

PEP WAVE

Broadband Possibilities

User Manual







Pepwave MAX Mobile Router

Document Rev. 1.0
August 09

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. Copyright © 2009 Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Pepwave Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

1	INTRODUCTION AND SCOPE	4
2	GLOSSARY	5
3	PRODUCT FEATURES	6
	3.1 SUPPORTED NETWORK FEATURES	6
	3.2 OTHER SUPPORTED FEATURES	6
4	PACKAGE CONTENT	8
5	PEPWAVE MAX MOBILE ROUTER OVERVIEW	9
	5.1 FRONT PANEL APPEARANCE	9
	5.2 LED INDICATORS	9
	5.3 REAR PANEL APPEARANCE	10
	5.4 UNIT BASE APPEARANCE	10
6	INSTALLATION	11
	6.1 CONNECTING THE NETWORK WITH PEPWAVE MAX MOBILE ROUTER	11
7	CONNECTING TO WEB ADMIN INTERFACE	13
7	CONNECTING TO WEB ADMIN INTERFACE	13
8	CONFIGURATION OF LAN INTERFACE(S)	15
	8.1 BASIC SETTINGS	15
	8.2 WI-FI AP	18
9	CONFIGURATION OF WAN INTERFACE(S)	20
	9.1  ETHERNET WAN	20
	9.2  EXPRESS CARD /  PC CARD /  USB1 /  USB2	28
	9.3  WI-FI WAN	31
	9.4 WAN HEALTH CHECK	34
	9.5 BANDWIDTH ALLOWANCE MONITOR	36
10	WI-FI SETTINGS	37
	10.1 STP (SPANNING TREE PROTOCOL)	40
11	SITE-TO-SITE VPN	41
	11.1 CONFIGURATION OF SITE-TO-SITE VPN	42
	11.2 PEPWAVE MAX BEHIND NAT ROUTER	44
	11.3 VPN STATUS	44
12	OUTBOUND POLICY	45
	12.1 CUSTOM RULES FOR OUTBOUND TRAFFIC MANAGEMENT	46
13	SERVICE FORWARDING	52
	13.1 SMTP FORWARDING	52
	13.2 WEB PROXY FORWARDING	53
	13.3 DNS FORWARDING	53
14	PORT FORWARDING	54
	14.1 PORT FORWARDING SERVICE	54
	14.2 UPNP / NAT-PMP SETTINGS	57
15	NAT MAPPINGS	58

16	FIREWALL.....	60
	16.1 OUTBOUND AND INBOUND FIREWALL	60
	16.2 INTRUSION DETECTION AND DoS PREVENTION	64
17	TRAFFIC PRIORITIZATION.....	65
18	PPTP SERVER.....	67
19	SERVICE PASSTHROUGH	68
20	SYSTEM SETTINGS	70
	20.1 ADMIN SECURITY	70
	20.2 FIRMWARE UPGRADE.....	73
	20.3 TIME	74
	20.4 EMAIL NOTIFICATION	75
	20.5 REMOTE SYSLOG	77
	20.6 SNMP.....	78
	20.7 SAVING AND LOADING CONFIGURATIONS	80
	20.8 FLASH MANAGEMENT.....	81
	20.9 REBOOT.....	82
	20.10 PING TEST	83
	20.11 TRACEROUTE TEST.....	84
21	STATUS 85	
	21.1 DEVICE.....	85
	21.2 ACTIVE SESSIONS.....	86
	21.3 CLIENT LIST.....	87
	21.4 SITE-TO-SITE VPN	87
	21.5 UPNP / NAT-PMP	88
	21.6 EVENT LOG	89
	21.7 BANDWIDTH	90
APPENDIX A.	RESTORATION OF FACTORY DEFAULTS.....	94
APPENDIX B.	PRODUCT SPECIFICATIONS	95
	B.1 PEPWAVE MAX MOBILE ROUTER	95

1 Introduction and Scope

The Pepwave MAX Mobile Router provides link aggregation and load balancing across six WAN connections, allowing a combination of technologies like 3G HSDPA, EVDO, Wi-Fi, WiMAX, and Satellite to be utilized to connect to the Internet.

This manual presents how to set up the Pepwave MAX Mobile Router and provides an introduction to the features and usage of Pepwave MAX Mobile Router.

2 Glossary

The following terms, acronyms, and abbreviations are frequently used in this manual:

Term	Definition
3G	3 rd Generation family of standards for wireless communications
DHCP	Dynamic Host Configuration Protocol
WINS	Windows Internet Name Service
DNS	Domain Name System
EVDO	Evolution-Data Optimized
HSDPA	High-Speed Downlink Packet Access
HTTP	Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC Address	Media Access Control Address
MTU	Maximum Transmission Unit
MSS	Maximum Segment Size
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
Wi-Fi	Trademark of Wi-Fi Alliance for certified products based on IEEE 802.11 standards
WiMAX	Worldwide Interoperability for Microwave Access

3 Product Features

The following is the list of supported features on Pepwave MAX Mobile Router:

3.1 Supported Network Features

3.1.1 WAN

- Ethernet WAN 10/100 Mbps Connection in Full/Half Duplex
- USB WAN connections
- PC Card WAN connection
- Express Card WAN connection
- Wi-Fi WAN connection
- Network Address Translation (NAT)
- Inbound and Outbound NAT mapping
- IPsec NAT-T and PPTP packet passthrough
- MAC address clone
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS (Supported service providers: changeip.com, dyndns.org, no-ip.org and tzo.com)

3.1.2 LAN

- Wi-Fi AP
- Ethernet LAN ports
- DHCP server on LAN
- Static routing rules

3.1.3 Site-to-Site VPN

- Secure Site-to-Site VPN
- VPN load balancing and failover among selected WAN connections

3.1.4 Firewall

- Outbound (LAN to WAN) firewall rules
- Inbound (WAN to LAN) firewall rules per WAN connection
- Intrusion detection and prevention
- Specification of NAT mappings

3.1.5 Outbound Policy

- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
- Traffic Prioritization and DSL optimization

3.2 Other Supported Features

- User-friendly web-based administration interface
- HTTP and HTTPS support for Web Admin Interface
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, Ping, and Traceroute via Web Admin

Interface

- Remote web based configuration (via WAN and LAN interfaces)
- Quality of Service for Voice over IP and Secure Web
- Time server synchronization
- SNMP
- Email notification
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Event Log
- Active Sessions
- Client List
- UPnP / NAT-PMP

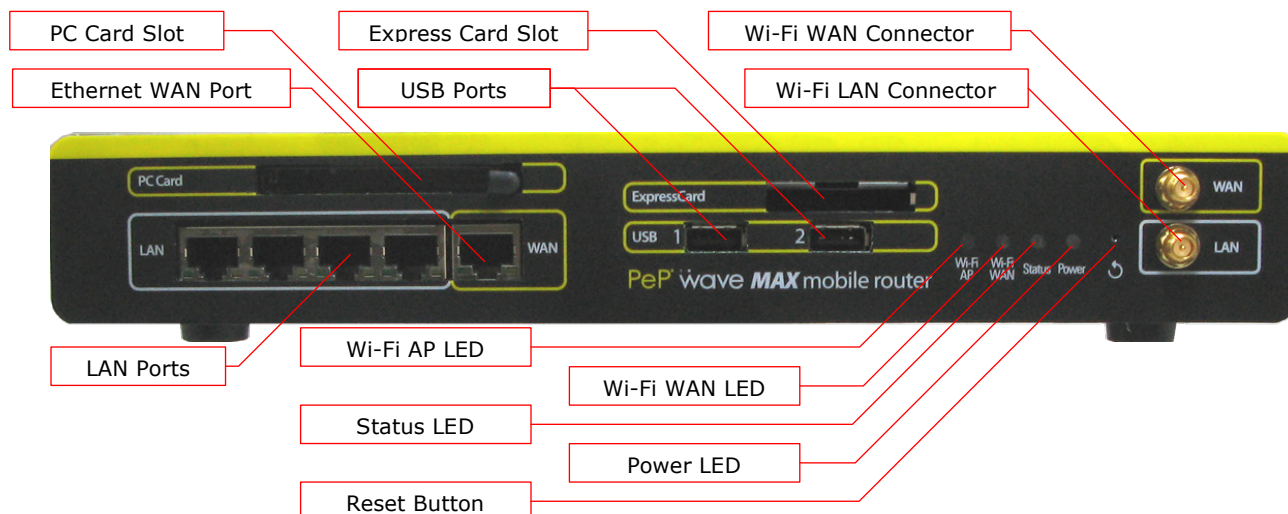
4 Package Content

The Pepwave MAX Mobile Router package includes the following:

- Pepwave MAX Mobile Router unit
- Power adapter
- 2 x Wi-Fi antenna
- Information slip
- Rack mount kit

5 Pepwave MAX Mobile Router Overview

5.1 Front Panel Appearance



5.2 LED Indicators

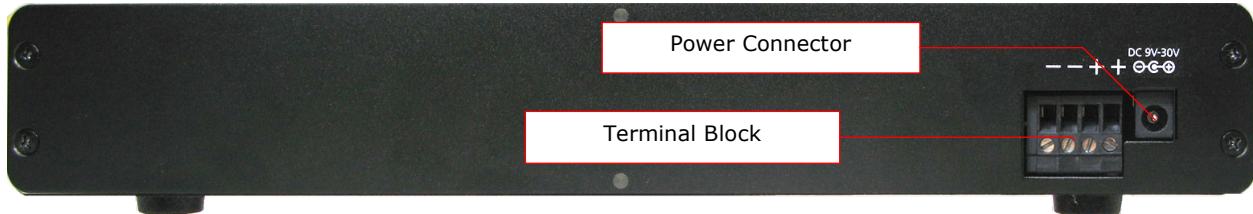
The statuses indicated by the Front Panel LEDs are as follows:

Power and Status Indicators	
Power	OFF – Power off Green – Power on
Status	OFF – System initializing Red – Booting up or busy Green – Ready state

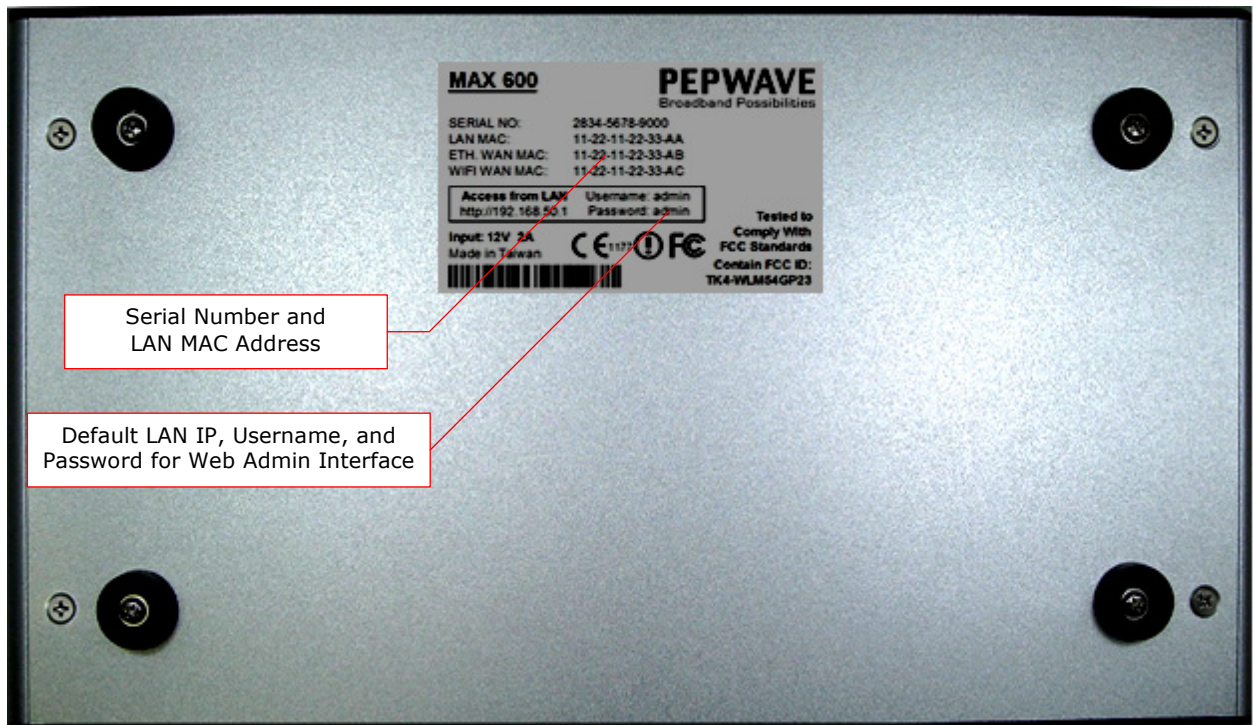
Wi-Fi AP and Wi-Fi WAN Indicators	
Wi-Fi WAN	OFF – Disabled Intermittent Blinking – Trying to connect but not connected to any wireless network ON – Connected to wireless network(s) without traffic Continuous Blinking – Transferring data
Wi-Fi AP	OFF – Disabled Intermittent Blinking – Enabled but no client associated ON – Client(s) associated to wireless network Continuous Blinking – Transferring data to wireless network

LAN and Ethernet WAN Ports	
Green LED	ON – 100 Mbps OFF – 10 Mbps
Yellow LED	Solid – Port is connected without traffic Blinking – Data is transferring OFF – Port is not connected
Note:	They are auto MDI/MDI-X ports

5.3 Rear Panel Appearance



5.4 Unit Base Appearance



6 Installation

6.1 Connecting the Network with Pepwave MAX Mobile Router

6.1.1 Preparation

Before installing Pepwave MAX Mobile Router, please prepare the following:

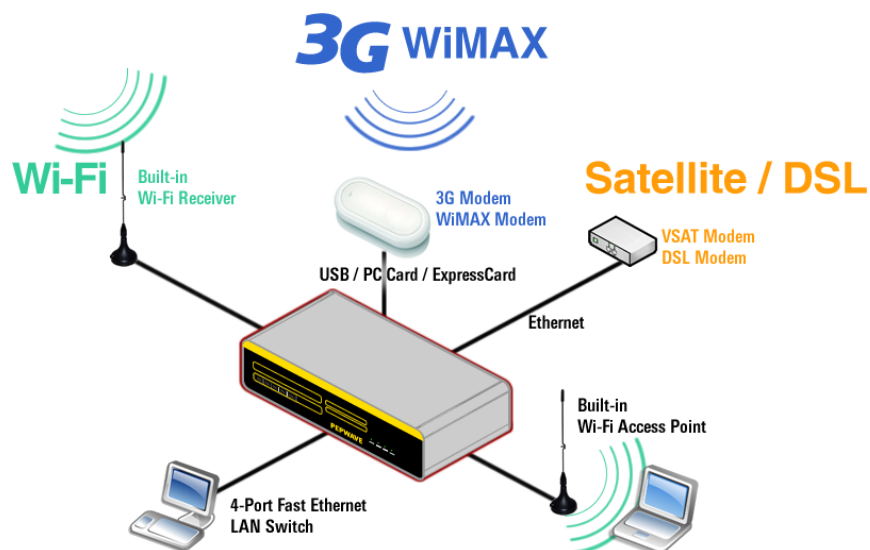
- At least one Internet/WAN access account and/or Wi-Fi access information.
- For each network connection,
 - **Ethernet WAN:** A 10/100BaseT UTP cable with RJ45 connector
 - **USB:** A USB modem
 - **Wi-Fi WAN:** A Wi-Fi antenna
 - **PC Card / Express Card WAN:** A PC Card/Express Card for the corresponding card slot.
- A computer with TCP/IP network protocol and a web browser installed. Supported browsers include Microsoft Internet Explorer 6.0 or above, Mozilla Firefox 2.0 or above, Apple Safari 3.1.1 or above, and Google Chrome 2.0 or above.

6.1.2 Constructing the Network

At the high level, construct the network according to the following steps:

1. With an Ethernet cable, connect a computer to one of the LAN ports on the Pepwave MAX. Repeat with different cables for up to 4 computers to be connected.
2. With another Ethernet cable or a USB modem / Wi-Fi antenna / PC Card / Express Card, connect it to one of the WAN ports on the Pepwave MAX. Repeat the same procedure for other WAN ports.
3. Connect the power adapter to the power connector on the rear panel of Pepwave MAX, and then plug it into a power outlet.

The following figure schematically illustrates the configuration that results:



6.1.3 Configuring the Network Environment

To ensure that Pepwave MAX works properly in the LAN environment and can access the Internet via the WAN connections, please refer to the following setup procedures:

- PC Configuration on the LAN
Section 6.2, **Configuring Computers on the LAN**
- LAN Configuration
For basic configuration, refer to Section 7, **Connecting to Web Admin Interface**.
For advanced configuration, go to Section 8, **Configuration of LAN Interface(s)**.
- WAN Configuration
For basic configuration, refer to Section 7, **Connecting to Web Admin Interface**.
For advanced configuration, go to Section 9, **Configuration of WAN Interface(s)**.

7 Connecting to Web Admin Interface

1. Start a web browser on a computer that is connected with Pepwave MAX through LAN.
2. To connect to Web Admin Interface of Pepwave MAX, enter the following LAN IP address in the address field of the web browser:

`http://192.168.50.1`

(This is the default LAN IP address of Pepwave MAX.)

3. When prompted for **User Name** and **Password** to access the Web Admin Interface, enter the following to proceed.

User Name: admin

Password: admin

(This is the default Username and Password of Pepwave MAX. The Password can be changed in the page **System > Admin Security** of the Web Admin Interface.)

4. After successful login, the **Dashboard** of Web Admin Interface will be displayed. It looks similar to the following:

The screenshot displays the Pepwave MAX Web Administration Interface. The top navigation bar includes the 'PEPWAVE' logo and tabs for 'Dashboard', 'Network', 'Advanced', 'System', and 'Status'. An 'Apply Changes' button is located on the right. The left sidebar identifies the interface as 'Pepwave MAX Web Administration Interface'. The main content area is divided into several sections:

- WAN Connection Status:** Shows connection details for Priority 1 (Ethernet WAN1, Connected), Priority 2 (USB WAN, Standby; Wi-Fi Network, Standby), Priority 3 (Drag desired connections here), and Disabled (Express Card, Disabled).
- LAN Interface:** Displays the Router IP Address as 192.168.50.1.
- Wi-Fi AP:** Shows the status as ON, with options for PEPWAVE and Hotspot 2.
- Device Information:** Lists Model: Pepwave MAX 600, Firmware: v4.8.1, and Uptime: 0 day 1 hour 0 minute.

Copyright © Pepwave. All rights reserved.

Dashboard shows the current WAN, LAN, Wi-Fi AP settings and statuses. You can simply change priority of WAN connections and switch on / off Wi-Fi AP in here. For further information about how-to set up these connections, please refer to Section 8 and 9.

Device Information shows the details about the device, including Model name, Firmware version and Uptime. For further information related, please refer to Section 21.

Important Note

Configuration changes (e.g. WAN, LAN, Admin settings, etc.) will only take effect after clicking the **Save** button at the bottom of each page. The **Save** button causes the changes to be saved and applied.

8 Configuration of LAN Interface(s)

8.1 Basic Settings

The LAN Interface settings are located in **Network > LAN > Basic Settings**:

IP Settings	
IP Address *	<input type="text" value="192.168.50.1"/>
Subnet Mask *	<input type="text" value="255.255.255.0"/>
Speed	<input type="text" value="Auto"/>

DHCP Server Settings							
DHCP Server	<input checked="" type="checkbox"/> Enable						
IP Range	<input type="text" value="192.168.50.10"/> - <input type="text" value="192.168.50.200"/>						
Subnet Mask	<input type="text" value="255.255.255.0"/>						
Lease Time	<input type="text" value="1"/> Days <input type="text" value="0"/> Hours <input type="text" value="0"/> Mins <input type="text" value="0"/> Seconds						
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically						
WINS Servers	<input checked="" type="checkbox"/> Assign WINS server WINS server 1: <input type="text"/> WINS server 2: <input type="text"/>						
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>	Option	Value	No Extended DHCP Option		<input type="button" value="Add"/>	
Option	Value						
No Extended DHCP Option							
<input type="button" value="Add"/>							
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	Name	MAC Address	Static IP			
Name	MAC Address	Static IP					



Static Route Settings							
Static Route	<table border="1"> <thead> <tr> <th>Destination Network</th> <th>Subnet Mask</th> <th>Gateway</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	Destination Network	Subnet Mask	Gateway			
Destination Network	Subnet Mask	Gateway					



DNS Proxy Settings					
DNS Caching	<input type="checkbox"/> Enable				
Local DNS Records	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Host Name	IP Address		
Host Name	IP Address				



* Required

IP Settings	
IP Address & Subnet Mask	The IP address of Pepwave MAX on LAN.
Speed	<p>This setting specifies the speed of the LAN Ethernet Port.</p> <p>By default, Auto is selected and the appropriate data speed is automatically detected by Pepwave MAX.</p> <p>In the event of negotiation issues, the port speed can be manually specified to circumvent the issues. You can also choose whether or not to advertise the speed to the peer by selecting the Advertise Speed checkbox.</p>

DHCP Server Settings	
DHCP Server	<p>When this setting is enabled, the DHCP server of Pepwave MAX automatically assigns an IP address to each computer that is connected via LAN and is configured to obtain an IP address via DHCP.</p> <p>Pepwave MAX's DHCP server can prevent IP address collision on LAN.</p>
IP Range & Subnet Mask	This setting allocates a range of IP address that will be assigned to LAN computers by the DHCP server of Pepwave MAX.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the Lease Time, the assigned IP address will no longer be valid and the renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to the DHCP clients. If Assign DNS server automatically is selected, the Pepwave MAX's built-in DNS server address (i.e. LAN IP address) will be offered.
WINS Server	This option allows you to input the WINS server addresses to be offered to the WINS clients. If Assign WINS server is selected, you can enter the WINS server addresses manually.
Extended DHCP Option	<p>In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional Extended DHCP Options defined in RFC 2132. In this case, you can pass additional configuration information to LAN hosts.</p> <p>To define an Extended DHCP Option, click the Add button, choose the option that you want to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option is allowed to be defined once only.</p>

DHCP Reservation	<p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses.</p> <p>The fixed IP address assignment is displayed as a cross-reference list between the computers' Name, MAC addresses and fixed IP addresses.</p> <p>The field Name (an optional field) is for you to define a name to represent the device. MAC addresses should be in the format of 00:AA:BB:CC:DD:EE</p> <p>Press  to create a new record. Press  to remove a record.</p>
---------------------	--

Static Route Settings	
Static Route	<p>This table is for defining static routing rules for the LAN segment.</p> <p>A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in the format of w.x.y.z</p> <p>Press  to create a new route. Press  to remove a route.</p>

DNS Proxy Settings	
DNS Caching	<p>This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can help improve the DNS lookup time. However, it cannot return the most updated result for those frequently updated DNS records.</p> <p>By default, it is disabled.</p>
Local DNS Records	<p>This table is for defining custom local DNS records.</p> <p>A static local DNS record consists of a Host Name and an IP Address. When looking up the Host Name from the LAN to LAN IP of Pepwave MAX, the corresponding IP Address will be returned.</p> <p>Press  to create a new record. Press  to remove a record.</p>

8.2 Wi-Fi AP

The Wi-Fi LAN settings can be configured in **Network > LAN > Wi-Fi AP**:

Wireless Network Settings	
Network Name (SSID)	<input type="text" value="PEPWAVE"/>
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Broadcast SSID	<input checked="" type="checkbox"/> Enable
Multicast Filter	<input type="checkbox"/> Enable
Multicast Rate	1M

Wireless Security Settings	
Security Policy	Open (No Encryption)

Access Control Settings	
Restriction Mode	None

Wireless Network Settings	
Network Name (SSID)	This setting allows you to specify a name to represent the virtual AP to be scanned by Wi-Fi clients.
Enable	When Yes is selected, this virtual AP is enabled. Select No to disable it. By default, it is enabled. You can also choose to enable or disable this virtual AP on the <i>Dashboard - Connection Status of Wi-Fi AP</i> , please refer to section 7 for information.
Broadcast SSID	When the box Enable is checked, this SSID can be scanned by Wi-Fi clients. By default, it is enabled.
Multicast Filter	When the box Enable is checked, multicast network traffic to the wireless SSID will be filtered. By default, it is disabled.
Multicast Rate	This field allows you to specify the transmit rate to be used for sending multicast network traffic. By default, Multicast Rate is set to 1M .

Wireless Security Settings

Security Policy	<p>This setting specifies which security policy will be used for this wireless network.</p> <p>Available options:</p> <ul style="list-style-type: none">• Open (No Encryption)• WPA/WPA2 – Personal• WPA/WPA2 – Enterprise• 802.1X• Static WEP
-----------------	---

Access Control Settings

Restriction Mode	<p>This option allows you to perform access control through MAC address filtering.</p> <p>Available options are None, Deny all except listed, and Accept all except listed.</p>
------------------	--

9 Configuration of WAN Interface(s)

The WAN Interface settings are located at: Network > WAN

To reorder different WANs' priority, just drag on the appropriate WAN by holding the left mouse button, move it to the desired priority (the first one would be the highest priority, the second one would be lower priority, and so on) and drop it by releasing the mouse button.








To disable a particular WAN connection, just drag on the appropriate WAN by holding the left mouse button, move it to the **DISABLED** row and drop it by releasing the mouse button.

You can also do the above priority setting on the **Dashboard**, please refer to Section 7 for information.

Important Note

Connection Details will be changed and become effective right AFTER clicking the **Save and Apply** button.

9.1 Ethernet WAN

WAN Port	
WAN Connection Name	Ethemet WAN1 Default
Connection Method 	DHCP 
IP Address	10.10.10.123
Subnet Mask	255.255.0.0
Default Gateway	10.10.10.1
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 10.9.1.1 <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname
Standby State 	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Upstream Bandwidth 	100 Mbps 
Downstream Bandwidth 	100 Mbps 

Health Check DNS Servers	Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers
Timeout	5 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Recovery Retries	3
Dynamic DNS	Disabled
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st of each month at 00:00 midnight
Monthly Allowance	10 GB
Port Speed	Auto
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: 1440 <input type="button" value="Default"/>
MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>
MAC Address Clone	00 : 1A : 11 : BB : AA : 22 <input type="button" value="Default"/>
Reply to ICMP PING	<input checked="" type="radio"/> Yes <input type="radio"/> No

Ethernet WAN Settings	
WAN Connection Name	This field is for defining a name to represent this WAN connection.
Connection Method	<p>There are three possible connection methods for Ethernet WAN:</p> <ul style="list-style-type: none"> • DHCP • Static IP • PPPoE <p>The connection method and details are determined by, and can be obtained from, the ISP.</p> <p>See the Sections 9.1.1, 9.1.2, and 9.1.3 for details of each connection method.</p>



Ethernet WAN Settings	
Standby State	<p>This setting specifies the state of the WAN connection. The available options are Remain connected and Disconnect.</p> <p>The default state is Remain Connected.</p>
Upstream Bandwidth	<p>This setting specifies the data bandwidth in the outbound direction from the LAN through the WAN interface.</p>
Downstream Bandwidth	<p>This setting specifies the data bandwidth in the inbound direction from the WAN interface to the LAN.</p> <p>This value is referenced as the default weight value when using the custom rule <i>Default (Auto)</i>, the algorithm <i>Least Used</i>, or the algorithm <i>Persistence (Auto)</i> in Outbound Policy with <i>Managed by Custom Rules</i> chosen (see Section 12.1).</p>
Health Check Method	<p>This setting specifies the health check method for the WAN connection. The value of method can be configured as Disabled, Ping or DNS Lookup. The default method is Disabled.</p> <p>See Section 9.4 for configuration details.</p>
Dynamic DNS	<p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> <ul style="list-style-type: none"> • changeip.com • dyndns.org • no-ip.org • tzo.com <p>Select Disabled to disable this feature.</p> <p>See Section 9.1.4 for configuration details.</p>
Bandwidth Allowance Monitor	<p>This option allows you to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.</p> <p>See Section 9.5 for configuration details.</p>
Port Speed	<p>This setting specifies port speed and duplex configurations of the WAN Port.</p> <p>By default, Auto is selected and the appropriate data speed is automatically detected by Pepwave MAX.</p> <p>In the event of negotiation issues, the port speed can be manually specified to circumvent the issues. You can also choose whether or not to advertise the speed to the peer by selecting the Advertise Speed checkbox.</p>

Ethernet WAN Settings

MTU	<p>This setting specifies the Maximum Transmission Unit.</p> <p>By default, MTU is set to Custom 1440.</p> <p>You may adjust the MTU value by editing the text field. Click Default to restore the default MTU value. Select Auto and the appropriate MTU value will be automatically detected. The auto-detection will run each time when the WAN connection establishes.</p>
MSS	<p>This setting should be configured based on the maximum payload size that the local system can handle. The MSS (Maximum Segment Size) is computed from the MTU minus 40 bytes for TCP over IPv4.</p> <p>If MTU is set to Auto, the MSS will also be set automatically.</p> <p>By default, MSS is set to Auto.</p>
MAC Address Clone	<p>This setting allows you to configure the MAC address.</p> <p>Some service providers (e.g. cable providers) identify the client's MAC address and require the client to always use the same MAC address to connect to the network. In such cases, change the WAN interface's MAC address to the original client PC's one via this field.</p> <p>The default MAC Address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking the Default button restores the MAC Address to the default value.</p>
Reply to ICMP PING	<p>If this field is disabled, the WAN connection will not respond to ICMP PING requests.</p> <p>By default, this is enabled.</p>

9.1.1 DHCP Connection




The DHCP connection method is suitable if the ISP provides an IP address automatically by DHCP (e.g. Satellite Modem, WiMAX Modem, Cable, Metro Ethernet, etc.).

Connection Method 	DHCP 
IP Address	123.123.123.10
Subnet Mask	255.255.255.0
Default Gateway	123.123.123.1
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 123.123.123.1 210.210.210.1 <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

DHCP Settings	
IP Address / Subnet Mask / Default Gateway	This information is obtained from the ISP automatically.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) Servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS Servers to be assigned by the WAN DHCP Server to be used for outbound DNS lookups over the connection. (The DNS Servers are obtained along with the WAN IP address assigned from the DHCP server.)</p> <p>When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>
Hostname (Optional)	If your service provider's DHCP server requires you to supply a <i>hostname</i> value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.

9.1.2 Static IP Connection



This Static IP connection method is suitable if ISP provides a static IP address to connect directly.

Connection Method 	Static IP 
IP Address	<input type="text"/>
Subnet Mask	255.255.255.0 
Default Gateway	<input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

Static IP Settings	
IP Address / Subnet Mask / Default Gateway	<p>These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address.</p> <p>The information is typically determined by and can be obtained from the ISP.</p>
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This field specifies the DNS (Domain Name System) Servers to be used when a DNS lookup is routed through this connection.</p> <p>You can input the ISP provided DNS server addresses into the DNS server 1 and DNS server 2 fields. If no address is entered here, this link will not be used for DNS lookups.</p>

9.1.3 PPPoE Connection

This connection method is suitable if ISP provides login ID / password to connect via PPPoE.


Connection Method 	PPPoE 
IP Address	123.123.123.10
Subnet Mask	255.255.255.0
Default Gateway	123.123.123.1
PPPoE User Name	<input type="text"/>
PPPoE Password	<input type="password"/>
Confirm PPPoE Password	<input type="password"/>
Service Name (Optional)	<input type="text"/> Leave it blank unless it's provided by ISP
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 123.123.123.1 210.210.210.1 <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

PPPoE Settings	
IP Address / Subnet Mask / Default Gateway	This information is obtained from the ISP automatically.
PPPoE User Name / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name	Service Name is provided by the ISP. Note: Leave this field blank unless it is provided by your ISP.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) Servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS Servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS Servers are obtained along with the WAN IP address assigned from the PPPoE server.)</p> <p>When Use the following DNS server address(es) is selected, you can put custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>

9.1.4 Dynamic DNS Settings

Pepwave MAX provides the functionality to register the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name.

Either upon a change in IP address or every 23 days without link reconnection, Pepwave MAX will connect to the dynamic DNS service provider to perform an IP address update within the provider's records.

Dynamic DNS	 changeip.com
Account Name	demo
Password	••••••
Confirm Password	••••••
Hosts	

Dynamic DNS Settings	
Dynamic DNS	<p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> <ul style="list-style-type: none"> • changeip.com • dyndns.org • no-ip.org • tzo.com <p>Select Disabled to disable this feature.</p>
Account Name / Email Address	<p>This setting specifies the registered user name for the dynamic DNS service.</p>
Password / TZO Key	<p>This setting specifies the password for the dynamic DNS service.</p>
Hosts / Domain	<p>This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection.</p> <p>If you need to enter more than one host, you can use a carriage return to separate them.</p>

Important Note


In order to use dynamic DNS services, appropriate host name registration(s) as well as

a valid account with a supported dynamic DNS service provider are required.

A dynamic DNS update is performed whenever a WAN's IP address changes. E.g. IP is changed after a DHCP IP refresh, reconnection, etc.

Due to dynamic DNS service providers' policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long time. Therefore Pepwave MAX performs an update every 23 days even if a WAN's IP address has not changed.

9.2 Express Card / PC Card / USB1 / USB2

Express Card / PC Card / USB1 / USB2	
Wireless Adaptor	USB-WAN (Hidden)
SIM Card IMSI	XXXXXXXXXXXX
Carrier	XXXXXXXXXX
Country/Region	United States
Signal Strength	-75 dBm 
IP Address	10.10.10.111
DNS Servers	10.10.10.11 10.10.10.12
WAN Connection Name	USB WAN Default
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	-
Login	-
Password	-
Dial Number	-
SIM PIN (Optional)	•••• <input checked="" type="checkbox"/> Hide Characters
Health Checking Settings	
Method	SmartCheck ▾
Timeout	5 ▾ second(s)
Health Check Interval	5 ▾ second(s)
Health Check Retries	3 ▾
Recovery Retries	3 ▾
Bandwidth Allowance Monitor	<input type="checkbox"/> Enable
Modem Specific Settings	
Network Type	3G preferred ▾
GSM Frequency Band	All Bands ▾

Save and Apply


Cancel


Express Card / PC Card / USB Settings



Express Card / PC Card / USB Settings	
SIM Card IMSI	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. <i>This is applicable to 3G modems only.</i>
Carrier	This field shows the name of the carrier who issues the SIM card (for 3G) or the modem (for EVDO).
Country/Region	This is the country/region of the carrier who issues the EVDO modem.
Signal Strength	This field shows the signal strength of the connection.
IP Address	This information is obtained from the carrier automatically.
DNS Servers	Each carrier may provide a set of DNS servers for DNS lookups. This field specifies the DNS (Domain Name System) Servers are currently effective when a DNS lookup is routed through this connection. This information is obtained from the carrier automatically or can be entered manually by users.
WAN Connection Name	This field is for defining a name to represent this WAN connection.
Operator Settings	This setting applies to 3G / EDGE / GPRS modem only. It does not apply to EVDO / EVDO Rev. A modem. This allows you to configure the APN settings of your connection. If Auto is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically afterwards. If there is any difficulty in making connection, you may select Custom to enter your carrier's APN, Login, Password, and Dial Number settings manually. The correct values can be obtained from your carrier. The default and recommended Operator Settings is Auto .
APN / Login / Password / Dial Number / SIM PIN	When Auto is selected, the information in these fields will be filled automatically. Select the option Custom and you may customize these parameters. The parameters values are determined by and can be obtained from the ISP.
Health Checking Settings	This setting allows you to specify the health check method for the WAN connection. The as available options are Disabled and SmartCheck . The default method is SmartCheck . See Section 9.4 for configuration details.

Express Card / PC Card / USB Settings	
Bandwidth Allowance Monitor	<p>This option allows you to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.</p> <p>See Section 9.5 for configuration details.</p>
Modem Specific Settings	<p>The settings under this category may or may not be available depending on the model of the connected device.</p>
Network Type	<p>This setting allows you to define your preference of using the 3G and/or 2G networks. 3G networks include HSPA / UMTS; 2G networks include EDGE / GPRS.</p> <p>If 3G only or 2G only is chosen, only the HSPA / UMTS or EDGE / GPRS network will be used, respectively. If the chosen network is not available, no other network will be used regardless of its availability. The modem connection will remain offline.</p> <p>If 3G preferred or 2G preferred is chosen, the chosen network will be used when it is available. If the chosen network is not available, the other network will be used whenever available.</p> <p>The default Network Type is 3G preferred.</p>
GSM Frequency Band	<p>This setting allows you to specify which GSM frequency band to be used.</p> <p>GSM1900 is used in United States, Canada, and many other countries in the Americas.</p> <p>GSM900 / GSM1800 / GSM2100 is used in Europe, Middle East, Africa, Asia, Oceania, and Brazil.</p> <p>If All Bands is chosen, the appropriate frequency band will be used automatically.</p> <p>The default GSM Frequency Band is All Bands.</p>

9.3 Wi-Fi WAN

Wi-Fi WAN	
Network Name (SSID)	Wi-Fi Hotspot1 Wireless Networks
MAC Address (BSSID)	06:11:88:DD:BB:FF
Signal Strength	-45 dBm 
IP Address	10.10.10.123
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1
DNS Servers	10.10.10.1 10.10.10.2
WAN Connection Name	Wi-Fi Network Default
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Health Check Method	DNS Lookup
Health Check DNS Servers	Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers
Timeout	5 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Bandwidth Allowance Monitor	<input type="checkbox"/> Enable
Wi-Fi Association Mode	<input type="radio"/> Stronger Signal Strength <input checked="" type="radio"/> Profile Priority
Connect to Any Open Mode AP	<input type="radio"/> Yes <input checked="" type="radio"/> No
Reply to ICMP PING	<input checked="" type="radio"/> Yes <input type="radio"/> No

Wi-Fi Connection Profiles  Drag and drop to change the profile priority ?

Network Name (SSID)	Security	
Wi-Fi Hotspot1	WPA/WPA2-Personal	
Wi-Fi Hotspot2	Open	

[Create Profile...](#)

Wi-Fi WAN Settings	
Network Name (SSID)	This is the Wi-Fi connection name broadcast from the Wi-Fi access point.
MAC Address (BSSID)	This field shows the MAC address of the device at the Wi-Fi access point.

Wi-Fi WAN Settings

Signal Strength	This field shows the signal strength of the Wi-Fi connection.
IP Address / Subnet Mask / Default Gateway / DNS Servers	This information is obtained from the Wi-Fi access point automatically.
WAN Connection Name	This field is for defining a name to represent this WAN connection.
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are Remain Connected (<i>hot standby</i>) and Disconnect (<i>cold standby</i>).
Health Check Method	This setting allows you to specify the health check method for the WAN connection. The available options are Disabled , Ping , and DNS Lookup . The default method is Disabled . See Section 9.4 for configuration details.
Bandwidth Allowance Monitor	This option allows you to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this is not enabled, bandwidth usage of each month is still being tracked but no action will be taken. See Section 9.5 for configuration details.
Wi-Fi Association Mode	This option is to specify the Wi-Fi access point selection criteria during association. When Stronger Signal Strength is selected, the access point that matches one of the listed Wi-Fi Connection Profiles and has the strongest received signal will be selected regardless of its profile priority. When Profile Priority is selected, the access point that matches one of the listed of Wi-Fi Connection Profiles and has the highest priority will be selected. By default, Stronger Signal Strength is selected.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access point it finds. By default, this is disabled.
Reply to ICMP PING	If this field is disabled, the WAN connection will not respond to ICMP PING requests. By default, this is enabled.

9.3.1 Create Wi-Fi Connection Profile

You can manually create a profile to connect to a Wi-Fi connection. It is useful for creating a profile for connecting to hidden-SSID access points. Click on the link **Create Profile...** and the following window will be displayed.

Wi-Fi Connection	
Network Name (SSID)	Wi-Fi Hotspot 1
Security	WEP
Encryption Key <input checked="" type="checkbox"/> Hide Characters
IP Address	<input checked="" type="radio"/> Obtain an IP address automatically <input type="radio"/> Static

Create Wi-Fi Connection Profile Settings	
Network Name (SSID)	This field is for defining a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network. Available options: <ul style="list-style-type: none"> • Open • WEP • WPA/WPA2 – Personal • WPA/WPA2 – Enterprise The settings to be displayed under this row will vary depending on the selected security policy.

9.4 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, Pepwave MAX provides the functionality to periodically check the health of each WAN connection.

Health Check Settings	
Health Check Disabled	
Health Check Method	<div style="border: 1px solid #ccc; padding: 5px;"> Health Check disabled. Network problem cannot be detected. Disabled </div>
<p>When Disabled is chosen in the Method field, the WAN connection will always be considered as <i>up</i>. The connection will not be treated as down in the event of IP routing errors.</p>	
Health Check Method: PING	
Method	Ping
Ping Hosts	<div style="border: 1px solid #ccc; padding: 5px;"> Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Ping Hosts </div>
<p>The ICMP PING packets will be issued to test the connectivity with a configurable target IP address or host name. A WAN connection is considered as <i>up</i> if PING responses are received from either one or both of the PING Hosts.</p>	
PING Hosts	<p>This setting specifies IP addresses or host names with which connectivity is to be tested via ICMP Ping.</p> <p>If Use first two DNS servers as Ping Hosts is checked, the target PING Host will be the first DNS server for the corresponding WAN connection.</p> <p>Reliable PING hosts with a high uptime should be considered.</p> <p>By default, the first two DNS servers of the WAN connection are used as the PING Hosts.</p>
Health Check Method: DNS Lookup	
Method	DNS Lookup
Health Check DNS Servers	<div style="border: 1px solid #ccc; padding: 5px;"> Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers </div>
<p>DNS lookups will be issued to test the connectivity with target DNS servers. The connection will be treated as <i>up</i> if DNS responses are received from either one or both of the servers, regardless of whether the result was positive or negative.</p>	

Health Check Settings

Health Check DNS Servers

This field allows you to specify two DNS hosts' IP address with which connectivity is to be tested via DNS Lookup.

If **Use first two DNS servers as Health Check DNS Servers** is checked, the target DNS hosts will be the first two DNS servers assigned to this WAN connection.

Reliable targets with a high uptime should be considered.





By default, the first two DNS servers of the WAN connection are used as the Health Check DNS Servers.

Health Check Method: SmartCheck

Method		SmartCheck
--------	---	------------

SmartCheck monitors the link status and is optimized for mobile networks with high traffic latency.

Other Health Check Settings

Timeout		5	second(s)
Health Check Interval		5	second(s)
Health Retries		3	
Recovery Retries		3	

Timeout

This setting specifies the timeout, in seconds, for ping/DNS lookup requests. Default Timeout is set to **5** second.

Health Check Interval

This setting specifies the time interval, in seconds, between ping or DNS lookup requests. Default Health Check Interval is **5** seconds.

Health Check Retries

This setting specifies the number of consecutive ping/DNS lookup timeouts after which Pepwave MAX is to treat the corresponding WAN connection as *down*. Default Health Retries is set to **3**.

For example, with the default Health Retries setting of 3, after consecutive 3 timeouts, the corresponding WAN connection will be treated as *down*.



Recovery Retries

This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before Pepwave MAX treats a previously *down* WAN connection to be *up* again.

By default, Recover Times is set to **3**. For example, a WAN connection that is treated as *down* will be considered to be *up* again upon receiving 3 consecutive successful ping/DNS lookup responses.

9.5 Bandwidth Allowance Monitor

Bandwidth Allowance Monitor helps keep track of your network usage.

Bandwidth Allowance Monitor 	<input checked="" type="checkbox"/> Enable
Action 	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On <input type="text" value="1st"/> of each month at 00:00 midnight
Monthly Allowance	<input type="text" value="10"/> <input type="text" value="GB"/>

Bandwidth Allowance Monitor	
Action	<p>If the feature <i>Email Notification</i> is enabled, you will be notified through email when usage hits 75% and 95% of the monthly allowance.</p> <p>If the box Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.</p>
Start Day	This option allows you to define which day in the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

10 Wi-Fi Settings

Wi-Fi settings can be configured at **Advanced > Wi-Fi Settings**:

Wi-Fi AP Radio Settings	
Protocol	802.11b/g
Operating Country	US
Channel	1 (2.412 GHz)
Output Power	23 dBm (200 mW)

Wi-Fi WAN Radio Settings	
Output Power	23 dBm (200 mW)

Wi-Fi AP Advanced Settings	
STP	<input type="checkbox"/> Enable
Layer 2 Communication	<input checked="" type="checkbox"/> Enable
802.1X Version	<input type="radio"/> V1 <input checked="" type="radio"/> V2
Beacon Rate	1Mbps
Beacon Interval	100ms
DTIM	1
RTS Threshold	0
Slot Time	9 μ s
ACK Timeout	48 μ s
CTS Timeout	48 μ s

Save

Wi-Fi AP Radio Settings	
Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are 802.11b/g , 802.11b Only , and 802.11g Only . By default, 802.11b/g is selected.
Operating Country	This option shows the country whose regulations the Pepwave MAX follows.
Channel	This option allows you to select which 802.11 RF channel will be utilized.

Wi-Fi AP Radio Settings	
	Channel 1 (2.412 GHz) is selected by default.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. By default, 23 dBm (200 mW) is selected.




Wi-Fi WAN Radio Settings	
Output Power	This option is for specifying the transmission output power for the Wi-Fi WAN. By default, 23 dBm (200 mW) is selected.

Wi-Fi AP Advanced Settings	
STP	This option allows you to enable the Spanning Tree Protocol to prevent path redundancy. By default, it is disabled. See Section 10.1 for details.
Layer 2 Communication	This option allows you to choose whether clients on the network should be able to communicate with each other directly. If the checkbox Enable is selected, clients are allowed to communicate with each other directly, and traffic will not be passed to any uplink equipment. If this option is disabled, clients are not allowed to communicate directly. Traffic will be passed to uplink equipments/uplink routers before communication can be established among clients. By default, it is enabled.
802.1X Version	This option allows you to select between V1 or V2 of the 802.1X EAPOL. When V1 is selected, both V1 and V2 clients are allowed to associate with this Wi-Fi AP. When V2 is selected, only V2 clients can associate with this Wi-Fi AP. Most wireless clients support V2. Select the option V1 in case if there are stations that do not support V2. By default, V2 is selected.
Beacon Rate	This option is for setting the transmit bit rate for sending a beacon.

Wi-Fi AP Advanced Settings

	By default, 1Mbps is selected.
Beacon Interval	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM	This field allows you to set the frequency for the beacon to include Delivery Traffic Indication Message. The interval is measured in millisecond. The default value is set to 1 ms.
RTS Threshold	This field allows you to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting this field to zero will disable this option. The default value is set to 0 .
Slot Time	This field is for specifying the unit wait time before it transmits a packet. By default, this field is set to 9 μ s.
ACK Timeout	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 μ s.
CTS Timeout	This field is for specifying the timeout interval for the unit to wait for a CTS response in the RTS/CTS handshake. By default, this field is set to 48 μ s.

10.1 STP (Spanning Tree Protocol)

STP		<input checked="" type="checkbox"/> Enable
Bridge Priority		<input type="text" value="32768"/>
Ethernet Path Cost		<input type="text" value="100"/>

STP Settings	
Bridge Priority	<p>This parameter is set to give the likeliness for root switch election.</p> <p>By default, it is set to 32768.</p>
Ethernet Path Cost	<p>This parameter specifies the preference to provide the best path from the switch to the root switch.</p> <p>By default, it is set to 100.</p>

11 Site-to-Site VPN

Pepwave Site-to-Site VPN functionality securely connects your MAX in different branch to another Pepwave MAX or Peplink device (*only Peplink Balance 210/310/380/390/700/710 are available for this function*). The data, voice, or video communications between these locations are kept confidential across the public Internet.

The Site-to-Site VPN of the Pepwave MAX is specifically designed for multi-WAN environment. The Pepwave MAX can aggregate all WAN connections' bandwidth for routing Site-to-Site VPN traffic. Unless all the WAN connections of one site are down, the Pepwave MAX can still maintain VPN up and running.

Tip

You can define firewall rules to control access within the VPN network. For outbound policy, you can create a custom outbound rule and choose **Any** for the **WAN Connection** field.

11.1 Configuration of Site-to-Site VPN

Pepwave MAX supports making single Site-to-Site VPN connection with a remote Pepwave MAX unit or a Peplink Balance 210/310/380/390/700/710.

To configure, navigate to **Advanced > Site-to-Site VPN**:

VPN Settings	
Active	<input checked="" type="checkbox"/>
Peer Serial Number	<input type="text" value="1824-1212-2C2C"/> <input type="checkbox"/> Remote client is set up in high availability mode.
Peer IP Addresses / Host Names (Optional)	<input type="text" value="121.121.121.1"/> <small>If this field is empty, this field on the peer site must be filled</small>

WAN Connection Priority	
1. Ethernet WAN	Priority: 1 (Highest) ▼
2. Express Card	Priority: 1 (Highest) ▼
3. PC Card	Priority: 1 (Highest) ▼
4. USB1	Priority: --- OFF --- ▼
5. USB2	Priority: 1 (Highest) ▼
6. Wi-Fi Hotspot	Priority: 1 (Highest) ▼

Session Failover	
Session Failover Time	<input checked="" type="radio"/> Normal (Failover Time: 16 secs; Recommended Option) <input type="radio"/> Fast (Failover Time: 6 secs) <input type="radio"/> Fastest (Failover Time 2 secs; More Health Checks and Higher Bandwidth Overhead)

VPN Settings	
Active	Check this box to enable the VPN.
Peer Serial Number	Pepwave MAX only establishes VPN connection with a remote peer that has a serial number specified here. If the remote peer is in high availability setup, you can check the box Remote client is set up in high availability mode , and enter the second unit's serial number into the second text box.
Peer IP Addresses / Host Names	Enter the remote peer's WAN IP address(es) or host name(s) here. Dynamic-DNS host names are accepted.

	<p>This field is optional. With this field filled, the Pepwave MAX will initiate connection to each of the remote IP addresses until success. If the field is empty, the Pepwave MAX will wait for connection from the remote peer. Therefore, at least one side of the two VPN peers has to have the field filled. Otherwise, VPN connection cannot be established.</p> <p>Enter one IP address or host name per line.</p>
--	---

WAN Connection Priority

<p>WAN Connection Priority</p>	<p>You can specify the priority of the WAN connections to be used for making VPN connections. WAN connections set to OFF will never be used. Only available WAN connections with the highest priority will be used for making VPN connections. Outgoing traffic will be distributed evenly if there is more than one connection having the same priority.</p>
--	--

Session Failover

<p>Session Failover Time</p>	<p>The Site-to-Site VPN supports TCP/UDP session failover upon link or routing failure on a path between two sites. It can automatically detect any failure and route established sessions to a healthy link so that connected sessions can remain unaffected.</p> <p>Health check packets are sent between two sites in order to detect any failure. The more frequent checks it sends, the faster failover it can perform, but the higher bandwidth overhead will be consumed.</p> <p>If different options are selected on the two peers for this setting, the faster one will be used.</p> <p>Select Fastest when the highest failover speed is request. By default, Normal failover time is selected.</p>
----------------------------------	---

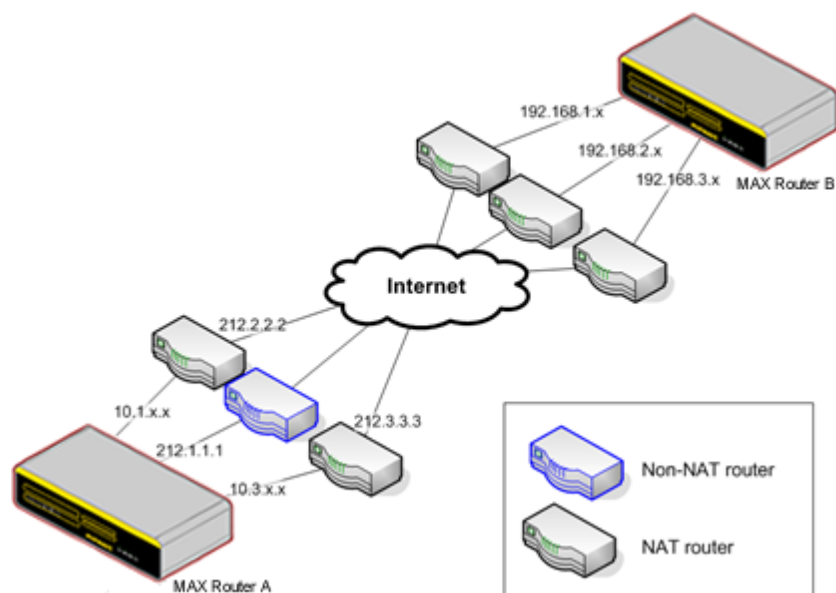
11.2 Pepwave MAX Behind NAT Router

The Pepwave MAX supports establishing Site-to-Site VPN over WAN connections which are behind a NAT (Network Address Translation) router.

To be able for a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to forward TCP port 32015 to it.

If one or more WAN connections on *Unit A* can accept VPN connections (by means of port forwarding or not) while none of the WAN connections on the peer *Unit B* can do so, you should put all public IP addresses or host names of the *Unit A* to the *Unit B*'s **Peer IP Addresses / Host Names** field. Leave the field in *Unit A* blank. With such setting, site-to-site VPN connection can be set up and all WAN connections on both sides will be utilized.

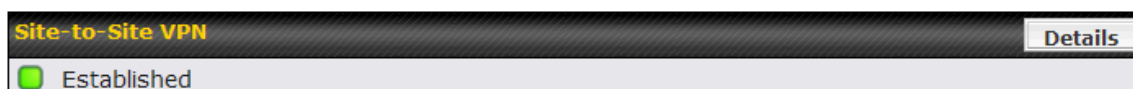
For example, see the following diagram:



One of the WANs of *Unit A* is non-NAT'd (212.1.1.1). The rest of the WANs on *Unit A* and all WANs on *Unit B* are NAT'd. In such case, the **Peer IP Addresses / Host Names** field on the *Unit B* should be filled with all of the *Unit A*'s public IP addresses (i.e. 212.1.1.1, 212.2.2.2 and 212.3.3.3), and the field on the *Unit A* should be left blank.

11.3 VPN Status

VPN Status is shown on the **Dashboard** as follows:



If you have set up VPN service at **Advanced > Site-to-Site VPN**, you can find the VPN status at **Status > Site-to-Site VPN** as well. For further information please refer to Section 20.4.

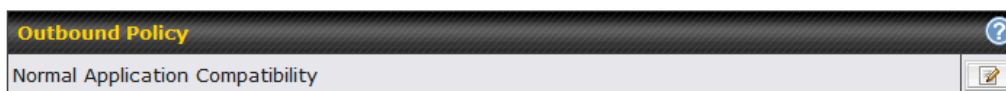
12 Outbound Policy

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**:



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


- High Application Compatibility
- Normal Application Compatibility
- Managed by Custom Rules

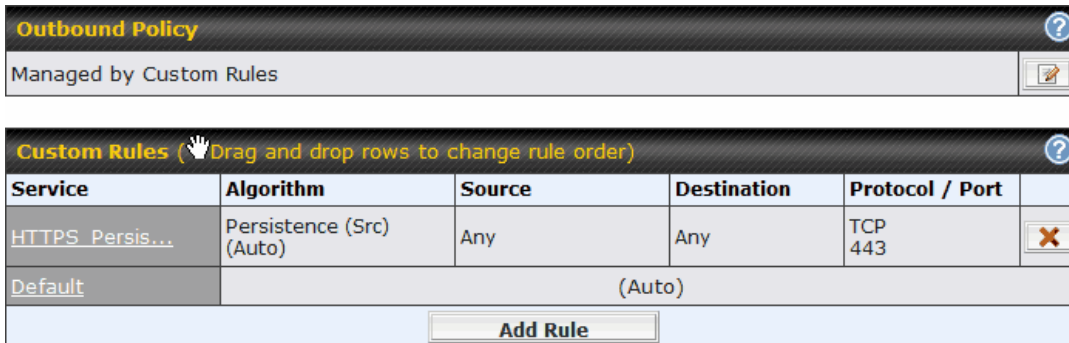
The selections are explained as follows:

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.
Managed by Custom Rules	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**.

12.1 Custom Rules For Outbound Traffic Management

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

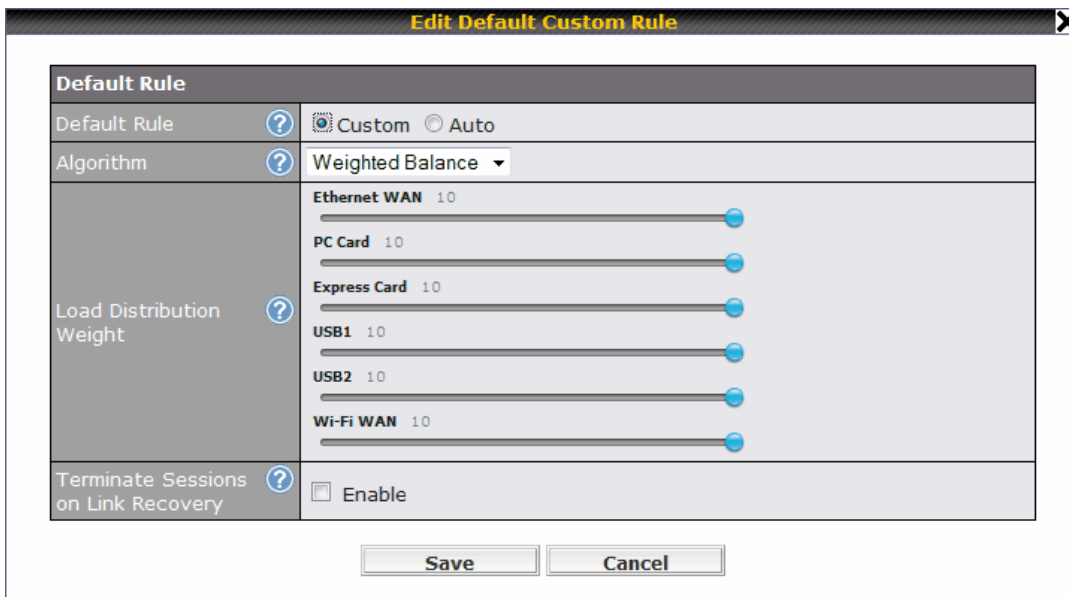


The screenshot shows two stacked windows. The top window, titled "Outbound Policy", has a dropdown menu set to "Managed by Custom Rules". The bottom window, titled "Custom Rules", contains a table with the following data:

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

Below the table is an "Add Rule" button.

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.



The screenshot shows the "Edit Default Custom Rule" window. It contains the following settings:

- Default Rule:** Custom (selected), Auto
- Algorithm:** Weighted Balance
- Load Distribution Weight:**
 - Ethernet WAN: 10
 - PC Card: 10
 - Express Card: 10
 - USB1: 10
 - USB2: 10
 - Wi-Fi WAN: 10
- Terminate Sessions on Link Recovery:** Enable

At the bottom are "Save" and "Cancel" buttons.

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:

Add a New Custom Rule ✕

New Custom Rule	
Service Name *	<input type="text"/>
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Source	IP Network <input type="text"/> Mask: 255.255.255.0 <input type="text"/>
Destination	IP Network <input type="text"/> Mask : 255.255.255.0 <input type="text"/>
Protocol	TCP <input type="text"/> ← :: Protocol Selection Tool :: <input type="text"/>
Port *	Any Port <input type="text"/>
Algorithm	Weighted Balance <input type="text"/>
Load Distribution Weight	Ethernet WAN 10 <input type="text"/>
	Express Card 10 <input type="text"/>
	PC Card 10 <input type="text"/>
	USB1 10 <input type="text"/>
	USB2 10 <input type="text"/>
	Wi-Fi WAN 10 <input type="text"/>
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 custom rule will take effect.</p> <p>When Yes is selected, the custom rule takes effect. If the outbound traffic matches the specified IP/Protocol/Port, action will be taken by Pepwave MAX based on the other parameters of the rule.</p> <p>When No is selected, the custom rule does not take effect. 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	This setting specifies the destination IP Address or IP Network for outbound traffic that matches the 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.

New Custom Rule Settings	
Algorithm	<p>This setting specifies the behavior of Pepwave MAX for the custom rule.</p> <p>One of the following values can be selected:</p> <ul style="list-style-type: none"> • Weighted Balance • Persistence • Enforced • Priority • Least Used • Lowest Latency <p>The upcoming sections present the details of the listed algorithms.</p>
Terminate Sessions on Link Recovery	<p>This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the Algorithms: Weighted, Persistence and Priority.</p> <p>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.</p>

12.1.1 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	Weighted Balance
Load Distribution Weight	Ethernet WAN 10
	Express Card 10
	PC Card 10
	USB1 10
	USB2 10
	Wi-Fi WAN 10
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 WAN: 10
- PC Card: 0
- Express Card: 0

- USB1: 10
- USB2: 0
- Wi-Fi WAN: 5

Total weight is 25 = (10 + 0 + 0 + 10 + 0 + 5)

Matching traffic distributed to Ethernet WAN is 40% = (10 / 25) x 100%

Matching traffic distributed to PC Card is 0% = (0 / 25) x 100%

Matching traffic distributed to Express Card is 0% = (0 / 25) x 100%

Matching traffic distributed to USB1 is 40% = (10 / 25) x 100%

Matching traffic distributed to USB2 is 0% = (0 / 25) x 100%

Matching traffic distributed to Wi-Fi WAN is 20% = (5 / 25) x 100%

12.1.2 Algorithm: Persistence

The configuration of using Persistence for 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.

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 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 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 type="radio"/> By Source <input checked="" type="radio"/> By Destination
Load Distribution	<input type="radio"/> Auto <input checked="" type="radio"/> Custom
Load Distribution Weight	Ethernet WAN 10 Express Card 10 PC Card 10 USB1 10 USB2 10 Wi-Fi WAN 10
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

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 9 **Configuration of WAN Interface(s)**). If you choose **Custom**, you can customize the weight of each WAN manually by using the sliders.

12.1.3 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		Ethernet WAN

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

12.1.4 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.

Default Rule		
Default Rule		<input checked="" type="radio"/> Custom <input type="radio"/> Auto
Algorithm		Priority
Priority Order		<div style="border: 1px solid gray; padding: 2px;"><p>Highest Priority</p><p>Ethernet WAN </p><p>Express Card</p><p>PC Card</p><p>USB1</p><p>USB2</p><p>Wi-Fi Hotspot</p><p>Lowest Priority</p></div>
Terminate Sessions on Link Recovery		<input type="checkbox"/> Enable

Tip

Configure multiple distribution rules to accommodate different kinds of services.

12.1.5 Algorithm: Least Used

Algorithm	<input type="button" value="?"/> Least Used
Connection	<input checked="" type="checkbox"/> Ethernet WAN <input checked="" type="checkbox"/> Express Card <input checked="" type="checkbox"/> PC Card <input checked="" type="checkbox"/> USB1 <input checked="" type="checkbox"/> USB2 <input checked="" type="checkbox"/> Wi-Fi WAN

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.

12.1.6 Algorithm: Lowest Latency

Algorithm	<input type="button" value="?"/> Lowest Latency Note: Use of Lowest Latency will incur additional network usage.
Connection	<input checked="" type="checkbox"/> Ethernet WAN <input checked="" type="checkbox"/> Express Card <input checked="" type="checkbox"/> PC Card <input checked="" type="checkbox"/> USB1 <input checked="" type="checkbox"/> USB2 <input checked="" type="checkbox"/> Wi-Fi WAN

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:

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

13 Service Forwarding

Service Forwarding settings are located at **Advanced > Service Forwarding**:

13.1 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.

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 11.1).

13.2 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.

13.3 DNS Forwarding

DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	<input checked="" 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.

14 Port Forwarding

14.1 Port Forwarding Service

When operating under NAT mode, Pepwave MAX acts 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.

Important Note

Port Forwarding applies only to WAN connections that are operating under NAT mode. For WAN connections operating under IP forwarding, inbound traffic is forwarded to the LAN by default.

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

Service	IP Address(es)	Server	Protocol	Action
Web	Ethernet WAN: default	192.168.1.10	TCP:80	Delete
<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 *	web																												
IP Protocol	TCP <input type="button" value="←"/> :: Protocol Selection Tool :: <input type="button" value="→"/>																												
Port	Single Port <input type="button" value="↓"/> Service Port: 80																												
Inbound IP Address(es) * (Require at least one IP address)	<table border="1"><thead><tr><th colspan="2">Connection / IP Address(es)</th><th>All</th><th>Clear</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> Ethernet WAN</td><td><input checked="" type="checkbox"/> 123.123.123.1 (Interface IP)</td><td></td><td></td></tr><tr><td><input type="checkbox"/> Express Card</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> PC Card</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> USB1</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> USB2</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> Wi-Fi Hotspot</td><td></td><td></td><td></td></tr></tbody></table>	Connection / IP Address(es)		All	Clear	<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			
Connection / IP Address(es)		All	Clear																										
<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																													
Server IP Address	<input type="text"/>																												

* Required Fields

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 Pepwave MAX based on the other parameters of the rule.</p> <p>When No is selected, the inbound service rule does not take effect. 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 Pepwave MAX via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the Servers setting.</p> <p>(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 fill in the Protocol and a single 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>

Port Forwarding Settings

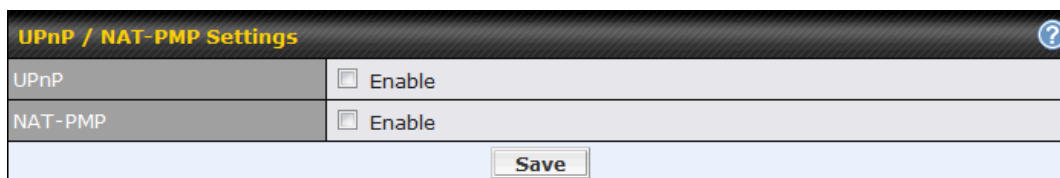
Port	<p>The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p> <p style="text-align: center;">Any Port, Single Port, Port Range and Port Map</p> <p>Any Port: All traffic that is received by Pepwave MAX via the specified protocol is forwarded to the servers specified by the Servers setting.</p> <p>For example, with IP Protocol set to TCP, and Port set to Any Port, all TCP traffic is forwarded to the configured servers.</p> <p>Single Port: Traffic that is received by Pepwave MAX via the specified protocol at the specified port is forwarded via the same port to the servers specified by the Servers setting.</p> <p>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.</p> <p>Port Range: Traffic that is received by 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.</p> <p>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.</p> <p>Port Map: Traffic that is received by Pepwave MAX via the specified protocol at the specified port is forwarded via a different port to the servers specified by the Servers setting.</p> <p>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.</p> <p>(Please see below for details on the Servers setting.)</p>
Inbound IP Address(es)	<p>This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.</p> <p>It is required to click at least one IP address.</p>
Server IP Address	<p>This setting specifies the LAN IP address of the server that handles the requests for the service.</p>

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

15 NAT Mappings

The configuration of NAT Mappings allows the IP address mapping of all inbound and outbound NAT'ed 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 Host	?	192.168.50.12
Inbound Mappings	?	Connection / Inbound 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 checked="" type="checkbox"/> Wi-Fi Hotspot <input checked="" type="checkbox"/> Interface IP
Outbound Mappings	?	Connection / Outbound IP Address
		Ethernet WAN 123.123.123.1 (Interface IP) ▾
		Express Card Interface IP ▾
		PC Card Interface IP ▾
		USB1 Interface IP ▾
		USB2 Interface IP ▾
		Wi-Fi Hotspot Interface IP ▾
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

NAT Mapping Settings	
LAN Host	This is the IP address of the host on the LAN that the system should map the selected connection IP address correspondences.
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>Note 1: Inbound Mapping is not needed for WAN connections in 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 IP address of each WAN connection to be used for any outgoing traffic originating from the LAN Host.</p> <p>Note 1: If you do not want to use a specific WAN for outgoing accesses, you should still choose <i>default</i> here, then customize the outbound access rule in the <i>Outbound Policy</i> section.</p>

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

Important Note
Inbound firewall rules override the Inbound Mapping settings.

16 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 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 Site-to-Site VPN enabled (see Section 10), the firewall rules also apply to VPN tunneled traffic.

16.1 Outbound and Inbound Firewall

The outbound and inbound firewall settings are located in **Advanced > Firewall:**

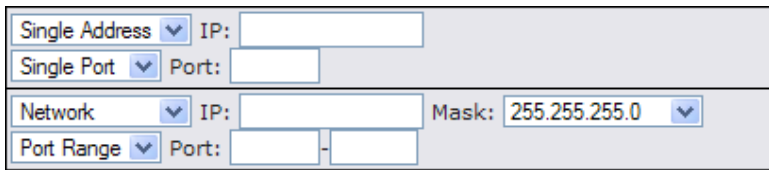
The image shows two screenshots of the firewall rule configuration interface. The top screenshot is titled "Outbound Firewall Rules" and includes a header with a hand icon and the text "Drag and drop rows to change rule order". It contains a table with columns: Rule, Protocol, Source IP Port, Destination IP Port, Policy, and an empty column. The "Default" row shows Protocol: Any, Source IP Port: Any, Destination IP Port: Any, and Policy: Allow. Below the table is an "Add Rule" button. The bottom screenshot is titled "Inbound Firewall Rules" and includes a similar header. Its table has columns: Rule, Protocol, WAN, Source IP Port, Destination IP Port, Policy, and an empty column. The "Default" row shows Protocol: Any, WAN: Any, Source IP Port: Any, Destination IP Port: Any, and Policy: Allow. Below the table is an "Add Rule" button.

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

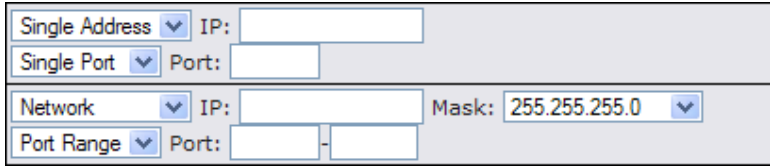
The image shows a dialog box titled "Add a New Inbound Firewall Rule" with a close button (X) in the top right corner. The dialog contains a "New Firewall Rule" section with the following fields:

- Rule Name *: [Empty text box]
- Enable: Yes No
- WAN Connection: [?] Any [Dropdown]
- Protocol: [?] Any [Dropdown] ← :: Protocol Selection Tool :: [Dropdown]
- Source IP & Port: [?] Any Address [Dropdown]
- Destination IP & Port: [?] Any Address [Dropdown]
- Action: [?] Allow Deny
- Event Logging: [?] Enable

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

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 Pepwave MAX based on the other parameters of the rule.</p> <p>When No is selected, the firewall rule does not take effect. Pepwave MAX will disregard the other parameters of the rule.</p>
WAN Connection	<p><i>This setting is applicable to Inbound Firewall Rules only.</i></p> <p>This setting specifies which WAN connection(s) the rule applies to:</p> <ul style="list-style-type: none"> • Any (applies to all WAN connections) • Ethernet WAN • PC Card • Express Card • USB1 • USB2 • Wi-Fi WAN
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>The screenshot shows a configuration window with four sections:</p> <ul style="list-style-type: none"> Single Address: A dropdown menu set to 'Single Address' followed by an 'IP:' label and an empty text input field. Single Port: A dropdown menu set to 'Single Port' followed by a 'Port:' label and an empty text input field. Network: A dropdown menu set to 'Network' followed by an 'IP:' label, an empty text input field, a 'Mask:' label, and a dropdown menu showing '255.255.255.0'. Port Range: A dropdown menu set to 'Port Range' followed by a 'Port:' label, an empty text input field, a hyphen, and another empty text input field. <p>In addition, a single port, or a range of ports, can be specified for the Source IP & Port setting.</p>

Inbound / Outbound Firewall Settings

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>  <p>The screenshot shows a configuration interface with four rows of options for the Source IP & Port setting:</p> <ul style="list-style-type: none"> Single Address: IP: [input field] Single Port: Port: [input field] Network: IP: [input field] Mask: 255.255.255.0 [dropdown] Port Range: Port: [input field] - [input field]
Action	<p>This setting specifies the action to be taken by Pepwave MAX upon encountering traffic that matches the both of the following:</p> <ul style="list-style-type: none"> • Source IP & Port • Destination IP & Port <p>With the value of Allow for the Action setting, the matching traffic passes through Pepwave MAX (to be routed to the destination).</p> <p>If the value of the Action setting is set to Deny, the matching traffic does not pass through Pepwave MAX (and is discarded).</p>
Event Logging	<p>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page Status > Event Log. A sample message is as follows:</p> <pre>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</pre> <ul style="list-style-type: none"> • CONN: The connection where the log entry refers to • SRC: Source IP address • DST: Destination IP address • LEN: Packet length • PROTO: Protocol • SPT: Source port • DPT: Destination port

Upon clicking **Save** after entering required information, the following screen appears.

Outbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	
Default	Any	Any	Any	Allow	

Add Rule

To create an additional firewall rule, click **Add Rule** and repeat the above steps.

To reorder a rule's position, just drag the rule by holding the left mouse button, move it to the desired position, and place it by releasing the mouse button.

Outbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	
No FTP access	TCP	Any Any	Any 21	Deny	
Default	Any	Any	Any	Allow	

Add Rule

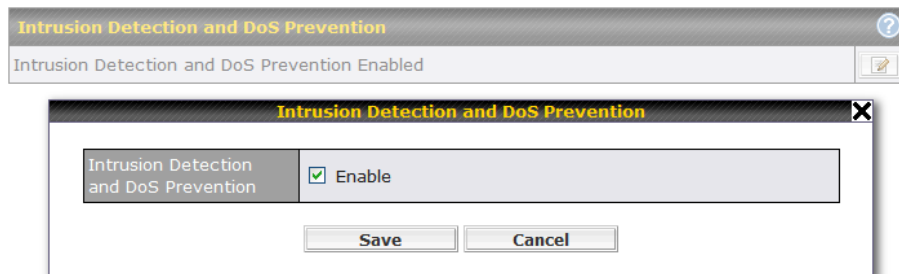
To remove a rule, click


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 accesses.

Tip
<p>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.</p>

16.2 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

17 Traffic Prioritization

Pepwave MAX provides the functionality to prioritize Voice over IP, VPN, video streaming, Secure Web over the other Internet traffic.

The settings for configuring Quality of Service are located at **Advanced > Traffic Prioritization**:

Services	Traffic Prioritization 
SIP/Vonage	<input type="checkbox"/> Enable
PPTP and IPsec VPN	<input type="checkbox"/> Enable
Skype, Google Talk, RealVideo, and Windows Streaming Media	<input type="checkbox"/> Enable
Secure Web (HTTPS)	<input type="checkbox"/> Enable

DSL/Cable Optimization 
DSL/Cable Optimization <input checked="" type="checkbox"/> Enable

(Registered trademarks are copyrighted by their respective owner)

Traffic Prioritization	
SIP/Vonage	When enabled, any SIP and Vonage voice traffic will be prioritized.
PPTP and IPsec VPN	When enabled, any PPTP and IPsec traffic will be prioritized.
Skype, Google Talk, RealVideo, and Windows Streaming Media	When enabled, voice and video traffic of Skype, Google Talk, RealVideo and Windows Streaming Media will be prioritized. <i>(Registered trademarks are copyrighted by their respective owner)</i>
Secure Web (HTTPS)	When enabled, HTTPS (TCP port 443) traffic will be prioritized.

DSL/Cable Optimization

DSL/Cable Optimization	<p>For an asymmetric DSL (ADSL) or Cable based WAN connection, where the upstream bandwidth is lower than the downstream, with this option turned on, the WAN's downstream bandwidth can be fully utilized in any situation.</p> <p>When a DSL or a Cable circuit's uplink becomes busy, it is a fact that the downlink bandwidth is affected. Users cannot download data in full speed until the uplink becomes less congested. The DSL/Cable Optimization could relieve such problem. When it is enabled, the download speed will be less affected by upload traffic.</p> <p>By default, this feature is enabled.</p>
------------------------	---

Please note that the Pepwave MAX prioritizes only outbound packets. E.g. for secure web prioritization, the system will prioritize uploading traffic for outgoing connections and downloading traffic for incoming connections.


18 PPTP Server

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 > 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 19.3 for details.

PPTP Server															
Enable	<input checked="" type="checkbox"/>														
Listen On ?	<table border="1"> <thead> <tr> <th colspan="2">Connection / IP Address(es)</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Ethernet WAN</td> <td><input checked="" type="checkbox"/> 123.123.123.1 (Interface IP)</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> Express Card</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> PC Card</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> USB1</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> USB2</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> Wi-Fi Hotspot</td> </tr> </tbody> </table>	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	
	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 ?	<table border="1"> <tr> <td colspan="2" style="text-align: center;">No User Account</td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </table>	No User Account		<input type="button" value="Add"/>											
No User Account															
<input type="button" value="Add"/>															
<input type="button" value="Save"/>															

PPTP Server Setting	
Listen On	This setting is for specifying the WAN connection(s) and IP address(es) where the PPTP server should listen on.
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 a username to edit the account password. Click the button  to delete the account in its corresponding row.

19 Service Passthrough

Service Passthrough settings can be found in **Advanced > Service Passthrough**:

Service Passthrough Support	
SIP Passthrough (Standard SIP, Vonage)	<input checked="" type="checkbox"/> Always Enabled <input type="checkbox"/> Define custom signal ports
FTP Passthrough	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Define custom control ports
TFTP Passthrough	<input checked="" type="checkbox"/> Enable
IPsec NAT-T Passthrough	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Define custom ports <input type="checkbox"/> Route IPsec Site-to-Site VPN

(Registered trademarks are copyrighted by their respective owner)

Save

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 Passthrough	<p>Session Initiation Protocol, aka SIP, is a voice-over-IP protocol. 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.</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>
FTP Passthrough	<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 Passthrough	<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 Passthrough	<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>
-------------------------	--

20 System Settings

20.1 Admin Security

For security reasons, after logging in to the administration interface at the first time, changing the administrator password is recommended.

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

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

Admin Settings	
Router Name	MAX 600
Admin Password *	••••••••
Confirm Admin Password *	••••••••
Security	HTTP / HTTPS ▾
Web Admin Port	HTTP: 80 HTTPS: 443 Default
Web Admin Access	HTTP: LAN/WAN ▾ HTTPS: LAN Only ▾

WAN Connection Access Settings																													
Allowed Source IP Subnets	<input type="radio"/> Any <input checked="" type="radio"/> Allow access from the following IP subnets only 12.23.34.0/24 12.34.56.0/24																												
Allowed WAN IP Address(es)	<table border="1"><thead><tr><th colspan="2">Connection / IP Address(es)</th><th>All</th><th>Clear</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> Ethernet WAN</td><td><input checked="" type="checkbox"/> 123.123.123.1 (Interface IP)</td><td></td><td></td></tr><tr><td><input type="checkbox"/> Express Card</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> PC Card</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> USB1</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> USB2</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/> Wi-Fi Hotspot</td><td></td><td></td><td></td></tr></tbody></table>	Connection / IP Address(es)		All	Clear	<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			
Connection / IP Address(es)		All	Clear																										
<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																													

* Required

Save

Admin Settings	
Router Name	This field allows you to define a name for this Pepwave MAX unit.
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.
Security	<p>This option is for specifying the protocol(s) through which the Web Admin Interface can be accessible:</p> <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	<p>This option is for specifying the network interfaces through which the Web Admin Interface can be accessible:</p> <ul style="list-style-type: none"> • LAN only • LAN/WAN <p>If LAN/WAN is chosen, a WAN Connection Access Settings form will be displayed.</p>

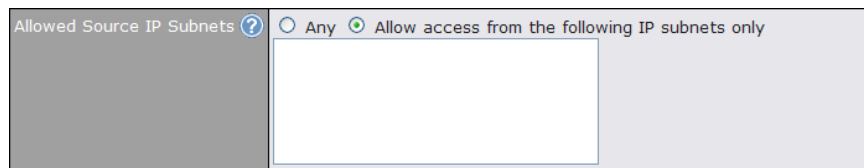
WAN Connection Access Settings

Allowed Source IP Subnets

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

Any - Allow web admin accesses to be from anywhere, without IP address restriction.

Allow access from the following IP subnets only - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:



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

where $w.x.y.z$ is an IP address (e.g. 192.168.0.0), and

m is the subnet mask in CIDR format, which is between 0 and 32 inclusively. For example: 192.168.0.0/24

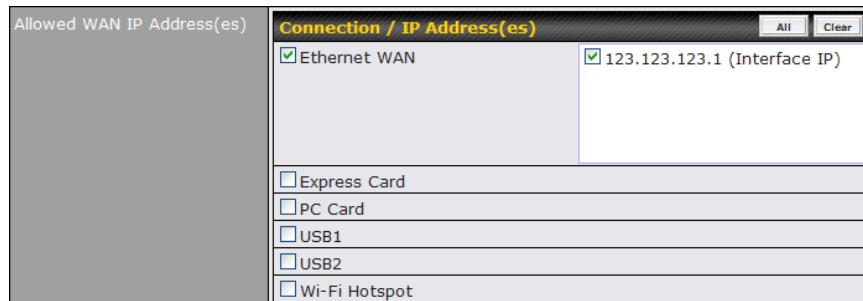
To define multiple subnets, separate each IP subnet one in a line. For example:

192.168.0.0/24

10.8.0.0/16

Allowed WAN IP Address(es)

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



20.2 Firmware Upgrade

The firmware of Pepwave MAX is upgradeable through Web Administration Interface.

Firmware upgrade functionality is located at **System > Firmware**:

The screenshot displays two sections of the firmware upgrade interface. The top section, titled "Online Firmware Upgrade", shows a "Last Status" of "Your firmware is already up to date" and a "Check again" button. The bottom section, titled "Manual Firmware Upgrade", features a "Firmware Image" input field with a "Browse..." button and an "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 firmware will be automatically downloaded by Pepwave MAX. The upgrade process will subsequently be automatically initiated.

You may also download a firmware image from the Pepwave web site (<http://www.pepwave.com/>) and update the unit manually. Click **Browse** to select the firmware file from the local computer, and then click **Upgrade** to send the firmware to Pepwave MAX. Pepwave MAX will then automatically initiate the firmware upgrade process.

Firmware Upgrade Status

Status LED Information during firmware upgrade:

- OFF – Firmware upgrade in progress (DO NOT disconnect power.)
- Red – Unit is rebooting
- Green – Firmware upgrade successfully completed

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 Mobile Router with an invalid firmware file will damage the unit, and may void the warranty.

20.3 Time

The Time Server functionality enables the system clock of 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 (Greenwich Mean Time) <input type="button" value="v"/>
Time Server	time.nist.gov <input type="button" value="Default"/>

Time Server Settings	
Time Zone	<p>This specifies the time zone (along with the corresponding Daylight Savings Time scheme) in which Pepwave MAX operates.</p> <p>The Time Zone value affects the time stamps in the Event Log of Pepwave MAX and E-mail notifications.</p>
Time Server	<p>This setting specifies the NTP network time server to be utilized by Pepwave MAX.</p>

20.4 Email Notification

The Email Notification functionality of 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

Email Notification Settings	
Email Notification	<p>This option is for enabling Email Notification.</p> <p>If the box Enable is checked, 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 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>

Email Notification Settings	
SMTP Port	This field is for specifying the SMTP Port number. By default, this is set to 25 ; when the SSL Encryption box is checked, the default port number will be set to 465 . You may customize the port number by editing this field. Click the button Default to restore to default.
SMTP User Name / Password	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.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the sender email address reported by the email messages sent by Pepwave MAX.
Recipient's Email Address	This setting specifies the email addresses to which Pepwave MAX should send the email messages to. You may enter multiple recipients' email addresses in this field.

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

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.

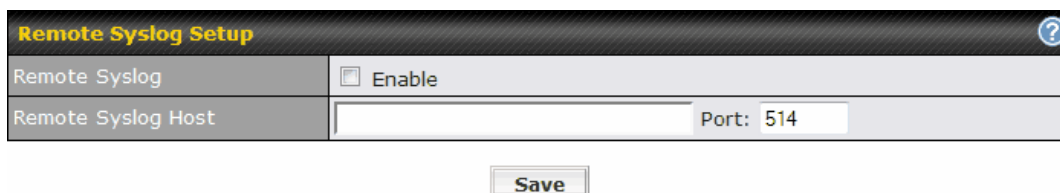
Test Result

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

20.5 Remote Syslog

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

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



Remote Syslog Setup	
Remote Syslog	<input type="checkbox"/> Enable
Remote Syslog Host	<input type="text"/> Port: 514

Remote Syslog Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote Syslog server.
Remote Syslog Host	This setting specifies the IP address or 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.

20.6 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 600
SNMPv1	<input checked="" type="checkbox"/> Enable
SNMPv2	<input checked="" type="checkbox"/> Enable
SNMPv3	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/>	

Community Name	Allowed Source Network	Access Mode	
MyCompany	192.168.1.20/24	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 .
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 Setting	
Community Name	MyCompany
Allowed Source Subnet Address	192.168.1.20
Allowed Source Subnet Mask	255.255.255.0 ▾
<input type="button" value="Save"/>	

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).
Allowed Source Subnet Mask	This setting specifies the subnet mask that corresponds to the subnet specified via Allowed Source Subnet Address (e.g. 255.255.255.0).

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 Setting	
User Name	snmpuser
Authentication Protocol	MD5 ▾
Authentication Password	mypassword
Privacy Protocol	DES ▾
Privacy Password	myprivpasswd

SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu the one of the following valid authentication protocols: <ul style="list-style-type: none"> • NONE • MD5 • SHA
Authentication Password	This setting specifies the authentication password, and is applicable only if the MD5 or SHA authentication protocol is selected.
Privacy Protocol	This setting specifies via a drop-down menu the one of the following valid privacy protocols: <ul style="list-style-type: none"> • NONE • DES
Privacy Password	This setting specifies the privacy password, and is applicable only if the DES privacy protocol is selected.

20.7 Saving and Loading Configurations

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**:

The image displays three screenshots of the Pepwave MAX configuration interface, separated by horizontal lines. Each screenshot has a dark header bar with a question mark icon in the top right corner.

- Restore Configuration to Factory Settings:** The header is yellow. Below it is a light blue bar containing a button labeled "Restore Factory Settings".
- Download Active Configurations:** The header is yellow. Below it is a light blue bar containing a button labeled "Download".
- Upload Configurations:** The header is yellow. Below it is a light blue bar containing a button labeled "Upload". Above this bar is a section with a grey background labeled "Configuration File". It contains a text input field and a "Browse..." button.

20.7.1 Restore Configuration to Factory Settings

The **Restore Factory Settings** button is to reset the configuration to the factory default settings. You have to click the **Apply Changes** button to make the settings effective.

20.7.2 Downloading Active Configurations

The **Download** button is to backup the current active settings. Click **Download** and save the configuration file.

20.7.3 Uploading Configurations

To restore or change settings based on a configuration file, click **Browse...** 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 discard at the Main page of Web Administration Interface.

20.8 Flash Management

The Pepwave MAX is equipped with dual flash memory modules. Each flash memory stores one firmware image. It does not only allow improved flexibility but also facilitates more effective management of the flash contents. It is possible to upgrade the firmware on the module/partition that is not designated for booting, so that the boot flash is unaffected by firmware upgrade process or any potential power failures throughout.

Flash module management is located at **System > Flash Management**:

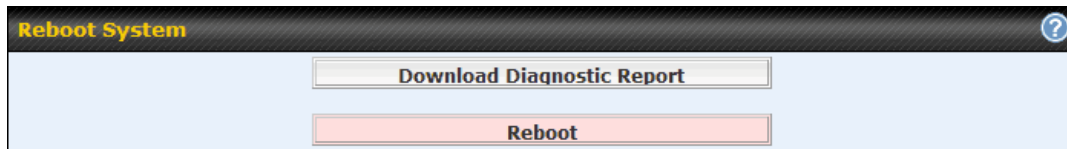
	Flash 1	Flash 2
Firmware Version	v4.8.1	v4.8.1
Flash Status	Bootable	Bootable
Boot from...	★	[Select this]
Next Firmware Upgrade Target	[Select this]	★

Flash Management	
Firmware Version	This displays the firmware version on each flash module/partition (i.e. Flash 1 or Flash 2)
Flash Status	This shows the status of the flash module.
Boot from...	The star indicates the flash module/partition from which Pepwave MAX will perform its next boot.
Next Firmware Upgrade Target	The star indicates the flash module that is the target of the next firmware upgrade. By default, the target of the next firmware upgrade is the flash module that is NOT designated for the next boot.

The configuration parameters will be applied upon clicking **Apply Changes** on the page header of Web Administration Interface.

20.9 Reboot

This page provides a Reboot button for restarting the system.



Important Note

Download Diagnostic Report button is for exporting a report file required for system investigation. If you encounter issues and would like to contact Pepwave Support Team (email: support@pepwave.com), please download this file and attach it along with a description of your encountered issue.

20.10 Ping Test

The Ping Test tool in Pepwave MAX performs Pings through a specified Ethernet interface.

The Ping utility is located at **System > Tools > Ping**. The Ping utility is displayed as a pop-up window, illustrated as follows:

Ping Test

IP Address or Domain Name:

Interface:

Number of times to Ping:

```
PING 10.9.30.1 (10.9.30.1) from 10.9.2.29 ixp1: 56(84) bytes of data.  
64 bytes from 10.9.30.1: icmp_seq=1 ttl=128 time=1.97 ms  
64 bytes from 10.9.30.1: icmp_seq=2 ttl=128 time=0.785 ms  
64 bytes from 10.9.30.1: icmp_seq=3 ttl=128 time=0.596 ms  
64 bytes from 10.9.30.1: icmp_seq=4 ttl=128 time=0.614 ms  
64 bytes from 10.9.30.1: icmp_seq=5 ttl=128 time=0.600 ms  
  
--- 10.9.30.1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4041ms  
rtt min/avg/max/mdev = 0.596/0.914/1.978/0.537 ms
```

Tip

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

20.11 Traceroute Test

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

The Traceroute Test utility is located at **System > Tools > Traceroute**. The Traceroute Test utility is displayed as a pop-up window, illustrated as follows:

Traceroute Test

IP Address or Domain Name:

Interface:

```
traceroute to 218.103.62.122 (218.103.62.122), 30 hops max, 40 byte packets
 1 Balance A (10.9.1.1) 0.879 ms 0.900 ms 1.842 ms
 2 Balance B (10.1.9.1) 2.878 ms 3.069 ms 0.978 ms
```

Tip

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

21 Status

This section displays the information of Pepwave MAX on the **Device**, **Active Sessions**, **Client List**, **Site-to-Site VPN**, **UPnP / NAT-PMP**, **Event Log**, and **Bandwidth**.

21.1 Device

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

System Information	
Router Name	MAX 600
Model	Pepwave MAX 600
Serial Number	2814-1234-ABCD
Firmware	v4.8.0
Uptime	4 days 3 hours 59 minutes
System Time	Sat Aug 01 15:36:15 UDT 2009

Interface	MAC Address
LAN	00:11:22:AA:BB:CC
Ethernet WAN	00:11:22:AA:BB:CD
Wi-Fi WAN	00:11:22:AA:BB:CE

System Information	
Router Name	This is the name specified in the field <i>Router Name</i> located in System > Admin Security .
Model	This shows the model name and number 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.
Uptime	This shows the length of time since the device is rebooted.
System Time	This shows the current system time.

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

21.2 Active Sessions

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

Inbound TCP			
WAN1			
Source IP	Destination IP	Connection Type	Idle Time
10.10.10.115:3023	10.10.10.102:80	www-http	00:00:01
WAN2			
(No connections)			
WAN3			
(No connections)			
Outbound TCP			
WAN1			
Source IP	Destination IP	Connection Type	Idle Time
10.10.10.102:1619	123.123.123.11:80	www-http	00:00:01
WAN2			
(No connections)			
WAN3			
(No connections)			
Inbound UDP			
WAN1			
Source IP	Destination IP	Connection Type	Idle Time
102.101.103.11:123	10.10.10.102:80	www-http	00:00:15
WAN2			
(No connections)			
WAN3			
(No connections)			
Outbound UDP			
WAN1			
Source IP	Destination IP	Connection Type	Idle Time
10.10.10.102:1029	77.101.136.220:11777	www-http	00:00:22
10.10.10.102:2580	123.123.111.11:2233	www-http	00:00:30
10.10.10.102:22098	10.10.10.1:53	domain	00:00:25
10.10.10.102:22121	10.10.10.1:53	domain	00:00:20
10.10.10.102:22145	10.10.10.1:53	domain	00:00:15
10.10.10.102:22168	10.10.10.1:53	domain	00:00:10
10.10.10.102:22190	10.10.10.1:53	domain	00:00:05
WAN2			
(No connections)			
WAN3			
(No connections)			

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

21.3 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) and MAC addresses that the Peplink Balance 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.

If PPTP Server in section 17.3 is enabled, you may see the corresponding connection name would be listed in the field of *Name*.

Client List				
IP Address ▲	Name	MAC Address	Network Name (SSID)	Signal
<input checked="" type="checkbox"/> 192.168.50.10		00:21:22:23:24:aa	Wi-Fi AP	 -69dBm
<input type="checkbox"/> 192.168.50.11		00:1a:2b:3c:44:55		
<input type="checkbox"/> 192.168.50.12		00:1a:22:3c:4d:55		
<input type="checkbox"/> 192.168.50.13		00:1a:2b:33:44:5e		

21.4 Site-to-Site VPN

This is a page showing the current status of Site-to-Site VPN, located at: **Status > Site-to-Site VPN**







Details about peer's WAN connections would be listed as below.


Site-to-Site VPN	
VPN Status	Established
WAN1	<input checked="" type="checkbox"/> In Use

21.5 UPnP / NAT-PMP


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

This section appears only if you have enabled the function of UPnP / NAT-PMP as mentioned in Section 13.2.

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 the 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**.

21.6 Event Log

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

Event Log		Show [50 100 all]	Refresh	Clear Log
Jul 30 19:36:55	Link health check monitor started			
Jul 30 19:40:31	WAN Priority Changed: (Priority 1:Ethernet WAN, Wi-Fi WAN Priority 2: USB1)			
Jul 30 19:42:43	Health check status changed: (Ethernet WAN: UP)			
Jul 30 19:42:43	Time synchronization successful			
Jul 31 09:50:38	Wi-Fi AP: Client 00:11:22:AA:BB:CE Associated with wi-fi ap			

The log section displays a list of events that has taken place on the Pepwave MAX unit. Click the **Refresh** button to retrieve log entries again. Click the **Clear Log** button to clear the log. Select **50**, **100**, or **all** to show the corresponding number of events in the log.

21.7 Bandwidth

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

21.7.1 Real-Time

Data transferred since last reboot

[\[Add Trip Counter \]](#)

	Inbound (MBytes)	Outbound (MBytes)
1. Ethernet WAN	364	114
2. Express Card	0	0
3. PC Card	0	0
4. USB1	269	201
5. USB2	0	0
6. Wi-Fi WAN	136	41

Current Transfer Rate

1. Ethernet WAN	Inbound (Kbps)	Outbound (Kbps)
Overall	364	114
HTTP	289	114
HTTPS	75	0
IMAP	0	0
POP3	0	0
SMTP	0	0
Others	0	0

Current Transfer Rate

2. Express Card	Inbound (Kbps)	Outbound (Kbps)
Overall	0	0
HTTP	0	0
HTTPS	0	0
IMAP	0	0
POP3	0	0
SMTP	0	0
Others	0	0

Current Transfer Rate

3. PC Card	Inbound (Kbps)	Outbound (Kbps)
Overall	0	0
HTTP	0	0
HTTPS	0	0
IMAP	0	0
POP3	0	0
SMTP	0	0
Others	0	0

Current Transfer Rate

4. USB1	Inbound (Kbps)	Outbound (Kbps)
Overall	269	201
HTTP	167	188
HTTPS	0	0
IMAP	0	0
POP3	102	13
SMTP	0	0
Others	0	0

Current Transfer Rate

5. USB2	Inbound (Kbps)	Outbound (Kbps)
Overall	0	0
HTTP	0	0
HTTPS	0	0
IMAP	0	0
POP3	0	0
SMTP	0	0
Others	0	0

Current Transfer Rate

6. Wi-Fi WAN	Inbound (Kbps)	Outbound (Kbps)
Overall	136	41
HTTP	136	41
HTTPS	0	0
IMAP	0	0
POP3	0	0
SMTP	0	0
Others	0	0

21.7.2 Daily

This page shows the daily bandwidth usage for 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 10.3, the **Current Billing Cycle** table for that WAN connection will be shown as follows.

Daily Usage			
Connection		Ethernet WAN ▾	
Date	Download	Upload	Total
2009-07-09	1 MB	12 MB	13 MB
2009-07-08	101 MB	9 MB	110 MB
2009-07-07	55 MB	50 MB	105 MB
2009-07-06	144 MB	87 MB	231 MB
2009-07-05	32 MB	3 MB	35 MB
2009-07-04	115 MB	5 MB	120 MB
2009-07-03	30 MB	61 MB	91 MB
2009-07-02	69 MB	82 MB	151 MB
2009-07-01	0 MB	2 MB	2 MB
2009-06-30	6 MB	46 MB	52 MB
2009-06-29	16 MB	4 MB	20 MB
2009-06-28	0 MB	2 MB	2 MB
2009-06-27	32 MB	3 MB	35 MB
2009-06-26	16 MB	2 MB	18 MB
2009-06-25	1 MB	0 MB	1 MB
2009-06-24	0 MB	0 MB	0 MB
2009-06-23	0 MB	0 MB	0 MB
2009-06-22	0 MB	0 MB	0 MB

Current Billing Cycle (2009-07-01 to now)	
Down	550 MB
Up	315 MB
Total	865 MB
Allowance	10 240 MB
Used	8%


Current Month	
Down	550 MB
Up	315 MB
Total	865 MB

Scale: MB GB

21.7.3 Monthly

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

If you have enabled **Bandwidth Monitoring** feature as shown in section 10.3, you can choose a particular connection to check its usage and select to show the monthly usage period in **Billing Cycle** or **Calendar Month**.

Monthly Usage			
Connection	Ethernet WAN 		
Period	<input type="radio"/> Billing Cycle <input checked="" type="radio"/> Calendar Month		

Date	Download	Upload	Total
2009-07-01 to now	550 MB	316 MB	866 MB
2009-06-01 to 2009-06-30	72 MB	61 MB	133 MB
2009-05-31 to 2009-05-31	0 MB	0 MB	0 MB

Scale: MB GB

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 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. Product Specifications

B.1 Pepwave MAX Mobile Router

Routing

- NAT
- Flexible Custom Outbound Routing Policy

WAN Support

- DHCP, Static IP, and PPPoE
- Outbound Link Load Balance

Device Management

- Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Configurations Upload and Download

Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

Security

- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Site-to-Site VPN encrypted with 256-bit AES
- Intrusion Detection System

Physical Interface

- One RJ-45 for an IEEE 802.3u 10/100M WAN
- One PC Card Slot for WAN connection
- One Express Card Slot for WAN connection
- Two USB Ports for WAN connection
- One Wi-Fi WAN Connector
- One Wi-Fi AP Connector for LAN
- Four RJ-45 for an IEEE 802.3u 10/100M LAN

Power Specification

- AV Input 100-240V, DC Output 9-30V

Operating Environment

- Temperature: 0°C - 50°C
- Humidity: 10% - 90% (non-condensing)

PEP WAVE

Broadband Possibilities

www.pepwave.com

Contact Us:

Sales

sales@pepwave.com

Support

support@pepwave.com

Business Development and Partnerships

partners@pepwave.com

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

17/F, Park Building,
476 Castle Peak Road
Cheung Sha Wan
Hong Kong

Tel: +852 2990 7600

Fax: +852 3007 0588