

## 15 Outbound Policy Management

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

### Important Note

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

The settings for managing and load balancing outbound traffic are located at **Advanced>Outbound Policy** or **Advanced>PepVPN**, depending on model.

Service	Algorithm	Source	Destination	Protocol / Port
HTTPS_Persistence	(Auto)	Any	Any	TCP 443
Default	(Auto)			

Outbound policies for managing and load balancing outbound traffic are located at **Network>Outbound Policy** or **Advanced>PepVPN>Outbound Policy**.

Outbound Policy  
Select an Outbound Policy  
Policy: High Application Compatibility  
Save Cancel

### 15.1 Outbound Policy

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.

# Pepwave Routers User Manual

Load Distribution Weight
WAN 1 10
WAN 2 10
WAN 3 10
WAN 4 10
WAN 5 10
WAN 6 10
WAN 7 10
WAN 8 10
WAN 9 10
WAN 10 10
WAN 11 10
WAN 12 10
Mobile Internet 10

Terminate Sessions on Link Recovery  Enable

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.

### 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!

peplink Dashboard Setup Wizard Network System Status Apply Changes

New Custom Rule

Service Name: Any

Source: Any

Destination: Domain Name

Protocol: Any

Algorithm: Weighted Balance

Load Distribution Weight

WAN 1 10

WAN 2 10

WAN 3 10

WAN 4 10

WAN 5 10

WAN 6 10

WAN 7 10

WAN 8 10

WAN 9 10

WAN 10 10

WAN 11 10

WAN 12 10

Mobile Internet 10

Terminate Sessions on Link Recovery  Enable

http://youtu.be/rKH4AS\_bQnE

## 15.2 Custom Rules for Outbound Policy

Click in the **Outbound Policy** form. Choose **Custom** and press the **Save** button.

Service	Algorithm	Source	Destination	Protocol / Port
HTTPS_Persistence	(Auto)	Any	Any	TCP 443
Default	(Auto)			

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.

# Pepwave Routers User Manual

To create a custom rule, click **Add Rule** at the bottom of the table. Note that some Pepwave routers display this button at [Advanced>PepVPN>PepVPN Outbound Custom Rules](#).

Add a New Custom Rule

Service Name:

Enable:

Source: Any

Destination: Domain Name

Protocol: Any

Algorithm: Weighted Balance

Load Distribution Weight

WAN 1 10

WAN 2 10

WAN 3 10

WAN 4 10

WAN 5 10

WAN 6 10

WAN 7 10

WAN 8 10

WAN 9 10

WAN 10 10

WAN 11 10

WAN 12 10

Mobile Internet 10

Terminate Sessions on Link Recovery  Enable

Save Cancel

### New Custom Rule Settings

<b>Service Name</b>	This setting specifies the name of the outbound traffic rule.
<b>Enable</b>	This setting specifies whether the outbound traffic rule takes effect. When <b>Enable</b> 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 <b>Enable</b> is unchecked, the rule does not take effect; the Pepwave router disregards the other parameters of the rule.
<b>Source</b>	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.
<b>Destination</b>	This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.

Destination	Domain Name <input type="text"/>
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> IP Address <input type="radio"/> IP Network
Algorithm	<input checked="" type="radio"/> Domain Name <input type="radio"/> IP Address
<p>If Domain Name is chosen, any domain name, such as <code>foobar.com</code>, is entered, any outgoing accesses to <code>foobar.com</code> and <code>*.foobar.com</code> 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 <code>foobar*</code>, for example, <code>www.foobar.com</code>, <code>www.foobar.co.jp</code>, or <code>foobar.co.uk</code> will also match. Placing wildcards in any other position is not supported.</p> <p>NOTE: If a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.</p>	
<b>Protocol and Port</b> This setting specifies the IP protocol and port of traffic that matches this rule.	
<p>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):</p> <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Weighted Balance</li> <li><input type="radio"/> Persistence</li> <li><input type="radio"/> Enforced</li> <li><input type="radio"/> Priority</li> <li><input type="radio"/> Overflow</li> <li><input type="radio"/> Least Used</li> <li><input type="radio"/> Lowest Latency</li> </ul> <p>The upcoming sections detail the listed algorithms.</p>	
<p><b>Terminate Sessions on Link Recovery</b> 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 <b>Weighted</b>, <b>Persistence</b>, and <b>Priority</b> algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.</p>	

### 15.2.1 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	<input checked="" type="radio"/> Weighted Balance						
Load Distribution Weight	<table border="1"> <tr><td>WAN 1: 10</td></tr> <tr><td>WAN 2: 10</td></tr> <tr><td>Wi-Fi WAN: 10</td></tr> <tr><td>Cellular 1: 10</td></tr> <tr><td>Cellular 2: 10</td></tr> <tr><td>USB: 10</td></tr> </table>	WAN 1: 10	WAN 2: 10	Wi-Fi WAN: 10	Cellular 1: 10	Cellular 2: 10	USB: 10
WAN 1: 10							
WAN 2: 10							
Wi-Fi WAN: 10							
Cellular 1: 10							
Cellular 2: 10							
USB: 10							
<p>Terminate Sessions on Link Recovery <input type="checkbox"/> Enable</p>							

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%).

### 15.2.2 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	<input checked="" type="radio"/> Persistence			
Persistence Mode	<input checked="" type="radio"/> By Source <input type="radio"/> By Destination			
Load Distribution	<input checked="" type="radio"/> Auto <input type="radio"/> Custom			
Load Distribution Weight	<table border="1"> <tr><td>WAN 1: 10</td></tr> <tr><td>WAN 2: 10</td></tr> <tr><td>WAN 3: 10</td></tr> </table>	WAN 1: 10	WAN 2: 10	WAN 3: 10
WAN 1: 10				
WAN 2: 10				
WAN 3: 10				

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

<b>By Source:</b>	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.
<b>By Destination:</b>	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.

### 15.2.3 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**.

Algorithm	<input checked="" type="radio"/> Enforced													
Enforced Connection	<table border="1"> <tr><td>WAN: WAN 1</td></tr> <tr><td>WAN: WAN 2</td></tr> <tr><td>WAN: WAN 3</td></tr> <tr><td>WAN: WAN 4</td></tr> <tr><td>WAN: WAN 5</td></tr> <tr><td>WAN: WAN 6</td></tr> <tr><td>WAN: WAN 7</td></tr> <tr><td>WAN: WAN 8</td></tr> <tr><td>WAN: WAN 9</td></tr> <tr><td>WAN: WAN 10</td></tr> <tr><td>WAN: WAN 11</td></tr> <tr><td>WAN: WAN 12</td></tr> <tr><td>WAN: Mobile Internet</td></tr> </table>	WAN: WAN 1	WAN: WAN 2	WAN: WAN 3	WAN: WAN 4	WAN: WAN 5	WAN: WAN 6	WAN: WAN 7	WAN: WAN 8	WAN: WAN 9	WAN: WAN 10	WAN: WAN 11	WAN: WAN 12	WAN: Mobile Internet
WAN: WAN 1														
WAN: WAN 2														
WAN: WAN 3														
WAN: WAN 4														
WAN: WAN 5														
WAN: WAN 6														
WAN: WAN 7														
WAN: WAN 8														
WAN: WAN 9														
WAN: WAN 10														
WAN: WAN 11														
WAN: WAN 12														
WAN: Mobile Internet														
<p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p>														

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.

### 15.2.4 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	<input checked="" type="radio"/> Priority																												
Priority Order	<table border="1"> <tr><td>Highest Priority</td><td>Not In Use</td></tr> <tr><td>WAN: WAN 1</td><td><input checked="" type="checkbox"/> WAN: WAN 7</td></tr> <tr><td>WAN: WAN 2</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 3</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 4</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 5</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 6</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 8</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 9</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 10</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 11</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: WAN 12</td><td><input type="checkbox"/></td></tr> <tr><td>WAN: Mobile Internet</td><td><input type="checkbox"/></td></tr> <tr><td colspan="2">Lowest Priority</td></tr> </table>	Highest Priority	Not In Use	WAN: WAN 1	<input checked="" type="checkbox"/> WAN: WAN 7	WAN: WAN 2	<input type="checkbox"/>	WAN: WAN 3	<input type="checkbox"/>	WAN: WAN 4	<input type="checkbox"/>	WAN: WAN 5	<input type="checkbox"/>	WAN: WAN 6	<input type="checkbox"/>	WAN: WAN 8	<input type="checkbox"/>	WAN: WAN 9	<input type="checkbox"/>	WAN: WAN 10	<input type="checkbox"/>	WAN: WAN 11	<input type="checkbox"/>	WAN: WAN 12	<input type="checkbox"/>	WAN: Mobile Internet	<input type="checkbox"/>	Lowest Priority	
Highest Priority	Not In Use																												
WAN: WAN 1	<input checked="" type="checkbox"/> WAN: WAN 7																												
WAN: WAN 2	<input type="checkbox"/>																												
WAN: WAN 3	<input type="checkbox"/>																												
WAN: WAN 4	<input type="checkbox"/>																												
WAN: WAN 5	<input type="checkbox"/>																												
WAN: WAN 6	<input type="checkbox"/>																												
WAN: WAN 8	<input type="checkbox"/>																												
WAN: WAN 9	<input type="checkbox"/>																												
WAN: WAN 10	<input type="checkbox"/>																												
WAN: WAN 11	<input type="checkbox"/>																												
WAN: WAN 12	<input type="checkbox"/>																												
WAN: Mobile Internet	<input type="checkbox"/>																												
Lowest Priority																													

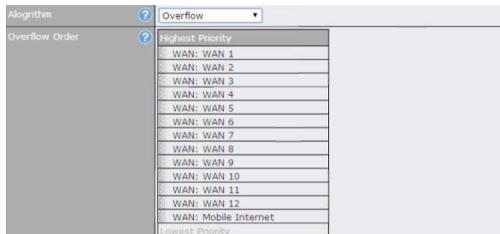
Starting from Firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion™ connection(s). By default, VPN connections are not included in the priority list.

**Tip**

Configure multiple distribution rules to accommodate different kinds of services.

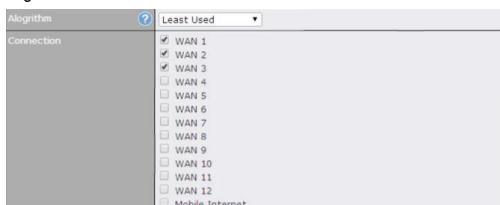
## 15.2.5 Algorithm: Overflow

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.



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.

## 15.2.6 Algorithm: Least Used



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.

## 15.2.7 Algorithm: Lowest Latency

Algorithm	Lowest Latency
Connection	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input type="checkbox"/> WAN 6 <input type="checkbox"/> WAN 7 <input type="checkbox"/> WAN 8 <input type="checkbox"/> WAN 9 <input type="checkbox"/> WAN 10 <input type="checkbox"/> WAN 11 <input type="checkbox"/> WAN 12 <input type="checkbox"/> Mobile Internet

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 round trip 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;
- A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN's available bandwidth.

## 15.2.8 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.

**Help** **Close**  
This table allows you to fine tune how the outbound traffic should be distributed across the WAN connections.  
Click the **Add Rule** button to add a new rule. Click the **Up** and **Down** buttons to re-order the rule. Drag a rule to promote or demote its position. The position of a rule signifies a higher precedence. You may change the default outgoing connection by clicking the **Default** link.  
If you require advanced control of S2S VPN traffic, turn on **Expert Mode**.

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

Custom Rules (Drag and drop rows to change rule order)				
Service	Algorithm	Source	Destination	Protocol / Port
HTTPS_Pass...	Persistence (Src) (Auto)	Any	IP Network 192.168.50.0/24	TCP 443
Site-to-Site VPN Routes				
Default	Lowest Latency			
<a href="#">Add Rule</a>				

## 16 Inbound Access

### 16.1 Port Forwarding Service

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		
	<a href="#">Add Service</a>		

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

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Service Name	Service_1
IP Protocol	TCP
Port	Single Port
Inbound IP Address(es)	(Require at least one IP address)
Connection / IP Address(es)	<input checked="" type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB
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 host(s) 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.

## Pepwave Routers User Manual

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

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

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

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

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

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

**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.

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

### 16.1.1 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.

<http://www.pepwave.com>

93

Copyright @ 2014 Pepwave

## Pepwave Routers User Manual

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

**UPnP / NAT-PMP Settings**

UPnP	<input checked="" type="checkbox"/> Enable
NAT-PMP	<input checked="" type="checkbox"/> 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**.

## Pepwave Routers User Manual

### 17 NAT Mappings

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

LAN Host	Inbound Mappings	Outbound Mappings	Action
192.168.1.23	(WAN1):29.123.123.13	(WAN1):29.123.123.13	<input type="button" value="Delete"/>
192.168.1.24	(WAN2):30.21.21.12	(WAN2):30.21.21.12	<input type="button" value="Delete"/>

**Add NAT Rule**

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

<b>Inbound Mappings</b>	<b>Connection / Inbound IP Address(es)</b>												
	<ul style="list-style-type: none"> <li>WAN 1</li> <li>WAN 2</li> <li>Wi-Fi WAN</li> <li>Cellular 1</li> <li>Cellular 2</li> <li>USB</li> </ul>												
<b>Outbound Mappings</b>	<b>Connection / Outbound IP Address</b>												
	<table border="1"> <tr> <td>WAN 1</td> <td>10.90.0.74 (Interface IP)</td> </tr> <tr> <td>WAN 2</td> <td>10.90.0.67 (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	10.90.0.74 (Interface IP)	WAN 2	10.90.0.67 (Interface IP)	Wi-Fi WAN	Interface IP	Cellular 1	Interface IP	Cellular 2	Interface IP	USB	Interface IP
WAN 1	10.90.0.74 (Interface IP)												
WAN 2	10.90.0.67 (Interface IP)												
Wi-Fi WAN	Interface IP												
Cellular 1	Interface IP												
Cellular 2	Interface IP												
USB	Interface IP												

## Pepwave Routers User Manual

### 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.

### NAT Mapping Settings

<b>LAN Client(s)</b>	NAT mapping rules can be defined for a single LAN IP Address, an IP Range, or an IP Network.
<b>Address</b>	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 <b>IP Address</b> is selected.
<b>Range</b>	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 <b>IP Range</b> is selected.
<b>Network</b>	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 <b>IP Network</b> is selected.

<http://www.pepwave.com>

95

Copyright @ 2014 Pepwave

<http://www.pepwave.com>

96

Copyright @ 2014 Pepwave

## 18 QoS

### 18.1 User Groups

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

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

Click the **Add** button to define clients and their user group. Click the **X** 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.

Client	Subnet / IP Address	Group
Staff A	IP Address - 192.168.1.99	Manager
		(192.168.1.99)

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

**Group** This field is to define which **User Group** the specified subnet / IP address belongs to.

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

### 18.3.2 Prioritization for Custom Applications

Click the **Add** button to define a custom application. Click the button **X** 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.

Type	Supported Applications	Custom Applications
Category	Audio/Video Streaming	
Application	Audio/Video Streaming	

### 18.3.3 DSL/Cable Optimization

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

DSL/Cable Optimization	Enable
------------------------	--------

## 18.2 Bandwidth Control

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

User Bandwidth Limit	Download	Upload
Manager: Unlimited	0 Mbps	0 Mbps
Staff:	(0: unlimited)	(0: unlimited)
Guest:	(0: unlimited)	(0: unlimited)

## 18.3 Application

### 18.3.1 Application Prioritization

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

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	Normal
All Email Protocols	High	High	High	Normal
MySQL	High	Normal	Low	Normal
SIP	High	Low	Low	Low

## 19 Firewall

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

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

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

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

Outbound Firewall Rules	Drag and drop rows to change rule order			
Rule	Protocol	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Allow

Inbound Firewall Rules	Drag and drop rows to change rule order			
Rule	Protocol	WAN Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Allow

Intrusion Detection and DoS Prevention	Disabled
----------------------------------------	----------

### 19.1 Outbound and Inbound Firewall Rules

#### 19.1.1 Access Rules

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

Outbound Firewall Rules	Drag and drop rows to change rule order			
Rule	Protocol	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Allow

## Pepwave Routers User Manual

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

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

Inbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	WAN	Source IP & Port	Destination IP & Port	Policy
Default	Any	Any	Any	Any	Allow

Add Rule

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

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

http://www.pepwave.com 101 Copyright @ 2014 Pepwave

## Pepwave Routers User Manual

matching traffic does not pass through the router (and is discarded).

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.

### 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.

## Pepwave Routers User Manual

### Inbound / Outbound Firewall Settings

<b>Rule Name</b>	This setting specifies a name for the firewall rule.
<b>Enable</b>	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/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.
<b>WAN Connection (Inbound)</b>	Select the WAN connection that this firewall rule should apply to.
<b>Protocol</b>	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• IP</li> </ul> Alternatively, the <b>Protocol Selection Tool</b> drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remains manually modifiable.
<b>Source IP &amp; Port</b>	This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the <b>Source IP &amp; Port</b> setting, as indicated by the following screenshot:
<b>Destination IP &amp; Port</b>	This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the <b>Destination IP &amp; Port</b> setting, as indicated by the following screenshot:
<b>Action</b>	This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following: <ul style="list-style-type: none"> <li>• Source IP &amp; port</li> <li>• Destination IP &amp; port</li> </ul> With the value of <b>Allow</b> for the <b>Action</b> setting, the matching traffic passes through the router (to be routed to the destination). If the value of the <b>Action</b> setting is set to <b>Deny</b> , the

http://www.pepwave.com 102 Copyright @ 2014 Pepwave

## Pepwave Routers User Manual

### 19.1.1.1 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 for **Intrusion Detection and DoS Prevention**, 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

http://www.pepwave.com

103

Copyright @ 2014 Pepwave

http://www.pepwave.com

104

Copyright @ 2014 Pepwave

## 19.1.2 Web Blocking

Web Blocking	
Web Site Domain Name	<input type="text"/>
<b>Exempted User Groups</b>	
Manager	<input checked="" type="checkbox"/> Exempt
Staff	<input checked="" type="checkbox"/> Exempt
Guest	<input checked="" type="checkbox"/> Exempt
<b>Exempted Subnets</b>	
Network	<input type="text"/> Subnet Mask
255.255.255.0 (/24) <input type="button" value="+"/>	

### 19.1.2.1 Web Blocking

Enter an appropriate website address, and the Pepwave router will block and disallow LAN/PPTP-SpeedFusion™ peer clients to access these websites. Exceptions can be added using the instructions in [Sections 19.1.2.2 and 19.1.2.3](#).

You may enter a wildcard “\*” 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.\**, [www.foobar.com](http://www.foobar.com), [www.foobar.co.jp](http://www.foobar.co.jp), and [www.foobar.co.uk](http://www.foobar.co.uk) will be blocked. Placing the wildcard in any other position is not supported. The Pepwave router will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

### 19.1.2.2 Exempted User Groups

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

### 19.1.2.3 Exempted Subnets

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

You can configure high availability at [Advanced>Misc. Settings>High Availability](#).

Interface for Master Router

High Availability	
Enable	Checking this box specifies that the Pepwave router is part of a high availability configuration.
Group Number	This number identifies a pair of Pepwave routers operating in a high availability configuration. The two Pepwave routers in the pair must have the same <b>Group Number</b> 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 <b>Master</b> mode is selected in <b>Preferred Role</b> . If this option is enabled, once the device has recovered from an outage, it will take over and resume its <b>Master</b> role from the slave unit.
Configuration Sync.	This option is displayed when <b>Slave</b> mode is selected in <b>Preferred Role</b> . If this option is enabled and the <b>Master Serial Number</b> entered matches with the actual master unit's, the master unit will automatically transfer the configuration to this unit. Please make sure the <b>Lan IP Address</b> and the <b>Subnet Mask</b> fields are set correctly in the LAN settings page. You can refer to the <a href="#">Event Log</a> for the configuration synchronization status.
Master Serial Number	If <b>Configuration Sync.</b> 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 <b>Virtual IP</b> . The <b>Virtual IP</b> and the <b>Lan Administration IP</b> 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.

### High Availability

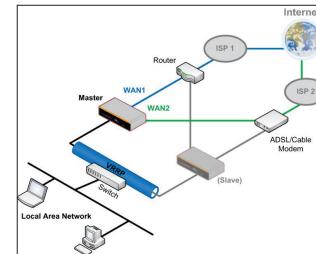
<b>Enable</b>	Checking this box specifies that the Pepwave router is part of a high availability configuration.
<b>Group Number</b>	This number identifies a pair of Pepwave routers operating in a high availability configuration. The two Pepwave routers in the pair must have the same <b>Group Number</b>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

## 20 Miscellaneous Settings

The miscellaneous settings include configuration for high availability, PPTP server, service forwarding, and service passthrough.

### 20.1 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.



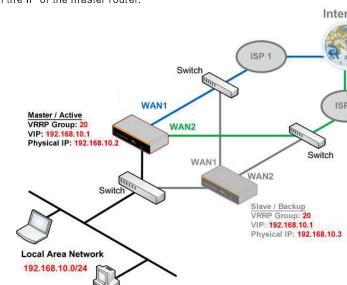
In the diagram, the WAN ports of each Pepwave router connect to the router and to the modem. Both Pepwave routers connect to the same LAN switch via a LAN port.

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

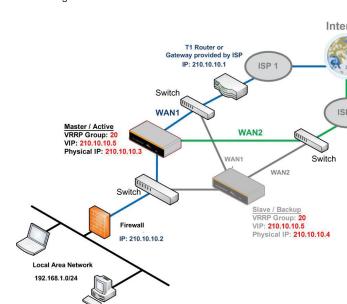
- In an HA configuration, the two Pepwave routers communicate with each other using VRRP over the LAN.
- The two Pepwave routers broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the master Pepwave router is received 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.

### 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.



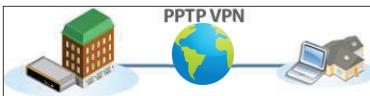
In drop-in mode, no other configuration needs to be set.



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

## Pepwave Routers User Manual

### 20.2 PPTP Server



Pepwave routers feature a built-in PPTP server, which enables remote computers to conveniently and securely access the local network. PPTP server settings are located at **Advanced>Misc. Settings>PPTP Server**.

Check the box to enable PPTP server functionality. All connected PPTP sessions are displayed at **Status>Client List**. Please refer to **Section 23.3** for details. Note that available options vary by model.

## Pepwave Routers User Manual

Connection / IP Address(es)	
WAN 1	10.90.0.74 (Interface IP)
WAN 2	10.90.0.67 (Interface IP)
Wi-Fi WAN	Interface IP
Cellular 1	Interface IP
Cellular 2	Interface IP
USB	Interface IP

User Accounts	
Username	Password

**PPTP Server Settings**

**Listen On** This setting is for specifying the WAN connection(s) and IP address(es) that the PPTP server should listen on.

**Authentication** This setting is for specifying the user database source for PPTP authentication. Three sources can be selected: Local User Accounts, LDAP Server, or RADIUS Server.

- Local User Accounts** - User accounts are stored in the Pepwave router locally. You can add/modify/delete accounts in the User Accounts table.
- LDAP Server** - Authenticate with an external LDAP server. This has been tested with Open LDAP servers where passwords are NTLM hashed. Active Directory is not supported. (You can choose to use RADIUS to authenticate with a Windows server.)
- RADIUS Server** - Authenticate with an external RADIUS server. This has been tested with Microsoft Windows Internet Authentication Service and FreeRADIUS servers where passwords are NTLM hashed or in plain text.

## Pepwave Routers User Manual

**User Accounts** This setting allows you to define PPTP user accounts for authentication via local 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. Click to delete the account in its corresponding row.

### 20.3 Certificate Manager

Certificate Manager			
VPN Certificate	No Certificate	Assign	
Web Admin SSL Certificate	No Certificate	Assign	
Captive Portal SSL Certificate	No Certificate	Assign	

This section allows you to assign certificates for local VPN and web admin SSL. The local keys will not be transferred to another device by any means.

### 20.4 Service Forwarding

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

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

Service Forwarding	
<b>SMTP Forwarding</b>	When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting Enable.
<b>Web Proxy Forwarding</b>	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.
<b>DNS Forwarding</b>	When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the 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.

## Pepwave Routers User Manual

### 20.4.1 SMTP Forwarding

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

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

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

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

#### Note

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

## Pepwave Routers User Manual

### 20.4.2 Web Proxy Forwarding

Proxy Server	IP Address	Port
WAN 1	192.168.1.100	:80
WAN 2	192.168.1.101	:80
Wi-Fi WAN	192.168.1.102	:80
Cellular 1	192.168.1.103	:80
Cellular 2	192.168.1.104	:80
USB	192.168.1.105	:80

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.

### 20.4.3 DNS Forwarding

Enable

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

## Pepwave Routers User Manual

site VPN traffic, check **Route IPsec Site-to-Site VPN** and choose the WAN connection to route the traffic to.

### 20.6 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**.

Enable	<input checked="" type="checkbox"/>
Server	Server IP Address / Host Name: 192.168.1.100 Port: 11513 Protocol: UDP Report Interval: 1 second(s)
GPS Report Format	<input checked="" type="radio"/> NMEA <input type="radio"/> TAIP
NMEA Sentence Type	<input checked="" type="checkbox"/> GPRMC <input type="checkbox"/> GPGGA <input type="checkbox"/> GPGSV <input type="checkbox"/> GPGSA <input type="checkbox"/> GPGSV

### GPS Forwarding

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

## Pepwave Routers User Manual

### 20.5 Service Passthrough

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

SIP	<input checked="" type="checkbox"/> Standard Mode <input type="checkbox"/> Compatibility Mode <input checked="" type="checkbox"/> Define custom signal ports 1. 192.168.1.100 2. 192.168.1.101 3. 192.168.1.102
H.323	<input checked="" type="checkbox"/> Enable
FTP	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Define custom control ports 1. 21 2. 22 3. 23
TFTP	<input checked="" type="checkbox"/> Enable
IPsec NAT-T	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Define custom ports 1. 500 2. 4500 3. 10000 <input checked="" type="checkbox"/> Route IPsec Site-to-Site VPN via WAN 1

(Registered trademarks are copyrighted by their respective owner)

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.

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

## Pepwave Routers User Manual

### 21 AP Controller

The AP controller acts as a centralized controller of Pepwave AP devices. With this feature, users can customize and manage multiple APs from a single Pepwave router interface.

#### Special Note

Each Pepwave router can control a limited number of routers without additional cost. To manage more, a Full Edition license is required. Please contact your Authorized Reseller or the PepLink Sales Team for more information and pricing details.

To configure, navigate to the **AP** tab.

#### 21.1 Wireless SSID

This menu is the first one that appears after clicking the **AP** tab. This screen can also be reached by clicking **AP>Wireless SSID**. Note the appearance of this screen varies by model.

SSID	Integrated AP <input checked="" type="checkbox"/> External AP <input type="checkbox"/>
Permitted AP	<input checked="" type="radio"/> Any <input type="radio"/> Approved List
(One serial number per line)	

InControl management enabled. Wireless SSID can now be configured on InControl.

SSID	Security Policy
PEPWAVE_8D1C	WPA/WPA2 - Personal

New SSID

#### AP Controller

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.

**AP Management** 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.

## Pepwave Routers User Manual

SSID	Security Policy	MAC Address (BSSID)
PEPWAVE_6C9	WPA/WPA2 - Personal	00:1A:DD:C6:A7:48
<input type="button" value="Add"/> <input type="button" value="Delete"/>		

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.

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

## Pepwave Routers User Manual

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

The configuration of **Static WEP** parameters enables pre-shared WEP key encryption. Authentication is not supported by this method. The security level of this method is known to be weak.

**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.

RADIUS Server Settings	Primary Server	Secondary Server
Host		
Secret		
Authentication Port	1812 [Default]	1812 [Default]
Accounting Port	1813 [Default]	1813 [Default]

### RADIUS Server Settings

<b>Host</b>	Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.
<b>Secret</b>	Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
<b>Authentication Port</b>	In field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter 1812.
<b>Accounting Port</b>	In field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter 1813.

## Pepwave Routers User Manual

<b>Multicast Filter<sup>A</sup></b>	This setting enables the filtering of multicast network traffic to the wireless SSID.
<b>Multicast Rate<sup>A</sup></b>	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected <b>Protocol</b> and <b>Channel Bonding</b> settings will affect the rate options and values available here.
<b>IGMP Snooping A</b>	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
<b>DHCP Option 82 A</b>	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
<b>Network Priority (QoS) A</b>	Select from <b>Gold</b> , <b>Silver</b> , and <b>Bronze</b> to control the QoS priority of this wireless network's traffic.
<b>Layer 2 Isolation A</b>	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
<b>Band Steering A</b>	Band steering allows the Pepwave router to steer AP clients from the 2.4 GHz band to the 5 GHz band for better usage of bandwidth. To make steering mandatory, select <b>Enforce</b> . To cause the Pepwave router to preferentially choose steering, select <b>Prefer</b> . The default for this setting is <b>Disable</b> .

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

Security Settings	
<b>Security Policy</b>	This setting configures the wireless authentication and encryption methods. Available options are <b>Open</b> (No Encryption), <b>WPA/WPA2 - Personal</b> , <b>WPA/WPA2 - Enterprise</b> and <b>Static WEP</b> .

Access Control	
<b>Restricted Mode</b>	The settings allow administrator to control access using MAC address filtering. Available options are <b>None</b> , <b>Deny all except listed</b> , <b>Accept all except listed</b> , and <b>RADIUS MAC Authentication</b> .

## Pepwave Routers User Manual

### 21.2 Settings

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

InControl management enabled. Settings can now be configured on InControl.

### AP Settings

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 router 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.

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.