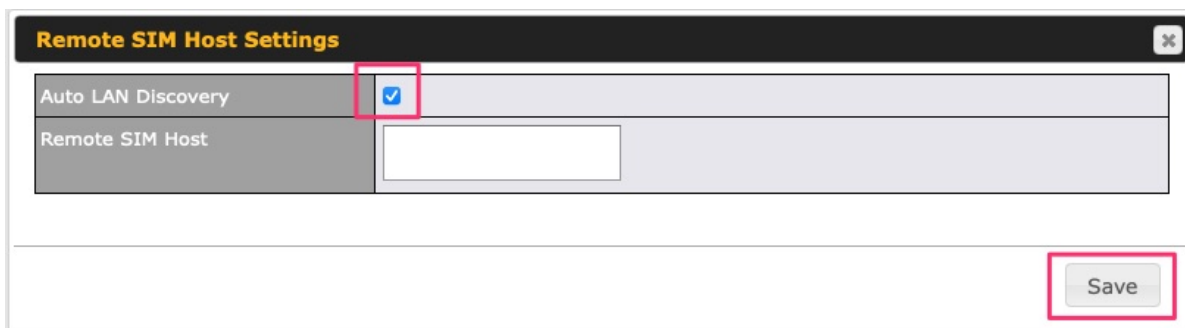
Configuring the Cellular Router

Step 1. Enable the SIM Injector communication protocol.

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



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



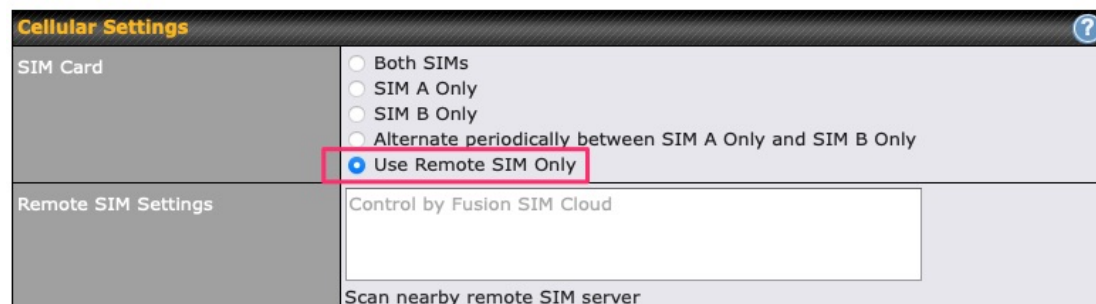
5. Click **Save** and then **Apply Changes**.

Step 2. Enable RemoteSIM for the selected Cellular interface.

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

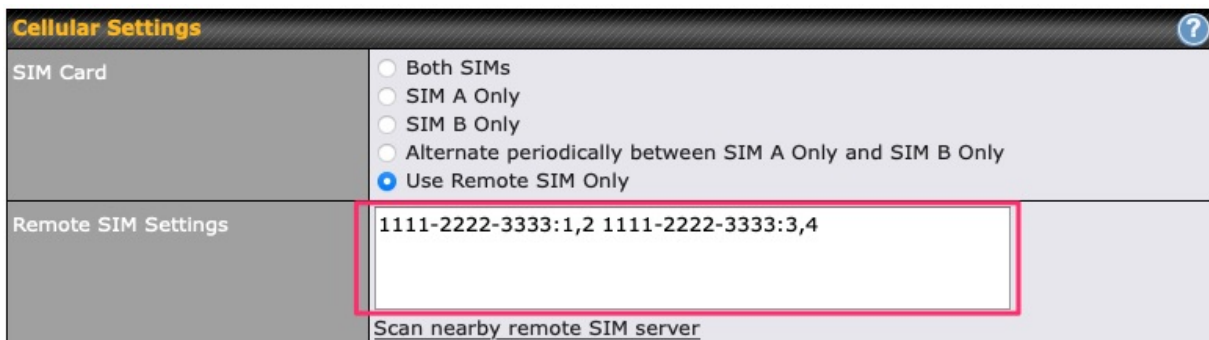


2. Scroll down to **Cellular settings**.
3. In the **SIM Card** section, select **Use Remote SIM Only**.



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

- A. Defining SIM Injector(s)
 - Format: <S/N>
 - Example 1: 1111-2222-3333
 - Example 2: 1111-2222-3333 4444-5555-6666
- B. Defining SIM Injector(s) SIM slot(s):
 - Format: <S/N:slot number>
 - Example 1: 1111-2222-3333:7,5 (the Cellular Interface will use SIM in slot 7, then 5)
 - Example 2: 1111-2222-3333:1,2 1111-2222-3333:3,4 (the cellular Interface will use SIM in slot 1, then in 2 from the first SIM Injector, and then it will use 3 and 4 from the second SIM Injector).



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

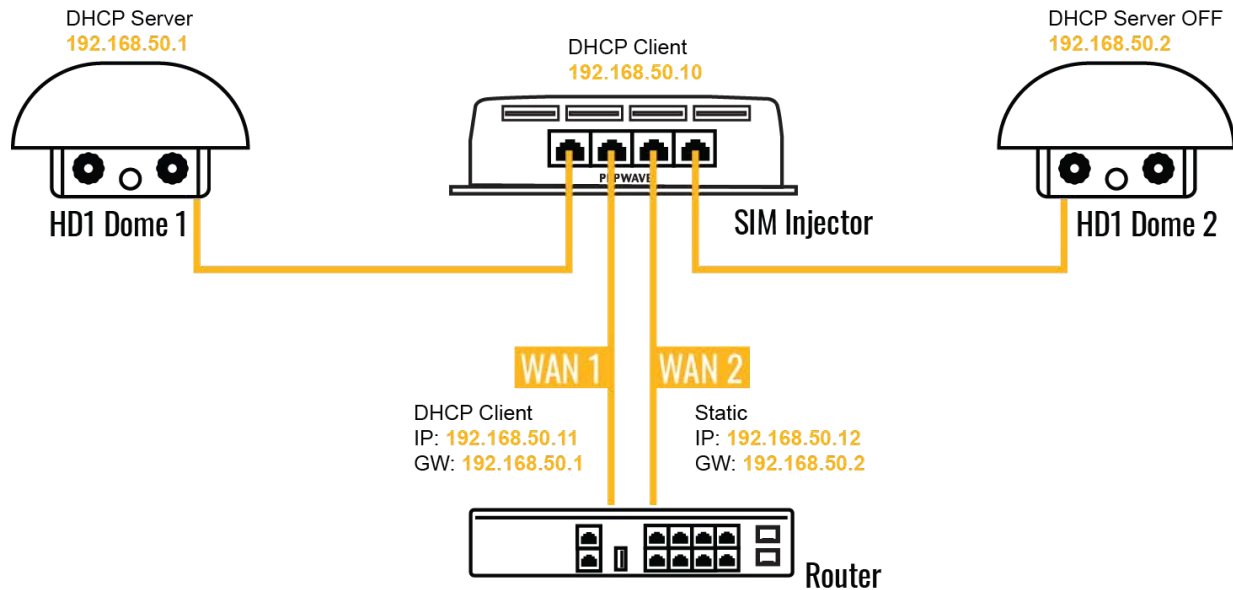
5. Click **Save** and **Apply Changes**.

Step 3. (Optional) Custom SIM cards settings.

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

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

Setup topology



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

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

Additional configurations for Cellular Routers

Step 1. Disable the DHCP server.

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