

Pepwave MAX and Surf User Manual

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			
Add Service			

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 <input type="button" value="←"/> :: Protocol Selection Tool :: <input type="button" value="▼"/>																												
Port	Any Port <input type="button" value="▼"/>																												
Inbound IP Address(es) (Require at least one IP address)	<table border="1"><thead><tr><th colspan="2">Connection / IP Address(es)</th><th>All</th><th>Clear</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> WAN 1</td><td><input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)</td><td></td><td></td></tr><tr><td><input type="checkbox"/> WAN 2</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> Wi-Fi WAN</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> Cellular 1</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> Cellular 2</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> USB</td><td></td><td></td><td></td></tr></tbody></table>	Connection / IP Address(es)		All	Clear	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)			<input type="checkbox"/> WAN 2				<input type="checkbox"/> Wi-Fi WAN				<input type="checkbox"/> Cellular 1				<input type="checkbox"/> Cellular 2				<input type="checkbox"/> USB			
Connection / IP Address(es)		All	Clear																										
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)																												
<input type="checkbox"/> WAN 2																													
<input type="checkbox"/> Wi-Fi WAN																													
<input type="checkbox"/> Cellular 1																													
<input type="checkbox"/> Cellular 2																													
<input type="checkbox"/> USB																													
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.

Pepwave MAX and Surf 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

Port	?	Any Port
------	---	----------

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.

Port	?	Single Port	Service Port: 80
------	---	-------------	------------------

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

Port	?	Port Range	Service Ports: 80 - 88
------	---	------------	------------------------

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	?	Port Mapping	Service Port: 80	Map to Port: 88
------	---	--------------	------------------	-----------------

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.)

Port	?	Range Mapping	Service Ports: 80 - 88	Map to Ports: 88 - 96
------	---	---------------	------------------------	-----------------------

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.

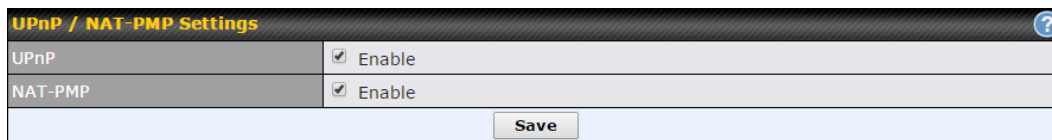
Pepwave MAX and Surf User Manual

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.

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
<input type="button" value="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**.

17 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	<input type="text"/>												
Inbound Mappings	Connection / Inbound IP Address(es) <ul style="list-style-type: none"> <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB 												
Outbound Mappings	Connection / Outbound IP Address <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <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> </tbody> </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.

Pepwave MAX and Surf 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.

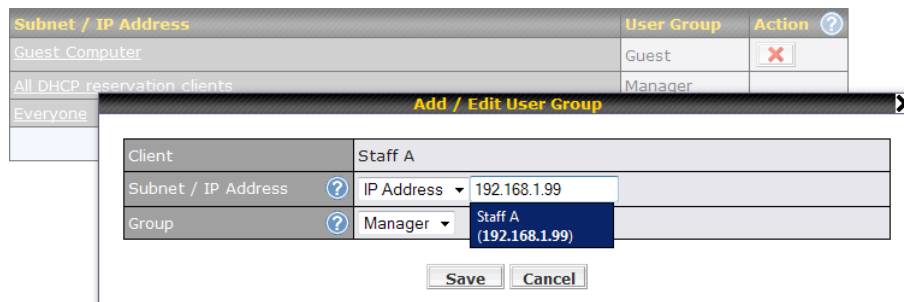
18 QoS

18.1 User Groups

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

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

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



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

Staff A (192.168.1.99)

Save Cancel

Add / Edit User Group

Subnet / IP Address

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

Group

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

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

18.2 Bandwidth Control

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

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


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

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

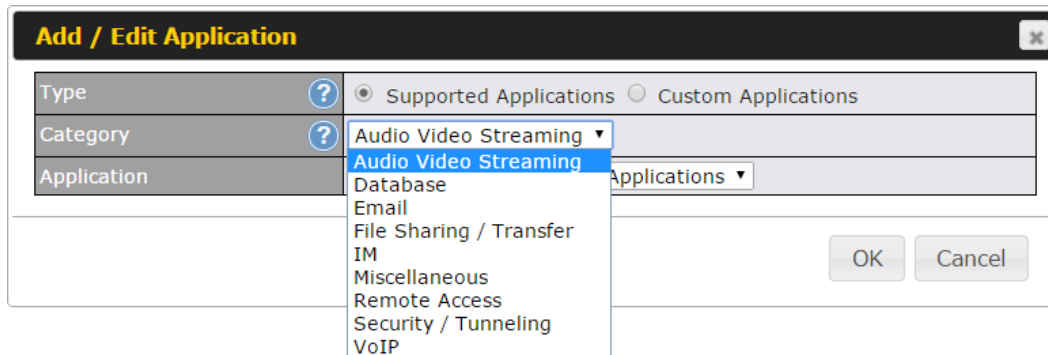
Application	Priority			
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High	— Normal	↑ High	✘
All Email Protocols	↑ High	↑ High	↑ High	✘
MySQL	↑ High	— Normal	↓ Low	✘
SIP	↑ High	↓ Low	↓ Low	✘
<input type="button" value="Add"/>				

Pepwave MAX and Surf User Manual

18.3.2 Prioritization for Custom Applications

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

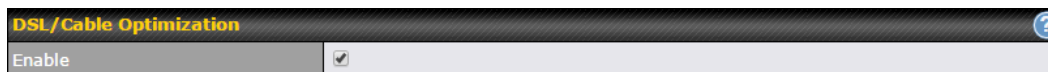
When **Supported Applications** is selected, the Pepwave router will inspect network traffic and prioritize the selected applications. Alternatively, you can select **Custom Applications** and define the application by providing the protocol, scope, port number, and DSCP value.



Add / Edit Application	
Type	<input checked="" type="radio"/> Supported Applications <input type="radio"/> Custom Applications
Category	Audio Video Streaming
Application	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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	<input checked="" type="checkbox"/>

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	
<input type="button" value="Add Rule"/>					

Inbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Any	Allow
<input type="button" value="Add Rule"/>					

Apply Firewall Rules to PepVPN Traffic	
Enabled	<input type="button" value=""/>

Intrusion Detection and DoS Prevention	
Disabled	<input type="button" value=""/>

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	
<input type="button" value="Add Rule"/>					

Pepwave MAX and Surf User Manual

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

The screenshot shows a dialog box titled "Add a New Outbound Firewall Rule". It contains a form for configuring a new firewall rule. The form fields are as follows:

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

At the bottom right of the dialog box are "Save" and "Cancel" buttons.

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

The screenshot shows a table titled "Inbound Firewall Rules" with a header row and one data row. Below the table is an "Add Rule" button.

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

Below the table is an "Add Rule" button.

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

The screenshot shows a dialog box titled "Add a New Inbound Firewall Rule". It contains a form for configuring a new firewall rule. The form fields are as follows:

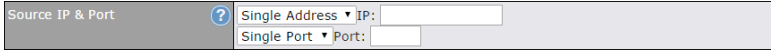
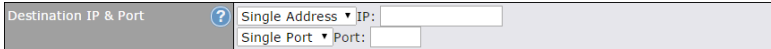
New Firewall Rule	
Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/>
WAN Connection	Any
Protocol	Any <input type="button" value="Protocol Selection Tool"/>
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	<input checked="" type="radio"/> Allow <input type="radio"/>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

At the bottom right of the dialog box are "Save" and "Cancel" buttons.

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.

Pepwave MAX and Surf User Manual

Inbound / Outbound Firewall Settings

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

Pepwave MAX and Surf User Manual

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
```

Event Logging

- **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:

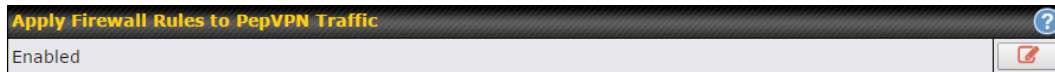
- Hold the left mouse button on the rule.
- Move it to the desired position.
- Drop it by releasing the mouse button.


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.

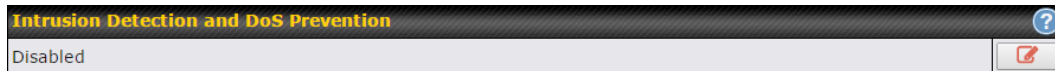
Pepwave MAX and Surf User Manual


19.1.2 Apply Firewall Rules to PepVpn Traffic



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

19.1.3 Intrusion Detection and DoS Prevention



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

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

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

Pepwave MAX and Surf User Manual

19.2 Content Blocking

Application Blocking

Please Select Application...

Web Blocking

Preset Category

High
 Moderate
 Low
 Custom

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

Customized Domains

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

Exempted Domains from Web Blocking

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

Exempted User Groups

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

Exempted Subnets

Network	Subnet Mask
	255.255.255.0 (/24)

URL Logging

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

19.2.1 Application Blocking

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

19.2.2 Web Blocking

Defines web site 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.

Pepwave MAX and Surf User Manual

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 traffic. Secure web (HTTPS) traffic is not supported.

19.2.3 Customized Domains

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

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

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

19.2.4 Exempted User Groups

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

19.2.5 Exempted Subnets

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

19.2.6 URL Logging

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

19.3 OSPF & RIPv2

The Peplink Balance supports OSPF and RIPv2 dynamic routing protocols. Click the **Network** tab from the top bar, and then click the **OSPF & RIPv2** item on the sidebar to reach the following menu:

Pepwave MAX and Surf User Manual

OSPF

Router ID

This field determines the ID of the router. By default, this is specified as the LAN IP address. If you want to specify your own ID, enter it in the **Custom** field.

Area

This is an overview of the OSPFv2 areas you have defined. Click on the area name to configure it. To set a new area, click **Add**. To delete an existing area, click .

OSPF Settings

Area ID

Determine the name of your **Area ID** to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.

Link Type

Choose the network type that this area will use.


Authentication

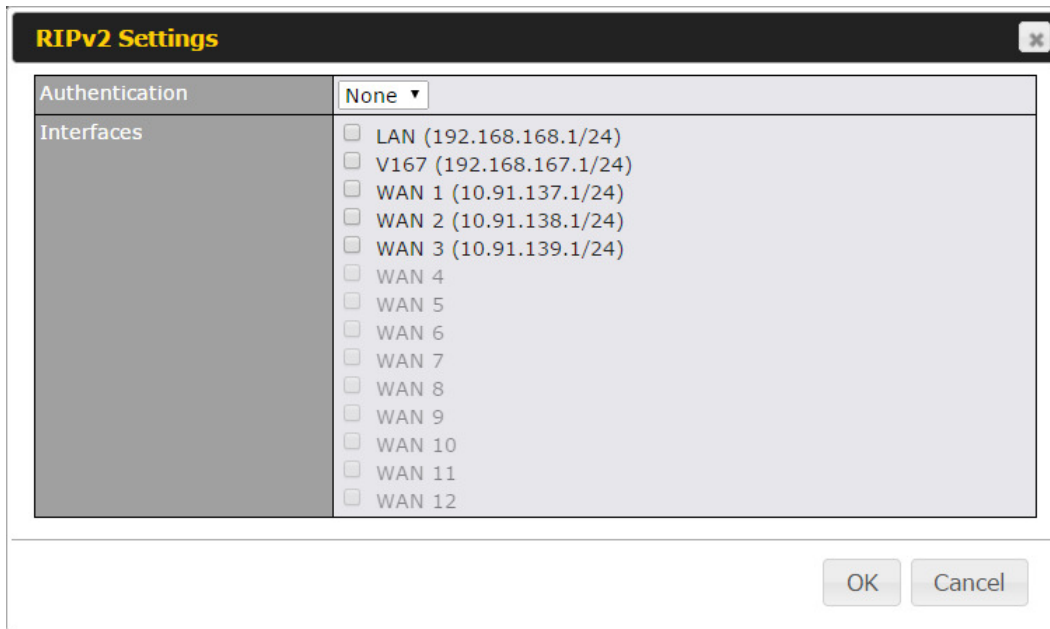
Choose an authentication method, if one is used, from this drop-down menu. Available options are **MD5** and **Text**. Enter the authentication key next to the drop-down menu.

Interfaces

Determine which interfaces this area will use to listen to and deliver OSPF packets

Pepwave MAX and Surf User Manual

To access RIPv2 settings, click .



Authentication	None ▾
Interfaces	<input type="checkbox"/> LAN (192.168.168.1/24) <input type="checkbox"/> V167 (192.168.167.1/24) <input type="checkbox"/> WAN 1 (10.91.137.1/24) <input type="checkbox"/> WAN 2 (10.91.138.1/24) <input type="checkbox"/> WAN 3 (10.91.139.1/24) <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

OK Cancel


RIPv2 Settings	
Authentication	Choose an authentication method, if one is used, from this drop-down menu. Available options are MD5 and Text . Enter the authentication key next to the drop-down menu.
Interfaces	Determine which interfaces this group will use to listen to and deliver RIPv2 packets.

19.4 Remote User Access

a Networks routed by a Peplink Balance can be remotely accessed via L2TP with IPsec or PPTP. To configure this feature, navigate to **Network > Remote User Access**

Pepwave MAX and Surf User Manual

Remote User Access Settings											
Enable	<input checked="" type="checkbox"/>										
VPN Type	<input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP IPsec NAT-Traversal will be enabled to ensure compatibility for most of the devices										
Preshared Key	<input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters										
Listen On	Connection / IP Address(es)										
	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> 10.10.12.47 (Interface IP)									
	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> Interface IP									
	<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> Interface IP									
	<input checked="" type="checkbox"/> Mobile Internet	<input checked="" type="checkbox"/> Interface IP									
User Accounts	<table border="1"> <thead> <tr> <th>Username</th> <th>Password</th> <th></th> </tr> </thead> <tbody> <tr> <td>admin</td> <td>.....</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td></td> <td></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Username	Password		admin	<input checked="" type="checkbox"/>			<input type="checkbox"/>	
	Username	Password									
	admin	<input checked="" type="checkbox"/>								
		<input type="checkbox"/>									
		<input checked="" type="checkbox"/>									
		<input type="checkbox"/>									

Remote User Access Settings	
Enable	Click the checkbox to enable Remote User Access.
VPN Type	Determine whether remote devices can connect to the Balance using L2TP with IPsec or PPTP. For greater security, we recommend you connect using L2TP with IPsec.
Preshared Key	Enter your preshared 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 where the PPTP server of the router should listen on.
User Accounts	<p>This setting allows you to define the PPTP 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 the button X to delete the account in its corresponding row.</p> <p>Click the  button to switch to enters user accounts by pasting the information in.CSV format.</p>

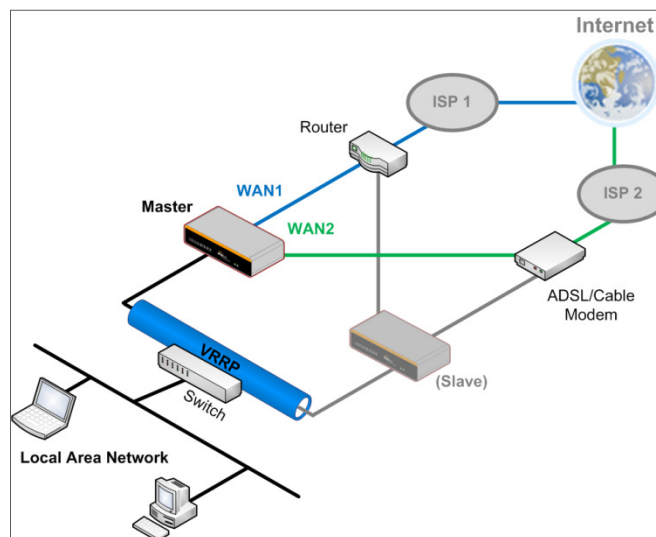
Pepwave MAX and Surf User Manual

Miscellaneous Settings

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

19.5 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.

Pepwave MAX and Surf User Manual

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

Interface for Master Router

Interface for Slave Router

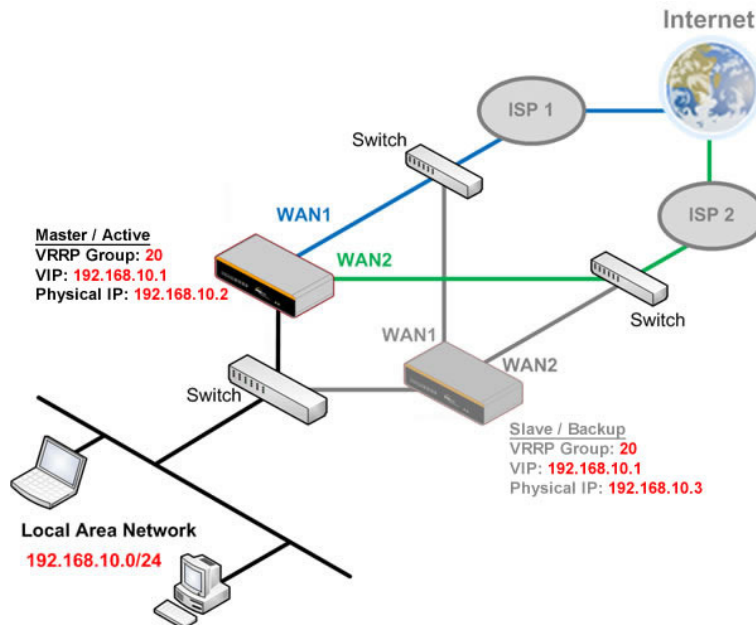
High Availability		High Availability	
Enable	<input checked="" type="checkbox"/>	Enable	<input checked="" type="checkbox"/>
Group Number	5	Group Number	5
Preferred Role	<input checked="" type="radio"/> Master <input type="radio"/> Slave	Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/> Slave
Resume Master Role Upon Recovery	<input checked="" type="checkbox"/>	Configuration Sync.	<input type="checkbox"/> Master Serial Number: 54BF-5WEY-E37Q
Virtual IP		Virtual IP	
LAN Administration IP	192.168.1.1	LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0	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.

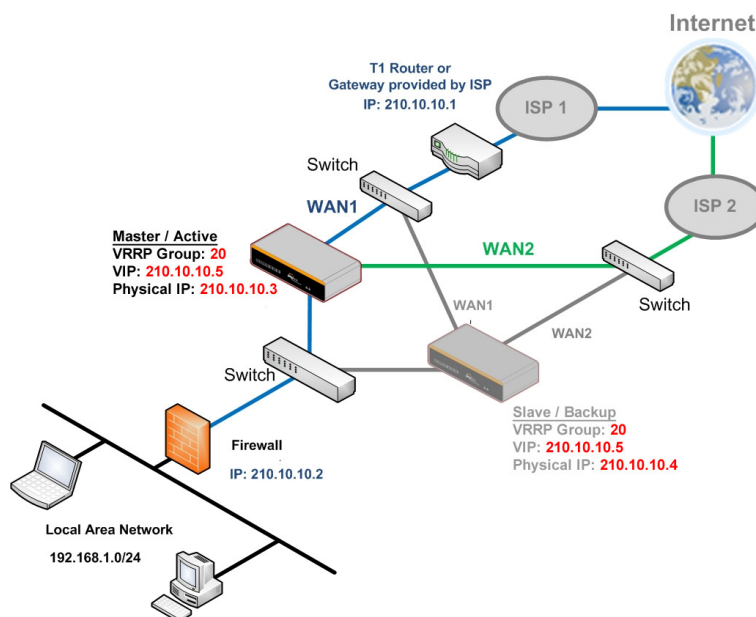
Pepwave MAX and Surf User Manual

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.



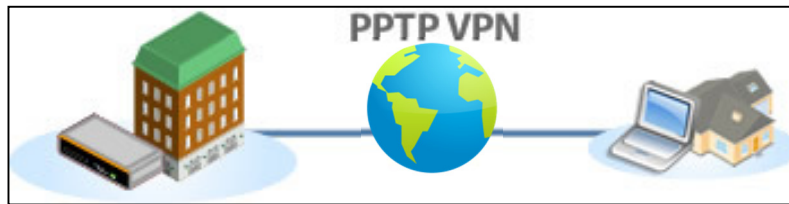
In drop-in mode, no other configuration needs to be set.



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

Pepwave MAX and Surf User Manual

19.6 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 22.3** for details. Note that available options vary by model.

PPTP Server		
Enable	<input checked="" type="checkbox"/>	
Listen On	Connection / IP Address(es)	
	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)
	<input checked="" type="checkbox"/> WAN 2	<input checked="" type="checkbox"/> Interface IP
	<input checked="" type="checkbox"/> Wi-Fi WAN	<input checked="" type="checkbox"/> Interface IP
	<input checked="" type="checkbox"/> Cellular 1	<input checked="" type="checkbox"/> Interface IP
	<input checked="" type="checkbox"/> Cellular 2	<input checked="" type="checkbox"/> Interface IP
	<input checked="" type="checkbox"/> USB	<input checked="" type="checkbox"/> Interface IP
Authentication	<input type="checkbox"/> Local User Accounts ▼	
User Accounts	<input type="checkbox"/> Username	<input type="checkbox"/> Password

Pepwave MAX and Surf User Manual

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.
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.



19.7 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.

19.8 Service Forwarding

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

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

Service Forwarding	
SMTP Forwarding	When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified

Pepwave MAX and Surf User Manual

	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.

19.8.1 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.

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

Pepwave MAX and Surf User Manual

in outbound policy (see **Section 14.2**).

19.8.2 Web Proxy Forwarding

The screenshot shows the 'Web Proxy Forwarding Setup' configuration page. At the top, there is a section for 'Web Proxy Forwarding' with an 'Enable' checkbox checked. Below this is the 'Web Proxy Interception Settings' section, which includes fields for 'Proxy Server' with 'IP Address' and 'Port' sub-fields, and a note '(Current settings in users' browser)'. The main part of the page is a table with three columns: 'Connection', 'Enable Forwarding?', and 'Proxy Server IP Address : Port'. The table lists six connection types: WAN 1, WAN 2, Wi-Fi WAN, Cellular 1, Cellular 2, and USB. Each row has a checkbox in the 'Enable Forwarding?' column and a text input field in the 'Proxy Server IP Address : Port' column.

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

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

19.8.3 DNS Forwarding

The screenshot shows the 'DNS Forwarding Setup' configuration page. It features a section for 'Forward Outgoing DNS Requests to Local DNS Proxy' with an 'Enable' checkbox.

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

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

19.8.4 Custom Service Forwarding

The screenshot shows the 'Custom Service Forwarding Setup' configuration page. It has an 'Enable' checkbox checked. Below is a 'Settings' section with a table for adding forwarding rules.

TCP Port	Server IP Address	Server Port	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>

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

Pepwave MAX and Surf User Manual

19.9 Service Passthrough

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

The screenshot shows the 'Service Passthrough Support' configuration page. It features a table with the following settings:

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

(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.

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


Pepwave MAX and Surf User Manual

to route the traffic to.

19.10 GPS Forwarding

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

GPS Forwarding				
Enable	<input checked="" type="checkbox"/>			
Server	Server IP Address / Host Name	Port	Protocol	Report Interval (s)
			UDP	1
GPS Report Format	<input checked="" type="radio"/> NMEA <input type="radio"/> TAIP			
NMEA Sentence Type	<input checked="" type="checkbox"/> GPRMC <input type="checkbox"/> GPGGA <input type="checkbox"/> GPVTG <input type="checkbox"/> GPGSA <input type="checkbox"/> GPGSV			
Vehicle ID (optional)	<input type="text"/>			

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.

Pepwave MAX and Surf User Manual

20 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.

20.1 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.

AP Controller	
AP Management	<input checked="" type="checkbox"/> Integrated AP <input checked="" type="checkbox"/> External AP
Permitted AP	<input type="radio"/> Any <input checked="" type="radio"/> Approved List
	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div> <p>(One serial number per line)</p>

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.

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.

SSID	Security Policy	
PEPWAVE_8D1C	WPA/WPA2 - Personal	<input type="button" value="X"/>

Pepwave MAX and Surf User Manual

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 screenshot shows a configuration window titled "SSID" with a close button in the top right. It is divided into three sections:


- SSID Settings:** Contains fields for SSID (PEPWAVE_8D1C), VLAN ID (LAN (No VLAN)), Broadcast SSID (checked), Data Rate (Auto selected), Multicast Filter (unchecked), Multicast Rate (MCS8/MCS0/6M), IGMP Snooping (unchecked), Layer 2 Isolation (unchecked), and Band Steering (Disable).
- Security Settings:** Contains a Security Policy dropdown menu set to Open (No Encryption).
- Access Control:** Contains a Restricted Mode dropdown menu set to None.

At the bottom right of the window are "Save" and "Cancel" buttons.

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Enable	Select Yes to enable the virtual AP.
VLAN ID	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.

Pepwave MAX and Surf User Manual

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.
Network Priority (QoS)^A	Select from Gold , Silver , and Bronze to control the QoS priority of this wireless network's traffic.
Layer 2 Isolation^A	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
Band Steering^A	Band steering allows the Pepwave router to steer AP clients from the 2.4GHz band to the 5GHz band for better usage of bandwidth. To make steering mandatory, select Enforce . To cause the Pepwave router to preferentially choose steering, select Prefer . The default for this setting is Disable .

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

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

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

Access Control	
Restricted Mode	Deny all except listed ▼
MAC Address List	<input type="text"/>

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

Pepwave MAX and Surf User Manual

this method, select the appropriate version using the **V1/V2** controls. The security level of this method is known to be very high.

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

The 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 the option selected in the previous field.

RADIUS Server Settings	Primary Server	Secondary Server
Host	<input type="text"/>	<input type="text"/>
Secret	<input type="text"/>	<input type="text"/>
Authentication Port	<input type="text" value="1812"/> Default	<input type="text" value="1812"/> Default
Accounting Port	<input type="text" value="1813"/> Default	<input type="text" value="1813"/> Default

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 field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the Default button to enter 1812 .
Accounting Port	In field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the Default button to enter 1813 .

Pepwave MAX and Surf User Manual

20.2 Settings

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

AP Settings	
AP Profile Name	<input type="text"/>
SSID	<input type="checkbox"/> 2.4 GHz <input type="checkbox"/> 5 GHz <input type="checkbox"/> PEPLINK_01AA
Operating Country	United States
Preferred Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz
5 GHz Protocol	802.11n/ac Integrated AP supports 802.11na only.
5 GHz Channel Width	20/40 MHz
5 GHz Channel	Auto <input type="button" value="Edit"/> Channels: 36 40 44 48 ...
2.4 GHz Protocol	802.11ng
2.4 GHz Channel Width	20 MHz
2.4 GHz Channel	Auto <input type="button" value="Edit"/> Channels: 1 2 3 4 5 6 ...
Management VLAN ID	(No VLAN)
Operating Schedule	Always on
Power Boost	<input type="checkbox"/>
Output Power	Max
Maximum number of clients	0 (0: Unlimited)
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)
Beacon Rate	1 Mbps 6 Mbps will be used for 5 GHz radio
Beacon Interval	100 ms
DTIM	1 <input type="button" value="Default"/>
RTS Threshold	0 <input type="button" value="Default"/>
Fragmentation Threshold	0 (0: Disable) <input type="button" value="Default"/>
Distance / Time Converter	4050 m Note: Input distance for recommended values
Slot Time	<input type="radio"/> Auto <input checked="" type="radio"/> Custom 9 <input type="button" value="Default"/> μ s
ACK Timeout	48 <input type="button" value="Default"/> μ s
Frame Aggregation	<input checked="" type="checkbox"/>
Aggregation Length	50000 <input type="button" value="Default"/>

AP Settings

AP Profile Name This field specifies the name of this AP profile.

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 Peplink Balance does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.

Operating


This drop-down menu specifies the national / regional regulations which the AP should

Pepwave MAX and Surf User Manual

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

Pepwave MAX and Surf User Manual

	give your AP further instructions.
Max number of Clients^A	This field determines the maximum clients that can be connected to APs under this profile.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
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 messages (DTIM). The interval unit is measured in milliseconds.
RTS Threshold^A	This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.
Fragmentation Threshold^A	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.
Distance/Time Converter^A	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
Slot Time^A	This field provides the option to modify the unit wait time before it transmits. The default value is 9µs .
ACK Timeout^A	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is 48µs .
Frame Aggregation^A	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.
Frame Length	This field is only available when Frame Aggregation is enabled. It specifies the frame length for frame aggregation. By default, it is set to 50000 .

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


Web Administration Settings (on External AP)	
Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	<input type="text" value="443"/>
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username	<input type="text" value="admin"/>
Admin Password	<input type="text" value="25db591396e0"/> <input type="button" value="Generate"/>

Web Administration Settings







Pepwave MAX and Surf User Manual

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	<input type="radio"/> Internal <input checked="" type="radio"/> External

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

Pepwave MAX and Surf User Manual

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 Surf SOHO 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.

20.3 Toolbox

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

Pepwave MAX and Surf User Manual



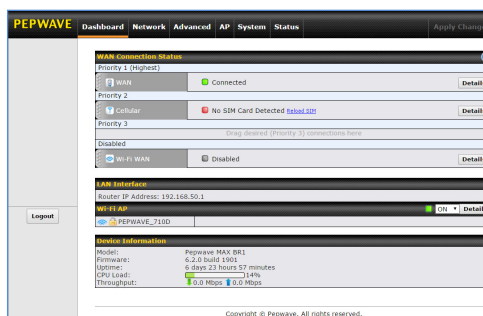
Firmware Packs

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.

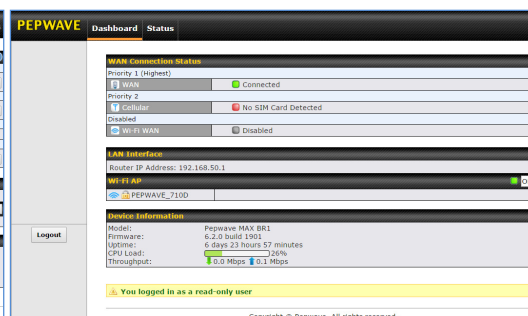
21 System Settings

21.1 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 administration 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.



Admin account UI



User account UI