

13 Management of Outbound Traffic to WAN

The Pepwave MAX provides the functionality to flexibly manage and load balance outbound traffic among the 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 in **Advanced > Outbound Policy**:

Service	Algorithm	Source	Destination	Protocol / Port
HTTPS Persis...	Persistence (Src) (Auto)	Any	Any	TCP 443
Default	(Auto)			

Network > Outbound Policy > Click on 

Service	Algorithm	Source	Destination	Protocol / Port
HTTPS Persis...	Persistence (Src) (Auto)	Any	Any	TCP 443
Default	(Auto)			

User Manual

PEPWAVE *MAX* mobile router

13.1 Outbound Policy

There are three main selections for the Outbound Policy for the Pepwave MAX:

- High Application Compatibility
- Normal Application Compatibility
- Custom

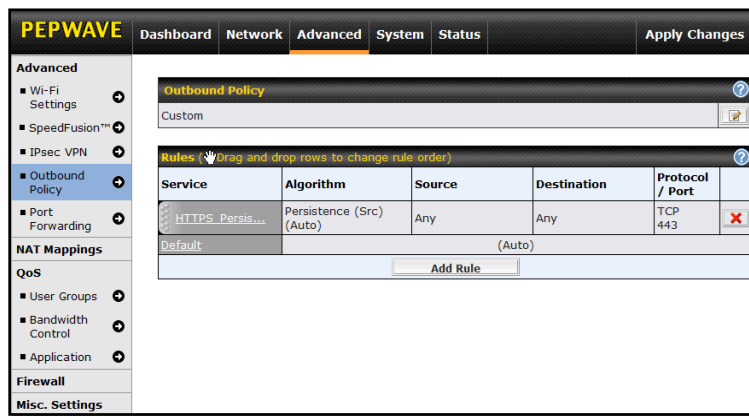
The selections are explained as follows:

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

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

Tip

Want to know more about how-to create outbound rules? Visit our [YouTube Channel](#) for a video tutorial!



http://youtu.be/rKH4AS_bQnE

User Manual

PEPWAVE *MAX* mobile router

13.2 Custom Rules For Outbound Policy

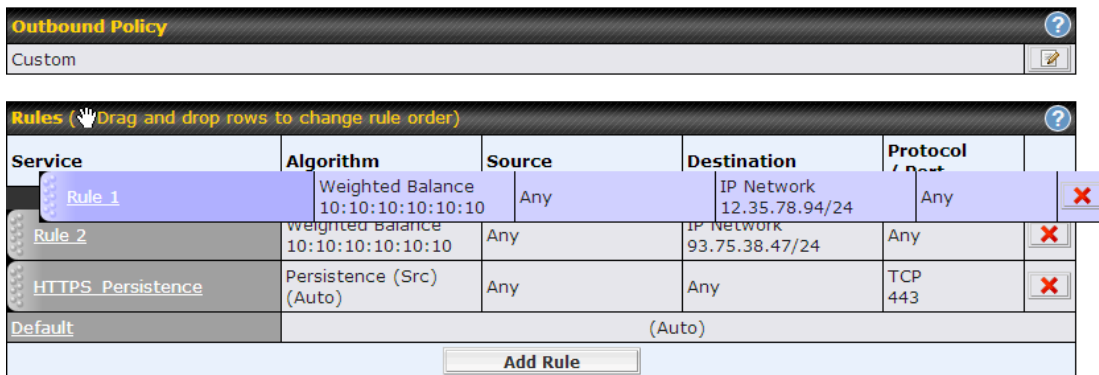
Click  in the Outbound Policy form. Choose **Managed by Custom Rules** and press the **Save** button. The following screen will then be displayed.




The bottom-most rule is **Default**. Edit this rule to change the device's default way to control outbound traffic for all connections that does not match any rules above it. Click on the service name **Default** to change its settings.



Service	Algorithm	Source	Destination	Protocol / Port	
Rule 1	Weighted Balance 10:10:10:10:10:10	Any	IP Network 12.35.78.94/24	Any	
Rule 2	Weighted Balance 10:10:10:10:10:10	Any	IP Network 93.75.38.47/24	Any	
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	
Default			(Auto)		

You may drag and drop a row to rearrange the priority of outbound rules.



Service	Algorithm	Source	Destination	Protocol / Port	
Rule 1	Weighted Balance 10:10:10:10:10:10	Any	IP Network 12.35.78.94/24	Any	
Rule 2	Weighted Balance 10:10:10:10:10:10	Any	IP Network 93.75.38.47/24	Any	
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	
Default			(Auto)		

By default, **Auto** is selected for the option **Default Rule**. You can select **Custom** in order to change the Algorithm to be used. Please refer to the upcoming sections for the details of the available algorithms.

To create a custom rule, click **Add Rule** at the bottom of the table, and the following window will be displayed:

User Manual

PEPWAVE *MAX* mobile router

Add a New Custom Rule ✕

New Custom Rule																			
Service Name *	<input style="width: 95%;" type="text"/>																		
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No																		
Source	IP Network ▼ <input style="width: 80%;" type="text"/> Mask: 255.255.255.0 ▼																		
Destination	IP Network ▼ <input style="width: 80%;" type="text"/> Mask : 255.255.255.0 ▼																		
Protocol	TCP ? ← :: Protocol Selection Tool :: ▼																		
Port *	Any Port ? ▼																		
Algorithm	Weighted Balance ? ▼																		
Load Distribution Weight ?	<table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 15%; font-size: small;">Ethernet WAN</td><td style="width: 10%; font-size: small;">10</td><td style="width: 75%;"><div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div></td></tr> <tr><td>Express Card</td><td>10</td><td><div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div></td></tr> <tr><td>PC Card</td><td>10</td><td><div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div></td></tr> <tr><td>USB1</td><td>10</td><td><div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div></td></tr> <tr><td>USB2</td><td>10</td><td><div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div></td></tr> <tr><td>Wi-Fi WAN</td><td>10</td><td><div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div></td></tr> </table>	Ethernet WAN	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>	Express Card	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>	PC Card	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>	USB1	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>	USB2	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>	Wi-Fi WAN	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>
Ethernet WAN	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>																	
Express Card	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>																	
PC Card	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>																	
USB1	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>																	
USB2	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>																	
Wi-Fi WAN	10	<div style="border: 1px solid #ccc; height: 10px; width: 100%; position: relative;"><div style="background-color: #ccc; width: 100%;"></div><div style="background-color: #00aaff; width: 100%; height: 2px;"></div></div>																	
Terminate Sessions on Link Recovery ?	<input type="checkbox"/> Enable																		

New Custom Rule Settings											
Service Name	This setting specifies the name of the custom rule.										
Enable	<p>This setting specifies whether the outbound traffic rule takes effect.</p> <p>With an Enable value of Yes, the rule takes effect: traffic is matched, and actions are taken, by the Pepwave MAX based on the other parameters of the rule.</p> <p>With an Enable value of No, the rule does not take effect and the Pepwave MAX will disregard the other parameters of the rule.</p>										
Source	This setting specifies the source IP Address, IP Network or MAC Address for outbound traffic that matches the rule.										
Destination	<p>This setting specifies the destination IP Address or IP Network or Domain Name for traffic that matches the rule.</p> <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 20%; font-size: small;">Destination</td><td style="font-size: small;">Domain Name ▼</td></tr> <tr><td style="font-size: small;">Protocol ?</td><td style="font-size: small;">Any</td></tr> <tr><td style="font-size: small;">Algorithm ?</td><td style="font-size: small;">IP Address</td></tr> <tr><td></td><td style="font-size: small;">IP Network</td></tr> <tr><td></td><td style="font-size: small; background-color: #00aaff; color: white;">Domain Name</td></tr> </table> </div>	Destination	Domain Name ▼	Protocol ?	Any	Algorithm ?	IP Address		IP Network		Domain Name
Destination	Domain Name ▼										
Protocol ?	Any										
Algorithm ?	IP Address										
	IP Network										
	Domain Name										
Domain Name	<p>If Domain Name is chosen and a domain name, such as foobar.com, is entered, any outgoing accesses to foobar.com and *.foobar.com will match this criterion. You may enter a wildcard (*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter .*, for example, then www.foobar.com, www.foobar.co.jp, or foobar.co.uk will also match. Placing wildcards in any other position is not supported.</p>										

User Manual

PEPWAVE *MAX* mobile router

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

Protocol and Port

This setting specifies the IP Protocol and Port of outbound traffic that matches this rule. You may select some common protocol from the **Protocol Selection Tool** drop-down menu.

Algorithm

This setting specifies the behavior of the Pepwave MAX for the custom rule. One of the following values can be selected:

- Weighted Balance
- Persistence
- Enforced
- Priority
- Overflow
- Least Used
- Lowest Latency

The upcoming sections present the details of the listed algorithms.

Terminate Sessions on Link Recovery

This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the Algorithms: **Weighted**, **Persistence** and **Priority**.

By default, this is disabled. In this case, all existing IP sessions will not be terminated or affected when any other WAN connection is recovered. If it is set to enabled, existing IP sessions may be terminated when another WAN connection is recovered such that only the preferred healthy WAN connection(s) are used at any point in time.

User Manual

PEPWAVE *MAX* mobile router

13.2.1 Algorithm: Weighted Balance

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

Algorithm	<input type="text" value="Weighted Balance"/>
Load Distribution Weight	<p>WAN 1 10 </p> <p>WAN 2 10 </p> <p>Wi-Fi WAN 10 </p> <p>Cellular 1 10 </p> <p>Cellular 2 10 </p> <p>USB 10 </p>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

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 the weight for each WAN.

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%

User Manual

PEPWAVE *MAX* mobile router

13.2.2 Algorithm: Persistence

The Persistence algorithm is the solution to the few situations where link load distribution for Internet services is undesirable.

For example, many e-banking and other secure websites, for security reasons, terminate the session when the client computer's Internet IP address changes during the 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.

The Pepwave MAX 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 MAX may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Pepwave MAX with three WAN connections may communicate on the Internet using three different IP addresses.

With the algorithm Persistence of the Pepwave MAX, 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 with the other end using one IP address and eliminate the issues.

Algorithm	<input type="text" value="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

There are two modes for Persistence: **By Source** and **By Destination**.

By Source	The same WAN connection will be used for traffic matching the rule and originating from the same machine regardless of its destination. This option will provide the highest level of application compatibility.
By Destination	The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute load 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** for **Load Distribution**, the weights will be automatically adjusted according to each WAN's Downstream Bandwidth which is specified in the WAN settings page (see Section 8.2 Captive Portal)

The Captive Portal serves as gateway that clients have to pass if they wish to access the internet using your router. To configure, navigate to **Network > Captive Portal** to see the following screen:

User Manual

PEPWAVE *MAX* mobile router

Captive Portal Settings	
Enable	<input checked="" type="checkbox"/> edit Guest_LAN (25)
Access Mode	<input checked="" type="radio"/> Open Access <input type="radio"/> User Authentication
Access Quota	720 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	<input checked="" type="radio"/> Daily at 00 :00 <input type="radio"/> 1440 minutes after quota reached
Splash Page	<input checked="" type="radio"/> Built-in <input type="radio"/> External, URL: <input type="text" value="http://"/>

Captive Portal Settings													
Apply On	<p>Clicking the edit button trigger a dialogue where you can choose which LAN / VLAN to apply your captive portal.</p>  <p>Click all LAN / VLAN that you wish to apply the captive portal to.</p>												
Access Mode	<p>Click Open Access to allow clients to freely access your router. Click User Authentication to force your clients to authenticate before accessing your router.</p>												
Radius Server	<p>This authenticates your clients through a Radius Server. Upon selecting this option, you will see the following fields:</p> <table border="1" data-bbox="467 1171 1307 1375"> <tbody> <tr> <td>Authentication</td> <td>RADIUS Server</td> </tr> <tr> <td>Auth Server</td> <td><input type="text"/> Port 1812 <input type="button" value="Default"/></td> </tr> <tr> <td>Auth Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Accounting Server</td> <td><input type="text"/> Port 1813 <input type="button" value="Default"/></td> </tr> <tr> <td>Accounting Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Network Connection</td> <td>LAN</td> </tr> </tbody> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	RADIUS Server	Auth Server	<input type="text"/> Port 1812 <input type="button" value="Default"/>	Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	Accounting Server	<input type="text"/> Port 1813 <input type="button" value="Default"/>	Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	Network Connection	LAN
Authentication	RADIUS Server												
Auth Server	<input type="text"/> Port 1812 <input type="button" value="Default"/>												
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters												
Accounting Server	<input type="text"/> Port 1813 <input type="button" value="Default"/>												
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters												
Network Connection	LAN												
LDAP Server	<p>This authenticates your clients through a LDAP Server. Upon selecting this option, you will see the following fields:</p> <table border="1" data-bbox="467 1554 1323 1711"> <tbody> <tr> <td>Authentication</td> <td>LDAP Server</td> </tr> <tr> <td>LDAP Server</td> <td><input type="text"/> Port 389 <input type="button" value="Default"/></td> </tr> <tr> <td></td> <td><input type="checkbox"/> Use DN/Password to bind to LDAP Server</td> </tr> <tr> <td>Base DN</td> <td><input type="text"/></td> </tr> <tr> <td>Base Filter</td> <td><input type="text"/></td> </tr> </tbody> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	LDAP Server	LDAP Server	<input type="text"/> Port 389 <input type="button" value="Default"/>		<input type="checkbox"/> Use DN/Password to bind to LDAP Server	Base DN	<input type="text"/>	Base Filter	<input type="text"/>		
Authentication	LDAP Server												
LDAP Server	<input type="text"/> Port 389 <input type="button" value="Default"/>												
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server												
Base DN	<input type="text"/>												
Base Filter	<input type="text"/>												
Access Quota	<p>Set a time and data cap to each user's Internet usage.</p>												

User Manual



PEPWAVE *MAX* mobile router

Quota Reset Time

This menu determines how your usage quota resets. Setting it to **daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.

Splash Page

Here, you can choose between using the MAX router's built-in captive portal and redirecting clients to a URL you define.

The Portal Customization menu has two options: **Preview** and . Clicking will result in a pop-up previewing the captive portal that your clients will see. Clicking  will result in the appearance of following menu:

Portal Customization	
Logo Image	<input checked="" type="radio"/> No image [Use default Logo Image] <input type="radio"/> Use default Logo Image <input type="radio"/> <input type="button" value="Choose File"/> No file chosen <small>NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.</small>
Message	<div style="border: 1px solid gray; height: 100px;"></div>
Terms & Conditions	<div style="border: 1px solid gray; height: 100px; text-align: center;">[Use default Terms & Conditions]</div>
Custom Landing Page	<input checked="" type="checkbox"/> <input type="text" value="http://"/>
<input type="button" value="Save"/>	

Portal Customization

Logo Image

Click the **Choose File** button to select an logo to use for the built-in portal

User Manual

PEPWAVE *MAX* mobile router

Message	If you have any additional messages for your users, place it on this field.
Terms & Conditions	If you would like to use your own set of terms and conditions, please place it here. If left empty, the built-in portal will display the default terms and conditions.
Custom Landing Page	Fill in this field to redirect clients to an external URL.

14 Configuration of WAN Interface(s)

). If you choose **Custom**, you can customize the weight of each WAN manually by using the sliders.

User Manual

PEPWAVE *MAX* mobile router

14.1.1 Algorithm: Enforced

This setting specifies the WAN connection usage to be applied on the specified IP Protocol & Port, and is applicable only when the Algorithm is set to **Enforced**.

Algorithm ?	Enforced
Enforced Connection ?	WAN: WAN 1
	WAN: WAN 1
	WAN: WAN 2
	WAN: Wi-Fi WAN
	WAN: Cellular 1
	WAN: Cellular 2
	WAN: USB
	VPN: FL Office
	Cancel

Matching traffic will be routed through the specified WAN connection regardless of the connection's health check status.

Starting from firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

14.1.2 Algorithm: Priority

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

Algorithm ?	Priority
Priority Order ?	Highest Priority
	WAN: WAN 1
	WAN: WAN 2
	WAN: Wi-Fi WAN
	WAN: Cellular 1
	WAN: Cellular 2
	WAN: USB
	Lowest Priority
	Not In Use
	VPN: FL Office
Terminate Sessions on Link Recovery ?	<input type="checkbox"/> Enable

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

Tip

Configure multiple distribution rules to accommodate different kinds of services.

User Manual

PEPWAVE *MAX* mobile router

14.1.3 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.

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

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

14.1.4 Algorithm: Least Used

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

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

User Manual

PEPWAVE *MAX* mobile router

14.1.5 Algorithm: Lowest Latency

Algorithm	<input style="float: left; margin-right: 5px;" type="button" value="?"/> Lowest Latency <input type="button" value="v"/>
Note: Use of Lowest Latency will incur additional network usage.	
Connection	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> Wi-Fi WAN <input checked="" type="checkbox"/> Cellular 1 <input checked="" type="checkbox"/> Cellular 2 <input checked="" type="checkbox"/> USB

The traffic matching this rule will be routed through the healthy WAN connection that is selected in the field *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 up” link can be higher than that of a “2M down / 2M up” link. It is because the overall round trip time is lengthened by its lower upstream bandwidth despite of its higher downlink speed. Therefore this algorithm is good for two scenarios:

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

14.1.6 Expert Mode

Expert Mode is also available for advance users. Click the help test balloon and click the link turn on Expert Mode to switch on the feature.

Under Expert Mode, a special rule - "SpeedFusion™Routes" is displayed on the Custom Rules table. It represents all SpeedFusion™routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. That means traffic for remote VPN subnets will be routed to its corresponding VPN peer. You can create custom Priority or Enforced rules and move them above the bar to override the SpeedFusion™Routes.

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

Rules <input type="button" value="Hand"/> Drag and drop rows to change rule order					
Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persis...	Persistence (Src) (Auto)	Any	Any	TCP 443	<input type="button" value="X"/>
Default (Auto)					
<input type="button" value="Add Rule"/>					

Help

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

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

If you require advanced control of S2S VPN traffic, [turn on Expert Mode](#).

15 Port Forwarding

15.1 Port Forwarding Service

The Pepwave MAX can act as a firewall that blocks, by default, all inbound access from the Internet. By using **Port Forwarding**, Internet users can access the servers behind Pepwave MAX.

Inbound Port Forwarding rules can be defined at **Advanced > Port Forwarding**:

Service	IP Address(es)	Server	Protocol	
Service_1	WAN 1: Interface IP	120.78.95.7	TCP:80	
<input type="button" value="Add Service"/>				

To define a new service, click the **Add Service** button, upon which the following appears:

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No												
Service Name	<input type="text" value="Service_1"/>												
IP Protocol	TCP :: Protocol Selection Tool ::												
Port	Single Port Service Port: <input type="text" value="80"/>												
Inbound IP Address(es) (Require at least one IP address)	<div style="border: 1px solid black; padding: 2px;"> <p style="text-align: right; margin: 0;">Connection / IP Address(es) <input type="button" value="All"/> <input type="button" value="Clear"/></p> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"><input checked="" type="checkbox"/> WAN 1</td> <td style="width: 50%;"><input checked="" type="checkbox"/> 10.8.9.86 (Interface IP)</td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Wi-Fi WAN</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 1</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> USB</td> <td></td> </tr> </table> </div>	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.8.9.86 (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	
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.8.9.86 (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	<input type="text" value="120.78.95.7"/>												

Port Forwarding Settings

Enable	<p>This setting specifies whether the inbound service rule takes effect.</p> <p>When Yes is selected, the inbound service rule takes effect. If the inbound traffic matches the specified IP Protocol and Port, action will be taken by the Pepwave MAX based on the other parameters of the rule.</p> <p>When No is selected, the inbound service rule does not take effect. The Pepwave MAX will disregard the other parameters of the rule.</p>
Service Name	<p>This setting identifies the service to the System Administrator.</p> <p>Valid values for this setting consist only of alphanumeric and the underscore “_” characters.</p>
IP Protocol	<p>The IP Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP or IP.</p> <p>Traffic that is received by the Pepwave MAX 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.)</p> <p>Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically</p>

User Manual

PEPWAVE *MAX* mobile router

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 remains manually modifiable.

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

Any Port, Single Port, Port Range and Port Map

Port

Any Port: All traffic that is received by the Pepwave MAX 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 Service Port:

Single Port: Traffic that is received by the Pepwave MAX 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 Service Ports: -

Port Range: Traffic that is received by the Pepwave MAX 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 **Single Port** and **Service Port 80-88**, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.

Port Service Port:
Map to Port:

Port Mapping: Traffic that is received by the Pepwave MAX 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 Map**, **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 Service Ports: -
Map to Ports: -

Range Mapping: traffic that is received by the Pepwave MAX 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.

It is required to select at least one IP address.

Server IP Address

This setting specifies the LAN IP address of the server that handles the requests for the service.

User Manual

PEPWAVE *MAX* mobile router

15.1.1 UPnP / NAT-PMP Settings

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



UPnP / NAT-PMP Settings	
UPnP	<input checked="" type="checkbox"/> Enable
NAT-PMP	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/>	

A table listing all the forwarded ports under these two protocols can be found at **Status > UPnP / NAT-PMP**.

16 NAT Mappings

The configuration of NAT Mappings allows the IP address mapping of all inbound and outbound NAT'd traffic to and from an internal client IP address.

The 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	Delete
192.168.1.24	(WAN2):30.21.21.12	(WAN2):30.21.21.12	Delete
Add NAT Rule			

To add a rule for NAT Mappings, click **Add NAT Rule**, upon which the following screen will be displayed:

LAN Client(s)	?	IP Address
Address	?	<input type="text"/>
Inbound Mappings	?	Connection / Inbound IP Address(es) <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB
Outbound Mappings	?	Connection / Outbound IP Address WAN 1: 10.8.9.86 (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.

User Manual

PEPWAVE *MAX* mobile router

Network	<p>The IP network refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of public IP addresses, specified below, to facilitate outbound traffic.</p> <p>This option is only available when IP Network is selected.</p>
Inbound Mappings	<p>This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind on. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN Host.</p> <p>This option is only available when IP Address is selected in LAN Client(s) field.</p> <p>Note 1: Inbound Mapping is not needed for WAN connections in drop-in or IP forwarding mode.</p> <p>Note 2: Each WAN IP address can be associated to one NAT Mapping only.</p>
Outbound Mappings	<p>This setting specifies the WAN IP addresses should be used when an IP connection is made from a LAN host to the Internet.</p> <p>Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility).</p> <p>Note 1: 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.</p> <p>Note 2: WAN connections in drop-in or IP forwarding mode are not shown here.</p>

Important Note

Inbound firewall rules override the Inbound Mapping settings.

User Manual


PEPWAVE *MAX* mobile router

17 QoS

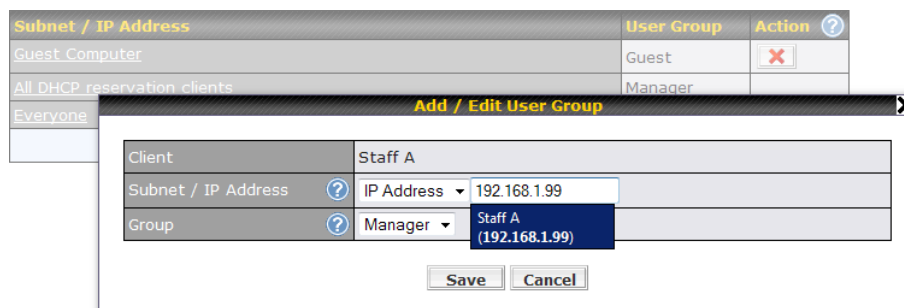
17.1 User Groups

LAN and PPTP clients can be categorized into three user groups - **Manager, Staff, and Guest**. This table 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.

The table is automatically sorted, and the table order signifies the rules' 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 bottommost. They are **All DHCP reservation clients** and **Everyone**, and they cannot be removed. **All DHCP reservation clients** represents the LAN clients defined in the DHCP Reservation table in the LAN settings page. **Everyone** represents all clients that are not defined in any rule above. Click on a rule to change its group.



Add / Edit User Group	
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.


User Manual

PEPWAVE *MAX* mobile router

17.2 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)	

User Manual

PEPWAVE *MAX* mobile router

17.3 Application

17.3.1 Application Prioritization

You can choose whether to apply the same Prioritization settings to all user groups or customize the settings for each group.

Application Prioritization
 Apply same settings to all users
 Customize

Three priority levels can be set for application prioritization: **↑ High**, **— Normal**, and **↓ Low**.


Four types of applications are predefined. Their priority for each user group can be selected from their corresponding drop down menu. Traffic types not defined in the table is assigned with normal priority.

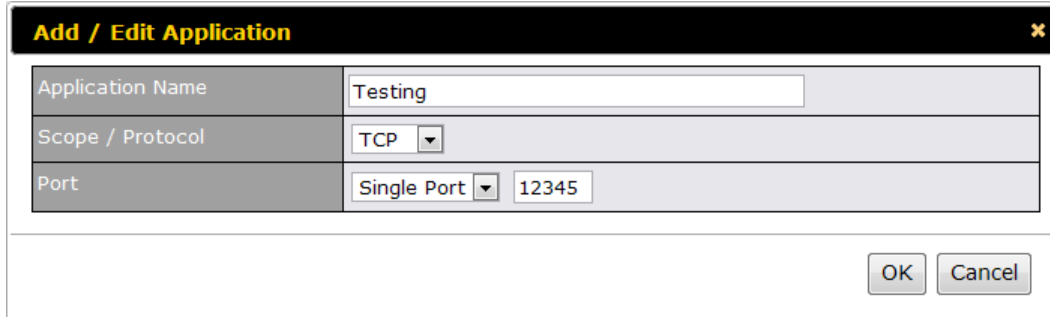
Application	Priority			Action
	Manager	Staff	Guest	
PPTP and IPsec VPN	— Normal	— Normal	— Normal	
SIP/Vonage	↑ High	↑ High	↑ High	
Skype, Google Talk, RealVideo, and Windows Streaming Media	— Normal	— Normal	— Normal	
Secure Web (HTTPS)	— Normal	— Normal	— Normal	
Custom Application				
Testing	↓ Low	↓ Low	↓ Low	
<input type="button" value="Add"/>				

User Manual

PEPWAVE *MAX* mobile router

17.3.2 Prioritization for Custom Application

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.



The dialog box titled "Add / Edit Application" contains the following fields:

Application Name	Testing
Scope / Protocol	TCP
Port	Single Port 12345

Buttons: OK, Cancel

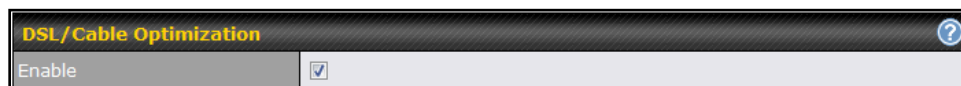
Application Prioritization	
PPTP and IPsec VPN	When enabled, any PPTP and IPsec traffic will be prioritized.
SIP/Vonage	When enabled, any SIP and Vonage voice traffic will be prioritized.
Skype, Google Talk, RealVideo, and Windows Streaming Media	When enabled, voice and video traffic of Skype, Google Talk, Real Video and Windows Streaming Media will be prioritized.
Secure Web (HTTPS)	When enabled, HTTPS (TCP port 443) traffic will be prioritized.

17.3.3 DSL/Cable Optimization

DSL/cable-based WAN connection has its upload bandwidth lower than the download bandwidth. When this option is enabled, the download bandwidth of the WAN can be fully utilized in any situation.

When a DSL/cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data in full speed until the uplink becomes less congested. The DSL/Cable Optimization can relieve such issue. When it is enabled, the download speed will become less affected by the upload traffic.

By default, this feature is **enabled**.



The "DSL/Cable Optimization" dialog box shows the "Enable" checkbox checked.

18 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, offensive Web sites, and/or other inappropriate uses.

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

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)
- Intrusion Detection and DoS Prevention

With SpeedFusion™ enabled (see Section 11), the firewall rules also apply to VPN tunneled traffic.

18.1 Outbound and Inbound Firewall

18.1.1 Access Rules

The outbound firewall settings are located at: **Advanced > Firewall > Outbound Firewall Rule.**

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"/>					

Upon clicking **Add Rule**, the following screen appears:

Add a New Outbound Firewall Rule ✕

New Firewall Rule

Rule Name *	<input type="text"/>
Enable	<input checked="" type="checkbox"/>
Protocol	Any <input type="button" value="⌵"/> ← :: Protocol Selection Tool :: <input type="button" value="⌵"/>
Source IP & Port	Any Address <input type="button" value="⌵"/>
Destination IP & Port	Any Address <input type="button" value="⌵"/>
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

User Manual

PEPWAVE *MAX* mobile router

Inbound firewall settings are located at: **Advanced> Firewall> Inbound Firewall 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"/>						

Once you click on **Add Rule**, the following window will appear:

Add a New Inbound Firewall Rule

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

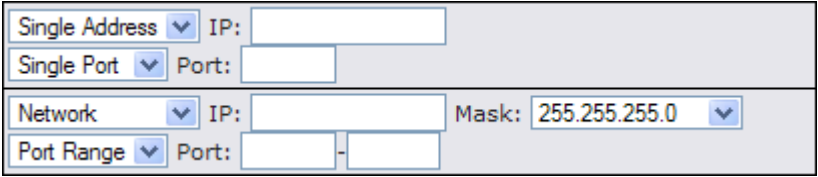
Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules is matching, the **Default** rule will be applied.

By default, the **Default** rule is set as **Allow** for both outbound and inbound access.

User Manual

PEPWAVE *MAX* mobile router

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.</p> <p>When Yes is selected, the firewall rule takes effect. If the traffic matches the specified Protocol/IP/Port, actions will be taken by the Pepwave MAX based on the other parameters of the rule.</p> <p>When No is selected, the firewall rule does not take effect. The Pepwave MAX will disregard the other parameters of the rule.</p>
WAN Connection	<p>This setting is applicable to Inbound Firewall Rules only.</p> <p>This setting specifies which WAN connection(s) the rule applies to:</p> <ul style="list-style-type: none"> • WAN 1 • WAN 2 • Wi-Fi WAN • Cellular 1 • Cellular 2 • USB <p>A value of WAN 1, WAN 2, Wi-Fi WAN, Cellular 1, Cellular 2, ... and USB specifies that the rule applies to all WAN connections, Ethernet WAN, PC Card, ... and Wi-Fi WAN, respectively.</p>
Protocol	<p>This setting specifies the protocol to be matched by the rule.</p> <p>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.)</p> <p>After selecting an item from the Protocol Selection Tool drop-down menu, the Protocol and Port number remains manually modifiable.</p>
Source IP & Port	<p>This specifies the source IP address(es) and port number(s) to be matched for a firewall rule.</p> <p>A single address, or a network, can be specified as the Source IP & Port setting, as indicated with the following screenshots:</p>  <p>In addition, a single port, or a range of ports, can be specified for the Source IP & Port setting.</p>
Destination IP & Port	<p>This specifies the destination IP address(es) and port number(s) to be matched for a firewall rule.</p> <p>A single address, or a network, can be specified as the Source IP & Port setting, as indicated with the following screenshots:</p>

User Manual

PEPWAVE *MAX* mobile router

Single Address	IP:	<input type="text"/>		
Single Port	Port:	<input type="text"/>		
Network	IP:	<input type="text"/>	Mask:	<input type="text" value="255.255.255.0"/>
Port Range	Port:	<input type="text"/>	-	<input type="text"/>

In addition, a single port, or a range of ports, can be specified for the Source IP & Port setting.

Action

This setting specifies the action to be taken by the Pepwave MAX upon encountering traffic that matches the both of the following:

- Source IP & Port
- Destination IP & Port
- With the value of **Allow** for the Action setting, the matching traffic passes through the Pepwave MAX (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 Pepwave MAX (and is discarded).

Event Logging

This setting specifies whether or not to log matched firewall events.

The logged messages are shown on the page **Status >Event Log**.

A sample message is as follows:

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

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

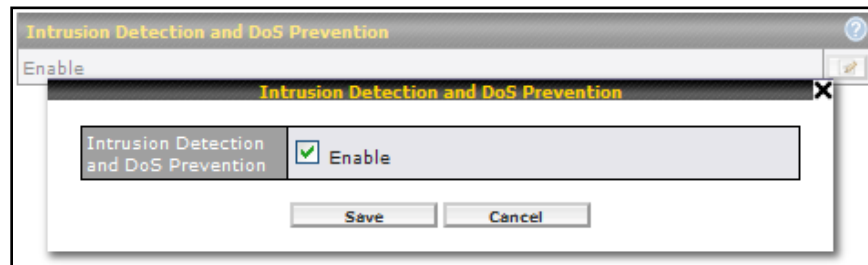
Tip


If the default inbound rule is set as **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 rules will be required.

User Manual

PEPWAVE *MAX* mobile router

18.1.1.1 Intrusion Detection and DoS Prevention



The Pepwave MAX supports detecting and preventing intrusions and Denial-of-Service (DoS) attacks from the Internet. To turn on this feature, click , check the box **Enable** for the **Intrusion Detection and DoS Prevention** and press the **Save** button.


When this feature is enabled, the Pepwave MAX will detect and protect the network from 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


User Manual

PEPWAVE *MAX* mobile router

18.1.2 Web Blocking

Web Blocking		
Web Site Domain Name		
<input type="text"/>		

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

Exempted Subnets		
Network	Subnet Mask	
<input type="text"/>	255.255.255.0 (/24) ▼	

18.1.2.1 Web Blocking

Enter an appropriate website address and the Pepwave MAX will block and disallow LAN/PPTP/SpeedFusion™ peer clients to access these websites.

You may enter the wild card ".*" at the end of a domain name to block any web site with a host name having the domain name in the middle.

For example, If you enter "foobar.*," then "www.foobar.com," "www.foobar.co.jp," or "foobar.co.uk" will be blocked.

Placing the wild card in any other position is not supported.

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

18.1.2.2 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 **Error! Reference source not found.** for details.

18.1.2.3 Exempted Subnets

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

User Manual

PEPWAVE *MAX* mobile router

19 Miscellaneous Settings

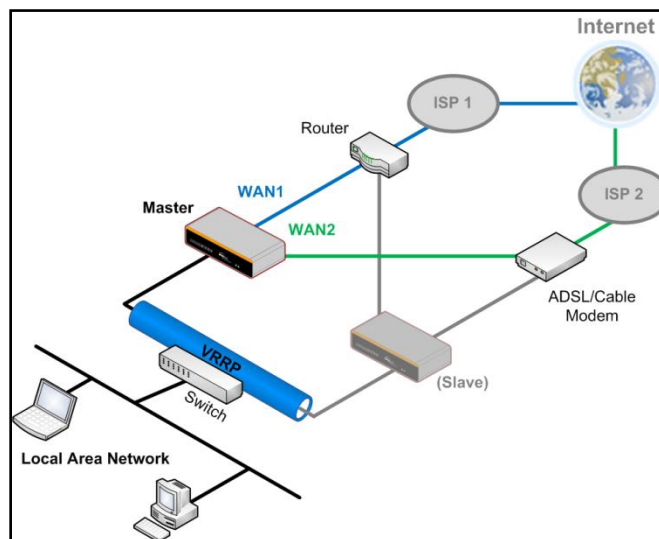
The miscellaneous settings include configuration for PPTP Server, Service Forwarding, and Service Passthrough.

19.1 High Availability

(Available on Pepwave MAXHD2 and 700)

The Pepwave MAX supports High Availability (HA) configurations via an open standard Virtual Router Redundancy Protocol (VRRP, RFC 3768).

In an HA configuration, two Pepwave MAX units 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 MAX unit connect to the router and to the modem. Both Pepwave MAX units connect to the same LAN switch via a LAN port.

An elaboration on the technical details of the implementation, by Pepwave MAX, of Virtual Router Redundancy Protocol (VRRP, RFC 3768) is as follows:

- In an HA configuration, the two Pepwave MAX units communicate with each other using VRRP over the LAN.
- The two Pepwave MAX units 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 MAX unit is received in 3 seconds (or longer) since the last heartbeat signal, the Slave Pepwave MAX unit becomes active.
- The Slave Pepwave MAX unit initiates the WAN connections, and binds to a previously configured LAN IP address.
- At a subsequent point when the Master Pepwave MAX unit recovers, it will once again become active.

You can configure High Availability at the following location: **Network > Misc. Settings > High Availability**.

Interface for Master Router

Interface for Slave Router

User Manual

PEPWAVE *MAX* mobile router

High Availability		High Availability	
Enable	<input checked="" type="checkbox"/>	Enable	<input checked="" type="checkbox"/>
Group Number	5	Group Number	5
Preferred Role	Master	Preferred Role	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

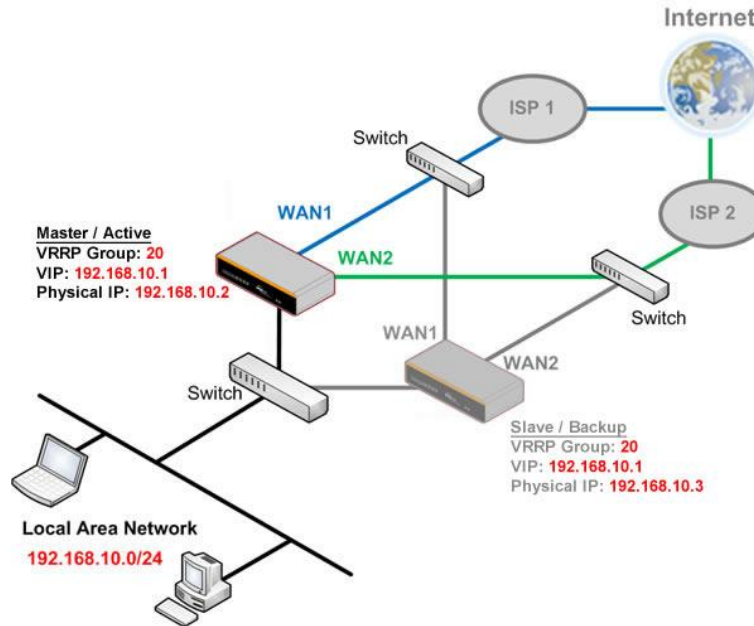
High Availability	
Enable	Checking this box specifies that the Pepwave MAX unit is part of a High Availability configuration.
Group Number	This number identifies a pair of Pepwave MAX units operating in a High Availability configuration. The two Pepwave MAX units in the pair must have the same Group Number value.
Preferred Role	This setting specifies whether the Pepwave MAX unit 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 the box 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. This 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.

User Manual

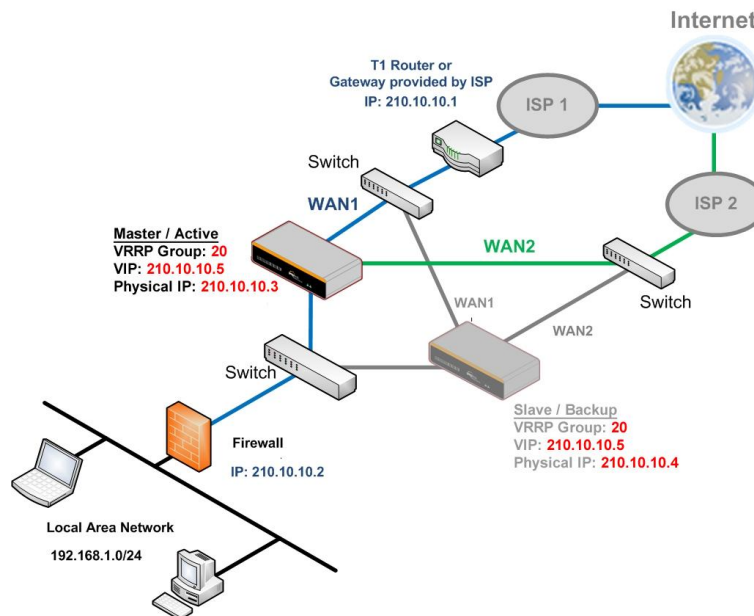
PEPWAVE *MAX* mobile router

Important Note

For MAXrouters in NAT mode, the Virtual IP (VIP) should be set as the default gateway for all hosts sitting on the LAN segment. For example, a firewall sitting behind the MAX router should set its default gateway as the Virtual IP instead of the IP of Master MAX unit.



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

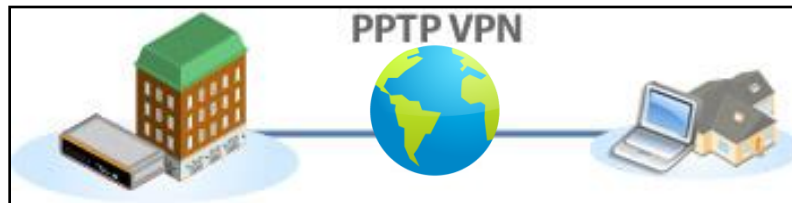


Please note that the Drop-in WAN cannot be configured as a LAN Bypass port while it is configured for High Availability.

User Manual

PEPWAVE *MAX* mobile router

19.2 PPTP Server



The Pepwave MAX has a built-in PPTP Server, which enables remote computers to conveniently and securely access the local network.

PPTP server setting is located at **Advanced > Misc. Settings > PPTP Server**.

Simply check the box to enable the PPTP server function. All connected PPTP sessions are displayed on the Client List at **Status > Client List**. Please refer to section 22.3 for details.

PPTP Server	
Enable	<input checked="" type="checkbox"/>
Listen On	Connection / IP Address(es)
	<input checked="" type="checkbox"/> Ethernet WAN <input checked="" type="checkbox"/> 123.123.123.1 (Interface IP)
	<input type="checkbox"/> Express Card
	<input type="checkbox"/> PC Card
	<input type="checkbox"/> USB1
	<input type="checkbox"/> USB2
<input type="checkbox"/> Wi-Fi Hotspot	
User Accounts	No User Account
	<input type="button" value="Add"/>

PPTP Server Setting

Listen On

This setting is for specifying the WAN connection(s) and IP address(es) where the PPTPserver should listen on.

Authentication

Select the source of user databases for PPTP authentication.

Local User Accounts - User accounts are stored in the device locally. You can add/modify/delete the accounts in the User Accounts table below, click **Add** to add a new account.

Authentication	<input type="button" value="?"/> Local User Accounts
User Accounts	<input type="button" value="?"/> No User Account
	<input type="button" value="Add"/>

LDAP Server - Authenticate with an external LDAP server. Tested with OpenLDAP server where passwords are NTLM hashed. Active Directory is not supported. (You can choose to

User Manual

PEPWAVE *MAX* mobile router


use RADIUS to authenticate with a Windows Server.)

Authentication	LDAP Server	
LDAP Server	<input type="text"/>	Port 389 <input type="button" value="Default"/>
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server	
Base DN	<input type="text"/>	
Base Filter	<input type="text"/>	

RADIUS Server - Authenticate with an external RADIUS server. Tested with Microsoft Windows Internet Authentication Service, and FreeRADIUS servers where passwords are NTLM hashed or in plain text.

Authentication	RADIUS Server	
Auth Server	<input type="text"/>	Port 1812 <input type="button" value="Default"/>
Auth Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters
Accounting Server	<input type="text"/>	Port 1813 <input type="button" value="Default"/>
Accounting Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters

2. User Accounts

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 username to edit the account password. Click the button  to delete the account in its corresponding row.

19.3 Certificate Manager

Certificate Manager		
VPN Certificate	No Certificate	Assign
Web Admin SSL Certificate	-----BEGIN CERTIFICATE----- MIIC2jCCAkOgAwIBAgIBADANBgkqhkiG9w0BAQUFADBkMQs...	Re-assign more details




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.

User Manual

PEPWAVE *MAX* mobile router

19.4 Service Forwarding

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

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

Service Forwarding	
SMTP Forwarding	When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting Enable .
Web Proxy Forwarding	When this option is enabled, all outgoing connections destined for the proxy server specified in Web Proxy Interception Settings will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web Proxy Interception Settings and proxy server settings for each WAN can be specified after selecting Enable .
DNS Forwarding	When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using 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.

19.4.1 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. The Pepwave MAX supports intercepting and redirecting all outgoing SMTP connections (destined for TCP port 25) via a WAN connection to the WAN's corresponding SMTP server.

User Manual

PEPWAVE *MAX* mobile router

SMTP Forwarding Setup ?			
SMTP Forwarding		<input checked="" type="checkbox"/> Enable	
Connection	Enable Forwarding?	SMTP Server	SMTP Port
Ethernet WAN	<input checked="" type="checkbox"/>	10.10.1.1	25
Express Card	<input type="checkbox"/>		
PC Card	<input type="checkbox"/>		
USB1	<input checked="" type="checkbox"/>	10.10.2.1	25
USB2	<input type="checkbox"/>		
Wi-Fi WAN	<input type="checkbox"/>		

To enable the feature, select the **Enable** check box under **SMTP Forwarding Setup**. Check the box **Enable Forwarding?** For the WAN connection(s) that needs such forwarding. Enter the ISP's e-mail server address and TCP port number for each WAN.

The Pepwave MAX will intercept SMTP connections, choose a WAN with reference to the Outbound Policy, and then forward the connection to the forwarded 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 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 rule in Outbound Policy (see section 13.2).

User Manual

PEPWAVE *MAX* mobile router

19.4.2 Web Proxy Forwarding

Web Proxy Forwarding Setup		
Web Proxy Forwarding	<input checked="" type="checkbox"/> Enable	
Web Proxy Interception Settings		
Proxy Server	IP Address <input type="text" value="202.43.66.76"/>	Port <input type="text" value="8080"/>
(Current settings in users' browser)		
Connection	Enable Forwarding?	Proxy Server IP Address : Port
Ethernet WAN	<input checked="" type="checkbox"/>	<input type="text" value="10.10.1.1"/> : <input type="text" value="8123"/>
Express Card	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
PC Card	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
USB1	<input checked="" type="checkbox"/>	<input type="text" value="10.10.2.1"/> : <input type="text" value="8080"/>
USB2	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
Wi-Fi WAN	<input checked="" type="checkbox"/>	<input type="text" value="10.10.3.1"/> : <input type="text" value="8080"/>

When this feature is enabled, the Pepwave MAX 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.

19.4.3 DNS Forwarding

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

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

User Manual

PEPWAVE *MAX* mobile router

19.5 Service Passthrough

Service Passthrough settings can be found in **Advanced > Misc. Settings > Service Passthrough**:

Service Passthrough Support	
SIP	<input checked="" type="radio"/> Standard Mode <input type="radio"/> Compatibility Mode <input checked="" type="checkbox"/> Define custom signal ports 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>
H.323	<input type="checkbox"/> Enable
FTP	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Define custom control ports
TFTP	<input type="checkbox"/> Enable
IPsec NAT-T	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Define custom ports <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 required to be specially handled in a multi-WAN environment. The Pepwave MAX supports handling such services correctly such that Internet applications do not notice it is behind a multi-WAN router. Settings for Service Passthrough Support are available here.

Service Passthrough Support	
SIP	<p>Session Initiation Protocol, aka SIP, is a voice-over-IP protocol. The Pepwave MAX 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.</p> <p>If your SIP server's signal port number is non-standard, you can check the box Define custom signal ports and input the port numbers to the text boxes.</p>
H.323	<p>With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and passthrough the device.</p>
FTP	<p>FTP sessions consist of two TCP connections; one for control and one for data. In multi-WAN situation, they have to be binded to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Pepwave MAX monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN.</p> <p>If you have an FTP server listening on a port number other than 21, you can check the box Define custom control ports and enter the port numbers to the text boxes.</p>
TFTP	<p>The Pepwave MAX monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select Enable if you want to enable the TFTP Passthrough support.</p>
IPsec NAT-T	<p>This field is for enabling the support of IPsec NAT-T Passthrough. UDP ports 500, 4500 and 10000 are monitored by default.</p> <p>You may add more custom data ports that your IPsec system uses by checking the box Define custom ports. If the VPN contains IPsec Site-to-Site VPN traffic, you have to check the box Route IPsec Site-to-Site VPN and choose the WAN connection to route the traffic to.</p> <p>If you have IPsec SpeedFusion™ traffic routed, check the Route IPsec SpeedFusion™ option and select a WAN to force routing such traffic to the specified WAN.</p>

User Manual

PEPWAVE *MAX* mobile router

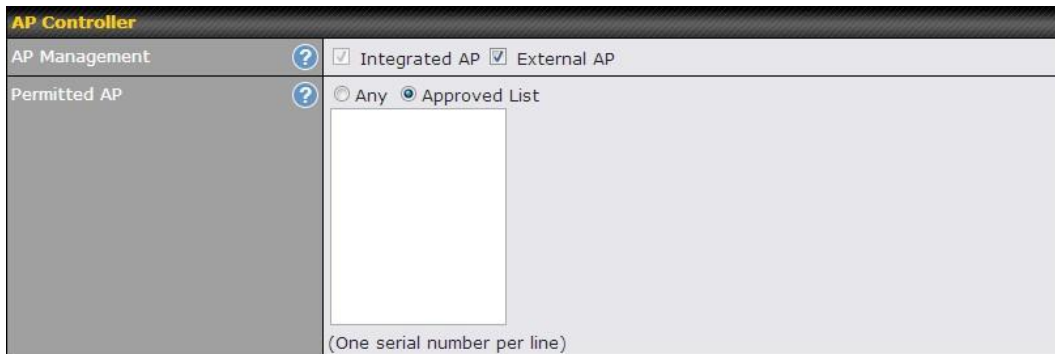
20 AP

The AP Controller acts as a centralized controller of Pepwave AP devices. With this feature, users will be able to customize and manage multiple AP one a single Peplink Balance Interface.

To configure, navigate to the **AP** tab and the following options will be shown.

20.1 Wireless SSID

This menu is the first one that appears upon clicking on the **AP** tab. This screen could also be reached by clicking on **AP > Wireless SSID**.



AP Controller

AP Management Integrated AP External AP

Permitted AP Any Approved List

(One serial number per line)

AP Controller

AP Management

The AP Controller for managing Pepwave APs can be enabled by this option.

By default, the Pepwave MAX has an **integrated AP**, which it will always control. By clicking the **External AP**, the MAX unit will also control access points connected on its LAN.

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 "wlancontroller" will added to the local DNS proxy.

Permitted AP

With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and passthrough the device.

User Manual

PEPWAVE *MAX* mobile router

20.2 Settings

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

AP Settings	
SSID	<input checked="" type="checkbox"/> 2.4 GHz <input checked="" type="checkbox"/> 5 GHz <small>Integrated AP supports 2.4GHz only. PEPWAVE_DEF1</small>
Operating Country	United States
Preferred Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz <small>Integrated AP supports 2.4GHz only.</small>
5 GHz Protocol	802.11na
5 GHz Channel Bonding	20 MHz
5 GHz Channel	Auto <input type="button" value="Edit"/> Channels:
2.4 GHz Protocol	802.11ng
2.4 GHz Channel Bonding	20 MHz
2.4 GHz Channel	1 (2.412 GHz)
Management VLAN ID	LAN (No VLAN)
Power Boost	<input type="checkbox"/>
Output Power	Max
Beacon Rate	1Mbps <input type="button" value="Default"/>
Beacon Interval	100ms <input type="button" value="Default"/>
DTIM	1 <input type="button" value="Default"/>
Slot Time	9 <input type="button" value="Default"/> μ s
ACK Timeout	48 <input type="button" value="Default"/> μ s
Frame Aggregation	<input checked="" type="checkbox"/>

AP Settings	
SSID	<p>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.</p>
Operating Country	<p>This drop-down menu specifies the national / regional regulations which the AP should follow.</p> <ul style="list-style-type: none"> If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). <p>NOTE: Users are required to choose an option suitable to local laws and regulations.</p> <p>The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation 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 AP that can transmit at both 5.4GHz and 5GHz</p>

User Manual

PEPWAVE *MAX* mobile router

	frequencies,
Protocol (5GHz, 2.4 GHz)	This section displays the wireless protocols which your AP are using.
Channel Bonding (5GHz, 2.4 GHz)	<p>This drop-down menu is only available for 802.11bgn or 802.11n protocols only.</p> <p>There are three options: 20 MHz, 20/40 MHz and 40 MHz</p> <p>With this feature enabled, it allows the Wi-Fi system to use two channels at once. Using two channels improves the performance of the Wi-Fi connection</p>
Channel (5GHz, 2.4 GHz)	<p>This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 for the country setting of North America and from 1 to 13 for the country setting of Europe regionn, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.)</p> <p>If Auto is set, the system would perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.</p>
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as AP to AP-controller communication traffic. The value is zero 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.
Power Boost^A	With this option enabled, the AP under this profile will transmit using additional power. Please note that using this option with several AP in close proximity will lead to increased interference.
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 AP 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 give your AP further instructions.</p>
Beacon Rate^A	This drop-down menu provides the option to send beacon in different transmit bit rate and the bit rates are: 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps.
Beacon Interval^A	This drop-down menu provides the option to set the time between each beacon send. Available options are: 100ms, 250ms and 500ms.
DTIM^A	This field provides the option to set the frequency for beacon to include Delivery Traffic Indication Message, DTIM. The interval unit is measured in milliseconds.
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

User Manual

PEPWAVE *MAX* mobile router

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.

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

Web Administration Settings	
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="a33d3f7b2aab"/> <input type="button" value="Generate"/>


Web Administration Settings (on External AP)	
Enable	Check the box to allow Peplink Balance 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 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 be redirect to HTTPS automatically.
Admin User Name	This field specifies the administrator username of the web admin. It is set as admin 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.

20.3 Toolbox

Additional tools for managing firmware packs can be found under **AP > Toolbox**.

Firmware Packs				
	Pack ID	Release Date	Details	Action
1.	1126	2013-08-26		

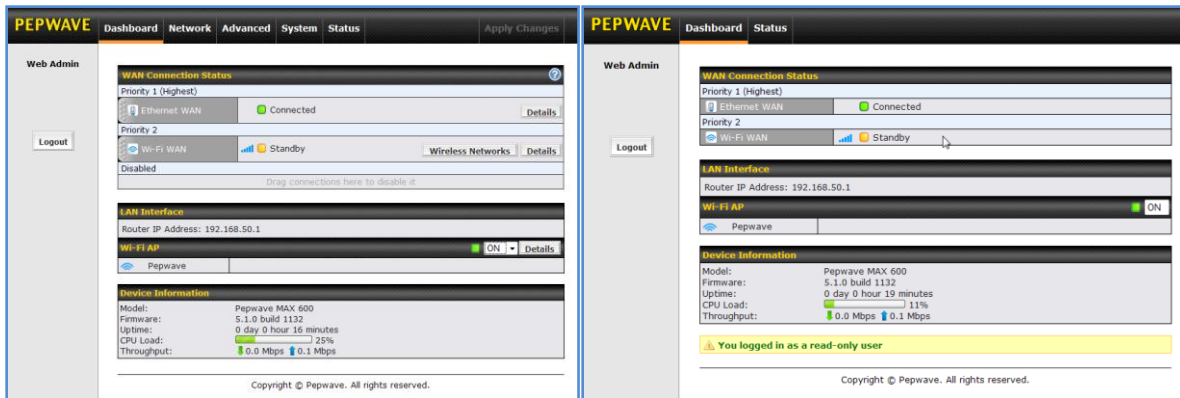
Firmware Packs

This is the first menu that will appear. 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 either press to download new packs or you can press to manually upload a firmware pack. Press to define which firmware pack is default.

21 System Settings

21.1 Admin Security

There are two user accounts available for accessing the Web Admin. Usernames are **admin** and **user**. They represent two user levels - **admin** has full administration access, while **user** is a read-only account. The read-only account can only access the device's status information and cannot make any change on the device.



Admin Account UI

User Account UI

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

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

Default: 4 hours 0 minutes.

For security reason, after logging in to the Web Admin Interface for the first time, it is recommended to change the administrator password.

Configuring the administration interface to be accessible only from the LAN can further improve system security.

User Manual

PEPWAVE *MAX* mobile router

Administrative Settings configuration is located at **System>Admin Security**.

Admin Settings	
Router Name	MAX_HD2_DEF1 hostname: max-hd2-def1
Admin User Name	admin
Admin Password
Confirm Admin Password
Read-only User Name	user
User Password	
Confirm User Password	
Web Session Timeout	4 Hours 0 Minutes
Authentication by RADIUS	<input checked="" type="checkbox"/> Enable
Auth Protocol	MS-CHAP v2
Auth Server	Port <input type="text"/> Default
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Auth Timeout	3 seconds
Accounting Server	Port <input type="text"/> Default
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Network Connection	LAN
CLI SSH	<input checked="" type="checkbox"/> Enable
CLI SSH Port	22
CLI SSH Access	LAN/WAN
Security	HTTP
Web Admin Port	80 Default
Web Admin Access	LAN/WAN

Admin Settings

Router Name	This field allows you to define a name for this Pepwave MAX unit. By default, Router Name is set as MAX_XXXX , where XXXX refers to the last 4 digits of the serial number of the device.
Admin User Name	It is set as admin by default and is not customizable.
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	It is set as user by default and is not customizable.
User Password	This field allows you to specify a new user password. Once the user password is set, the feature of read-only user will be enabled.
Confirm User Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the device terminates its access to Web Admin Interface. By default, it is set as 4 hours .
Authentication by RADIUS	With this box is checked, Web Admin will authenticate using an external RADIUS server. Authenticated users are treated as "admin" with full read-write permission or "user" with read-only access. Local "admin" and "user" accounts will be disabled. When the

User Manual

PEPWAVE *MAX* mobile router

	device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Authentication options will be available once this box is checked.
Auth Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
Auth Server	This specifies the access address of the external RADIUS server.
Auth Server Secret	This is the secret for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address of the external Accounting server.
Accounting Server Secret	This is the secret for accessing the Accounting server.
Network Connection	This option is for specifying the network connection which will be used for authentication connection. Users can choose from LAN, WAN and VPN connections.
CLI SSH	CLI (Command Line Interface) can be accessed via SSH. This field enables the CLI support.
CLI SSH Port, CLI SSH Access	These settings specify which TCP port and which interface(s) to accept remote SSH CLI access. The user name and password used for remote SSH CLI access are the same as those for web admin access.
Security	This option is for specifying the protocol(s) through which the Web Admin Interface can be accessible: <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/HTTPS
Web Admin Port	These fields are for specifying the port number at which the Web Admin Interface can be accessible.
Web Admin Access	This option is for specifying the network interfaces through which the Web Admin Interface can be accessible: <ul style="list-style-type: none"> • LAN only • LAN/WAN • If LAN/WAN is chosen, a WAN Connection Access Settings form will be displayed.

WAN Connection Access Settings

Allowed Source IP Subnets ? Any Allow access from the following IP subnets only

Allowed WAN IP Address(es)

Connection / IP Address(es)	
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.8.9.86 (Interface IP)
<input checked="" type="checkbox"/> WAN 2	<input checked="" type="checkbox"/> Interface IP

User Manual

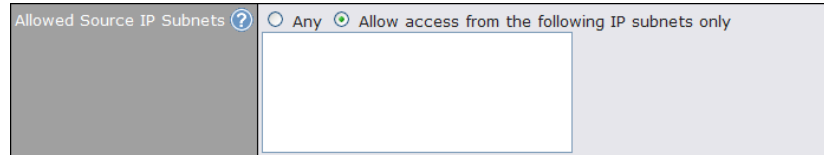
PEPWAVE *MAX* mobile router

WAN Connection Access Settings

This field allows you to restrict web admin access only from defined IP subnets.

- **Any** - Allow web admin accesses to be from anywhere, without IP address restriction.
- **Allow access from the following IP subnets only** - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:

Allowed Source IP Subnets



The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of w.x.y.z/m

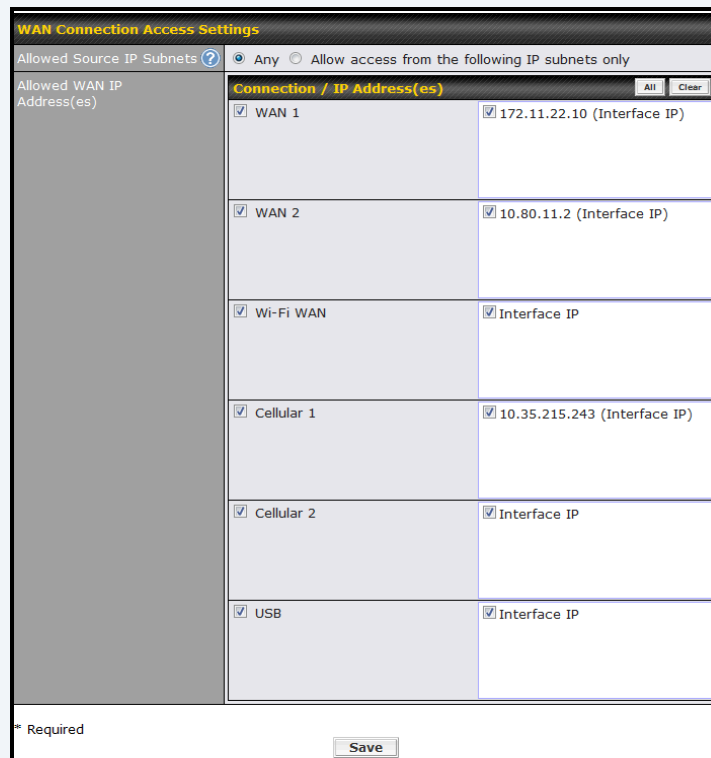
Where w.x.y.z is an IP address (e.g. 192.168.0.0), and m is the subnet mask in CIDR format, which is between 0 and 32 inclusively. For example: 192.168.0.0/24

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

- 192.168.0.0/24
- 10.8.0.0/16

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

Allowed WAN IP Address(es)



Connection / IP Address(es)	IP Address(es)
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 172.11.22.10 (Interface IP)
<input checked="" type="checkbox"/> WAN 2	<input checked="" type="checkbox"/> 10.80.11.2 (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"/> 10.35.215.243 (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

User Manual

PEPWAVE *MAX* mobile router

21.2 Firmware Upgrade

The firmware of the Pepwave MAX is upgradeable through Web Admin Interface. Firmware upgrade functionality is located at **System > Firmware**:

The screenshot shows two sections of the Web Admin Interface. The top section, titled "Firmware Upgrade", displays the current firmware version as 6.1.0 and indicates it is pending a firmware check. Below this is a "Check for Firmware" button. The bottom section, titled "Manual Firmware Upgrade", features a "Firmware Image" label, a "Choose File" button, and a text field showing "No file chosen". Below this is a "Manual Upgrade" button.

There are two ways to upgrade the unit. The first method is online firmware upgrade. The system can Check, Download and Upgrade over the Internet. The second method is to upload a firmware file manually. Click on the **Check again** button to use online upgrade. With online upgrade, Pepwave MAX checks online for new firmware. If a new firmware is available, the Pepwave MAX will automatically download the firmware. The upgrade process will subsequently be automatically initiated.

You may also download a firmware image from the [Pepwave web site](#) and update the unit manually. Click **Browse** to select the firmware file from the local computer, and then click **Manual Upgrade** to send the firmware to the Pepwave MAX. The Pepwave MAX will then automatically initiate the firmware upgrade process.

Please note that all Pepwave devices are equipped to be able to store two different firmware versions in two different partitions. A firmware upgrade performed will always replace the inactive partition. If you want to keep the inactive firmware, you can simply reboot your device with the inactive firmware and then perform the firmware upgrade.

Important Note

The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the Release Notes for the particular firmware version. Do not disconnect the power during firmware upgrade process. Do not attempt to upload a non-firmware file, or a firmware file that is not qualified, or not supported, by Pepwave. Upgrading a Pepwave MAX with an invalid firmware file will damage the unit, and may void the warranty.

Important Note

If the firmware is rolled back from 5.x to 4.x, the configurations will be lost.

User Manual

PEPWAVE *MAX* mobile router

21.3 Time

The Time Server functionality enables the system clock of the Pepwave MAX to be synchronized with a specified Time Server.

The settings for Time Server configuration are located at **System > Time**:

Time Settings	
Time Zone	(GMT-08:00) Pacific Time (US & Canada) <input type="checkbox"/> Show all
Time Server	time.nist.gov <input type="button" value="Default"/>

Time Server Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme) in which the Pepwave MAX operates. The Time Zone value affects the time stamps in the Event Log of the Pepwave MAX and E-mail notifications. Checked the box Show all to show all available time zone options.
Time Server	This setting specifies the NTP network time server to be utilized by the Pepwave MAX.

21.4 Email Notification

The Email Notification functionality of the Pepwave MAX provides a System Administrator with up-to-date information on network status.

The settings for configuring Email Notification are found at **System > Email Notification**:

Email Notification Setup ?	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	smtp.mycompany.com <input checked="" type="checkbox"/> Require authentication
SSL Encryption	<input type="checkbox"/> (Note: any server certificate will be accepted)
SMTP Port	25 <input type="button" value="Default"/>
SMTP User Name	smtpuser
SMTP Password	••••••
Confirm SMTP Password	••••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

User Manual

PEPWAVE *MAX* mobile router

Email Notification Settings

Email Notification	<p>This option is for enabling Email Notification.</p> <p>If the box Enable is checked, the Pepwave MAX sends email messages to a System Administrator when the WAN status changes, or when new firmware is available.</p> <p>If the box Enable is not checked, Email Notification is disabled and the Pepwave MAX will not send email messages.</p>
SMTP Server	<p>This field is for specifying the SMTP server to be used for sending email. If the server requires authentication, check the box Require authentication.</p>
SSL Encryption	<p>Check the box to enable SMTPS. When the box is checked, the next field SMTP Port will be changed to 465 automatically.</p>
SMTP Port	<p>This field is for specifying the SMTP Port number.</p> <p>By default, this is set to 25; when the SSL Encryption box is checked, the default port number will be set to 465.</p> <p>You may customize the port number by editing this field. Click the button Default to restore to default.</p>
SMTP User Name / Password	<p>This setting specifies the SMTP username and password while sending email. These options are shown only if Require authentication check box is checked in SMTP Server setting.</p>
Confirm SMTP Password	<p>This field allows you to verify and confirm the new administrator password.</p>
Sender's Email Address	<p>This setting specifies the sender email address reported by the email messages sent by the Pepwave MAX.</p>
Recipient's Email Address	<p>This setting specifies the email addresses to which the Pepwave MAX should send the email messages to. You may enter multiple recipients' email addresses in this field.</p>

User Manual

PEPWAVE *MAX* mobile router

After you have completed the settings, you can click the **Test Email Notification** button to test the settings before saving it. After it is clicked, you will see this screen to confirm the settings:

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	25
SMTP User Name	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Click **Yes** to confirm. Wait a few seconds, and you will see a return message and the detailed test result.

Test email sent. Email notification settings are not saved, it will be saved after clicked the 'Save' button.

Test Result

```
[INFO] Try email through connection #3
[<-] 220 ESMTTP
[->] EHLO balance
[<-] 250-smtp Hello balance [210.210.210.210]
250-SIZE 100000000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250-STARTTLS
```

User Manual

PEPWAVE *MAX* mobile router

21.5 EventLog

The Remote Syslog functionality of thePepwave MAX enables event logging at a specified remote Syslog server.

The settings for configuring Remote System Log are found at **System>Event Log**:

The screenshot shows two configuration sections. The first section, titled "Send Events to Remote Syslog Server", has a "Remote Syslog" checkbox that is checked and a "Remote Syslog Host" text input field. The second section, titled "Push Events to Mobile Devices", has a "Push Events" checkbox that is checked. Both sections include a help icon (question mark) in the top right corner.

Remote Syslog Settings	
Remote Syslog	Remote Syslog allows syslog message to be sent to a specified remote syslog server. You can configure a remote syslog host either in the form of an IP address or a server domain name.
Remote Syslog Host	This setting specifies the IP address or host name of the remote Syslog server.
Port	This setting specifies the port number of the remote Syslog service. By default, the Port setting has value is 514 .

User Manual

PEPWAVE *MAX* mobile router

21.6 SNMP

SNMP or Simple Network Management Protocol is an open standard that can be used to collect information from the Pepwave MAX Mobile Router.

SNMP configuration is located at **System > SNMP**.

SNMP Settings	
SNMP Device Name	MAX
SNMP Port	161 <input type="button" value="Default"/>
SNMPv1	<input checked="" type="checkbox"/> Enable
SNMPv2c	<input checked="" type="checkbox"/> Enable
SNMPv3	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/>	

Community Name	Allowed Source Network	Access Mode	
kurt	192.168.50.1/24	Read Only	<input type="button" value="Delete"/>
<input type="button" value="Add SNMP Community"/>			

SNMPv3 User Name	Authentication / Privacy	Access Mode	
MyUser	MD5 / DES	Read Only	<input type="button" value="Delete"/>
<input type="button" value="Add SNMP User"/>			

SNMP Settings	
SNMP Device Name	This field shows the router name defined in System > Admin Security .
SNMP Port	This option specifies the port which SNMP used. The default port is set as 161 .
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.

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

SNMP Community ✕

Community Name	<input type="text" value="MyCompany"/>
Allowed Network	<input type="text" value="192.68.1.25"/> / <input type="text" value="255.255.255.0 (/24)"/> <input type="button" value="v"/>

User Manual

PEPWAVE *MAX* mobile router

SNMP Community Settings

Community Name	This setting specifies the SNMP Community Name.
Allowed Source Subnet Address	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g. 192.168.1.0), and specify your subnet mask using the pull-down menu.

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

SNMPv3 User ✕

User Name	<input type="text" value="User"/>
Authentication	MD5 <input type="text" value="Password"/>
Privacy	DES <input type="text" value="Password"/>

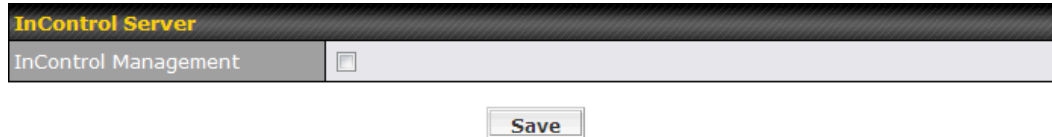
SNMPv3 User Settings

User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	<p>This setting specifies via a drop-down menu the one of the following valid authentication protocols:</p> <ul style="list-style-type: none">• NONE• MD5• SHA <p>Specify your password on the field to the right.</p>
Privacy Protocol	<p>This setting specifies via a drop-down menu the one of the following valid privacy protocols:</p> <ul style="list-style-type: none">• NONE• DES <p>Specify your password on the field to the right.</p>

User Manual

PEPWAVE *MAX* mobile router

21.7 InControl



The screenshot shows a web interface for configuring the InControl Server. At the top, there is a dark header with the text 'InControl Server' in yellow. Below this, there is a light gray section with the text 'InControl Management' and a small, unchecked checkbox. Below the checkbox is a button labeled 'Save'.

When this check box is checked, the device's status information, usage data, and configuration will be sent to Pepwave's InControl system. You can sign up for an InControl account at <https://incontrol.pepwave.com/> . You can register devices under the account, monitor device status and usage reports, and download backed up configuration files.

Default: Disabled

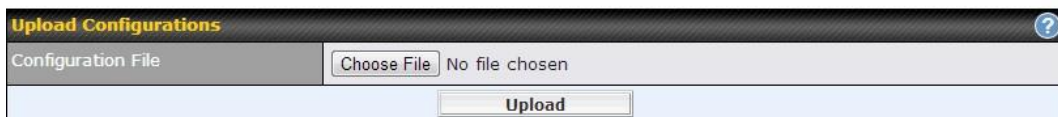
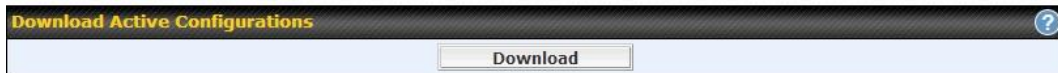
User Manual

PEPWAVE *MAX* mobile router

21.8 Configuration

Backing up the Pepwave MAX settings immediately after successful completion of the initial setup is strongly recommended.

The functionality to download and upload Pepwave MAX settings is found at **System > Configuration**



Configuration	
Restore Configuration to Factory Settings	The Restore Factory Settings button is to reset the configuration to the factory default settings. After clicking the button, you will need to click the Apply Changes button on the top right corner to make the settings effective.
Downloading Active Configurations	The purpose of the Download button is to backup the current active settings. Click Download and save the configuration file.
Uploading Configurations	To restore or change settings based on a configuration file, click Choose File to locate the configuration file on the local computer, and then click Upload . The new settings can then be applied by clicking the Apply Changes button on the page header, or you can cancel the procedure by pressing discard on the Main page of Web Admin Interface.
Uploading Configuration from High Availability Pair	(Available on Pepwave MAX HD2 and MAX 700) In a High Availability (HA) configuration, the MAX router can quickly load the configuration of its HA counterpart. To do so, click the Upload button. After loading the settings, configure the LAN IP address of the MAX router to be different from the HA counterpart.

User Manual

PEPWAVE *MAX* mobile router

21.9 Feature Add-ons

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



The screenshot shows a web interface titled "Feature Activation". It contains a label "Activation Key" on the left, a large empty text input field in the center, and a button labeled "Activate" centered below the input field.

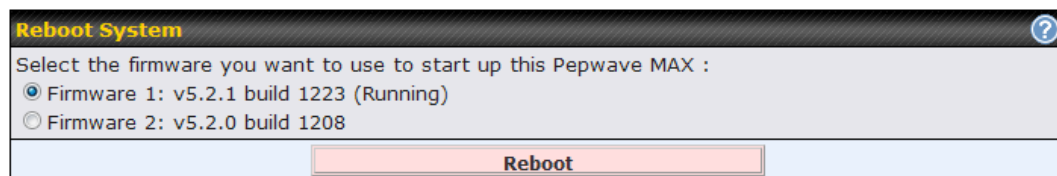
21.10 Reboot

This page provides a Reboot button for restarting the system.

For highest reliability, the Pepwave MAX is equipped with two copies of firmware of different version. You can select the firmware version you would like the device to reboot with.

The firmware marked with **(Running)** is the current system boot up firmware.

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



The screenshot shows a web interface titled "Reboot System" with a help icon (question mark) in the top right corner. The main text reads "Select the firmware you want to use to start up this Pepwave MAX :". Below this text are two radio button options: "Firmware 1: v5.2.1 build 1223 (Running)" which is selected, and "Firmware 2: v5.2.0 build 1208". At the bottom of the interface is a button labeled "Reboot".

User Manual

PEPWAVE *MAX* mobile router

21.11 Ping Test

The Ping Test tool in the Pepwave MAX performs Pings through a specified Ethernet interface or a SpeedFusion™ connection. You can specify the number of pings in the field **Number of times** to a maximum of 10 times, and Packet Size can be specified in the field **Packet Size** to a maximum of **1472** bytes.

The Ping utility is located at **System > Tools > Ping**, illustrated as follows:

The screenshot shows the 'Ping' utility interface. It has a 'Connection' dropdown menu set to 'WAN 1'. The 'Destination' field is empty. The 'Packet Size' is set to '56'. The 'Number of times' is set to '5' with a slider below it. There are 'Start' and 'Stop' buttons. Below the form is a 'Results' section with a 'Clear Log' button. The results text reads: 'PING 10.8.8.1 (10.8.8.1) from 5.192.62.250 56(84) bytes of data.'

Tip

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

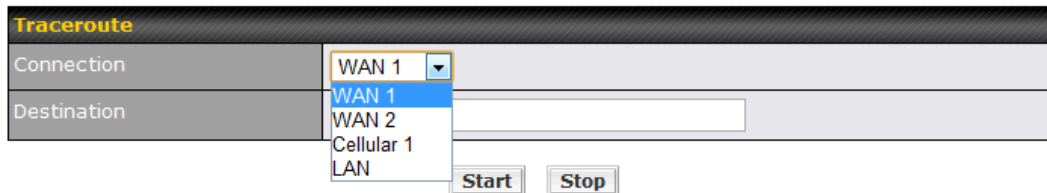
User Manual

PEPWAVE *MAX* mobile router

21.12 Traceroute Test

The Traceroute Test tool in the Pepwave MAX traces the routing path to the destination through a particular Ethernet interface or SpeedFusion™ connection.

The Traceroute Test utility is located at **System > Tools > Traceroute**, illustrated as follows:



Traceroute	
Connection	WAN 1
Destination	WAN 1 WAN 2 Cellular 1 LAN
<input type="button" value="Start"/> <input type="button" value="Stop"/>	

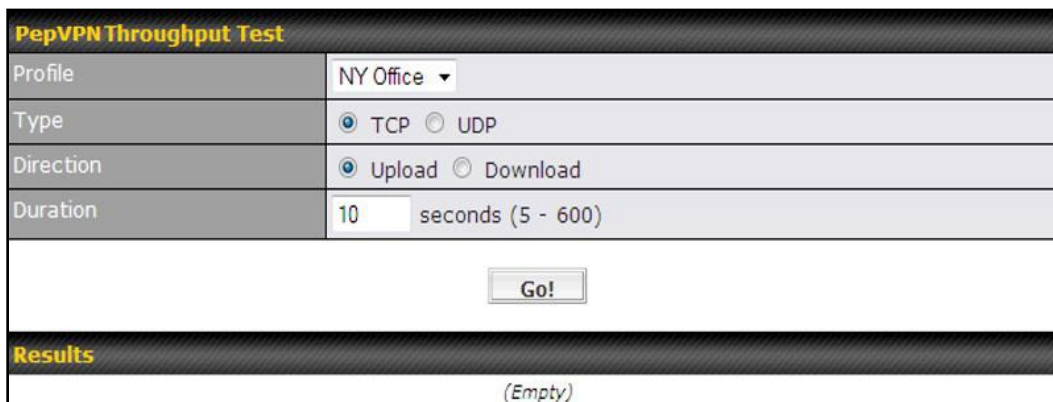
Tip

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

21.13 PepVPN Test

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

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



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

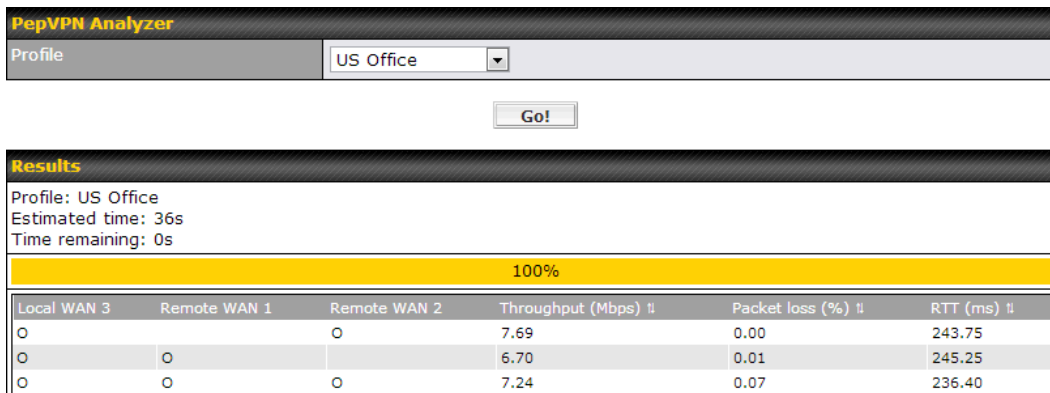
User Manual

PEPWAVE *MAX* mobile router

21.14 PepVPN Analyzer

The bandwidth bonding feature of PepVPN occurs when multiple WAN lines from one end merge with multiple WAN lines from the other end. For this to happen, each WAN line needs to form a connection with all the WAN lines on the opposite end. The function of the PepVPN Analyzer is to report the throughput, packet loss, and latency of all possible combinations of *connections*.

This feature is located in **System > PepVPN Analyzer**. To utilize this feature, simply choose your profile from the drop-down menu and click **Go!**



PepVPN Analyzer

Profile: US Office

Go!

Results

Profile: US Office
Estimated time: 36s
Time remaining: 0s

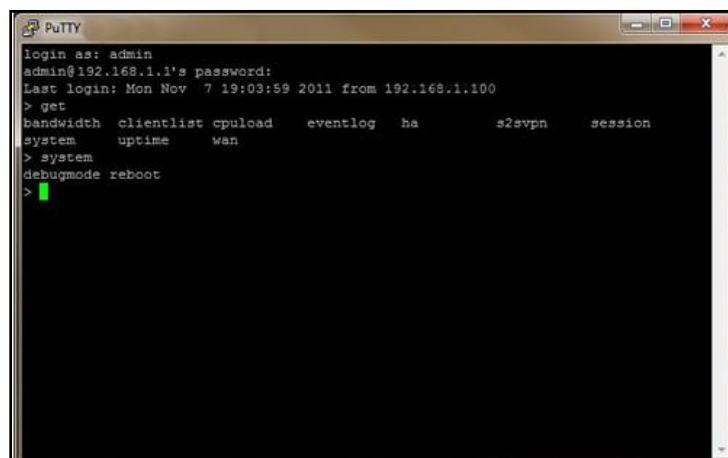
100%

Local WAN 3	Remote WAN 1	Remote WAN 2	Throughput (Mbps) †	Packet loss (%) †	RTT (ms) †
o		o	7.69	0.00	243.75
o	o		6.70	0.01	245.25
o	o	o	7.24	0.07	236.40

21.15 CLI (Command Line Interface Support)

The CLI (Command Line Interface) can be accessed via SSH. This field enables CLI support.

The below settings specify which TCP port and which interface(s) should accept remote SSH CLI access. The user name and password used for remote SSH CLI access are the same as those used for web admin access.



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

User Manual

PEPWAVE *MAX* mobile router

22 Status

This section displays the information of the Pepwave MAX on the **Device**, **ActiveSessions**, **Client List**, **WINS Client List**, **SpeedFusion™**, **UPnP / NAT-PMP**, **Event Log**, and **Bandwidth**.

22.1 Device

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

System Information	
Router Name	MAX_HD2_DEF1
Model	Pepwave MAX HD2
Hardware Revision	2
Serial Number	2830-A2D4-DEF1
Firmware	6.1.0 build 2472
PepVPN Version	3.0.0
Modem Support Version	1014 (Modem Support List)
Host Name	max-hd2-def1
Uptime	1 day 11 minutes
System Time	Fri Jan 03 09:20:45 WET 2014
Diagnostic Report	Download

System Information	
Router Name	This is the name specified in the field Router Name located in System > Admin Security .
Model	This shows the model name and number of this device.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version that this device is currently running.
Modem Support Version	This shows the modem support version of this device. A Modem Support List link redirects users to a list of cellular modems supported by this device.
Uptime	This shows the length of time since the device is rebooted.
System Time	This shows the current system time.
GPX File (HD2 and HD2 IP67 Only)	This contains the GPS data of the latest 7 days. A Download button is for exporting the data in GPX format of the selected date. For more information about how GPS works in HD2 and HD2 IP67, please refer to section 19.1.1.
Diagnostic Report	A Download button is for exporting a diagnostic report file required for system investigation.

Interface	MAC Address
LAN Port	00:1A:DD:BD:1D:80
WAN 1	00:1A:DD:BD:1D:81
WAN 2	00:1A:DD:BD:1D:82

The second table shows the MAC address of each LAN/WAN interface connected.

User Manual

PEPWAVE *MAX* mobile router

To view this you device's End User License Agreement (EULA), please click on the  icon.

Important Note

If you encounter issues and would like to contact PepwaveSupport Team (<http://www.pepwave.com/contact/>), please download the diagnostic report file and attach it along with a description of your encountered issue. In firmware 5.1 or before, Diagnostic Report file can be obtained at **System > Reboot**

22.1.1 GPS Data

The MAX HD2 and HD2 IP67 automatically stores up to seven days of GPS location data in GPS eXchange format (GPX). To review this data using third-party applications, click **Status > Device** and then download your GPX file.

The Pepwave MAX BR1, HD2 and HD2 IP67 export real-time location data in NMEA format through its LAN IP address at TCP port 60660. It is accessible from LAN or over a SpeedFusion connection. To access the data via a virtual serial port, you have to install a virtual serial port driver. Visit <http://www.peplink.com/index.php?view=faq&id=294> to download the driver.

User Manual

PEPWAVE *MAX* mobile router

22.2 Active Sessions

Information on Active Sessions is at **Status > Active Sessions > Overview**

Overview	Search	
Session data captured within one minute. Refresh		
Service	Inbound Sessions	Outbound Sessions
AIM/ICQ	0	1
Bittorrent	0	32
DNS	0	51
Flash	0	1
HTTPS	0	76
Jabber	0	5
MSN	0	11
NTP	0	4
QQ	0	1
Remote Desktop	0	3
SSH	0	12
SSL	0	64
XMPP	0	4
Yahoo	0	1
Interface	Inbound Sessions	Outbound Sessions
WAN 1	0	176
WAN 2	0	32
Wi-Fi WAN	0	51
Cellular 1	0	64
Cellular 2	0	0
USB	0	0
Top Clients		
Client IP Address	Total Sessions	
10.9.66.66	1069	
10.9.98.144	147	
10.9.2.18	63	
10.9.66.14	56	
10.9.2.26	33	

This screen displays the number of sessions initiated by each application. Click on each Service to obtain additional information. This screen also indicates the number of sessions initiated by each WAN port. Finally, you can see which clients are initiating the most sessions.

User Manual

PEPWAVE *MAX* mobile router

In addition, you can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to: **Status > Active Sessions > Search**

Overview
Search

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

IP / Subnet	Source or Destination <input type="text"/> / <input type="text" value="255.255.255.255 (/32)"/>
Port	Source or Destination <input type="text"/>
Protocol / Service	<input type="text" value="SSL"/>
Interface	<input type="checkbox"/> 1 WAN1 <input type="checkbox"/> 2 WAN2 <input type="checkbox"/> 3 WAN3 <input type="checkbox"/> Mobile Internet <input type="checkbox"/> VPN

Search

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
TCP	10.9.2.18:63700	74.125.71.17:443	HTTPS/SSL	Core	00:00:01
TCP	10.9.60.11:52204	74.125.71.138:443	HTTPS/SSL	Core	00:00:01
TCP	10.9.166.11:55879	74.125.71.102:443	HTTPS/SSL	Core	00:00:01
TCP	10.9.222.223:53474	74.125.71.102:443	HTTPS/SSL	Core	00:00:03
TCP	10.9.66.67:51211	63.150.131.43:443	HTTPS/SSL	Core	00:00:04
TCP	10.9.99.99:4715	74.125.71.18:443	HTTPS/SSL	Core	00:00:04
TCP	10.9.2.26:53786	74.125.71.17:443	HTTPS/SSL	Core	00:00:05
TCP	10.9.98.144:56428	74.125.71.106:443	HTTPS/SSL	Core	00:00:05
TCP	10.9.98.144:56435	74.125.71.84:443	HTTPS/SSL	Core	00:00:05
TCP	10.9.2.26:53780	74.125.71.139:443	HTTPS/SSL	Core	00:00:06
TCP	10.9.19.9:50903	74.125.71.113:443	HTTPS/SSL	Core	00:00:06
TCP	10.9.66.67:51118	74.125.71.19:443	HTTPS/SSL	Core	00:00:06
TCP	10.9.19.9:54822	74.125.71.19:443	HTTPS/SSL	Core	00:00:07
TCP	10.9.60.11:37178	184.31.32.225:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.60.11:37179	184.31.32.225:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.60.11:37181	184.31.32.225:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.66.67:51114	74.125.71.101:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.66.67:51207	74.125.71.101:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.2.18:63779	74.125.71.101:443	HTTPS/SSL	Core	00:00:10
TCP	10.9.99.99:4714	74.125.71.113:443	HTTPS/SSL	Core	00:00:11
TCP	10.9.60.11:40078	74.125.71.18:443	HTTPS/SSL	Core	00:00:12
TCP	10.9.66.66:52642	74.125.71.19:443	HTTPS/SSL	Core	00:00:12
TCP	10.9.166.11:50436	74.125.71.125:443	HTTPS/SSL	Core	00:00:13
TCP	10.9.2.26:53800	74.125.71.139:443	HTTPS/SSL	Core	00:00:14
TCP	10.9.98.144:56172	74.125.71.101:443	HTTPS/SSL	Core	00:00:14

Total searched results: 64 [Show All](#) | [Next >](#)

Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					


This Active Sessions section displays the active inbound / outbound and UDP / TCP sessions of each WAN connection on the Pepwave MAX.

A filter is available to help sort out the active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering.

User Manual


PEPWAVE *MAX* mobile router









22.3 Client List

The client list table is located at **Status > Client List**. It lists DHCP client IP addresses, their Names (retrieved from DHCP reservation table or defined by users), current **Download and Upload rate** and MAC addresses that the Pepwave MAX has offered IP addresses to since it is powered up. Network Name (SSID) and Signal refers to the information about Wi-Fi AP, which is the name of the Network and its signal strength. Clients can be imported into DHCP Reservation table by clicking the  button on the right-most column. Further update the record after the import by going to **Network > LAN**.

If PPTP Server in section 19.2 is enabled, you may see the corresponding connection name would be listed in the field of **Name**.

Filter Online Clients Only DHCP Clients Only

Client List 

IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal	Import
 192.168.50.1		0	0				
 192.168.1.6		65	13	08:00:22:11:DC:0D	Wi-Fi	 -69dBm	
 192.168.1.9		0	0	01:00:22:CC:CC:01			
 192.168.1.10		0	0	08:00:22:DD:CC:DD			
 192.168.1.15	<input type="text" value="desktop"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>	0	0	00:22:44:11:11:44			

Scale: kbps Mbps

User Manual

PEPWAVE *MAX* mobile router

22.4 WINS Client

The WINS client list table is located at **Status >WINS Client**. It lists WINS client IP addresses and their Names. This option will only be available when you have enabled the WINS Server in section 8.1.

Name of clients retrieved will be automatically matched into Client List in the previous section.

Click the button **Flush All** to flush all WINS client records.

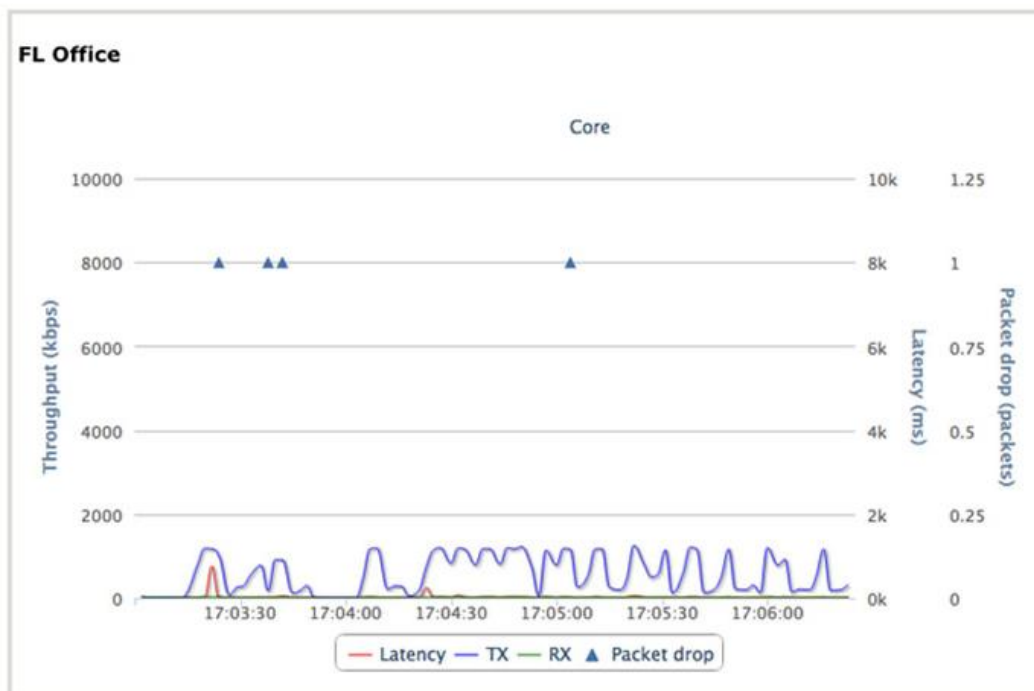
WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4

22.5 SpeedFusion™

This is a page showing the current status of SpeedFusion™, located at: **Status >SpeedFusion™**

Details about peer's WAN connections are listed as below.

SpeedFusion™					
Profile	Remote Networks				
FL Office	10.8.0.0/16 192.168.3.0/24				
WAN 2	Rx: 0 kbps	Tx: 1 kbps	Drop rate: 0.00/s	Latency: 3ms	
Wi-Fi WAN	Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a	
Cellular 1	Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a	
USB	Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a	
Total	Rx: 0 kbps	Tx: 1 kbps	Drop rate: 0.00/s		









User Manual


PEPWAVE *MAX* mobile router

22.6 UPnP / NAT-PMP


The table that shows the forwarded ports under UPnP and NAT-PMP protocols is located at **Status > UPnP / NAT-PMP**:

This section appears only if you have enabled the function of UPnP / NAT-PMP as mentioned in Section 15.1.1

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

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

Important Note

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

User Manual

PEPWAVE *MAX* mobile router

22.7 Event Log

Event Log information is located at **Status>Event Log**:

Overview Search

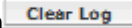
Session data captured within one minute. [Refresh](#)

Service	Inbound Sessions	Outbound Sessions
AIM/ICQ	0	1
Bittorrent	0	32
DNS	0	51
Flash	0	1
HTTPS	0	76
Jabber	0	5
MSN	0	11
NTP	0	4
QQ	0	1
Remote Desktop	0	3
SSH	0	12
SSL	0	64
XMPP	0	4
Yahoo	0	1

Interface	Inbound Sessions	Outbound Sessions
WAN 1	0	176
WAN 2	0	32
Wi-Fi WAN	0	51
Cellular 1	0	64
Cellular 2	0	0
USB	0	0

Top Clients

Client IP Address	Total Sessions
10.9.66.66	1069
10.9.98.144	147
10.9.2.18	63
10.9.66.14	56
10.9.2.26	33

The log section displays a list of events that has taken place on the Pepwave MAX unit. Click the Auto **Refresh** to retrieve log entries again. Click the **Clear Log** button  to clear the log.

User Manual

PEPWAVE *MAX* mobile router

22.8 Bandwidth

This section shows the bandwidth usage statistics, located at: **Status > Bandwidth**

Bandwidth usage at the LAN and when the device is switched off, bandwidth usage is not recorded and not shown.

22.8.1 Real-Time

The **Data transferred since installation** shows you how many network traffic has been processed by your device since first boot.

Click **Show Details** in the top right hand corner of each table and the details of data transferred will be shown.

The check box **Stacked** below the data transferred graph can be checked to show the aggregated transferred rate of both traffic directions.

Data transferred since installation (Tue Oct 12 23:11:14 PST 2010)

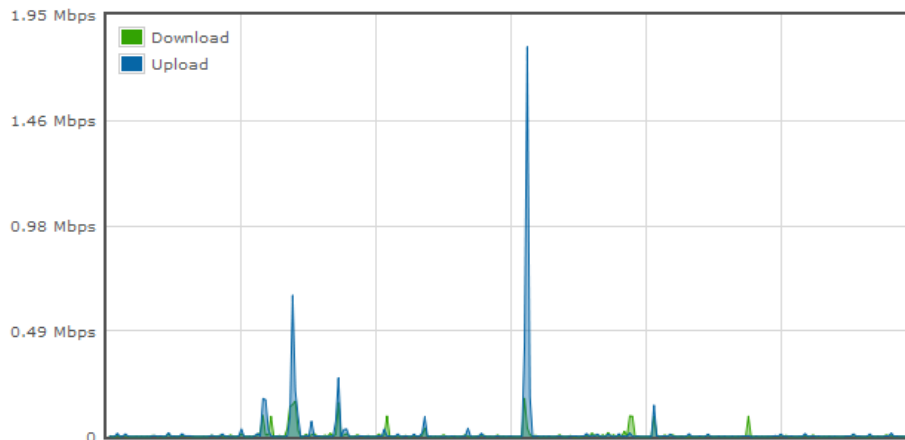
	Download	Upload	Total
All WAN Connections	10.63 GB	12.99 GB	23.62 GB

Data transferred since last reboot

[\[Hide Details \]](#)

	Download	Upload	Total
All WAN Connections	224 MB	178 MB	402 MB
Ethernet WAN	212 MB	175 MB	387 MB
Express Card	0 MB	0 MB	0 MB
PC Card	0 MB	0 MB	0 MB
USB1	0 MB	0 MB	0 MB
USB2	0 MB	0 MB	0 MB
Wi-Fi WAN	12 MB	3 MB	15 MB

Aggregated Transfer



Avg: ↓ 0.01 Mbps ↑ 0.02 Mbps Peak: ↓ 0.18 Mbps ↑ 1.80 Mbps

Stacked

	Download	Upload	Total
Overall	4 kbps	5 kbps	9 kbps

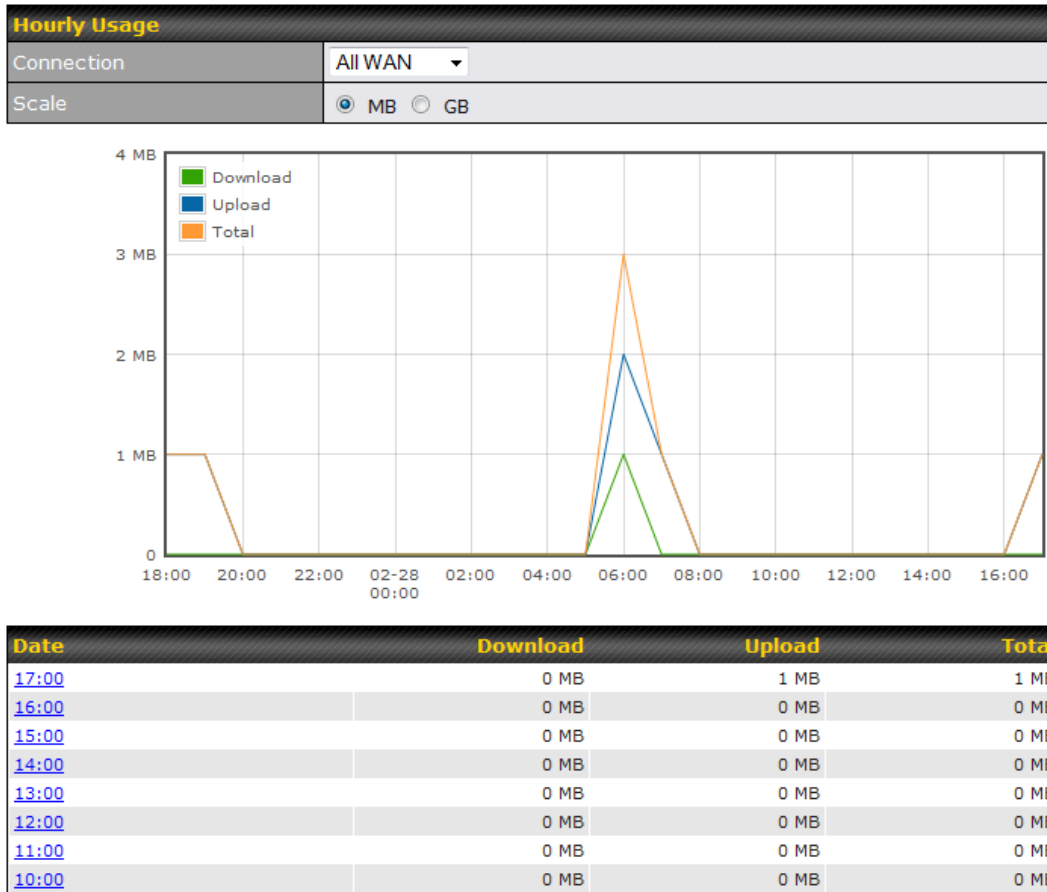
User Manual

PEPWAVE *MAX* mobile router

22.8.2 Hourly

This page shows the daily bandwidth usage for all and each WAN connection.

Select the connection in which you want to check its usage from the drop down menu



22.8.3 Daily

This page shows the daily bandwidth usage for all and each WAN connection.

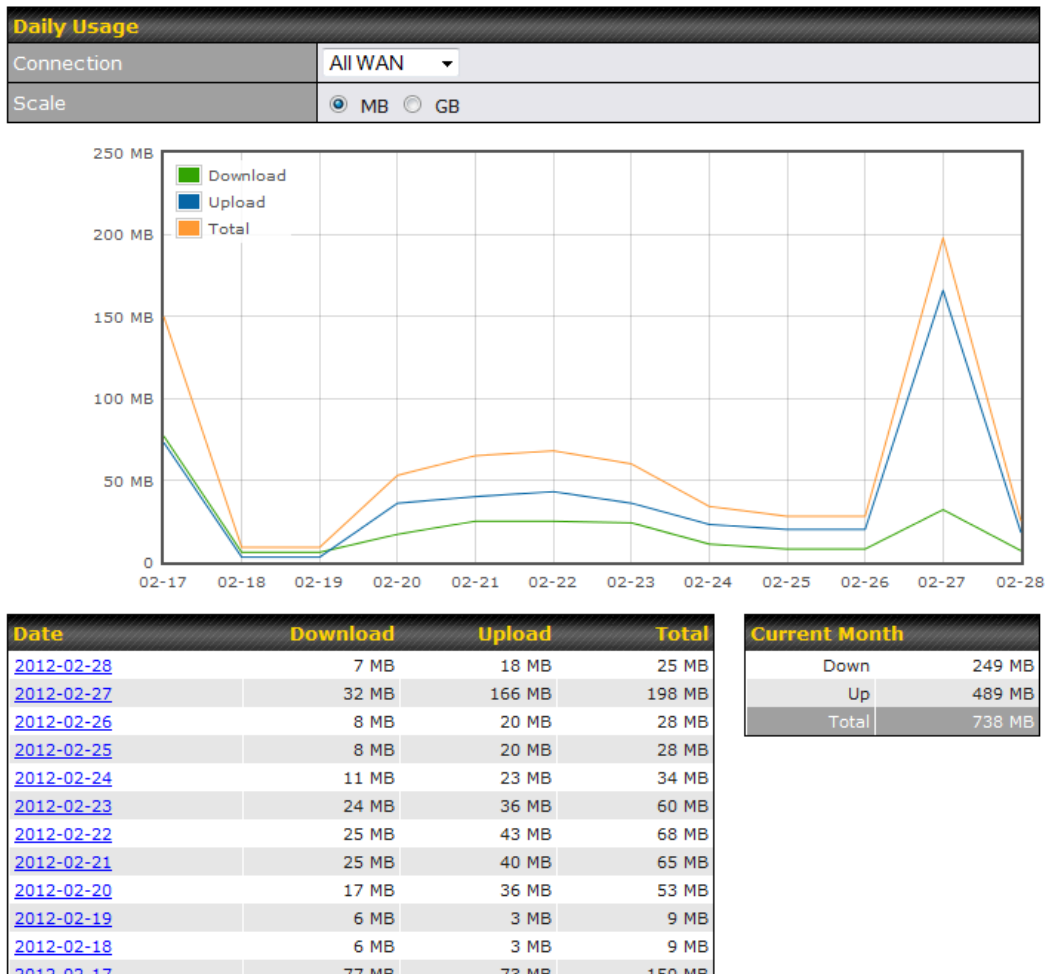
Select the connection in which you want to check its usage from the drop down menu. If you have enabled **Bandwidth Monitoring** feature as shown in section 9.5, the **Current Billing Cycle** table for that WAN connection will be displayed.

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

The Scale of the graph can be set to show in **Megabyte (MB)** or **Gigabyte (GB)**.

User Manual

PEPWAVE *MAX* mobile router



All WAN Daily Bandwidth Usage

22.8.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection.

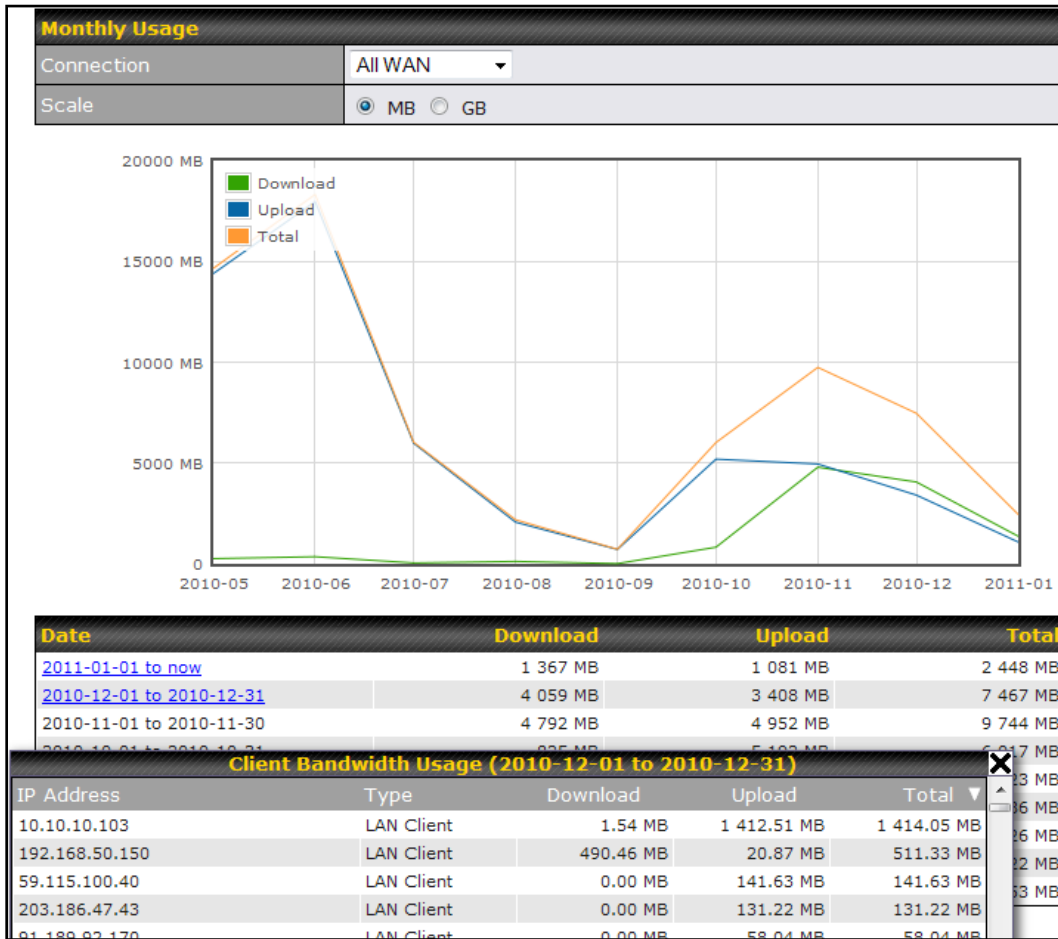
If you have enabled **Bandwidth Monitoring** feature as shown in section 9.5, you can choose a particular connection to check its usage and select to show the monthly usage period in **Billing Cycle** or **Calendar Month**.

Click the first or second row to view the client bandwidth usage of the current month. This feature is not available if you have chosen to view the bandwidth usage of only a particular WAN connection.

The Scale of the graph can be set to show in **Megabyte (MB)** or **Gigabyte (GB)**.

User Manual

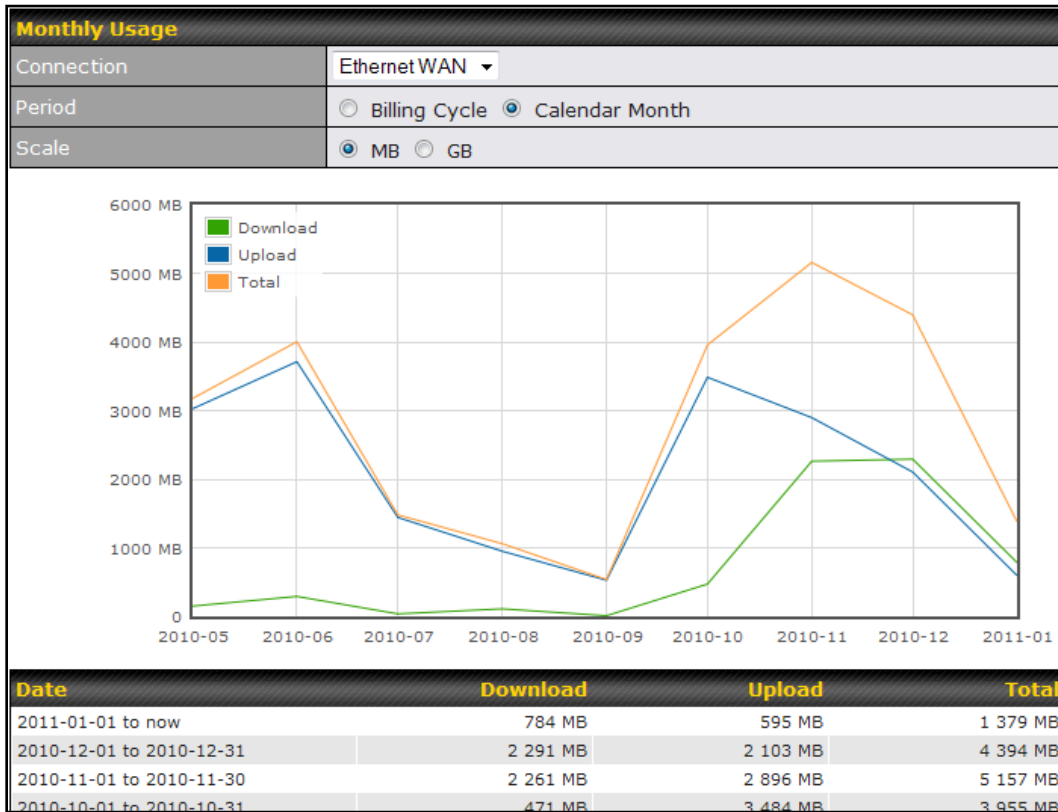
PEPWAVE *MAX* mobile router



All WAN Monthly Bandwidth Usage

User Manual

PEPWAVE *MAX* mobile router



Ethernet WAN Monthly Bandwidth Usage

Tip

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

Appendix A. Restoration of Factory Defaults

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

1. Locate the reset button on the front panel of Pepwave MAX unit.
2. With a paper clip, press the reset button and hold it for at least 10 seconds until the unit reboots itself.

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

Important Note

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

Appendix B. Declaration

1. **The device supports time division technology**
2. **Federal Communication Commission Interference Statement**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help. FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

IMPORTANT NOTE

FCC Radiation Exposure Statement (for MAX700/ HD2/ HD2 IP67/ BR1)

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

FCC Radiation Exposure Statement (for MAX On-The-Go)

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

1. 20cm minimum when the product is operated alone without co-transmitting with a plug-in 3G USB dongle device.
2. 65cm minimum when the product is operated with a plug-in 3G USB device which has maximum of 7W ERP output power.
3. For co-transmission scenario which is not covered above, please consult the RF technician or device supplier.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

User Manual

PEPWAVE *MAX* mobile router

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination.

3. CE Statement for MAX BR1

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1: 2006 + A11 : 2009+A1 : 2010+ A12: 2011
Safety of Information Technology Equipment
- EN50385 : 2002 / Article 3(1)(a)
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1: 2006
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 908-1 V5.2.1: 2011
Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third-Generation cellular networks; Part 1: Harmonized EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive
- EN 301 511 V9.0.2: 2003
Global System for Mobile communications (GSM); Harmonized standard for mobile stations in the GSM 900 and DCS 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC)
- EN 301 489-1 V1.9.2: 2008
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-7 V1.3.1: 2005
ElectroMagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment ad services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
- EN 301 489-17 V2.2.1: 2012
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment
- EN 301 489-24 V1.5.1: 2010
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA) for Mobile and portable (UE) radio and ancillary equipment

User Manual

PEPWAVE *MAX* mobile router



[cs] Česky [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
[da] Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[de] Deutsch [German]	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
[et] Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
[en] English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[es] Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[el] Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
[fr] Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
[it] Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoja, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[nl] Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
[mt] Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ftigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[hu] Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
[pl] Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[pt] Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
[sl] Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
[fi] Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[sv] Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

PEP WAVE

Broadband Possibilities

www.pepwave.com



What are we doing at the moment?
Follow us on [Twitter!](https://twitter.com/Peplink)
<http://twitter.com/Peplink>



Want to know more about us?
Add us on [Facebook!](https://www.facebook.com/peplink)
<http://www.facebook.com/peplink>



Difficulties when configuring the device?
Visit Our [YouTube Channel!](http://www.youtube.com/PeplinkChannel)
<http://www.youtube.com/PeplinkChannel>

Contact Us:

Sales

<http://www.pepwave.com/contact/sales/>

Support

<http://www.pepwave.com/contact/>

Business Development and Partnerships

<http://www.pepwave.com/partners/channel-partner-program/>

Address:

United States Office

800 West El Camino Real,
Mountain View
CA 94040
United States
Tel: +1 (650) 450 9669
Fax: +1 (866) 625 4664

Hong Kong Office

A5, 5/F, HK Spinners
Industrial Building, Phase 6,
481 Castle Peak Road,
Cheung Sha Wan,
Hong Kong
Tel: +852 2990 7600
Fax: +852 3007 0588