

# Pepwave MAX and Surf User Manual

Pepwave Products:

MAX 700/HD2/HD2 IP67/HD2 mini/HD4/Transit/BR1/BR1 Slim/BR1 ENT/BR1 Mini/BR1 Pro LTE/BR1 IP55/BR2 IP55/On-The-Go/MAX HD2/HD4 with MediaFast/Device Connector/ Surf SOHO

Pepwave Firmware 6.3  
June 2016

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. Copyright © 2016 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.

# Pepwave MAX and Surf User Manual

## Table of Contents

<b>1</b>	<b>INTRODUCTION AND SCOPE</b>	<b>6</b>
<b>2</b>	<b>GLOSSARY</b>	<b>7</b>
<b>3</b>	<b>PRODUCT FEATURES</b>	<b>8</b>
3.1	SUPPORTED NETWORK FEATURES	8
3.2	OTHER SUPPORTED FEATURES	10
<b>4</b>	<b>PEPWAVE MAX MOBILE ROUTER OVERVIEW</b>	<b>11</b>
4.1	MAX 700	11
4.2	MAX HD2	13
4.3	MAX HD2 IP67	15
4.4	MAX HD2 MINI	16
4.5	MAX TRANSIT	18
4.6	MAX HD4	19
4.7	MAX BR1	20
4.8	MAX BR1 MINI	22
4.9	MAX BR1 SLIM	23
4.10	MAX BR1 ENT	25
4.11	MAX BR1 PRO LTE	26
4.12	MAX BR1/2 IP55	27
4.13	MAX ON-THE-GO	29
4.14	SURF SOHO	30
<b>5</b>	<b>ADVANCED FEATURE SUMMARY</b>	<b>32</b>
5.1	DROP-IN MODE AND LAN BYPASS: TRANSPARENT DEPLOYMENT	32
5.2	QoS: CLEARER VOIP	32
5.3	PER-USER BANDWIDTH CONTROL	33
5.4	HIGH AVAILABILITY VIA VRRP	33
5.5	USB MODEM AND ANDROID TETHERING	34
5.6	BUILT-IN REMOTE USER VPN SUPPORT	34
5.7	SIM-CARD USSD SUPPORT	35
<b>6</b>	<b>INSTALLATION</b>	<b>36</b>
6.1	PREPARATION	36
6.2	CONSTRUCTING THE NETWORK	37
6.3	CONFIGURING THE NETWORK ENVIRONMENT	38
<b>7</b>	<b>MOUNTING THE UNIT</b>	<b>39</b>
7.1	WALL MOUNT	39
7.2	CAR MOUNT	39
7.3	IP67 INSTALLATION GUIDE	39

# Pepwave MAX and Surf User Manual

<b>8</b>	<b>CONNECTING TO THE WEB ADMIN INTERFACE .....</b>	<b>40</b>
<b>9</b>	<b>CONFIGURING THE LAN INTERFACE(S).....</b>	<b>42</b>
9.1	BASIC SETTINGS .....	42
9.2	CAPTIVE PORTAL.....	52
<b>10</b>	<b>CONFIGURING THE WAN INTERFACE(S) .....</b>	<b>54</b>
10.1	ETHERNET WAN .....	55
10.2	CELLULAR WAN .....	63
10.3	WI-FI WAN .....	68
10.4	WAN HEALTH CHECK.....	74
10.5	DYNAMIC DNS SETTINGS .....	76
<b>11</b>	<b>ADVANCED WI-FI SETTINGS.....</b>	<b>79</b>
<b>12</b>	<b>MEDIAFAST CONFIGURATION .....</b>	<b>82</b>
12.1	SETTING UP MEDIAFAST CONTENT CACHING .....	82
12.2	SCHEDULING CONTENT PREFETCHING.....	83
12.3	VIEWING MEDIAFAST STATISTICS .....	84
<b>13</b>	<b>BANDWIDTH BONDING SPEEDFUSION™ / PEPVPN .....</b>	<b>86</b>
13.1	PEPVPN .....	87
13.2	THE PEPWAVE ROUTER BEHIND A NAT ROUTER .....	93
13.3	SPEEDFUSION™ STATUS .....	94
<b>14</b>	<b>IPSEC VPN .....</b>	<b>95</b>
14.1	IPSEC VPN SETTINGS.....	95
<b>15</b>	<b>OUTBOUND POLICY MANAGEMENT .....</b>	<b>99</b>
15.1	OUTBOUND POLICY .....	99
15.2	CUSTOM RULES FOR OUTBOUND POLICY .....	100
<b>16</b>	<b>INBOUND ACCESS .....</b>	<b>109</b>
16.1	PORT FORWARDING SERVICE .....	109
<b>17</b>	<b>NAT MAPPINGS .....</b>	<b>112</b>
<b>18</b>	<b>QOS .....</b>	<b>114</b>
18.1	USER GROUPS .....	114
18.2	BANDWIDTH CONTROL.....	115
18.3	APPLICATION.....	115
<b>19</b>	<b>FIREWALL .....</b>	<b>117</b>
19.1	OUTBOUND AND INBOUND FIREWALL RULES .....	117
19.2	CONTENT BLOCKING .....	122
19.3	OSPF & RIPv2.....	123

# Pepwave MAX and Surf User Manual

19.4	REMOTE USER ACCESS .....	125
<b>MISCELLANEOUS SETTINGS.....</b>		<b>127</b>
19.5	HIGH AVAILABILITY .....	127
19.6	PPTP SERVER .....	130
19.7	CERTIFICATE MANAGER.....	131
19.8	SERVICE FORWARDING .....	131
19.9	SERVICE PASSTHROUGH.....	134
19.10	GPS FORWARDING.....	135
<b>20 AP CONTROLLER .....</b>		<b>136</b>
20.1	WIRELESS SSID .....	136
20.2	SETTINGS.....	140
20.3	TOOLBOX.....	144
<b>21 SYSTEM SETTINGS.....</b>		<b>145</b>
21.1	ADMIN SECURITY .....	145
21.2	FIRMWARE.....	149
21.3	TIME.....	150
21.4	SCHEDULE.....	150
21.5	EMAIL NOTIFICATION .....	151
21.6	EVENT LOG .....	153
21.7	SNMP.....	155
21.8	INCONTROL.....	157
21.9	CONFIGURATION .....	157
21.10	FEATURE ADD-ONS.....	159
21.11	REBOOT .....	159
21.12	PING.....	160
21.13	TRACEROUTE TEST.....	161
21.14	PEPVPN TEST .....	161
21.15	WAKE-ON-LAN.....	162
21.16	CLI (COMMAND LINE INTERFACE SUPPORT) .....	162
<b>22 STATUS.....</b>		<b>163</b>
22.1	DEVICE.....	163
22.2	ACTIVE SESSIONS .....	165
22.3	CLIENT LIST .....	167
22.4	WINS CLIENT .....	167
22.5	UPnP / NAT-PMP .....	168
22.6	SPEEDFUSION STATUS.....	168
22.7	EVENT LOG .....	172
22.8	BANDWIDTH .....	172
<b>APPENDIX A. RESTORATION OF FACTORY DEFAULTS.....</b>		<b>178</b>

# Pepwave MAX and Surf User Manual

- APPENDIX B. CASE STUDIES .....178**
  - MPLS ALTERNATIVE..... 178
  - NETWORK TRAFFIC DISTRIBUTION ..... 181
  - SINGAPORE NATIONAL DAY PARADE 2015 ..... 183
  - UNOLS (UNIVERSITY-NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM)..... 185
- APPENDIX C. DECLARATIONS.....188**
- APPENDIX D. PRODUCT DATASHEETS .....192**

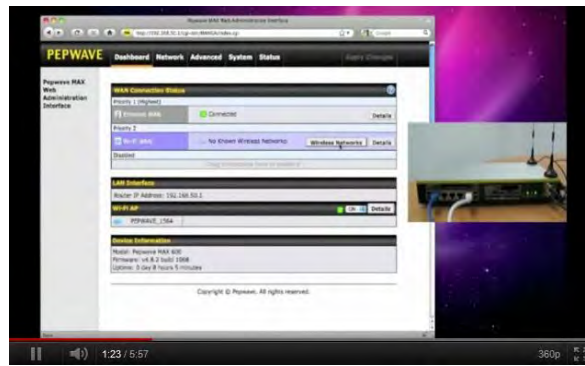
## 1 Introduction and Scope

Pepwave routers provide link aggregation and load balancing across multiple WAN connections, allowing a combination of technologies like 3G HSDPA, EVDO, 4G LTE, Wi-Fi, external WiMAX dongle, and satellite to be utilized to connect to the Internet.

This manual covers setting up Pepwave routers and provides an introduction to their features and usage.

### Tips

Want to know more about Pepwave routers? Visit our YouTube Channel for a video introduction!



<http://youtu.be/UckVQThLKO4>

## 2 Glossary

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

Term	Definition
3G	3rd Generation standards for wireless communications
4G	4th Generation standards for wireless communications
DHCP	Dynamic Host Configuration Protocol
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
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network

## 3 Product Features

Pepwave routers enable all LAN users to share broadband Internet connections, and they provide advanced features to enhance Internet access. Our Max BR wireless routers support multiple SIM cards. They can be configured to switch from using one SIM card to another SIM card according to different criteria, including wireless network reliability and data usage.

Our MAX HD series wireless routers are embedded with multiple 4G LTE modems, and allow simultaneous wireless Internet connections through multiple wireless networks. The wireless Internet connections can be bonded together using our SpeedFusion technology. This allows better reliability, larger bandwidth, and increased wireless coverage are comparing to use only one 4G LTE modem.

Below is a list of supported features on Pepwave routers. Features vary by model. For more information, please see [peplink.com/products](http://peplink.com/products).

### 3.1 Supported Network Features

#### 3.1.1 WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- Built-in HSPA and EVDO cellular modems
- USB mobile connection(s)
- Wi-Fi WAN connection
- Network address translation (NAT)/port address translation (PAT)
- Inbound and outbound NAT mapping
- IPsec NAT-T and PPTP packet passthrough
- MAC address clone and passthrough
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS (supported service providers: [changeip.com](http://changeip.com), [dyndns.org](http://dyndns.org), [no-ip.org](http://no-ip.org), [tzo.com](http://tzo.com) and [DNS-O-Matic](http://DNS-O-Matic))
- Ping, DNS lookup, and HTTP-based health check

#### 3.1.2 LAN

- Wi-Fi AP
- Ethernet LAN ports
- DHCP server on LAN
- Extended DHCP option support
- Static routing rules
- VLAN on LAN support



## 3.1.3 VPN

- PepVPN with SpeedFusion™
- PepVPN performance analyzer
- X.509 certificate support
- VPN load balancing and failover among selected WAN connections
- Bandwidth bonding and failover among selected WAN connections
- IPsec VPN for network-to-network connections (works with Cisco and Juniper only)
- Ability to route Internet traffic to a remote VPN peer
- Optional pre-shared key setting
- SpeedFusion™ throughput, ping, and traceroute tests
- PPTP server
- PPTP and IPsec passthrough

## 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
- Outbound firewall rules can be defined by destination domain name

## 3.1.5 Captive Portal

- Splash screen of open networks, login page for secure networks
- Customizable built-in captive portal
- Supports linking to outside page for captive portal

## 3.1.6 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
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms

## 3.1.7 AP Controller

- Configure and manage Pepwave AP devices

- Review the status of connected APs

## 3.1.8 QoS

- Quality of service for different applications and custom protocols
- User group classification for different service levels
- Bandwidth usage control and monitoring on group- and user-level
- Application prioritization for custom protocols and DSL/cable optimization

## 3.2 Other Supported Features

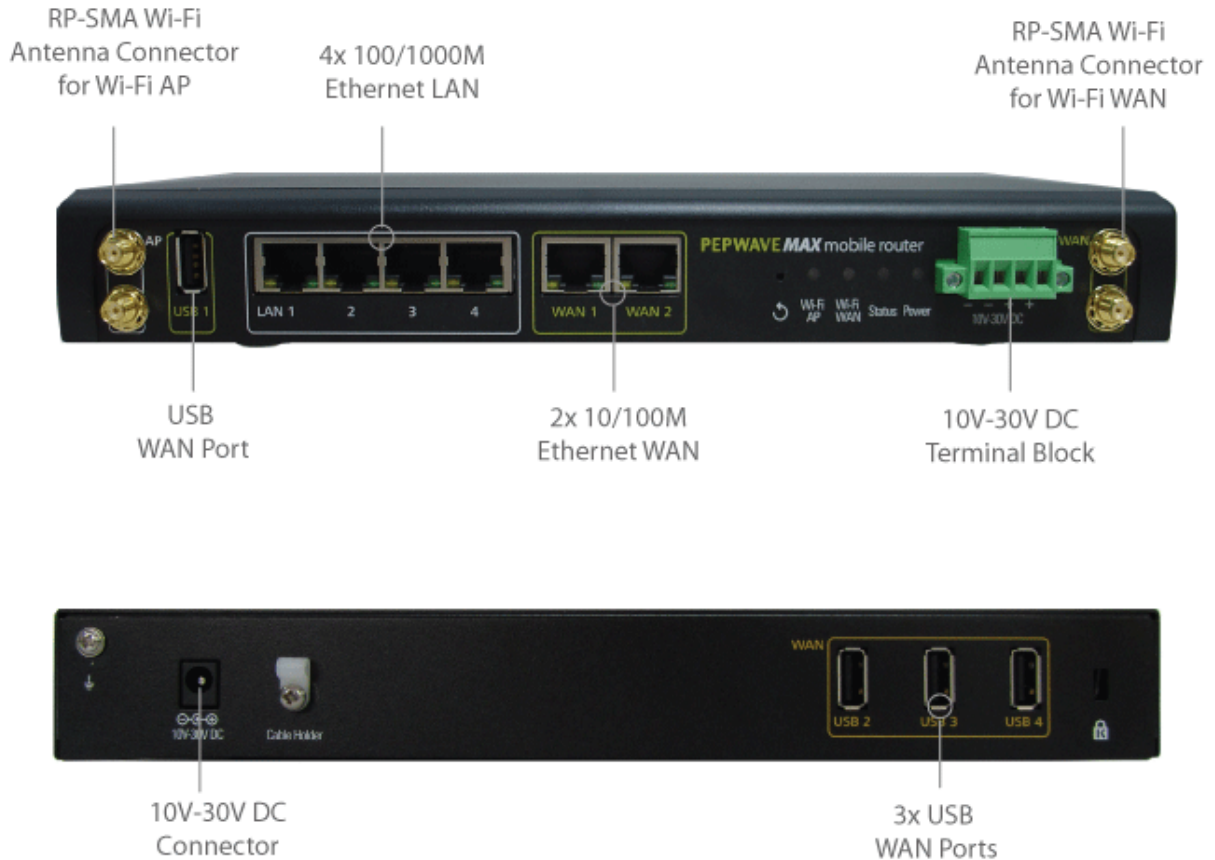
- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Time server synchronization
- SNMP
- Email notification
- Read-only user for web admin
- Shared IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Built-in WINS servers\*
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Event log
- Active sessions
- Client list
- WINS client list \*
- UPnP / NAT-PMP
- Real-time, hourly, daily, and monthly bandwidth usage reports and charts
- IPv6 support
- Support USB tethering on Android 2.2+ phones

\* Not supported on MAX Surf-On-The-Go, Surf SOHO, and BR1 variants

## 4 Pepwave MAX Mobile Router Overview

### 4.1 MAX 700

#### 4.1.1 Panel Appearance



# Pepwave MAX and Surf User Manual

## 4.1.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

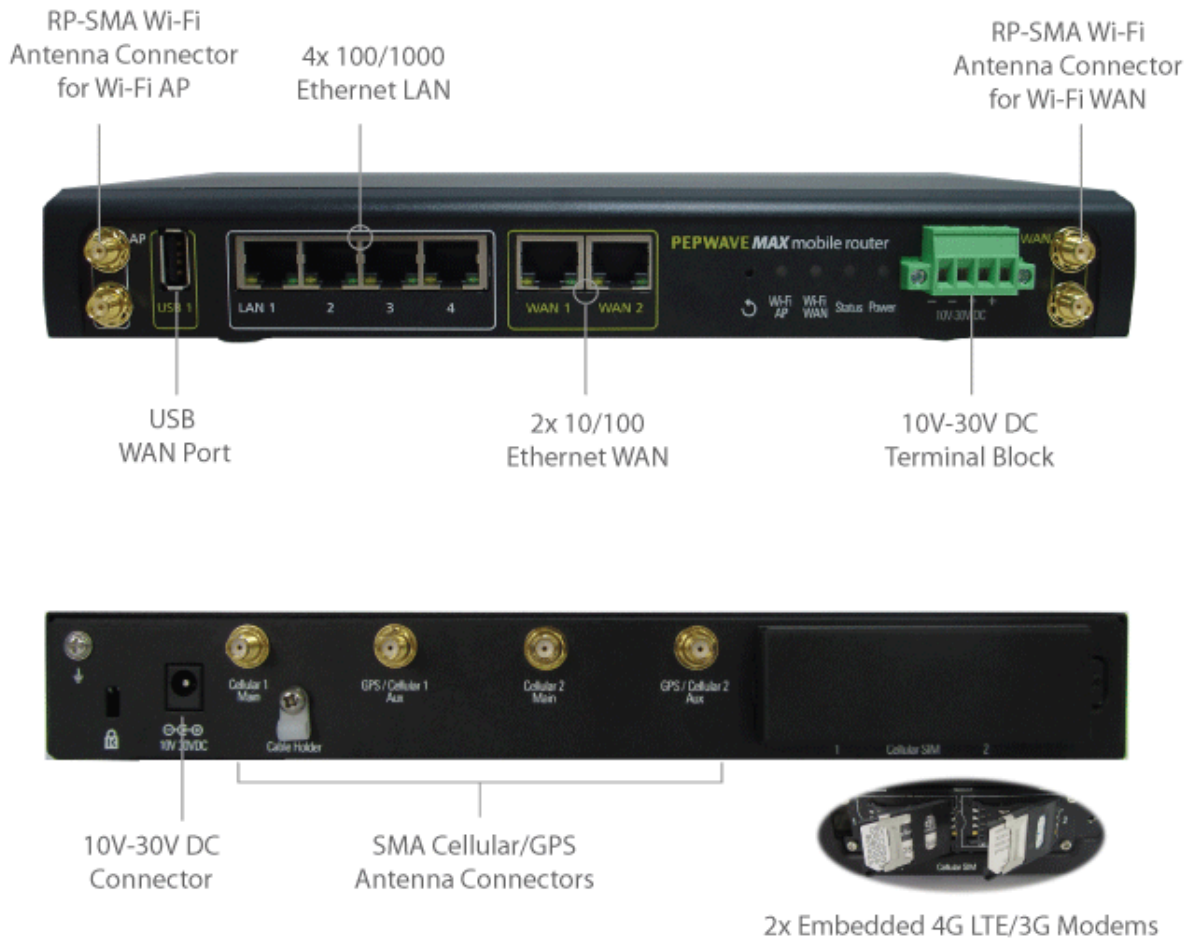
Wi-Fi AP and Wi-Fi WAN Indicators		
<b>Wi-Fi WAN</b>	OFF	Disconnected
	Blinking slowly	Connecting to network
	Blinking	Connected to network with traffic
	ON	Connected to network without traffic
<b>Wi-Fi AP</b>	OFF	Disabled
	Blinking slowly	Enabled but no client connected
	Blinking	Connected to network with traffic
	ON	Client(s) connected to wireless network

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	10 / 100/ 1000 Mbps
	Blinking	Data is transferring
<b>Orange LED</b>	OFF	No data is being transferred or port is not connected
	<b>Port Type</b>	Auto MDI/MDI-X ports

# Pepwave MAX and Surf User Manual

## 4.2 MAX HD2

### 4.2.1 Panel Appearance



## 4.2.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi AP and Wi-Fi WAN Indicators		
<b>Wi-Fi WAN / Cellular 1 / Cellular 2</b>	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	10 / 100 / 1000 Mbps
	Blinking	Data is transferring
<b>Orange LED</b>	OFF	No data is being transferred or port is not connected
	<b>Port Type</b>	Auto MDI/MDI-X ports

## 4.3 MAX HD2 IP67

### 4.3.1 Panel Appearance



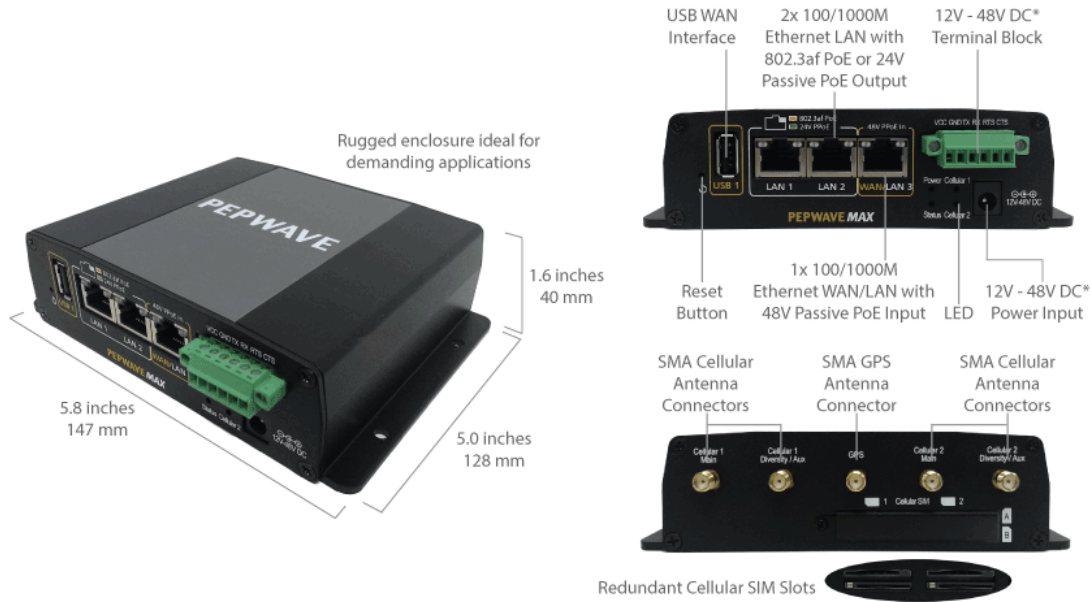
The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

# Pepwave MAX and Surf User Manual

## 4.4 MAX HD2 mini

### 4.4.1 Panel Appearance



\* With 48V DC power, all 3 Ethernet ports can act as 802.3af PoE or 24V Passive PoE outputs



## 4.4.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular WAN Indicators		
<b>Cellular 1 / Cellular 2</b>	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	10 / 100 / 1000 Mbps
	Blinking	Data is transferring
<b>Orange LED</b>	OFF	No data is being transferred or port is not connected
	<b>Port Type</b>	Auto MDI/MDI-X ports

## 4.5 MAX Transit

### 4.5.1 Panel Appearance



### 4.5.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular WAN Indicators		
<b>Cellular 1 / Cellular 2*</b>	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

\* For MAX-TST\_DUO

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	10 / 100 / 1000 Mbps
	Blinking	Data is transferring
<b>Orange LED</b>	OFF	No data is being transferred or port is not connected
	ON	
<b>Port Type</b>	Auto MDI/MDI-X ports	

# Pepwave MAX and Surf User Manual

## 4.6 MAX HD4

### 4.6.1 Panel Appearance



### 4.6.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi AP and Wi-Fi WAN Indicators		
<b>Wi-Fi WAN / Cellular 1 / Cellular 2</b>	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	10 / 100 / 1000 Mbps
	Blinking	Data is transferring
<b>Orange LED</b>	OFF	No data is being transferred or port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

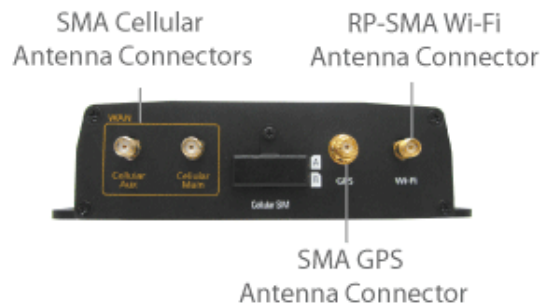
# Pepwave MAX and Surf User Manual

## 4.7 MAX BR1

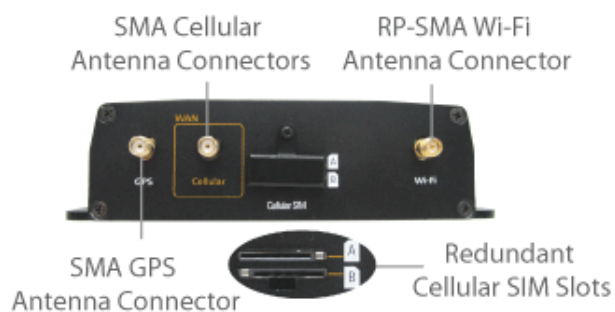
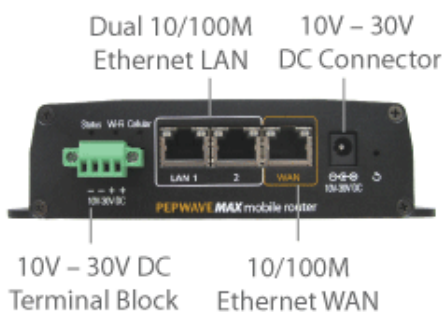
### 4.7.1 Panel Appearance



MAX-BR1-LTE Version



MAX-BR1 Version



### 4.7.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

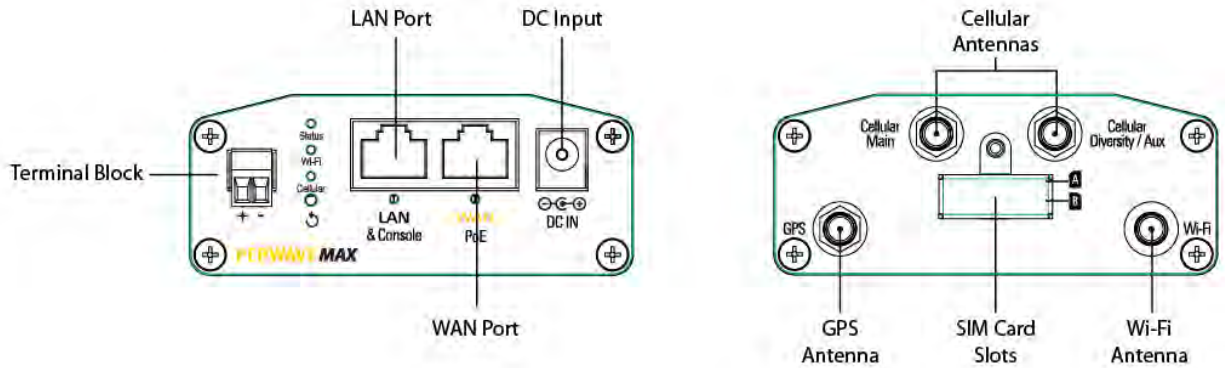
Wi-Fi Indicators		
<b>Wi-Fi</b>	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

Cellular Indicators		
<b>Cellular</b>	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	100 Mbps
	OFF	10 Mbps
<b>Orange LED</b>	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

## 4.8 MAX BR1 Mini

### 4.8.1 Panel Appearance



### 4.8.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

## 4.9 MAX BR1 Slim

### 4.9.1 Panel Appearance



### 4.9.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

•

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	100 Mbps
	OFF	10 Mbps
<b>Orange LED</b>	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

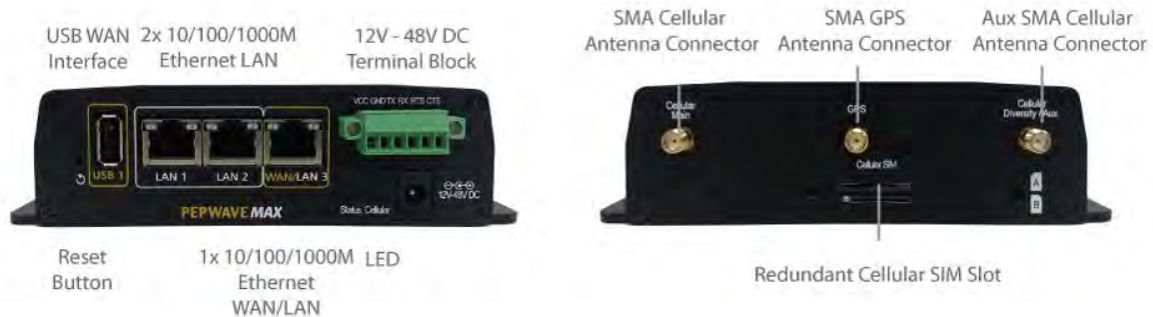
•



# Pepwave MAX and Surf User Manual

## 4.10 MAX BR1 ENT

### 4.10.1 Panel Appearance



### 4.10.2 LED Indicators

- The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

# Pepwave MAX and Surf User Manual

## 4.11 MAX BR1 Pro LTE

### 4.11.1 Panel Appearance



### 4.11.2 LED Indicators

- The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular Indicators		
<b>Cellular</b>	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	100 Mbps
	OFF	10 Mbps
<b>Orange LED</b>	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

# Pepwave MAX and Surf User Manual

## 4.12 MAX BR1/2 IP55

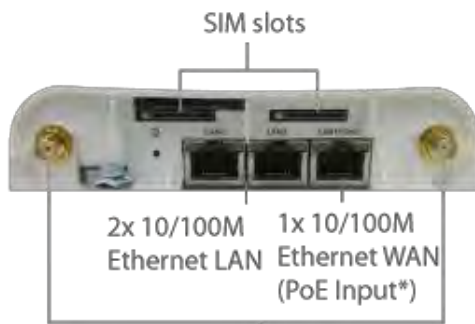
### 4.12.1 Panel Appearance



Built-In, Software-Selectable 10dBi MIMO Directional and 4dBi Omni Wi-Fi antennas



Screw-Holes for Wall Mounting (screws not included)



2 x SMA Cellular Antenna Connectors (optional)

### Accessory – Wall/Pole Mount with Ball Joint for IP55 Outdoor Products ^

Flexible ball joint allows for high-precision installation



To connect to MAX BR1 IP55/BR2 IP55

\* Requires 48V Pepwave Passive PoE input. Available separately. ^ Available separately.

### 4.12.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

# Pepwave MAX and Surf User Manual

Wi-Fi Indicators		
<b>Wi-Fi</b>	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

Cellular Indicators		
<b>Cellular</b>	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	100 Mbps
	OFF	10 Mbps
<b>Orange LED</b>	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

# Pepwave MAX and Surf User Manual

## 4.13 MAX On-The-Go

### 4.13.1 Panel Appearance



### 4.13.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Cellular Indicators		
WAN	OFF	Modem is not attached to the port
	Green	Modem is attached to the port

Wi-Fi Indicators		
Wi-Fi	OFF	Disconnected from AP
	Green	Connected to AP

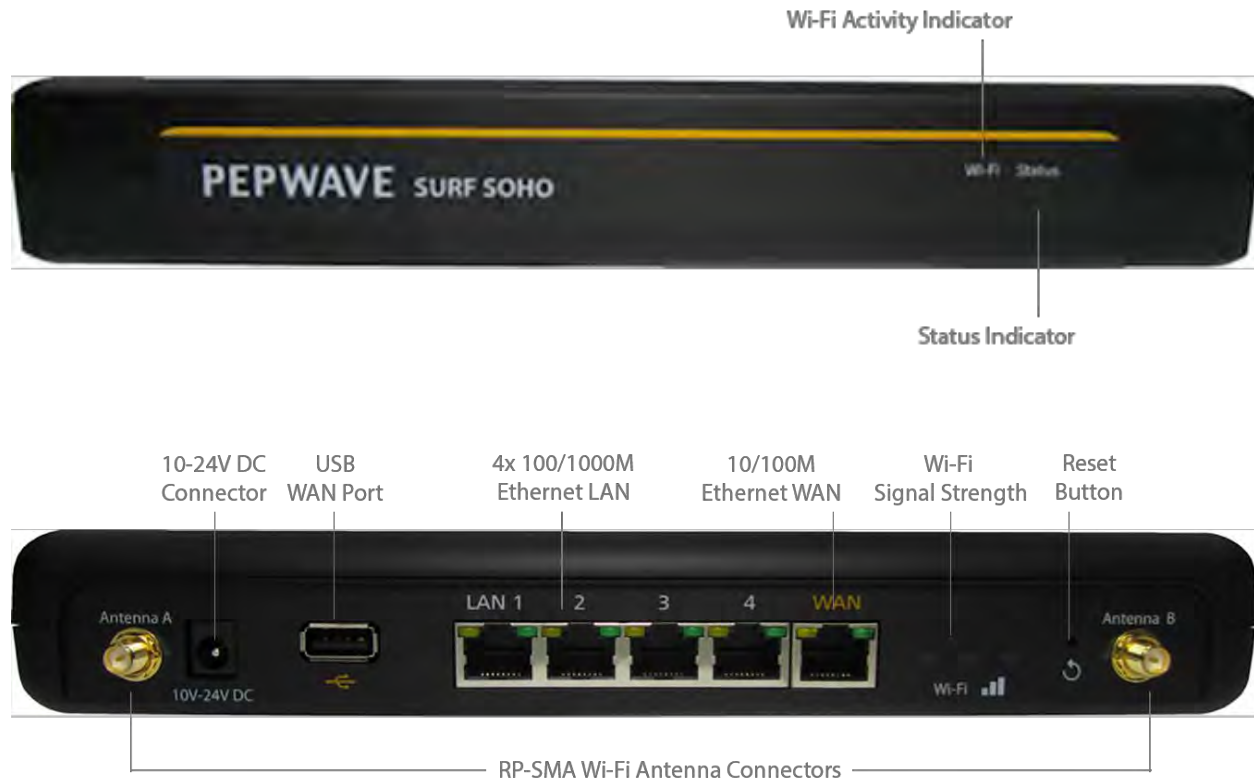
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Green	Ready

LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
Port Type	Auto MDI/MDI-X ports	

# Pepwave MAX and Surf User Manual

## 4.14 Surf SOHO

### 4.14.1 Panel Appearance



### 4.14.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Wi-Fi and Status Indicators		
<b>Wi-Fi</b>	OFF	Disabled Intermittent
	Blinking	Enabled but no client connected
	ON	Client(s) connected to wireless network
	Continuous blinking	Transferring data to wireless network
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Green	Ready state
LAN and Ethernet WAN Ports		
<b>Green LED</b>	ON	10 / 100 Mbps

# Pepwave MAX and Surf User Manual

<b>Orange LED</b>	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
<b>Port type</b>	Auto MDI/MDI-X ports	

Wi-Fi Signal	
Off	No connection
<b>Signal strength</b>	Wi-Fi signal strength (low, medium, and high)

## 5 Advanced Feature Summary

### 5.1 Drop-in Mode and LAN Bypass: Transparent Deployment



As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass** will safely and automatically bypass the Peplink router to resume your original network connection.

Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

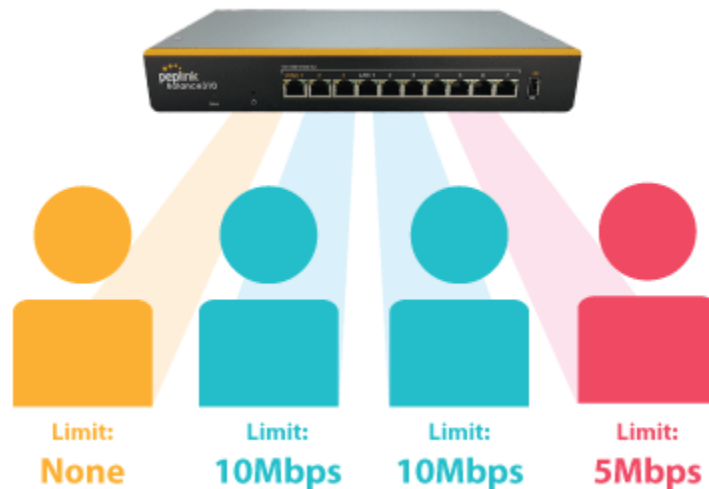
### 5.2 QoS: Clearer VoIP



VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.



## 5.3 Per-User Bandwidth Control



With per-user bandwidth control, you can define bandwidth control policies for up to 3 groups of users to prevent network congestion. Define groups by IP address and subnet, and set bandwidth limits for every user in the group.

## 5.4 High Availability via VRRP



When your organization has a corporate requirement demanding the highest availability with no single point of failure, you can deploy two Peplink routers in **High Availability mode**. With High Availability mode, the second device will take over when needed.

Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

## 5.5 USB Modem and Android Tethering



For increased WAN diversity, plug in a USB LTE modem as backup. Pepwave routers are compatible with over [200 modem types](#). You can also tether to smartphones running Android 4.1.X and above.

Compatible with: MAX 700, HD2 (all variants except IP67), HD4 (All variants)

## 5.6 Built-In Remote User VPN Support



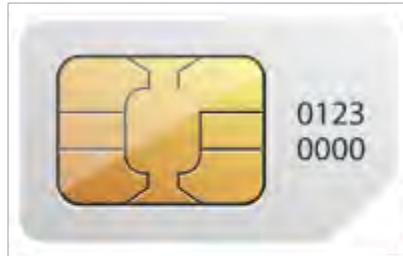
 **L2TP with IPsec and PPTP**



Use L2TP with IPsec to safely and conveniently connect remote clients to your private network. L2TP with IPsec is supported by most devices, but legacy devices can also connect using PPTP.

[Click here for full instructions on setting up L2TP with IPsec.](#)

## 5.7 SIM-card USSD support



Cellular-enabled routers can now use USSD to check their SIM card's balance, process pre-paid cards, and configure carrier-specific services. [Click here for full instructions on using USSD.](#)

## 6 Installation

The following section details connecting Pepwave routers to your network.

### 6.1 Preparation

Before installing your Pepwave router, please prepare the following as appropriate for your installation:

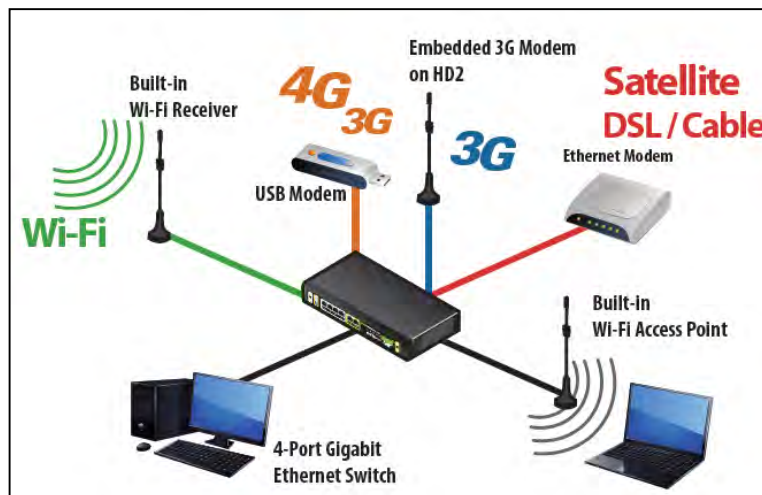
- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
  - **Ethernet WAN:** A 10/100/1000BaseT UTP cable with RJ45 connector
  - **USB:** A USB modem
  - **Embedded modem:** A SIM card for GSM/HSPA service
  - **Wi-Fi WAN:** Wi-Fi antennas
  - **PC Card/Express Card WAN:** A PC Card/ExpressCard for the corresponding card slot
- A computer installed with the TCP/IP network protocol and a supported web browser. Supported browsers include Microsoft Internet Explorer 8.0 or above, Mozilla Firefox 10.0 or above, Apple Safari 5.1 or above, and Google Chrome 18 or above.

## 6.2 Constructing the Network

At a 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 router. 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 to one of the WAN ports on the Pepwave router. Repeat the same procedure for other WAN ports.
3. Connect the power adapter to the power connector on the rear panel of the Pepwave router, and then plug it into a power outlet.

The following figure schematically illustrates the resulting configuration:



## 6.3 Configuring the Network Environment

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

- LAN configuration

For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.

For advanced configuration, go to **Section 9, Configuring the LAN Interface(s)**.

- WAN configuration

For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.

For advanced configuration, go to **Section 9.2, Captive Portal**.

## 7 Mounting the Unit

### 7.1 Wall Mount

The Pepwave MAX 700/HD2/On-The-Go can be wall mounted using screws. After adding the screw on the wall, slide the MAX in the screw hole socket as indicated below. Recommended screw specification: M3.5 x 20mm, head diameter 6mm, head thickness 2.4mm.

The Pepwave MAX BR1 requires four screws for wall mounting.

### 7.2 Car Mount

The Pepwave MAX700/HD2 can be mounted in a vehicle using the included mounting brackets. Place the mounting brackets by the two sides and screw them onto the device.



### 7.3 IP67 Installation Guide

Installation instructions for IP67 devices can be found here:  
[http://download.peplink.com/manual/IP67\\_Installation\\_Guide.pdf](http://download.peplink.com/manual/IP67_Installation_Guide.pdf)

## 8 Connecting to the Web Admin Interface

1. Start a web browser on a computer that is connected with the Pepwave router through the LAN.
2. To connect to the router's web admin interface, enter the following LAN IP address in the address field of the web browser:

http://192.168.50.1

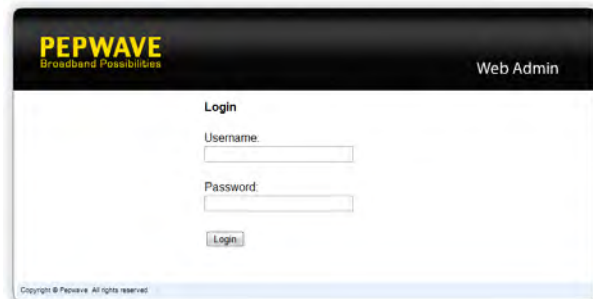
(This is the default LAN IP address for Pepwave routers.)

3. Enter the following to access the web admin interface.

**Username:** admin

**Password:** admin

(This is the default username and password for Pepwave routers. The admin and read-only user passwords can be changed at **System>Admin Security**.)



4. After successful login, the **Dashboard** will be displayed.

WAN Connection Status	
Priority 1 (Highest)	
1 WAN 1	Connected <a href="#">Details</a>
2 WAN 2	Connected <a href="#">Details</a>
Priority 2	
1 Cellular 1	No SIM Card Detected <a href="#">Reload SIM</a> <a href="#">Details</a>
2 Cellular 2	No SIM Card Detected <a href="#">Reload SIM</a> <a href="#">Details</a>
Priority 3	
Drag desired {Priority-3} connections here	
Disabled	
Wi-Fi WAN	Disabled <a href="#">Details</a>

LAN Interface	
Router IP Address: 192.168.50.1	
Wi-Fi AP <span style="float: right;">ON <a href="#">Details</a></span>	
PEPWAVE_8D1C	

Device Information	
Model:	Pepwave MAX HD2
Firmware:	6.2.0 build 2891
Uptime:	1 day 16 hours 35 minutes
CPU Load:	12%
Throughput:	0.0 Mbps ↓ 0.1 Mbps ↑

The **Dashboard** shows current WAN, LAN, and Wi-Fi AP statuses. Here, you can change WAN connection priority and switch on/off the Wi-Fi AP. For further information on setting up these connections, please refer to **Sections 8** and **9**.



**Device Information** displays details about the device, including model name, firmware version, and uptime. For further information, please refer to **Section 22**.


## Important Note

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

## 9 Configuring the LAN Interface(s)

### 9.1 Basic Settings

LAN interface settings are located at **Network>LAN>Basic Settings**.



The screenshot shows the 'IP Settings' configuration panel. It has a title bar with 'IP Settings' and a help icon. Below the title bar, there are two input fields: 'IP Address' with the value '192.168.50.1' and a subnet mask dropdown menu set to '255.255.255.0 (/24)'.

IP Settings	
<b>IP Address</b>	The IP address and subnet mask of the Pepwave router on the LAN.



The screenshot shows the 'Network Settings' configuration panel. It has a title bar with 'Network Settings' and a help icon. Below the title bar, there are four rows of settings: 'Name' with an empty text input field; 'VLAN ID' with an empty text input field; 'Inter-VLAN routing' with a checked checkbox; and 'Captive Portal' with an unchecked checkbox.



Network Settings	
<b>Name</b>	Enter a name for the LAN.
<b>VLAN ID</b>	Enter a number for your VLAN.
<b>Inter-VLAN routing</b>	Check this box to enable routing between virtual LANs.
<b>Captive Portal</b>	Check this box to turn on captive portals.

# Pepwave MAX and Surf User Manual

Drop-In Mode Settings	
Enable	<input checked="" type="checkbox"/>
WAN for Drop-In Mode	WAN 1 ▼
Share Drop-In IP	<input checked="" type="checkbox"/>
Shared IP Address	<input type="text"/> 255.255.255.0 (/24) ▼
WAN Default Gateway	<input type="text"/> <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) <input type="text"/> - <input type="text"/> <input type="button" value="↓"/> <input type="text"/> <input type="button" value="Delete"/>
WAN DNS Servers	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
<p>NOTE: The DHCP Server Settings will be overwritten.</p> <p>The following WAN 1 settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.</p> <p>The PPTP Server will be disabled.</p> <p>Tip: please review the DNS Forwarding setting under the Service Forwarding section.</p>	

Drop-in Mode Settings	
<b>Enable</b>	Drop-in mode eases the installation of Peplink routers on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature, if available on your model.
<b>WAN for Drop-In Mode</b>	Select the WAN port to be used for drop-in mode. If <b>WAN 1 with LAN Bypass</b> is selected, the high availability feature will be disabled automatically.
<b>Share Drop-In IP<sup>A</sup></b>	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Pepwave router will listen for this IP address when WAN hosts access services provided by the Pepwave router (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The Pepwave router will listen for this IP address when LAN hosts access services provided by the Pepwave router (web admin access from the WAN, DNS proxy, etc.).
<b>Shared IP Address<sup>A</sup></b>	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (web admin access from the WAN, DNS server, etc.)
<b>WAN Default Gateway</b>	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, check the <b>I have other host(s) on WAN segment</b> box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
<b>WAN DNS Servers</b>	Enter the selected WAN's corresponding DNS server IP addresses.

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

Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	 Connection 1
Spanning Tree Protocol	<input checked="" type="checkbox"/>
Override IP Address when bridge connected	 <input type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None

Layer 2 PepVPN Bridging	
<b>PepVPN Profiles to Bridge</b>	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
<b>Spanning Tree Protocol</b>	Click the box will enable STP for this layer 2 profile bridge.
<b>Override IP</b>	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.

# Pepwave MAX and Surf User Manual

## Address when bridge connected

If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.

DHCP Server Settings			
DHCP Server	<input checked="" type="checkbox"/>	Enable	
IP Range	<input type="text" value="192.168.50.10"/>	-	<input type="text" value="192.168.50.250"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>	(/24)	
Lease Time	<input type="text" value="1"/>	Days	<input type="text" value="0"/> Hours <input type="text" value="0"/> Mins
DNS Servers	<input checked="" type="checkbox"/>	Assign DNS server automatically	
WINS Server	<input checked="" type="checkbox"/>	Assign WINS server	
	<input checked="" type="radio"/>	Built-in	<input type="radio"/> External
BOOTP	<input checked="" type="checkbox"/>	Server IP Address:	<input type="text"/>
		Boot File:	<input type="text"/>
		Server Name:	<input type="text"/> (Optional)
Extended DHCP Option	<input type="text"/>	Option	Value
		No Extended DHCP Option	
		<input type="button" value="Add"/>	
DHCP Reservation	<input type="text"/>	Name	MAC Address
		Static IP	<input type="text"/>
			<input type="button" value="+"/>

## DHCP Server Settings

### DHCP Server

When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.

### IP Range & Subnet Mask

These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.

### 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 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 DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.

### WINS Server

This option allows you to optionally specify a Windows Internet Name Service (WINS) server. You may choose to use the **built-in WINS server** or **external WINS servers**.

When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP **WINS Server** setting. Afterward, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.

### BOOTP

Check this box to enable BOOTP on older networks that still require it.

### Extended DHCP Option



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, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.

To define an extended DHCP option, click the **Add** button, choose the option to define and

## DHCP Reservation

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 can be defined once only.

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. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.



**Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press  to create a new record. Press  to remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3**.

LAN Physical Settings	
Speed	Auto

## LAN Physical Settings

### Speed



This is the port speed of the LAN interface. It should be set to the same speed as the connected device to avoid port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device. **Auto** is selected by default. You can choose not to advertise the port speed if the port has difficulty negotiating with the peer device.

Static Route Settings			
Static Route		Destination Network	Subnet Mask
			Gateway
		255.255.255.0 (/24)	

## Static Route Settings

### Static Route

This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in *w.x.y.z* format.

The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press  to create a new route. Press  to remove a route.

WINS Server Settings	
Enable	<input type="checkbox"/>

## WINS Server Settings

### Enable

Check the box to enable the WINS server. A list of WINS clients will be displayed at **Status>WINS Clients**.

# Pepwave MAX and Surf User Manual

DNS Proxy Settings		
Enable	<input checked="" type="checkbox"/>	
DNS Caching	<input type="checkbox"/>	
Include Google Public DNS Servers	<input type="checkbox"/>	
Local DNS Records	Host Name	IP Address
	+	
DNS Resolvers	Connection	Current Status
	<input type="checkbox"/> WAN 1	10.88.3.1
	<input type="checkbox"/> WAN 2	
	<input type="checkbox"/> Wi-Fi WAN	
	<input type="checkbox"/> Cellular 1	
	<input type="checkbox"/> Cellular 2	
	<input type="checkbox"/> USB	
Connection	DNS Servers	
<input type="checkbox"/> LAN		
Preferred connections are shown with <input checked="" type="checkbox"/>		

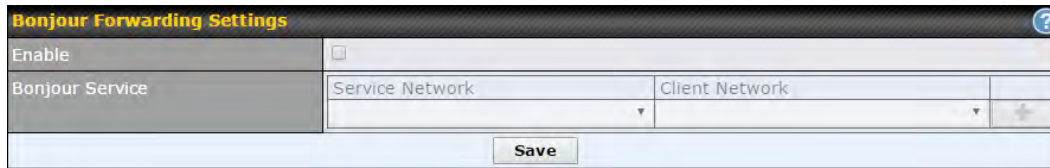
DNS Proxy Settings	
<b>Enable</b>	To enable the DNS proxy feature, check this box, and then set up the feature at <b>Network&gt;LAN&gt;DNS Proxy Settings</b> . A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the <b>DNS servers/resolvers</b> defined for each WAN connection.
<b>DNS Caching</b>	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 DNS lookup time. However, it cannot return the most up-to-date result for those frequently updated DNS records. By default, <b>DNS Caching</b> is disabled.
<b>Include Google Public DNS Servers</b>	When this option is <b>enabled</b> , the DNS proxy server will also forward DNS requests to Google's Public DNS Servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
<b>Local DNS Records</b>	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Pepwave router, the corresponding IP address will be returned. Press <input type="button" value="+"/> to create a new record. Press <input type="button" value="X"/> to remove a record.
<b>DNS Resolvers <sup>A</sup></b>	Check the box to enable the WINS server. A list of WINS clients will be displayed at <b>Network&gt;LAN&gt;DNS Proxy Settings&gt;DNS Resolvers</b> . This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

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



Finally, if needed, configure Bonjour forwarding, Apple's zero configuration networking

# Pepwave MAX and Surf User Manual

protocol. Once VLAN configuration is complete, click **Save** to store your changes.




The screenshot shows a web interface titled "Bonjour Forwarding Settings" with a help icon in the top right. It contains an "Enable" checkbox, a "Bonjour Service" section with two dropdown menus labeled "Service Network" and "Client Network", and a "Save" button at the bottom.

Bonjour Forwarding Settings	
<b>Enable</b>	Check this box to turn on Bonjour forwarding.
<b>Bonjour Service</b>	Choose <b>Service</b> and <b>Client</b> networks from the drop-down menus, and then click  to add the networks. To delete an existing Bonjour listing, click  .



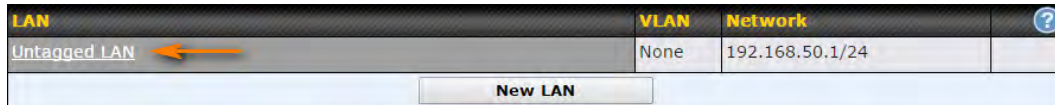
# Pepwave MAX and Surf User Manual

To enable VLAN configuration, click the  button in the **IP Settings** section.



The IP Settings form shows a header with the title "IP Settings" and a help icon. Below the header, there are two input fields: "IP Address" with the value "192.168.50.1" and a subnet mask dropdown menu showing "255.255.255.0 (/24)".

To add a new LAN, click the **New LAN** button. To change LAN settings, click the name of the LAN to change under the **LAN** heading.



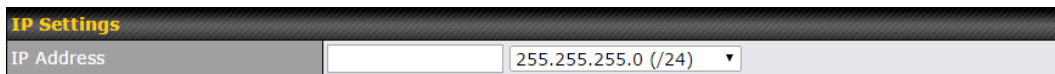
LAN	VLAN	Network	
Untagged LAN	None	192.168.50.1/24	

Below the table is a "New LAN" button. An orange arrow points to the "Untagged LAN" entry in the table.

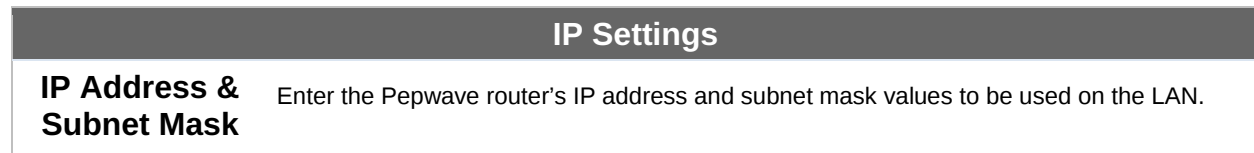
The following settings are displayed when creating a new LAN or editing an existing LAN.



A dark grey header bar with the word "LAN" in yellow text on the left and a close button (X) on the right.



The IP Settings form is shown again, with the "IP Address" field empty and the subnet mask dropdown menu set to "255.255.255.0 (/24)".



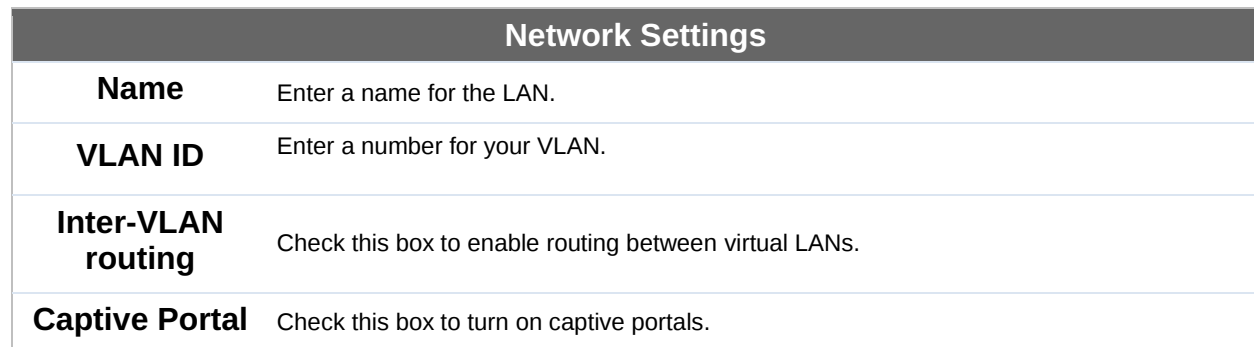
**IP Settings**

**IP Address & Subnet Mask** Enter the Pepwave router's IP address and subnet mask values to be used on the LAN.



The Network Settings form has a header with the title "Network Settings" and a help icon. It contains four rows of settings:



Name	<input type="text"/>
VLAN ID	<input type="text"/>
Inter-VLAN routing	<input checked="" type="checkbox"/>
Captive Portal	<input type="checkbox"/>






**Network Settings**


<b>Name</b>	Enter a name for the LAN.
<b>VLAN ID</b>	Enter a number for your VLAN.
<b>Inter-VLAN routing</b>	Check this box to enable routing between virtual LANs.
<b>Captive Portal</b>	Check this box to turn on captive portals.

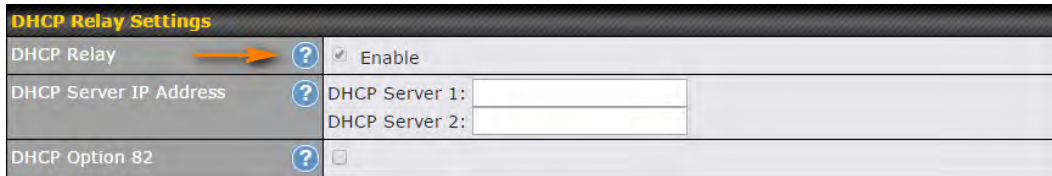
# Pepwave MAX and Surf User Manual

DHCP Server Settings			
DHCP Server		<input checked="" type="checkbox"/> Enable	
IP Range		-	255.255.255.0 (/24) ▼
Lease Time	1	Days	0 Hours 0 Mins
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically		
WINS Servers	<input type="checkbox"/> Assign WINS server		
BOOTP	<input type="checkbox"/>		
Extended DHCP Option	Option	Value	
	<i>No Extended DHCP Option</i>		
	<input type="button" value="Add"/>		
DHCP Reservation		Name	MAC Address
			Static IP
<input type="button" value="+"/>			

DHCP Server Settings	
<b>DHCP Server</b>	<p>When this setting is enabled, the Pepwave router's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collisions on the LAN.</p> <p>To enable DHCP bridge relay, please click the  icon on this menu item.</p>
<b>IP Range &amp; Subnet Mask</b>	These settings allocate a range of IP address that will be assigned to LAN computers by the Pepwave router's DHCP server.
<b>Lease Time</b>	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of <b>Lease Time</b> , the assigned IP address will no longer be valid and the IP address assignment must be renewed.
<b>DNS Servers</b>	This option allows you to input the DNS server addresses to be offered to DHCP clients. If <b>Assign DNS server automatically</b> is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
<b>WINS Servers</b>	This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their <b>DHCP WINS Servers</b> setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at <b>Status&gt;WINS Clients</b> .
<b>BOOTP</b>	Check this box to enable BOOTP on older networks that still require it.
<b>Extended DHCP Option</b>	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, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the <b>Add</b> button, choose the option to define, and then 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 can be defined once only.
<b>DHCP Reservation</b>	<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. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p><b>Name</b> (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of <b>00:AA:BB:CC:DD:EE</b>. Press  to create a new record. Press  to remove a record. Reserved clients information can be imported from the <b>Client List</b>, located at <b>Status&gt;Client List</b>. For more details, please refer to <b>Section</b></p>


## 22.3.

To configure DHCP relay, first click the  button found next to the **DHCP Server** option to display the settings.



The screenshot shows the 'DHCP Relay Settings' configuration window. It has a title bar 'DHCP Relay Settings' and three rows of settings:

DHCP Relay Settings	
DHCP Relay	<input checked="" type="checkbox"/> Enable
DHCP Server IP Address	DHCP Server 1: <input type="text"/> DHCP Server 2: <input type="text"/>
DHCP Option 82	<input type="checkbox"/>

DHCP Relay Settings	
<b>Enable</b>	Check this box to turn on DHCP relay. Click the  icon to disable DHCP relay.
<b>DHCP Server IP Address</b>	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in <b>DHCP Server 1</b> and <b>DHCP Server 2</b> .
<b>DHCP Option 82</b>	DCHP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device's MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.

Once DHCP is set up, configure **LAN Physical Settings**, **Static Route Settings**, **WINS Server Settings**, and **DNS Proxy Settings** as noted above.



## 9.2 Captive Portal





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

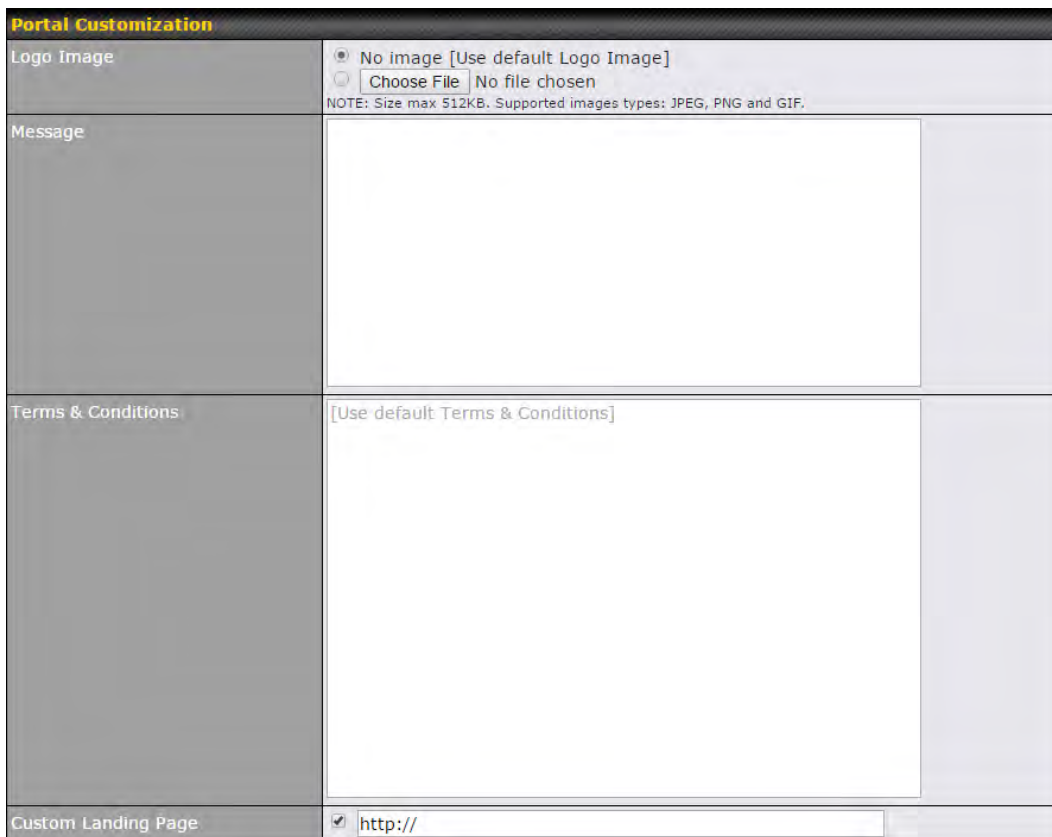
Captive Portal Settings	
Enable	<input checked="" type="checkbox"/> Untagged LAN
Hostname	<input type="text" value="captive-portal.peplink.com"/> <input type="button" value="Default"/>
Access Mode	<input checked="" type="radio"/> Open Access <input type="radio"/> User Authentication
Access Quota	30 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	<input checked="" type="radio"/> Daily at 00 :00 <input type="radio"/> 1440 minutes after quota reached
Allowed Networks	<input type="text" value="Domain Name / IP Address"/> <input type="button" value="+"/>
Allowed Clients	<input type="text" value="MAC / IP Address"/> <input type="button" value="+"/>
Splash Page	<input checked="" type="radio"/> Built-in <input type="radio"/> External, URL: <input type="text" value="http://"/>

Captive Portal Settings															
<b>Enable</b>	Check <b>Enable</b> and then, optionally, select the LANs/VLANs that will use the captive portal.														
<b>Hostname</b>	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click <b>Default</b> .														
<b>Access Mode</b>	Click <b>Open Access</b> to allow clients to freely access your router. Click <b>User Authentication</b> to force your clients to authenticate before accessing your router.														
<b>RADIUS Server</b>	<p>This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:</p> <table border="1"> <tbody> <tr> <td>Authentication</td> <td>RADIUS Server</td> </tr> <tr> <td>Auth Server</td> <td><input type="text"/> Port 1812 <input type="button" value="Default"/></td> </tr> <tr> <td>Auth Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>CoA-DM</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Accounting Server</td> <td><input type="text"/> Port 1813 <input type="button" value="Default"/></td> </tr> <tr> <td>Accounting Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Accounting Interim Interval</td> <td><input type="text"/> seconds</td> </tr> </tbody> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	RADIUS Server	Auth Server	<input type="text"/> Port 1812 <input type="button" value="Default"/>	Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	CoA-DM	<input type="checkbox"/>	Accounting Server	<input type="text"/> Port 1813 <input type="button" value="Default"/>	Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	Accounting Interim Interval	<input type="text"/> seconds
Authentication	RADIUS Server														
Auth Server	<input type="text"/> Port 1812 <input type="button" value="Default"/>														
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters														
CoA-DM	<input type="checkbox"/>														
Accounting Server	<input type="text"/> Port 1813 <input type="button" value="Default"/>														
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters														
Accounting Interim Interval	<input type="text"/> seconds														
<b>LDAP Server</b>	<p>This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:</p> <table border="1"> <tbody> <tr> <td>Authentication</td> <td>LDAP Server</td> </tr> <tr> <td>LDAP Server</td> <td><input type="text"/> Port 389 <input type="button" value="Default"/></td> </tr> <tr> <td></td> <td><input type="checkbox"/> Use DN/Password to bind to LDAP Server</td> </tr> <tr> <td>Base DN</td> <td><input type="text"/></td> </tr> <tr> <td>Base Filter</td> <td><input type="text"/></td> </tr> </tbody> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	LDAP Server	LDAP Server	<input type="text"/> Port 389 <input type="button" value="Default"/>		<input type="checkbox"/> Use DN/Password to bind to LDAP Server	Base DN	<input type="text"/>	Base Filter	<input type="text"/>				
Authentication	LDAP Server														
LDAP Server	<input type="text"/> Port 389 <input type="button" value="Default"/>														
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server														
Base DN	<input type="text"/>														
Base Filter	<input type="text"/>														

# Pepwave MAX and Surf User Manual

<b>Access Quota</b>	Set a time and data cap to each user's Internet usage.
<b>Quota Reset Time</b>	This menu determines how your usage quota resets. Setting it to <b>Daily</b> will reset it at a specified time every day. Setting a number of <b>minutes after quota reached</b> establish a timer for each user that begins after the quota has been reached.
<b>Allowed Networks</b>	To whitelist a network, enter the domain name / IP address here and click  . To delete an existing network from the list of allowed networks, click the  button next to the listing.
<b>Splash Page</b>	Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define.

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



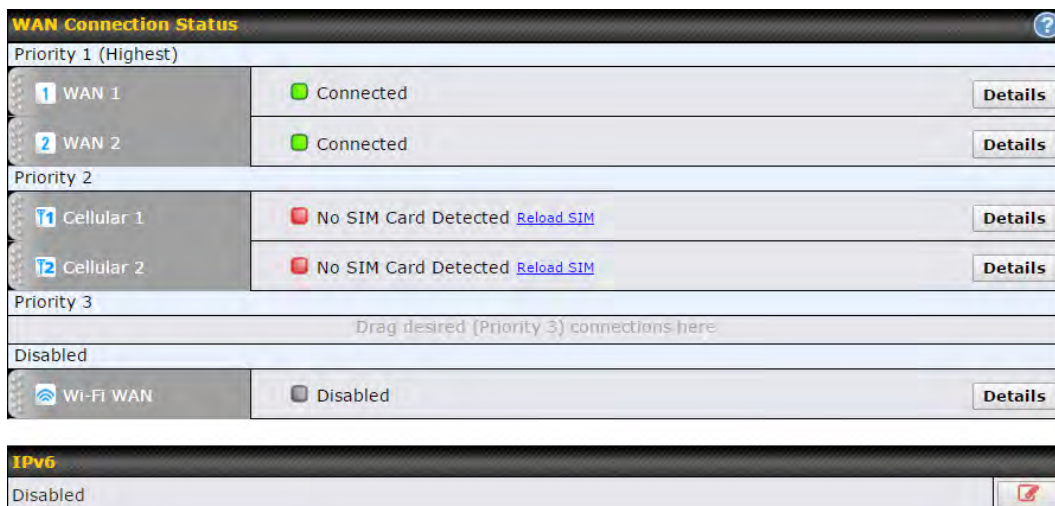
The screenshot shows the 'Portal Customization' interface. It has a dark header with the title 'Portal Customization'. Below the header, there are four main sections:

- Logo Image:** Contains two radio buttons. The first is 'No image [Use default Logo Image]' and the second is 'Choose File' with a text input field containing 'No file chosen'. Below this is a note: 'NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.'
- Message:** A large empty text area for entering a custom message.
- Terms & Conditions:** A large empty text area with the placeholder text '[Use default Terms & Conditions]'.
- Custom Landing Page:** A checkbox that is checked, followed by a text input field containing 'http://'.

Portal Customization	
<b>Logo Image</b>	Click the <b>Choose File</b> button to select a logo to use for the built-in portal.
<b>Message</b>	If you have any additional messages for your users, enter them in this field.
<b>Terms &amp; Conditions</b>	If you would like to use your own set of terms and conditions, please enter them here. If left empty, the built-in portal will display the default terms and conditions.
<b>Custom Landing Page</b>	Fill in this field to redirect clients to an external URL.

## 10 Configuring the WAN Interface(s)

WAN Interface settings are located at **Network>WAN**. To reorder WAN priority, 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, drag on the appropriate WAN by holding the left mouse button, move it the **Disabled** row, and drop it by releasing the mouse button. You can also set priorities on the **Dashboard**. Click the **Details** button in the corresponding row to modify the connection setting.

### Important Note

Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.



## 10.1 Ethernet WAN

From **Network>WAN**, choose a WAN connection and then click **Details**.

WAN Port	
WAN Connection Name	WAN 1 <span style="float: right;">Default</span>
Schedule	Always on ▼
Connection Method	<span>?</span> DHCP ▼
Routing Mode	<span>?</span> <input checked="" type="radio"/> NAT
IP Address	10.10.12.49
Subnet Mask	255.255.0.0
Default Gateway	10.10.10.1
Uptime	1795 mins
Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 10.10.10.1 <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

WAN Port (Section 1)	
<b>WAN Connection Name</b>	Enter a name to represent this WAN connection.
<b>Schedule</b>	Click the drop-down menu to apply a time schedule to this interface
<b>Connection Method</b>	<p>There are three possible connection methods for Ethernet WAN:</p> <ul style="list-style-type: none"> <li>• DHCP</li> <li>• Static IP</li> <li>• PPPoE</li> </ul> <p>The connection method and details are determined by, and can be obtained from, the ISP. See the following sections for details on each connection method.</p>
<b>Routing Mode</b>	This field shows that <b>NAT</b> (network address translation) will be applied to the traffic routed over this WAN connection. <b>IP Forwarding</b> is available when you click the link in the help text.
<b>IP Address/Subnet Mask/Default Gateway</b>	Enter the WAN IP address and subnet mask, as well as the IP address of the default gateway, in these fields.

# Pepwave MAX and Surf User Manual

**Hostname** Enter a hostname for this WAN port if needed.

**DNS Servers** Select a DNS server for this port to use. This port can either be automatically selected or manually designated.

Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Upstream Bandwidth	1 Gbps
Downstream Bandwidth	1 Gbps
Health Check Settings	
Health Check Method	PING
PING Hosts	Host 1: 8.8.8.8 Host 2: <input type="checkbox"/> Use first two DNS servers as PING Hosts
Timeout	5 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Recovery Retries	3

## WAN Port (Section 2)

**Standby State** This setting specifies the standby state of the WAN connection. The available options are **Remain connected** and **Disconnect**. The default state is **Remain Connected**.

**Upstream Bandwidth** This setting specifies the data bandwidth in the outbound direction from the LAN through the WAN interface.

**Downstream Bandwidth** This setting specifies the data bandwidth in the inbound direction from the WAN interface to the LAN. This value is referenced as the default weight value when using the algorithm **Least Used** or the algorithm **Persistence (Auto)** in outbound policy with **Managed by Custom Rules** chosen (see **Section 15.2**).

**Health Check Method** This setting specifies the health check method for the WAN connection. The value of method can be configured as **Disabled**, **Ping**, **DNS Lookup**, or **HTTP**. The default method is **Disabled**. See **Section 10.4** for configuration details.

These fields are for specifying the target DNS servers where DNS lookups will be sent to for health check.

**PING Hosts** If the box **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking the connection healthiness. If the box is not checked, the field **Host 1** must be filled and the field **Host 2** is optional.

The connection is considered to be up if DNS responses are received from any one of the



	health check DNS servers, regardless of whether the result is positive or negative.
<b>Timeout</b>	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
<b>Health Check Interval</b>	This is the number of consecutive check failures before treating a connection as down.
<b>Health Check Retries</b>	This is the number of consecutive check failures before treating a connection as down.
<b>Recovery Retries</b>	This is the number of responses required after a health check failure before treating a connection as up again.

Dynamic DNS Service Provider	<input type="text" value="Disabled"/>
Bandwidth Allowance Monitor	<input type="checkbox"/> Enable
Port Speed	<input type="text" value="Auto"/>
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: <input type="text" value="1440"/> <input type="button" value="Default"/>

## WAN Port (Section 3)

<b>Dynamic DNS Service Provider</b>	<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"> <li>• changeip.com</li> <li>• dyndns.org</li> <li>• no-ip.org</li> <li>• tzo.com</li> <li>• DNS-O-Matic</li> </ul> <p>Select <b>Disabled</b> to disable this feature. See <b>Section 9.5</b> for configuration details.</p>
<b>Bandwidth Allowance Monitor</b>	<p>This option enables bandwidth usage monitoring on this WAN connection for each billing cycle. When this setting is not enabled, each month's bandwidth usage is tracked, but no action will be taken.</p>
<b>Port Speed</b>	<p>This setting specifies port speed and duplex configurations of the WAN port. By default, <b>Auto</b> is selected and the appropriate data speed is automatically detected by the Pepwave router. In the event of negotiation issues, the port speed can be manually specified. You can also choose whether or not to advertise the speed to the peer by selecting the <b>Advertise Speed</b> checkbox.</p>
<b>MTU</b>	<p>This setting specifies the maximum transmission unit. By default, MTU is set to <b>Custom 1440</b>. You may adjust the MTU value by editing the text field. Click <b>Default</b> to restore the</p>

# Pepwave MAX and Surf User Manual

default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. Auto-detection will run each time the WAN connection establishes.

MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom Value: <input type="text"/>
MAC Address Clone	<input type="text" value="00"/> : <input type="text" value="1A"/> : <input type="text" value="DD"/> : <input type="text" value="BD"/> : <input type="text" value="54"/> : <input type="text" value="41"/> <input type="button" value="Default"/>
VLAN	<input checked="" type="checkbox"/> VLAN ID: <input type="text"/>
Reply to ICMP PING	<input checked="" type="radio"/> Yes <input type="radio"/> No
Additional Public IP Address	IP Address <input type="text"/>
	Subnet Mask <input type="text" value="255.255.255.0 (/24)"/> <input type="button" value="↓"/>
	<input type="button" value="Delete"/>

## WAN Port (Section 4)

### MSS

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. If MTU is set to **Auto**, the MSS will also be set automatically. By default, MSS is set to **Auto**.

### MAC Address Clone

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 MAC address via this field. The default MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking **Default** restores the MAC address to the default value.

### VLAN

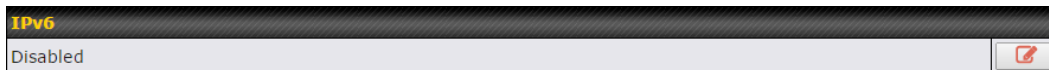
Click the square if you wish to enable VLAN functionality and enable multiple broadcast domains. Once you enable VLAN, you will be able to enter a name for your network.

### Reply to ICMP PING

If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this is **enabled**.

### Additional Public IP Address

The **IP Address** list represents the list of fixed Internet IP addresses assigned by the ISP, in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address** List.



IPv6	
<b>IPv6</b>	<p>IPv6 support can be enabled on one of the available Ethernet WAN ports. On this screen, you can choose which WAN will support IPv6. To enable IPv6 support on a WAN, the WAN router must respond to stateless address auto configuration advertisements and DHCPv6 requests. IPv6 clients on the LAN will acquire their IPv6, gateway, and DNS server addresses from it. The device will also acquire an IPv6 address for performing ping/traceroute checks and accepting web admin accesses. Note: This feature is only available on the Pepwave MAX 700, HD2, and HD2 IP67.</p>

## 10.1.1 DHCP Connection

There are four possible connection methods:

1. DHCP
2. Static IP
3. PPPoE
4. L2TP

The DHCP connection method is suitable if the ISP provides an IP address automatically using DHCP (e.g., satellite modem, WiMAX modem, cable, Metro Ethernet, etc.).



Connection Method	DHCP
Routing Mode	<input checked="" type="radio"/> NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 10.88.3.1 <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

DHCP Connection Settings	
<b>Routing Mode</b>	<p>NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the <b>IP Forwarding</b> option, if your network requires it.</p>

<b>IP Address/ Subnet Mask/ Default Gateway</b>	This information is obtained from the ISP automatically.
<b>Hostname (Optional)</b>	If your service provider's DHCP server requires you to supply a hostname 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.  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.
<b>DNS Servers</b>	Selecting <b>Obtain DNS server address automatically</b> results in the DNS servers being 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.)  When <b>Use the following DNS server address(es)</b> is selected, you may enter custom DNS server addresses for this WAN connection into the <b>DNS Server 1</b> and <b>DNS Server 2</b> fields.

## 10.1.2 Static IP Connection

The static IP connection method is suitable if your ISP provides a static IP address to connect directly.

Connection Method	 Static IP ▾
Routing Mode	 <input checked="" type="radio"/> NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
IP Address	<input type="text"/>
Subnet Mask	255.255.255.0 (/24) ▾
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

#### Routing Mode

NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.

#### IP Address / Subnet Mask / Default Gateway

These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.

#### DNS Servers

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. Selecting **Obtain DNS server address automatically** results in the DNS servers being 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.) When **Use the following DNS server address(es)** is

# Pepwave MAX and Surf User Manual

selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

## 10.1.3 PPPoE Connection

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

Connection Method	<input type="button" value="?"/> PPPoE
Routing Mode	<input type="button" value="?"/> <input checked="" type="radio"/> NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
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 is provided by ISP
IP Address (Optional)	<input type="text"/> Leave it blank unless it is provided by ISP
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 10.88.3.1 <input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

### PPPoE Settings

#### Routing Mode

NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.

#### 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 (Optional)

Service name is provided by the ISP.

**Note: Leave this field blank unless it is provided by your ISP.**

#### IP Address (Optional)

If your ISP provides a PPPoE IP address, enter it here.

**Note: Leave this field blank unless it is provided by your ISP.**

#### DNS Servers

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. Selecting **Obtain DNS server address automatically** results

# Pepwave MAX and Surf User Manual

in the DNS servers being 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.) 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.

## 10.1.4 L2TP Connection

L2TP has all the compatibility and convenience of PPTP with greater security. Combine this with IPsec for a good balance between ease of use and security.

Connection Method	<input type="text" value="L2TP"/>
Routing Mode	<input checked="" type="radio"/> NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
L2TP User Name	<input type="text"/>
L2TP Password	<input type="text"/>
Confirm L2TP Password	<input type="text"/>
Server IP Address / Host	<input type="text"/>
Address Type	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 10.88.3.1 <input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

### L2TP Settings

#### L2TP User Name / Password

Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.

#### Confirm L2TP Password

Verify your password by entering it again in this field.

#### Server IP Address / Host

L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.

#### Address Type

Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.

#### DNS Servers

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.

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.)



# Pepwave MAX and Surf User Manual

When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

## 10.2 Cellular WAN



To access cellular WAN settings, click **Network>WAN>Details**.  
(Available on the Pepwave MAX BR1, HD2, and HD2 IP67 only)


### Connection Details

Cellular 1 Status	
IMSI	(No SIM Card Detected)
MEID	A100001F7DC038 270113180708241208
ESN	8052FC8A
IMEI	356144040031862

Cellular Status	
<b>IMSI</b>	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
<b>MEID</b>	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
<b>ESN</b>	This serves the same purpose as MEID HEX but uses an older format.
<b>IMEI</b>	This is the unique ID for identifying the modem in GSM/HSPA mode.






# Pepwave MAX and Surf User Manual

WAN Connection Settings	
WAN Connection Name	Cellular 2 <span style="float: right;">Default</span>
Schedule	Always on ▼
Network Mode	<input checked="" type="radio"/> HSPA <input type="radio"/> Sprint,EV-DO <input type="radio"/> Verizon Wireless,EV-DO
Subnet Selection	<input checked="" type="radio"/> Auto
Routing Mode	<input checked="" type="radio"/> NAT
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

WAN Connection Settings	
<b>WAN Connection Name</b>	Enter a name to represent this WAN connection.
<b>Schedule</b>	Click the drop-down menu to apply a time schedule to this interface if needed.
<b>Network Mode</b>	Users have to specify the network they are on accordingly.
<b>Subnet Selection</b>	Auto: The subnet mask will be set automatically.  Force /31 Subnet: The subnet mask will be set as 255.255.255.254(/31), and the gateway IP address will be recalculated.
<b>Routing Mode</b>	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either <b>NAT</b> (network address translation) or <b>IP Forwarding</b> . Click the  button to enable IP forwarding.
<b>DNS Servers</b>	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.  Selecting <b>Obtain DNS server address automatically</b> 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.)  When <b>Use the following DNS server address(es)</b> is selected, you can enter custom DNS server addresses for this WAN connection into the <b>DNS server 1</b> and <b>DNS server 2</b> fields.




# Pepwave MAX and Surf User Manual


Cellular Settings	
Network Selection	 <input checked="" type="radio"/> Auto <input type="radio"/> Manual
3G/2G	 Auto ▾
Authentication	Auto ▾
Band Selection	<input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (800 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (850 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (900 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (1700 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (1900 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (2100 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (850 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (900 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (1800 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (1900 MHz)
Data Roaming	<input type="checkbox"/>
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
SIM PIN (Optional)	 <input type="text"/>
Bandwidth Allowance Monitor	 <input checked="" type="checkbox"/> Enable
Action	 <input type="checkbox"/> Disconnect when usage hits 100% <small>Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling <a href="#">Email Notification</a>.</small>
Start Day	On 1st ▾ of each month
Monthly Allowance	<input type="text"/> GB ▾

## Cellular Settings

### Network Selection

By default, the MAX router will automatically choose a network to connect to. If you wish to use only certain networks, click the  button beside the menu item.

### 3G/2G

This drop-down menu allows restricting cellular to particular band. Click the  button to enable the selection of specific bands.

### Authentication

Choose from **PAP Only** or **CHAP Only** to use those authentication methods exclusively. Select **Auto** to automatically choose an authentication method.

### Data Roaming

This checkbox enables data roaming on this particular SIM card. Please check your service provider's data roaming policy before proceeding.

# Pepwave MAX and Surf User Manual

<b>Operator Settings</b>	This setting applies to 3G/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems. This allows you to configure the APN settings of your connection. If <b>Auto</b> is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select <b>Custom</b> to enter your carrier's <b>APN, Login, Password, and Dial Number</b> settings manually. The correct values can be obtained from your carrier. The default and recommended setting is <b>Auto</b> .
<b>APN / Login / Password / SIM PIN</b>	When <b>Auto</b> is selected, the information in these fields will be filled automatically. Select <b>Custom</b> to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
<b>Bandwidth Allowance Monitor</b>	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
<b>Action</b>	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If <b>Disconnect when usage hits 100% of monthly allowance</b> 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.
<b>Start Day</b>	This option allows you to define which day of the month each billing cycle begins.
<b>Monthly Allowance</b>	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

General Settings	
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected
Idle Disconnect	<input checked="" type="checkbox"/> 3 minutes Time value is global. A change will affect all WAN profiles.

General Settings	
<b>Standby State</b>	This option allows you to choose whether to remain connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When <b>Remain connected</b> is chosen, bringing up this WAN connection to active makes it immediately available for use.
<b>Idle Disconnect</b>	When Internet traffic is not detected within the user-specified timeframe, the modem will automatically disconnect. Once the traffic is resumed by the LAN host, the connection will be re-activated.

Health Check Settings	
Health Check Method	<input type="text" value="SmartCheck"/>
Timeout	<input type="text" value="5"/> second(s)
Health Check Interval	<input type="text" value="10"/> second(s)
Health Check Retries	<input type="text" value="3"/>
Recovery Retries	<input type="text" value="3"/>

## Health Check Settings

<b>Health Check Method</b>	This setting allows you to specify the health check method for the cellular connection. Available options are <b>Disabled</b> , <b>Ping</b> , <b>DNS Lookup</b> , <b>HTTP</b> , and <b>SmartCheck</b> . The default method is <b>DNS Lookup</b> . See <b>Section 10.4</b> for configuration details.
<b>Timeout</b>	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
<b>Health Check Interval</b>	This is the time interval between each health check test.
<b>Health Check Retries</b>	This is the number of consecutive check failures before treating a connection as down.
<b>Recovery Retries</b>	This is the number of responses required after a health check failure before treating a connection as up again.

Dynamic DNS Settings	
Dynamic DNS Service Provider	<input type="text" value="Disabled"/>

## Dynamic DNS Settings

<b>Dynamic DNS Service Provider</b>	<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"><li>• changeip.com</li><li>• dyndns.org</li><li>• no-ip.org</li><li>• tzo.com</li><li>• DNS-O-Matic</li></ul> <p>Select <b>Disabled</b> to disable this feature. See <b>Section 9.5</b> for configuration details.</p>
-------------------------------------	--

## 10.3 Wi-Fi WAN

To access Wi-Fi WAN settings, click **Network>WAN>Details**.

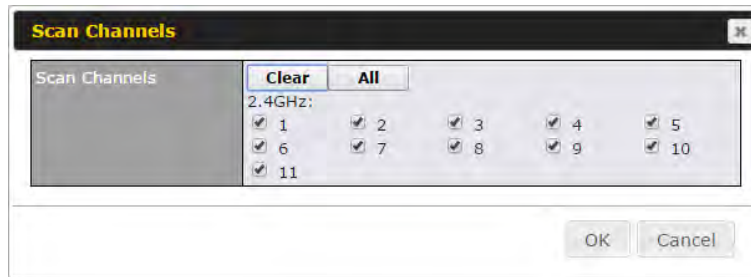
WAN Connection Settings	
WAN Connection Name	Wi-Fi WAN <span>Default</span>
Schedule	Always on ▼
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: 1500 <span>Default</span>
Reply to ICMP PING	<input checked="" type="radio"/> Yes <input type="radio"/> No

Wi-Fi Connection Settings	
<b>WAN Connection Name</b>	Enter a name to represent this WAN connection.
<b>Schedule</b>	Click the drop-down menu to apply a time schedule to this interface.
<b>Standby State</b>	This setting specifies the state of the WAN connection while in standby. The available options are <b>Remain Connected</b> (hot standby) and <b>Disconnect</b> (cold standby).
<b>MTU</b>	This setting specifies the maximum transmission unit. By default, MTU is set to <b>Custom 1440</b> . You may adjust the MTU value by editing the text field. Click <b>Default</b> to restore the default MTU value. Select <b>Auto</b> and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes
<b>Reply to ICMP PING</b>	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

Wi-Fi WAN Settings	
Channel Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
Roaming	<input type="checkbox"/>
Connect to Any Open Mode AP	<input type="radio"/> Yes <input checked="" type="radio"/> No



Wi-Fi WAN Settings	
<b>Channel Selection</b>	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:

# Pepwave MAX and Surf User Manual



**Roaming**      Checking this box will enable Wi-Fi roaming. Click the  icon for additional options.

**Connect to Any Open Mode AP**      This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.

Bandwidth Allowance Monitor	
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 <a href="#">Email Notification</a> . <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"/> MB

## Bandwidth Allowance Monitor

**Action**      If **Error! Reference source not found.** is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance.

If **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.

**Start Day**      This option allows you to define which day of the month each billing cycle begins.

**Monthly Allowance**      This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

# Pepwave MAX and Surf User Manual

Health Check Settings	
Health Check Method	<input type="text" value="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 <input type="checkbox"/> Include public DNS servers
Timeout	<input type="text" value="5"/> second(s)
Health Check Interval	<input type="text" value="5"/> second(s)
Health Check Retries	<input type="text" value="3"/>
Recovery Retries	<input type="text" value="3"/>

## Health Check Settings

### Method

This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

### Health Check Disabled

Health Check Settings	
Health Check Method	<input type="text" value="Disabled"/> <small>Health Check disabled. Network problem cannot be detected.</small>

When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

### Health Check Method: PING

Health Check Method	<input type="text" value="PING"/>
PING Hosts	Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

### PING Hosts

This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. 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. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

### Health Check Method: DNS Lookup

Health Check Method	<input type="text" value="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 <input type="checkbox"/> Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.



## Health Check DNS Servers

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

If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

### Health Check Method: HTTP

Health Check Method	<input type="text" value="HTTP"/>
URL 1	<input type="text" value="http://"/> Matching String: <input type="checkbox"/>
URL 2	<input type="text" value="http://"/> Matching String: <input type="checkbox"/>

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

## URL1





### WAN Settings>WAN Edit>Health Check Settings>URL1


The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

## URL 2

### WAN Settings>WAN Edit>Health Check Settings>URL2

If **URL2** is also provided, a health check will pass if either one of the tests passed.

Other Health Check Settings	
Timeout	 5 second(s)
Health Check Interval	 5 second(s)
Health Check Retries	 3
Recovery Retries	 3
<b>Timeout</b>	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is <b>5 seconds</b> .
<b>Health Check Interval</b>	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is <b>5 seconds</b> .
<b>Health Check Retries</b>	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to <b>3</b> . Using the default <b>Health Retries</b> setting of <b>3</b> , the corresponding WAN connection will be treated as down after three consecutive timeouts.
<b>Recovery Retries</b>	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink Balance treats a previously down WAN connection as up again. By default, <b>Recover Retries</b> is set to <b>3</b> . Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

Dynamic DNS Settings 	
Service Provider	DNS-O-Matic
Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Update All Hosts	<input type="checkbox"/>
Hosts / IDs	<input type="text"/>

Dynamic DNS Settings	
<b>Service Provider</b>	<p>This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:</p> <ul style="list-style-type: none"> <li>• changeip.com</li> <li>• dyndns.org</li> <li>• no-ip.org</li> <li>• tzo.com</li> <li>• DNS-O-Matic</li> </ul> <p>Select <b>Disabled</b> to disable this feature.</p>
<b>User ID / User / Email</b>	This setting specifies the registered user name for the dynamic DNS service.
<b>Password / Pass /</b>	This setting specifies the password for the dynamic DNS service.



TZO Key	
<b>Update All Hosts</b>	Check this box to automatically update all hosts.
<b>Hosts / Domain</b>	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

## Important Note

In order to use dynamic DNS services, appropriate hostname 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 is changed, such as when an IP is changed after a DHCP IP refresh or reconnection.

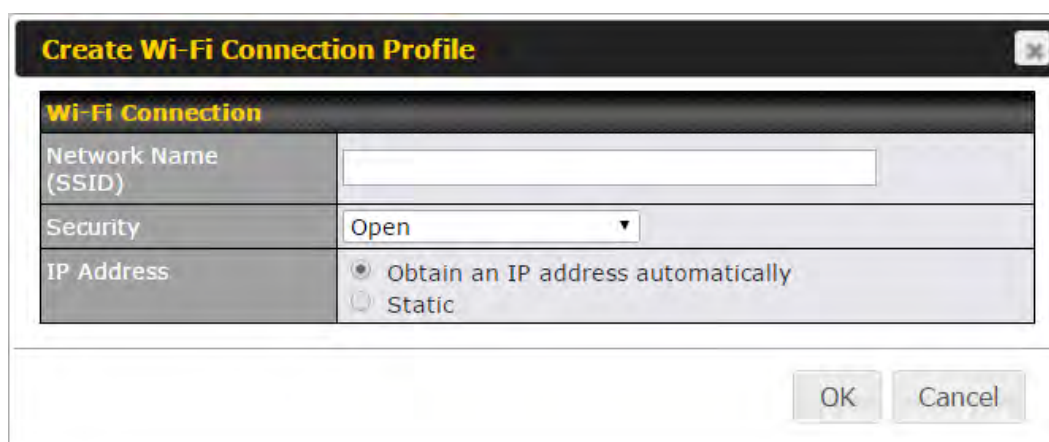
Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a WAN's IP address did not change.

### 10.3.1 Creating Wi-Fi Connection Profiles

You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden-SSID access points. Click **Network>WAN>Details>Create Profile...** to get started.



This will open a window similar to the one shown below:



## Wi-Fi Connection Profile Settings

**Type** Select whether the network will connect automatically or manually.

**Network Name (SSID)** Enter a name to represent this Wi-Fi connection.

This option allows you to select which security policy is used for this wireless network. Available options:

- Open**

Security	Open
----------	------
- WEP**

Security	WEP
Encryption Key	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
- WPA/WPA2 – Personal**

Security	WPA/WPA2-Personal
Shared Key	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
- WPA/WPA2 – Enterprise**

Security	WPA/WPA2-Enterprise
Login ID	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
EAP Method	PEAP
EAP Phase 2 Method	EAP/CHAP
EAP outer authentication identity	<input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/>

**Security**

## 10.4 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Pepwave router can periodically check the health of each WAN connection. The health check settings for each WAN connection can be independently configured via **Network>WAN>Details**.

## Health Check Settings

**Method** This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

**Health Check Disabled**

Health Check Method	<input type="button" value="?"/> Disabled <small>Health Check disabled. Network problem cannot be detected.</small>
---------------------	--

When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

## Health Check Method: PING

Health Check Method	<input type="button" value="?"/> PING
PING Hosts	<input type="button" value="?"/> Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

### PING Hosts

This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. 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. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

## Health Check Method: DNS Lookup

Health Check Method	<input type="button" value="?"/> DNS Lookup
Health Check DNS Servers	<input type="button" value="?"/> Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

### Health Check DNS Servers

This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS lookup.  
 If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.  
 If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.  
 Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

## Health Check Method: HTTP

Health Check Method	<input type="button" value="?"/> HTTP
URL 1	<input type="button" value="?"/> http:// <input type="text"/> Matching String: <input type="checkbox"/>
URL 2	<input type="button" value="?"/> http:// <input type="text"/> Matching String: <input type="checkbox"/>

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

### URL1





**WAN Settings>WAN Edit>Health Check Settings>URL1**  
 The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is

filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

## URL 2

### WAN Settings>WAN Edit>Health Check Settings>URL2

If **URL2** is also provided, a health check will pass if either one of the tests passed.


Timeout		10 ▾ second(s)
Health Check Interval		5 ▾ second(s)
Health Check Retries		3 ▾
Recovery Retries		3 ▾

## Other Health Check Settings

<b>Timeout</b>	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is <b>5 seconds</b> .
<b>Health Check Interval</b>	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is <b>5 seconds</b> .
<b>Health Check Retries</b>	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Pepwave router will treat the corresponding WAN connection as down. Default health retries is set to <b>3</b> . Using the default <b>Health Retries</b> setting of <b>3</b> , the corresponding WAN connection will be treated as down after three consecutive timeouts.
<b>Recovery Retries</b>	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Pepwave router treats a previously down WAN connection as up again. By default, <b>Recover Retries</b> is set to <b>3</b> . Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

## Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and health checks fail, the Pepwave router will automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:

 **Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.**

## 10.5 Dynamic DNS Settings

Pepwave routers are capable of registering 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. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address from the external, even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT

# Pepwave MAX and Surf User Manual

router), the public IP of each WAN will be automatically reported to the DNS service provider.

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

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network>WAN>Details>Dynamic DNS Service Provider/Dynamic DNS Settings**.

Dynamic DNS Service Provider	<input type="text" value="changeip.com"/>
User ID	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Hosts	<input type="text"/>

## Dynamic DNS Settings

### Dynamic DNS

This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:

- changeip.com
- dyndns.org
- no-ip.org
- tzo.com
- DNS-O-Matic
- Others...

Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.

Select **Disabled** to disable this feature.

### Account Name / Email Address

This setting specifies the registered user name for the dynamic DNS service.

### Password / TZO Key

This setting specifies the password for the dynamic DNS service.

### Hosts / Domain

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. If you need to enter more than one host, use a carriage return to separate them.

## Important Note

In order to use dynamic DNS services, appropriate host name registration(s) and 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., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service

# Pepwave MAX and Surf User Manual

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

## 11 Advanced Wi-Fi Settings

Wi-Fi settings can be configured at **Advanced>Wi-Fi Settings** (or **AP>Settings** on some models). Note that menus displayed can vary by model.



**Wi-Fi Radio Settings**

Operating Country	United States
-------------------	---------------

### Wi-Fi Radio Settings

**Operating Country**

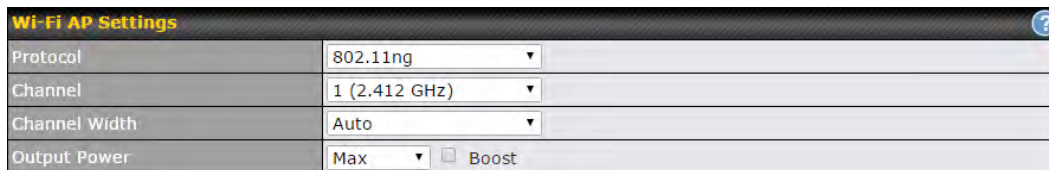
This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow.

- If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).
- If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).

NOTE: Users are required to choose an option suitable to local laws and regulations.

### Important Note

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



**Wi-Fi AP Settings**

Protocol	802.11ng
Channel	1 (2.412 GHz)
Channel Width	Auto
Output Power	Max <input type="checkbox"/> Boost

### Wi-Fi AP Settings

**Protocol**

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

**Channel**

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

**Channel Width**


Available options are **20 MHz**, **40 MHz**, and **Auto (20/40 MHz)** . Default is **Auto (20/40 MHz)**, which allows both widths to be used simultaneously.






**Output Power**

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



# Pepwave MAX and Surf User Manual

Advanced Wi-Fi AP settings can be displayed by clicking the  on the top right-hand corner of the **Wi-Fi AP Settings** section, which can be found at **AP>Settings**. Other models will display a separate section called **Wi-Fi AP Advanced Settings**, which can be found at **Advanced>Wi-Fi Settings**.

Beacon Rate		1Mbps
Beacon Interval		100ms
DTIM		1
Slot Time		9 $\mu$ s
ACK Timeout		48 $\mu$ s
Frame Aggregation		<input checked="" type="checkbox"/> Enable
Guard Interval		<input type="radio"/> Short <input checked="" type="radio"/> Long

Wi-Fi AP Advanced Settings	
<b>Beacon Rate</b> <sup>A</sup>	This option is for setting the transmit bit rate for sending a beacon. By default, <b>1Mbps</b> is selected.
<b>Beacon Interval</b> <sup>A</sup>	This option is for setting the time interval between each beacon. By default, <b>100ms</b> is selected.
<b>DTIM</b> <sup>A</sup>	This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to <b>1 ms</b> .
<b>Slot Time</b> <sup>A</sup>	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to <b>9 <math>\mu</math>s</b> .
<b>ACK Timeout</b> <sup>A</sup>	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to <b>48 <math>\mu</math>s</b> .
<b>Frame Aggregation</b> <sup>A</sup>	This option allows you to enable frame aggregation to increase transmission throughput.
<b>Guard Interval</b> <sup>A</sup>	This is where you opt for a short or long guard period interval for your transmissions.

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



# Pepwave MAX and Surf User Manual

Wi-Fi WAN settings can be configured at **Advanced>Wi-Fi Settings** (or **Advanced>Wi-Fi WAN** or some models).

Wi-Fi WAN Settings	
Channel Width	20/40 MHz ▾
Bit Rate	Auto ▾
Output Power	Max ▾ <input type="checkbox"/> Boost

## Wi-Fi WAN Settings

### Channel Width

Available options are **20/40 MHz** and **20 MHz**. Default is **20/40 MHz**, which allows both widths to be used simultaneously.

### Bit Rate

This option allows you to select a specific bit rate for data transfer over the device's Wi-Fi network. By default, **Auto** is selected.

### Output Power

This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country. Note that selecting the **Boost** option may cause the MAX's radio output to exceed local regulatory limits.

## 12 MediaFast Configuration

MediaFast settings can be configured from the **Network** menu.

### 12.1 Setting Up MediaFast Content Caching

To access MediaFast content caching settings, select **Advanced>Cache Control**.

Cache Control															
Domains / IP Addresses	<input type="radio"/> Cache all <input checked="" type="radio"/> Whitelist <input type="radio"/> Blacklist ted.com														
Source IP Subnet	<input type="radio"/> Any <input checked="" type="radio"/> Custom	<table border="1"> <thead> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td>10.8.41.0</td> <td>255.255.255.0 (/24)</td> <td>✖</td> </tr> <tr> <td>10.8.76.0</td> <td>255.255.255.0 (/24)</td> <td>✖</td> </tr> <tr> <td></td> <td>255.255.255.0 (/24)</td> <td>+</td> </tr> </tbody> </table>		Network	Subnet Mask		10.8.41.0	255.255.255.0 (/24)	✖	10.8.76.0	255.255.255.0 (/24)	✖		255.255.255.0 (/24)	+
Network	Subnet Mask														
10.8.41.0	255.255.255.0 (/24)	✖													
10.8.76.0	255.255.255.0 (/24)	✖													
	255.255.255.0 (/24)	+													
Content Type	<input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Images <input checked="" type="checkbox"/> OS / Application Updates														
Cache Lifetime Settings	<table border="1"> <thead> <tr> <th>File Extension</th> <th>Lifetime (days)</th> <th></th> </tr> </thead> <tbody> <tr> <td>jpg</td> <td>30</td> <td>✖</td> </tr> <tr> <td></td> <td></td> <td>+</td> </tr> </tbody> </table>			File Extension	Lifetime (days)		jpg	30	✖			+			
File Extension	Lifetime (days)														
jpg	30	✖													
		+													

Cache Control Settings	
<b>Domain</b>	Choose to <b>Cache on all domains</b> , or enter domain names and then choose either <b>Cache the specified domains only</b> or <b>Do not cache the specified domains</b> .
<b>Source IP Subnet</b>	This setting allows caching to be applied to the user-specified IP subnets. If "Any" is selected, then caching will apply to all subnets.
<b>Content Type</b>	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
<b>Cache Lifetime Settings</b>	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.

## 12.2 Scheduling Content Prefetching

Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Advanced >Prefetch Schedule**.





Prefetch Schedule							
Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
▶ Course Progress	Downloading	04-11 06:00	04-09 02:03	-		0 B	
▶ National Geog	Ready	04-11 00:00	04-09 00:00	00:01		4.98 kB	
▶ Syllabus	Downloading	04-11 06:00	04-09 06:00	-		0 B	
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01		115.91 kB	
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01		62.26 kB	

[New Schedule](#)

Tools	
<a href="#">Clear Web Cache</a>	<a href="#">Clear Statistics</a>

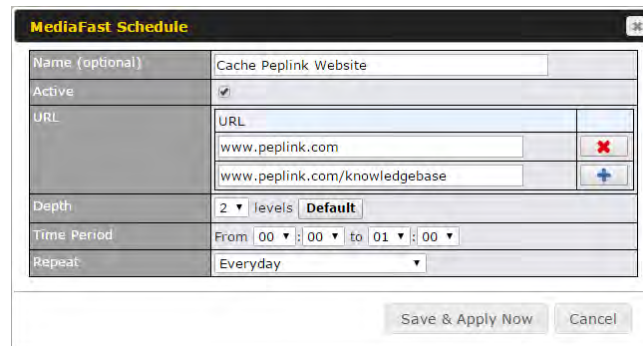
Prefetch Schedule Settings	
<b>Name</b>	This field displays the name given to the scheduled download.
<b>Status</b>	Check the status of your scheduled download here.
<b>Next Run Time/Last Run Time</b>	These fields display the date and time of the next and most recent occurrences of the scheduled download.
<b>Last Duration</b>	Check this field to ensure that the most recent download took as long as expected to complete. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time.
<b>Result</b>	This field indicates whether downloads are in progress () or complete () .
<b>Last Download</b>	Check this field to ensure that the most recent download file size is within the expected range. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time. This field is also useful for quickly seeing which downloads are consuming the most storage space.



## Actions

- To begin a scheduled download immediately, click .
- To cancel a scheduled download, click .
- To edit a scheduled download, click .
- To delete a scheduled download, click .

## New Schedule

Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:



Name (optional)	Cache Peplink Website
Active	<input checked="" type="checkbox"/>
URL	www.peplink.com 
	www.peplink.com/knowledgebase 
Depth	2 levels <input type="button" value="Default"/>
Time Period	From 00:00 to 01:00
Repeat	Everyday

Simply provide the requested information to create your schedule.

## Clear Web Cache

To clear all cached content, click this button. Note that this action cannot be undone.

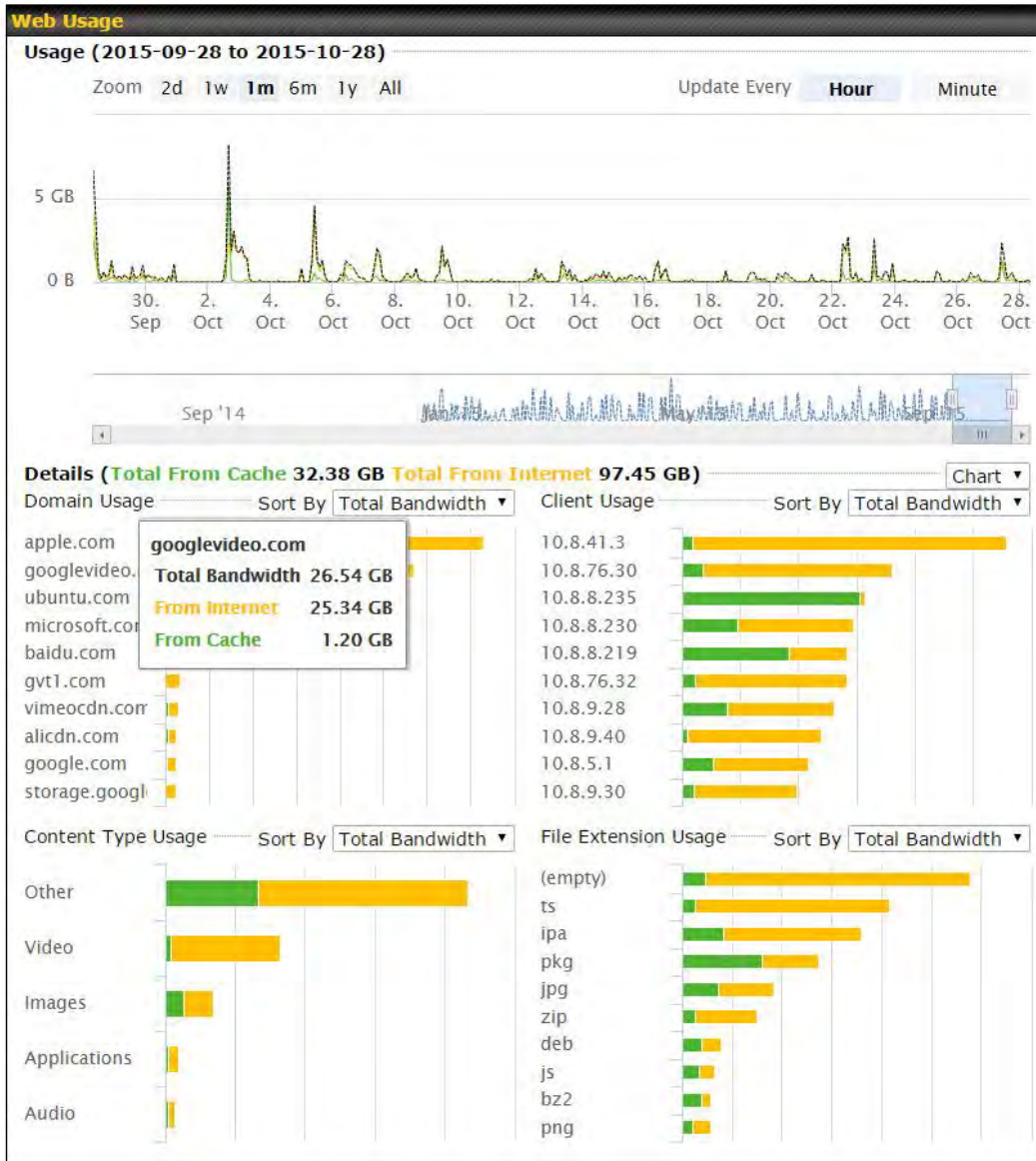
## Clear Statistics

To clear all prefetch and status page statistics, click this button.

## 12.3 Viewing MediaFast Statistics

To get details on storage and bandwidth usage, select **Status>MediaFast**.

# Pepwave MAX and Surf User Manual



## 13 Bandwidth Bonding SpeedFusion™ / PepVPN



Pepwave bandwidth bonding SpeedFusion™ is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion functionality securely connects your Pepwave router to another Pepwave or Peplink device (Peplink Balance 210/310/380/580/710/1350 only). Data, voice, or video communications between these locations are kept confidential across the public Internet.

Bandwidth bonding SpeedFusion™ is specifically designed for multi-WAN environments. In case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic.


Different models of our SD-WAN routers have different numbers of site-to-site connections allowed. End-users who need to have more site-to-site connections can purchase a SpeedFusion license to increase the number of site-to-site connections allowed.

Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.


VPN bandwidth bonding is supported in Firmware 5.1 or above. All available bandwidth will be utilized to establish the VPN tunnel, and all traffic will be load balanced at packet level across all links. VPN bandwidth bonding is enabled by default.




## 13.1 PepVPN

To configure PepVPN and SpeedFusion, navigate to **Advanced>SpeedFusion™** or **Advanced>PepVPN**.




### PepVPN with SpeedFusion™

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

Profile	Remote ID	Remote Address(es)	
 EL_Office	8345-5F7A-DE97		 



---

**Send All Traffic To**

No PepVPN profile selected 


---

**PepVPN**

Local ID  MAX\_HD2\_DEF1 

---

**Link Failure Detection**

Link Failure Detection Time   Recommended (Approx. 15 secs)  
 Fast (Approx. 6 secs)  
 Faster (Approx. 2 secs)  
 Extreme (Under 1 sec)  
Shorter detection time incurs more health checks and higher bandwidth overhead

The local LAN subnet and subnets behind the LAN (defined under **Static Route** on the LAN settings page) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to local subnets.

Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN using the 256-bit AES encryption standard. To configure, navigate to **Advanced>SpeedFusion™** or **Advanced>PepVPN** and click the **New Profile** button to create a new VPN profile (you may have to first save the displayed default profile in order to access the **New Profile** button). Each profile specifies the settings for making VPN connection with one remote Pepwave or Peplink device. Note that available settings vary by model.



# Pepwave MAX and Surf User Manual


PepVPN Profile	
Name	Balance 2942-1257-1241
Active	<input checked="" type="checkbox"/>
SpeedFusion	Supported
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key <input type="radio"/> X.509
Remote ID / Pre-shared Key	Remote ID
	Pre-shared Key
	Balance 9875-A63D-92AS
NAT Mode	<input type="checkbox"/>
Remote IP Address / Host Names (Optional)	<input type="text"/>
	If this field is empty, this field on the remote unit must be filled
Data Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>
Bandwidth Limit	<input type="checkbox"/>
Cost	10
WAN Smoothing	Off
Use IP ToS	<input type="checkbox"/>


A list of defined SpeedFusion connection profiles and a **Link Failure Detection Time** option will be shown. Click the **New Profile** button to create a new VPN connection profile for making a VPN connection to a remote Peplink Balance via the available WAN connections. Each profile is for making a VPN connection with one remote Peplink Balance.

PepVPN Profile Settings	
<b>Name</b>	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores ( _ ), dashes ( - ), and/or non-leading/trailing spaces ( ).
<b>Active</b>	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
<b>Encryption</b>	By default, VPN traffic is encrypted with <b>256-bit AES</b> . If <b>Off</b> is selected on both sides of a VPN connection, no encryption will be applied.
<b>Authentication</b>	Select from <b>By Remote ID Only</b> , <b>Preshared Key</b> , or <b>X.509</b> to specify the method the Peplink Balance will use to authenticate peers. When selecting <b>By Remote ID Only</b> , be sure to enter a unique peer ID number in the <b>Remote ID</b> field.
<b>Remote ID / Pre-shared Key</b>	This optional field becomes available when <b>Remote ID / Pre-shared Key</b> is selected as the Peplink Balance's VPN <b>Authentication</b> method, as explained above. <b>Pre-shared Key</b> defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.



# Pepwave MAX and Surf User Manual

	Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the  icon next to the "Remote ID / Preshared Key" setting.
<b>Remote ID/Remote Certificate</b>	These optional fields become available when <b>X.509</b> is selected as the Peplink Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the <b>Show Details</b> link below the field.
<b>Allow Shared Remote ID</b>	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
<b>NAT Mode</b>	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When <b>NAT Mode</b> is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
<b>Remote IP Address / Host Names (Optional)</b>	<p>If <b>NAT Mode</b> is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.</p> <p>This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.</p>
<b>Data Port</b>	This field is used to specify a UDP port number for transporting outgoing VPN data. If <b>Default</b> is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If <b>Custom</b> is selected, enter an outgoing port number from 1 to 65535.
<b>Bandwidth Limit</b>	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
<b>Cost</b>	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10
<b>WAN Smoothing<sup>A</sup></b>	Select the degree to which WAN Smoothing will be implemented across your WAN links.

<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner to activate. To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>Basic Settings>\*LAN Profile Name\*** and refer to instructions in section 9.1


# Pepwave MAX and Surf User Manual

WAN Connection Priority					
	Priority	Direction	Connect to Remote	Cut-off latency (ms)	Suspension Time after Packet Loss (ms)
1. WAN 1	1 (Highest) ▼	Up/Down ▼	All ▼		
2. WAN 2	1 (Highest) ▼	Up/Down ▼	All ▼		
3. Wi-Fi WAN	1 (Highest) ▼	Up/Down ▼	All ▼		
4. Cellular 1	1 (Highest) ▼	Up/Down ▼	All ▼		
5. Cellular 2	1 (Highest) ▼	Up/Down ▼	All ▼		
6. USB	1 (Highest) ▼	Up/Down ▼	All ▼		

## WAN Connection Priority

### WAN Connection Priority


If your device supports it, you can specify the priority of 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.

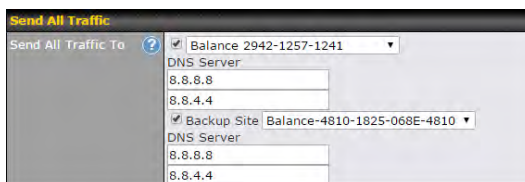
To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the  button.

### Send All Traffic To

No PepVPN profile selected

## Send All Traffic To

This feature allows you to redirect all traffic to a specified PepVPN connection. Click the  button to select your connection and the following menu will appear:



You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main PepVPN connection fail.

## Outbound Policy/PepVPN Outbound Custom Rules


Some models allow you to set outbound policy and custom outbound rules from **Advanced>PepVPN**. See **Section 14** for more information on outbound policy settings.

# Pepwave MAX and Surf User Manual

The image shows two screenshots from a web interface. The top screenshot is titled "Outbound Policy" and shows a dropdown menu set to "According to custom rules" with an edit icon. The bottom screenshot is titled "PepVPN Outbound Custom Rules" and shows a table with columns for Service, Algorithm, Source, Destination, and Protocol. The Source field is set to "(Auto)". There is an "Add Rule" button at the bottom.

The image shows a screenshot of the "PepVPN Local ID" configuration screen. It has a label "Local ID" and a text input field containing "MAX\_HD2\_8D1C". There is a question mark icon to the left of the input field and an edit icon to the right.

## PepVPN Local ID

The local ID is a text string to identify this local unit when establishing a VPN connection. When creating a profile on a remote unit, this local ID must be entered in the remote unit's **Remote ID** field. Click the  icon to edit **Local ID**.

The image shows a screenshot of the "PepVPN Settings" configuration screen. It has several sections: "Handshake Port" with radio buttons for "Default" and "Custom" and an input field; "Backward Compatibility" with radio buttons for "High (firmware 5.3+)" and "Latest (firmware 6.2+)"; and "Link Failure Detection Time" with radio buttons for "Recommended (Approx. 15 secs)", "Fast (Approx. 6 secs)", "Faster (Approx. 2 secs)", and "Extreme (Under 1 sec)". There is a question mark icon to the left of the "Link Failure Detection Time" section and a help icon in the top right corner. A note at the bottom states: "Shorter detection time incurs more health checks and higher bandwidth overhead".

## PepVPN Settings

### Handshake Port<sup>A</sup>

To designate a custom handshake port (TCP), click the **custom** radio button and enter the port number you wish to designate.

### Backward Compatibility

Determine the level of backward compatibility needed for PepVPN tunnels. The use of the **Latest** setting is recommended as it will improve the performance and resilience of SpeedFusion connections.

### Link Failure Detection Time

The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed. When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds. When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds. When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds. When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

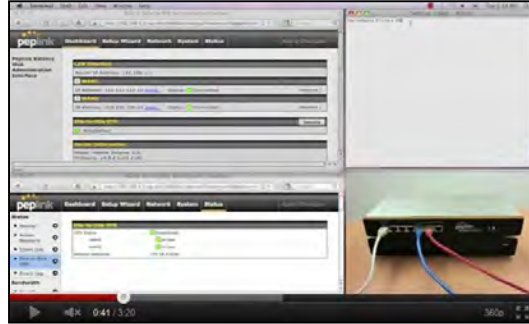
<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner to activate.

## Important Note

Peplink proprietary SpeedFusion™ uses TCP port 32015 and UDP port 4500 for establishing VPN connections. If you have a firewall in front of your Pepwave devices, you will need to add firewall rules for these ports and protocols to allow inbound and outbound traffic to pass through the firewall.

## Tip

Want to know more about VPN sub-second session failover? Visit our YouTube Channel for a video tutorial!



<http://youtu.be/TLQgdPSY88>

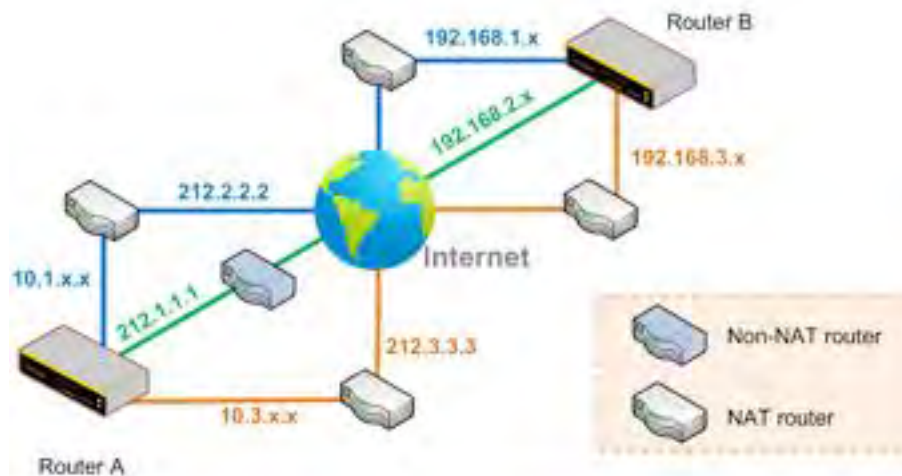
## 13.2 The Pepwave Router Behind a NAT Router

Pepwave routers support establishing SpeedFusion™ over WAN connections which are behind a NAT (network address translation) router.

To enable a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to inbound port-forward TCP port 32015 to the Pepwave router.

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 enter all of Unit A's public IP addresses or hostnames into Unit B's **Remote IP Addresses / Host Names** field. Leave the field in Unit A blank. With this setting, a SpeedFusion™ connection can be set up and all WAN connections on both sides will be utilized.



See the following diagram for an example of this setup in use:



One of the WANs connected to Router A is non-NAT'd (212.1.1.1). The rest of the WANs connected to Router A and all WANs connected to Router B are NAT'd. In this case, the **Peer IP Addresses / Host Names** field for Router B should be filled with all of Router A's hostnames or public IP addresses (i.e., 212.1.1.1, 212.2.2.2, and 212.3.3.3), and the field in Router A can be left blank. The two NAT routers on WAN1 and WAN3 connected to Router A should inbound port-forward TCP port 32015 to Router A so that all WANs will be utilized in establishing the VPN.

## 13.3 SpeedFusion™ Status

SpeedFusion™ status is shown in the **Dashboard**. The connection status of each connection profile is shown as below.

SpeedFusion™		Status
FL Office	 Established	
NY Office	 Established	

After clicking the **Status** button at the top right corner of the SpeedFusion™ table, you will be forwarded to **Status>SpeedFusion™**, where you can view subnet and WAN connection information for each VPN peer. Please refer to **Section 22.6** for details.

### IP Subnets Must Be Unique Among VPN Peers

The entire interconnected SpeedFusion™ network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

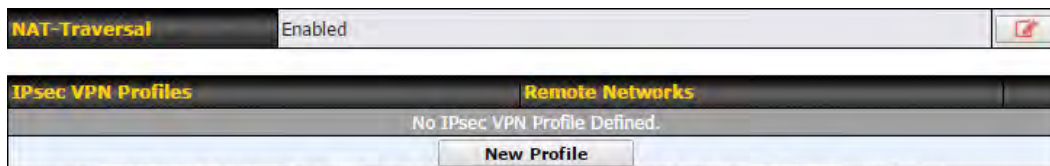
## 14 IPsec VPN

IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

IPsec VPN on Pepwave routers is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for a multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g., unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

### 14.1 IPsec VPN Settings

Many Pepwave products can make multiple IPsec VPN connections with Peplink, Pepwave, Cisco, and Juniper routers. Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other. All data can be routed over the VPN with a selection of encryption standards, such as 3DES, AES-128, and AES-256. To configure IPsec VPN on Pepwave devices that support it, navigate to **Advanced>IPsec VPN**.



Pepwave MAX IPsec only supports network-to-network connection with Cisco, Juniper or Pepwave MAX devices.

A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown. **NAT-Traversal** should be enabled if your system is behind a NAT router. Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Pepwave, Cisco, or Juniper routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.





# Pepwave MAX and Surf User Manual

Name	Profile 1		
Active	<input checked="" type="checkbox"/>		
Connect Upon Disconnection of	<input checked="" type="checkbox"/> WAN 2		
Remote Gateway IP Address / Host Name	12.12.12.12		
Local Networks	<p>Propose the following networks to remote gateway:</p> <p><input type="checkbox"/> 172.16.1.1/24</p> <p><input type="checkbox"/> 172.16.2.1/24</p> <p><input type="checkbox"/> 172.16.3.1/24</p> <p><input checked="" type="checkbox"/> 10.10.0.1/32</p> <p><input checked="" type="checkbox"/> 192.168.10.0/24</p> <p><input checked="" type="checkbox"/> 192.168.11.0/24</p> <p><input type="checkbox"/> <input type="text"/></p> <p>Apply the following NAT policies:</p> <p><input checked="" type="checkbox"/> 172.16.1.0/24      <input checked="" type="checkbox"/> 192.168.10.0/24</p> <p><input checked="" type="checkbox"/> 172.16.2.0/24      <input checked="" type="checkbox"/> 10.10.0.1/32</p> <p><input checked="" type="checkbox"/> 172.16.3.11/32      <input checked="" type="checkbox"/> 192.168.11.101/32</p> <p><input checked="" type="checkbox"/> 172.16.3.21/32      <input checked="" type="checkbox"/> 192.168.11.201/32</p> <p><input type="checkbox"/> Local Network      <input checked="" type="checkbox"/> NAT Network</p>		
Remote Networks	Network	Subnet Mask	
	192.167.11.193	255.255.255.0 (/24)	<input type="button" value="+"/>
Authentication	<input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate		
Mode	<input checked="" type="radio"/> Main Mode (All WANs need to have Static IP)		
	<input type="radio"/> Aggressive Mode		
Force UDP Encapsulation	<input type="checkbox"/>		
Preshared Key	<input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters		
Local ID	<input type="text"/>		
Remote ID	<input type="text"/>		
Phase 1 (IKE) Proposal	1	AES-256 & SHA1	<input type="button" value="v"/>
	2	-----	<input type="button" value="v"/>
Phase 1 DH Group	<input checked="" type="checkbox"/> Group 2: MODP 1024		
	<input type="checkbox"/> Group 5: MODP 1536		
Phase 1 SA Lifetime	3600	seconds	<input type="button" value="Default"/>
Phase 2 (ESP) Proposal	1	AES-256 & SHA1	<input type="button" value="v"/>
	2	-----	<input type="button" value="v"/>
Phase 2 PFS Group	<input checked="" type="radio"/> None		
	<input type="radio"/> Group 2: MODP 1024		
	<input type="radio"/> Group 5: MODP 1536		
Phase 2 SA Lifetime	28800	seconds	<input type="button" value="Default"/>

## IPsec VPN Settings

**Name** This field is for specifying a local name to represent this connection profile.

**Active** When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it



# Pepwave MAX and Surf User Manual

	will be disabled.
<b>Connect Upon Disconnection of</b>	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected.
<b>Remote Gateway IP Address / Host Name</b>	Enter the remote peer's public IP address. For <b>Aggressive Mode</b> , this is optional.
<b>Local Networks</b>	<p>Enter the local LAN subnets here. If you have defined static routes, they will be shown here.</p> <p>Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allow you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site.</p> <p>Two types of NAT policies can be defined:</p> <p><b>One-to-One NAT policy:</b> if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 &gt; 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too.</p> <p><b>Many-to-One NAT policy:</b> if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 &gt; 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.</p>
<b>Remote Networks</b>	Enter the LAN and subnets that are located at the remote site here.
<b>Authentication</b>	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the <b>Preshared Key</b> and <b>X.509 Certificate</b> methods of authentication.
<b>Mode</b>	Choose <b>Main Mode</b> if both IPsec peers use static IP addresses. Choose <b>Aggressive Mode</b> if one of the IPsec peers uses dynamic IP addresses.
<b>Force UDP Encapsulation</b>	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
<b>Pre-shared Key</b>	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
<b>Remote Certificate (pem encoded)</b>	Available only when <b>X.509 Certificate</b> is chosen as the <b>Authentication</b> method, this field allows you to paste a valid X.509 certificate.
<b>Local ID</b>	In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this

# Pepwave MAX and Surf User Manual

	field is typically a U-FQDN.
<b>Remote ID</b>	In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
<b>Phase 1 (IKE) Proposal</b>	In <b>Main Mode</b> , this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In <b>Aggressive Mode</b> , only one selection is permitted.
<b>Phase 1 DH Group</b>	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. <b>Group 2: 1024-bit</b> is the default value. <b>Group 5: 1536-bit</b> is the alternative option.
<b>Phase 1 SA Lifetime</b>	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at <b>3600</b> seconds.
<b>Phase 2 (ESP) Proposal</b>	In <b>Main Mode</b> , this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In <b>Aggressive Mode</b> , only one selection is permitted.
<b>Phase 2 PFS Group</b>	Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. <b>None</b> - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. <b>Group 2: 1024-bit</b> Diffie-Hellman group. The larger the group number, the higher the security. <b>Group 5: 1536-bit</b> is the third option.
<b>Phase 2 SA Lifetime</b>	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at <b>28800</b> seconds.

WAN Connection Priority	
Priority	WAN Selection
1	WAN 1
2	-----

## WAN Connection Priority

**WAN Connection** Select the appropriate WAN connection from the drop-down menu.

## 15 Outbound Policy Management

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

### Important Note

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

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

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

### 15.1 Outbound Policy

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

Select an Outbound Policy

Policy: Custom

- High Application Compatibility
- Normal Application Compatibility
- Custom

Save Cancel

There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

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

### Outbound Policy Settings

#### High

Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the

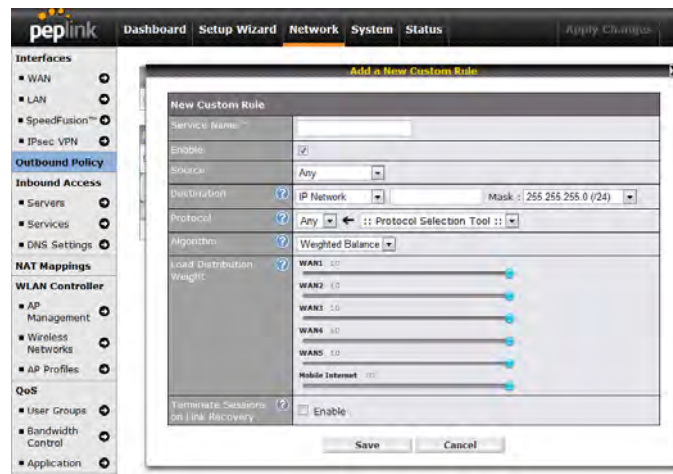
# Pepwave MAX and Surf User Manual

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

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


## Tip

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



[http://youtu.be/rKH4AS\\_bQnE](http://youtu.be/rKH4AS_bQnE)

## 15.2 Custom Rules for Outbound Policy

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

Service	Algorithm	Source	Destination	Protocol / Port
HTTPS Persistence	Persistence (Src) (Auto)	Any	IP Network 192.168.50.0/24	TCP 443

PepVPN Routes

Default	(Auto)
---------	--------

Add Rule

Expert Mode: Enabled

# Pepwave MAX and Surf User Manual

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

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

Edit Default Custom Rule																			
Default Rule	<input checked="" type="radio"/> Custom <input type="radio"/> Auto																		
Algorithm	Weighted Balance																		
Load Distribution Weight	<table><tr><td>WAN 1</td><td>10</td><td><input type="range"/></td></tr><tr><td>WAN 2</td><td>10</td><td><input type="range"/></td></tr><tr><td>Wi-Fi WAN</td><td>10</td><td><input type="range"/></td></tr><tr><td>Cellular 1</td><td>10</td><td><input type="range"/></td></tr><tr><td>Cellular 2</td><td>10</td><td><input type="range"/></td></tr><tr><td>USB</td><td>10</td><td><input type="range"/></td></tr></table>	WAN 1	10	<input type="range"/>	WAN 2	10	<input type="range"/>	Wi-Fi WAN	10	<input type="range"/>	Cellular 1	10	<input type="range"/>	Cellular 2	10	<input type="range"/>	USB	10	<input type="range"/>
WAN 1	10	<input type="range"/>																	
WAN 2	10	<input type="range"/>																	
Wi-Fi WAN	10	<input type="range"/>																	
Cellular 1	10	<input type="range"/>																	
Cellular 2	10	<input type="range"/>																	
USB	10	<input type="range"/>																	
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable																		

Save Cancel

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

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

# Pepwave MAX and Surf User Manual

**Add a New Custom Rule** ✕

Service Name *	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Source	Any ▾
Destination	<input type="text" value="IP Network"/> ▾ <input type="text" value="255.255.255.0 (/24"/> Mask:
Protocol	Any ▾ ← :: Protocol Selection Tool :: ▾
Algorithm	Weighted Balance ▾
Load Distribution Weight	<div style="margin-bottom: 2px;">WAN 1 10 <input type="range" value="10"/></div> <div style="margin-bottom: 2px;">WAN 2 10 <input type="range" value="10"/></div> <div style="margin-bottom: 2px;">Wi-Fi WAN 10 <input type="range" value="10"/></div> <div style="margin-bottom: 2px;">Cellular 1 10 <input type="range" value="10"/></div> <div style="margin-bottom: 2px;">Cellular 2 10 <input type="range" value="10"/></div> <div style="margin-bottom: 2px;">USB 10 <input type="range" value="10"/></div>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

## New Custom Rule Settings

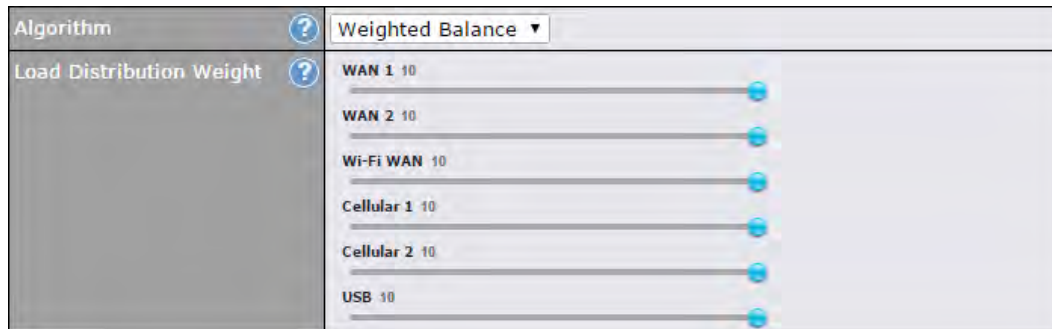
<b>Service Name</b>	This setting specifies the name of the outbound traffic rule.										
<b>Enable</b>	<p>This setting specifies whether the outbound traffic rule takes effect. When <b>Enable</b> is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When <b>Enable</b> is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule.</p> <p>Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.</p>										
<b>Source</b>	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.										
<b>Destination</b>	<p>This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Destination</td> <td>Domain Name ▾</td> </tr> <tr> <td>Protocol</td> <td>Any</td> </tr> <tr> <td>Algorithm</td> <td>IP Address</td> </tr> <tr> <td></td> <td>IP Network</td> </tr> <tr> <td></td> <td style="background-color: #007bff; color: white;">Domain Name</td> </tr> </table> </div> <p>If <b>Domain Name</b> is chosen and a domain name, such as <i>foobar.com</i>, is entered, any outgoing accesses to <i>foobar.com</i> and <i>*.foobar.com</i> will match this criterion. You may enter a wildcard (*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter <i>foobar.*</i>, for example, <i>www.foobar.com</i>, <i>www.foobar.co.jp</i>, or <i>foobar.co.uk</i> will also match. Placing wildcards in any other position is not supported.</p> <p>NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.</p>	Destination	Domain Name ▾	Protocol	Any	Algorithm	IP Address		IP Network		Domain Name
Destination	Domain Name ▾										
Protocol	Any										
Algorithm	IP Address										
	IP Network										
	Domain Name										

<b>Protocol and Port</b>	This setting specifies the IP protocol and port of traffic that matches this rule.
<b>Algorithm</b>	<p>This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected (note that some Pepwave routers provide only some of these options):</p> <ul style="list-style-type: none"><li>• Weighted Balance</li><li>• Persistence</li><li>• Enforced</li><li>• Priority</li><li>• Overflow</li><li>• Least Used</li><li>• Lowest Latency</li></ul> <p>The upcoming sections detail the listed algorithms.</p>
<b>Terminate Sessions on Link Recovery</b>	<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 <b>Weighted</b>, <b>Persistence</b>, and <b>Priority</b> algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.</p>



## 15.2.1 Algorithm: Weighted Balance

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



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

For example, with the following weight settings:

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

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

Matching traffic distributed to Ethernet WAN1 is 16.7% =  $(10 / 60) \times 100\%$ .

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

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

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

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

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



## 15.2.2 Algorithm: Persistence

The configuration of persistent services is the solution to the few situations where link load distribution for Internet services is undesirable. For example, for security reasons, many e-banking and other secure websites terminate the session when the client computer's Internet IP address changes mid-session.

In general, different Internet IP addresses represent different computers. The security concern is that an IP address change during a session may be the result of an unauthorized intrusion attempt. Therefore, to prevent damages from the potential intrusion, the session is terminated upon the detection of an IP address change.

Pepwave routers can be configured to distribute data traffic across multiple WAN connections. Also, the Internet IP depends on the WAN connections over which communication actually takes place. As a result, a LAN client computer behind the Pepwave router may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Pepwave router with three WAN connections may communicate on the Internet using three different IP addresses.

With the persistence feature, rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate using one IP address, eliminating the issues mentioned above.

Algorithm	Persistence
Persistence Mode	<input checked="" type="radio"/> By Source <input type="radio"/> By Destination
Load Distribution	<input type="radio"/> Auto <input checked="" type="radio"/> Custom
Load Distribution Weight	<p>WAN 1 10</p> <p>WAN 2 10</p> <p>Wi-Fi WAN 10</p> <p>Cellular 1 10</p> <p>Cellular 2 10</p> <p>USB 10</p>

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

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

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

## 15.2.3 Algorithm: Enforced

This setting specifies the WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Enforced**.

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

Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Starting from Firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

## 15.2.4 Algorithm: Priority

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

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

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

### Tip

Configure multiple distribution rules to accommodate different kinds of services.

## 15.2.5 Algorithm: Overflow

The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.

# Pepwave MAX and Surf User Manual

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

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

## 15.2.6 Algorithm: Least Used

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

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

## 15.2.7 Algorithm: Lowest Latency

Algorithm	Lowest Latency
	Note: Use of Lowest Latency will incur additional network usage.
Connection	<input checked="" type="checkbox"/> WAN 1
	<input checked="" type="checkbox"/> WAN 2
	<input checked="" type="checkbox"/> Wi-Fi WAN
	<input type="checkbox"/> Cellular 1
	<input type="checkbox"/> Cellular 2
	<input type="checkbox"/> USB

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

### Tip

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

- All WAN connections are symmetric; or

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

## 15.2.8 Expert Mode

**Expert Mode** is available on some Pepwave routers for use by advanced users. To enable the feature, click on the help icon and click **turn on Expert Mode**.

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

**Help** Close

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

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

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

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

Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	X
PepVPN Routes					
Default			(Auto)		
Add Rule					

## 16 Inbound Access

### 16.1 Port Forwarding Service


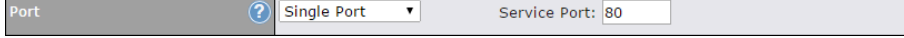
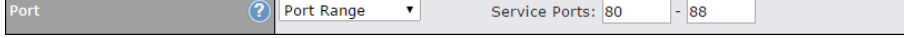
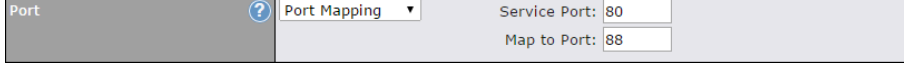
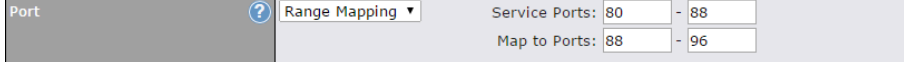
Pepwave routers can act as a firewall that blocks, by default, all inbound access from the Internet. By using port forwarding, Internet users can access servers behind the Pepwave router. Inbound port forwarding rules can be defined at **Advanced>Port Forwarding**.

Service	IP Address(es)	Server	Protocol
No Services Defined			
<a href="#">Add Service</a>			

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

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No																												
Service Name	Service_1																												
IP Protocol	TCP <input type="button" value="←"/> :: Protocol Selection Tool :: <input type="button" value="▼"/>																												
Port	Any Port <input type="button" value="▼"/>																												
Inbound IP Address(es) <small>(Require at least one IP address)</small>	<table border="1"> <thead> <tr> <th colspan="2">Connection / IP Address(es)</th> <th>All</th> <th>Clear</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> WAN 1</td> <td><input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Wi-Fi WAN</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 1</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 2</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> USB</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Connection / IP Address(es)		All	Clear	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)			<input type="checkbox"/> WAN 2				<input type="checkbox"/> Wi-Fi WAN				<input type="checkbox"/> Cellular 1				<input type="checkbox"/> Cellular 2				<input type="checkbox"/> USB			
Connection / IP Address(es)		All	Clear																										
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)																												
<input type="checkbox"/> WAN 2																													
<input type="checkbox"/> Wi-Fi WAN																													
<input type="checkbox"/> Cellular 1																													
<input type="checkbox"/> Cellular 2																													
<input type="checkbox"/> USB																													
Server IP Address	120.78.95.7																												

Port Forwarding Settings	
<b>Enable</b>	This setting specifies whether the inbound service takes effect. When <b>Enable</b> is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
<b>Service Name</b>	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.
<b>IP Protocol</b>	The <b>IP Protocol</b> setting, along with the <b>Port</b> setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the <b>Servers</b> setting. Please see below for details on the <b>Port</b> and <b>Servers</b> settings. Alternatively, the <b>Protocol Selection Tool</b> drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remain manually modifiable.

<p><b>Port</b></p>	<p>The <b>Port</b> setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p>
	<p><b>Any Port, Single Port, Port Range, Port Map, and Range Mapping</b></p>  <p><b>Any Port:</b> all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the <b>Servers</b> setting. For example, with <b>IP Protocol</b> set to <b>TCP</b>, and <b>Port</b> set to <b>Any Port</b>, all TCP traffic is forwarded to the configured servers.</p>
	 <p><b>Single Port:</b> traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the <b>Servers</b> setting. For example, with <b>IP Protocol</b> set to <b>TCP</b>, and <b>Port</b> set to <b>Single Port</b> and <b>Service Port</b> 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.</p>
	 <p><b>Port Range:</b> traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the <b>Servers</b> setting. For example, with <b>IP Protocol</b> set to <b>TCP</b>, and <b>Port</b> set to <b>Port Range</b> and <b>Service Ports</b> 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.</p>
	 <p><b>Port Mapping:</b> traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the <b>Servers</b> setting. For example, with <b>IP Protocol</b> set to <b>TCP</b>, and <b>Port</b> set to <b>Port Mapping</b>, <b>Service Port</b> 80, and <b>Map to Port</b> 88, TCP traffic on port 80 is forwarded to the configured servers via port 88. (Please see below for details on the <b>Servers</b> setting.)</p>
<p><b>Inbound IP Address(es)</b></p>	 <p><b>Range Mapping:</b> traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the <b>Servers</b> setting.</p>
<p><b>Server IP Address</b></p>	<p>This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.</p> <p>This setting specifies the LAN IP address of the server that handles the requests for the service.</p>

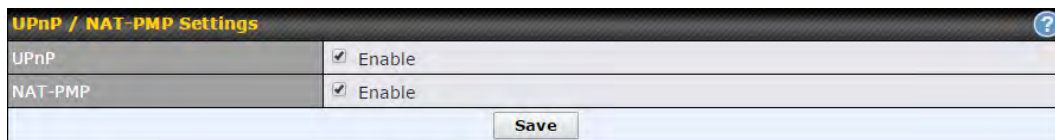


## 16.1.1 UPnP / NAT-PMP Settings

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

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

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



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

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



## 17 NAT Mappings

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

LAN Clients	Inbound Mappings	Outbound Mappings	
192.168.1.23	(WAN 1):10.88.3.158 (Interface IP)	Use <i>Interface IP</i> only	
<a href="#">Add NAT Rule</a>			

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

LAN Client(s)	IP Address ▾												
Address	<input type="text"/>												
Inbound Mappings	<b>Connection / Inbound IP Address(es)</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> WAN 1</li> <li><input type="checkbox"/> WAN 2</li> <li><input type="checkbox"/> Wi-Fi WAN</li> <li><input type="checkbox"/> Cellular 1</li> <li><input type="checkbox"/> Cellular 2</li> <li><input type="checkbox"/> USB</li> </ul>												
Outbound Mappings	<b>Connection / Outbound IP Address</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td>WAN 1</td> <td>10.88.3.158 (Interface IP) ▾</td> </tr> <tr> <td>WAN 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 1</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>USB</td> <td>Interface IP ▾</td> </tr> </tbody> </table>	WAN 1	10.88.3.158 (Interface IP) ▾	WAN 2	Interface IP ▾	Wi-Fi WAN	Interface IP ▾	Cellular 1	Interface IP ▾	Cellular 2	Interface IP ▾	USB	Interface IP ▾
WAN 1	10.88.3.158 (Interface IP) ▾												
WAN 2	Interface IP ▾												
Wi-Fi WAN	Interface IP ▾												
Cellular 1	Interface IP ▾												
Cellular 2	Interface IP ▾												
USB	Interface IP ▾												

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

## Inbound Mappings

This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when **IP Address** is selected in the **LAN Client(s)** field.

Note that inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Also note that each WAN IP address can be associated to one NAT mapping only.

## Outbound Mappings

This setting specifies the WAN IP addresses that should be used when an IP connection is made from a LAN host to the Internet. Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility).

Note that if you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the **Outbound Policy** section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.

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

### Important Note


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

## 18 QoS

### 18.1 User Groups

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

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

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

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

**Add / Edit User Group** ✕

Client	Staff A
Subnet / IP Address <span style="font-size: small;">?</span>	IP Address <span style="font-size: small;">?</span> 192.168.1.99
Group <span style="font-size: small;">?</span>	Manager <span style="font-size: small;">?</span> <span style="border: 1px solid blue; padding: 2px;">Staff A (192.168.1.99)</span>

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

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

## 18.2 Bandwidth Control

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

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

## 18.3 Application

### 18.3.1 Application Prioritization


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

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

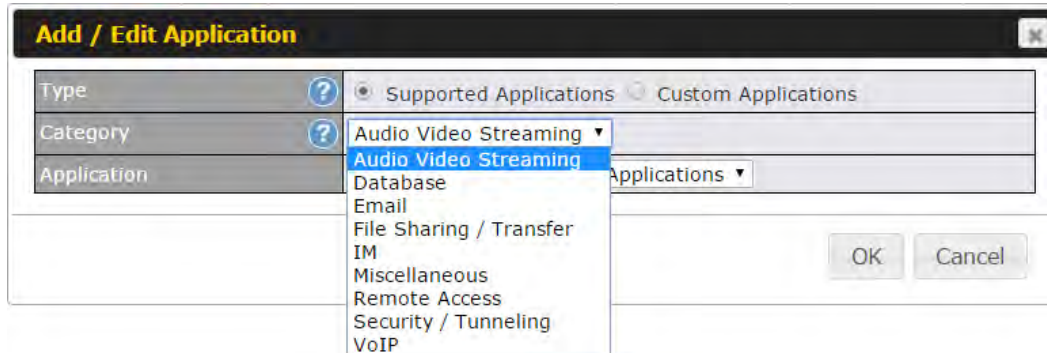
Three application priority levels can be set: **↑ High**, **— Normal**, and **↓ Low**. Pepwave routers can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference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

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

## 18.3.2 Prioritization for Custom Applications

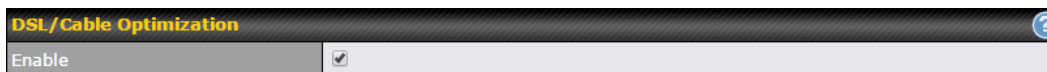
Click the **Add** button to define a custom application. Click the button  in the **Action** column to delete the custom application in the corresponding row.

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



## 18.3.3 DSL/Cable Optimization

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



## 19 Firewall

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

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

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

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

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

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

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

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

### 19.1 Outbound and Inbound Firewall Rules

#### 19.1.1 Access Rules

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

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

# Pepwave MAX and Surf User Manual

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

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

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

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

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

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

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

Below the table is an "Add Rule" button.

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

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

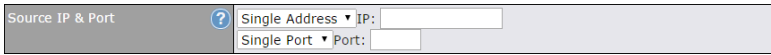
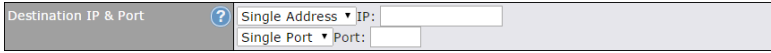
New Firewall Rule	
Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/>
WAN Connection	Any
Protocol	Any <input type="button" value="←"/> :: Protocol Selection Tool :: <input type="button" value="→"/>
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	<input checked=""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

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

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



## Inbound / Outbound Firewall Settings

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

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

## Event Logging

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

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

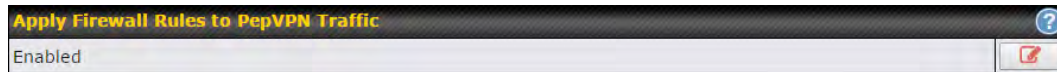
To change a rule's priority, simply drag and drop the rule:


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

## Tip

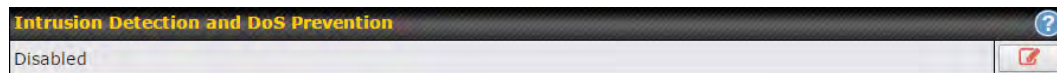
If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound Allow firewall rules will be required for inbound port forwarding and inbound NAT mapping rules. However, if the default inbound rule is set as **Deny**, a corresponding Allow firewall rule will be required.


## 19.1.2 Apply Firewall Rules to PepVpn Traffic



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

## 19.1.3 Intrusion Detection and DoS Prevention



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

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

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

## 19.2 Content Blocking

**Application Blocking**

Please Select Application...

**Web Blocking**

Preset Category

- High
- Moderate
- Low
- Custom

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

Customized Domains

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

Exempted Domains from Web Blocking

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

**Exempted User Groups**

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

**Exempted Subnets**

Network	Subnet Mask
	255.255.255.0 (/24)
	<input type="button" value="+"/>

**URL Logging**

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

### 19.2.1 Application Blocking

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

### 19.2.2 Web Blocking

Defines web site domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for those on the Exempted User Groups or Exempted Subnets defined below.

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

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

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

### 19.2.3 Customized Domains

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

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

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

### 19.2.4 Exempted User Groups

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

### 19.2.5 Exempted Subnets

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

### 19.2.6 URL Logging

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

## 19.3 OSPF & RIPv2

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

# Pepwave MAX and Surf User Manual

## OSPF

### Router ID

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

### Area

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

## OSPF Settings

### Area ID

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

### Link Type


Choose the network type that this area will use.

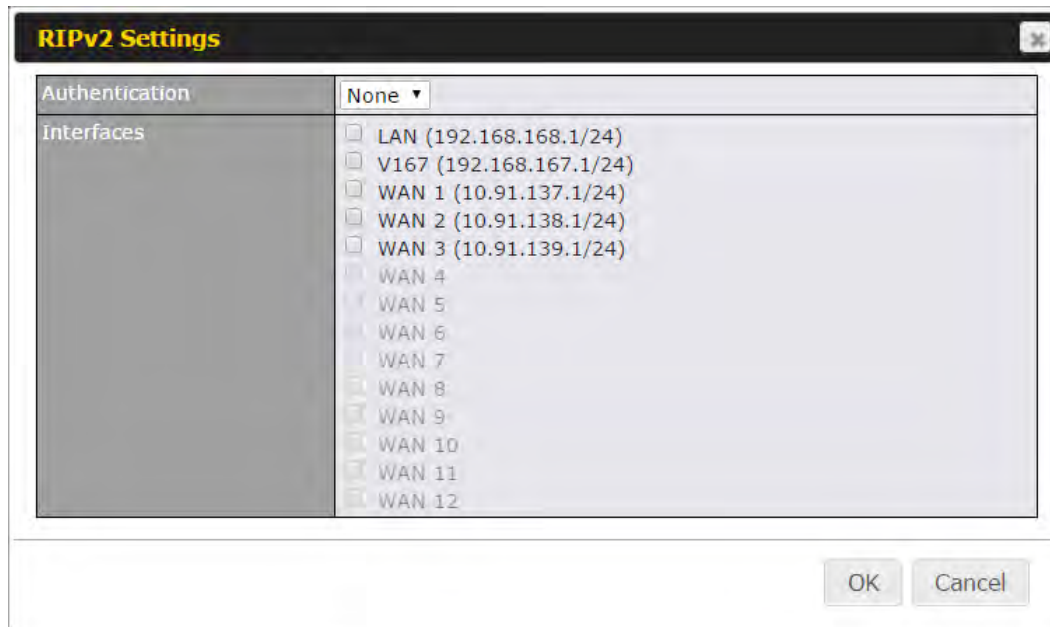
### Authentication

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

### Interfaces

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

To access RIPv2 settings, click .



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


## 19.4 Remote User Access

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



# Pepwave MAX and Surf User Manual

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

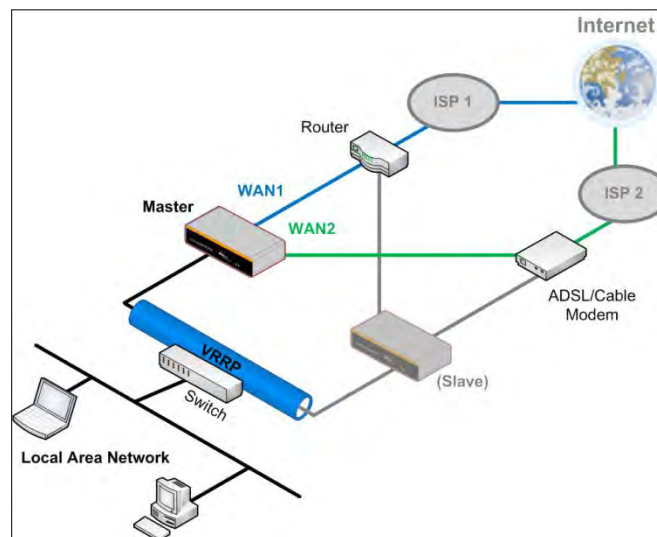
Remote User Access Settings	
<b>Enable</b>	Click the checkbox to enable Remote User Access.
<b>VPN Type</b>	Determine whether remote devices can connect to the Balance using L2TP with IPsec or PPTP. For greater security, we recommend you connect using L2TP with IPsec.
<b>Preshared Key</b>	Enter your preshared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
<b>Listen On</b>	This setting is for specifying the WAN IP addresses where the PPTP server of the router should listen on.
<b>User Accounts</b>	<p>This setting allows you to define the PPTP User Accounts. Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click the button X to delete the account in its corresponding row.</p> <p>Click the  button to switch to enters user accounts by pasting the information in.CSV format.</p>

## Miscellaneous Settings

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

### 19.5 High Availability

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



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

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

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

# Pepwave MAX and Surf User Manual

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

Interface for Master Router

Interface for Slave Router

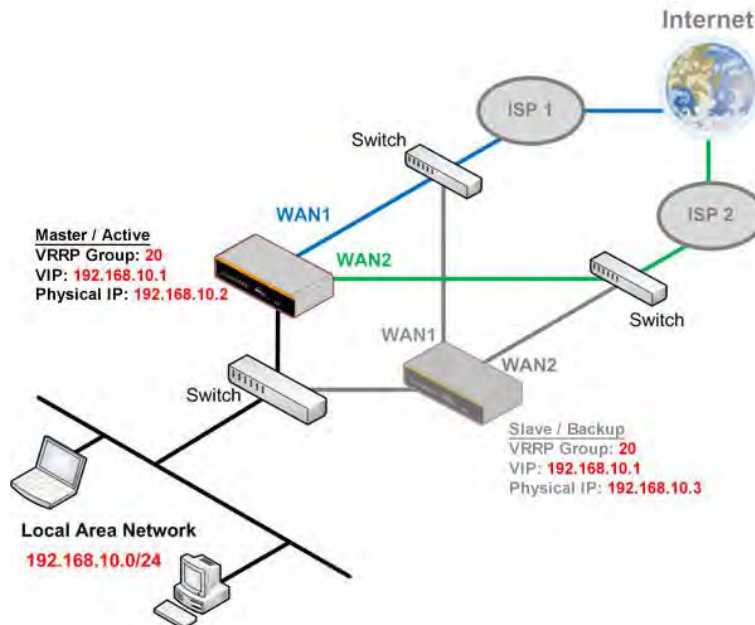
High Availability		High Availability	
Enable	<input checked="" type="checkbox"/>	Enable	<input checked="" type="checkbox"/>
Group Number	5	Group Number	5
Preferred Role	<input checked="" type="radio"/> Master <input type="radio"/> Slave	Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/>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

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

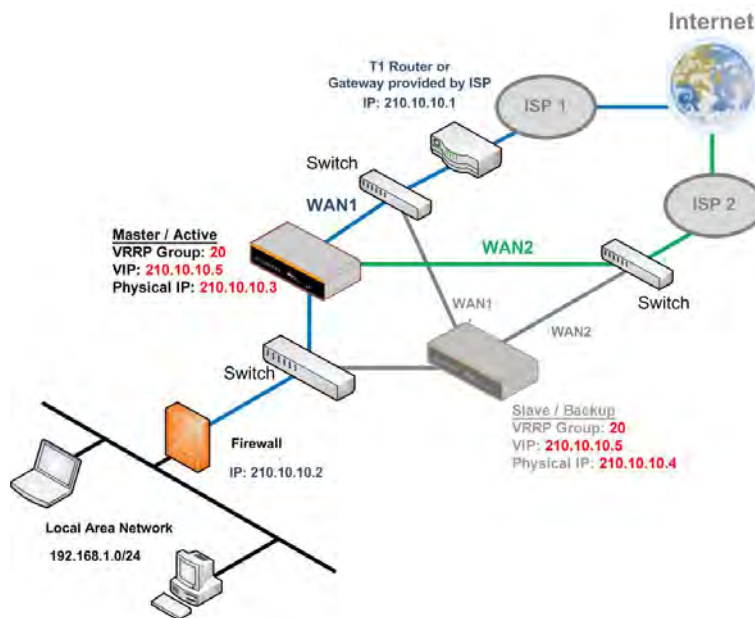
# Pepwave MAX and Surf User Manual

## Important Note

For Pepwave routers in NAT mode, the virtual IP (VIP) should be set as the default gateway for all hosts on the LAN segment. For example, a firewall sitting behind the Pepwave router should set its default gateway as the virtual IP instead of the IP of the master router.

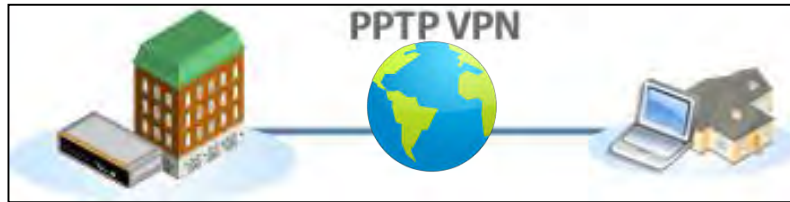


In drop-in mode, no other configuration needs to be set.



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

## 19.6 PPTP Server




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



Check the box to enable PPTP server functionality. All connected PPTP sessions are displayed at **Status>Client List**. Please refer to **Section 22.3** for details. Note that available options vary by model.

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



PPTP Server Settings	
<b>Listen On</b>	This setting is for specifying the WAN connection(s) and IP address(es) that the PPTP server should listen on.
<b>Authentication</b>	<p>This setting is for specifying the user database source for PPTP authentication. Three sources can be selected: <b>Local User Accounts</b>, <b>LDAP Server</b>, or <b>RADIUS Server</b>.</p> <p><b>Local User Accounts</b> - User accounts are stored in the Pepwave router locally. You can add/modify/delete accounts in the <b>User Accounts</b> table.</p> <p><b>LDAP Server</b> - Authenticate with an external LDAP server. This has been tested with Open LDAP servers where passwords are NTLM hashed. Active Directory is not supported. (You can choose to use RADIUS to authenticate with a Windows server.)</p> <p><b>RADIUS Server</b> - Authenticate with an external RADIUS server. This has been tested with Microsoft Windows Internet Authentication Service and FreeRADIUS servers where passwords are NTLM hashed or in plain text.</p>
<b>User Accounts</b>	<p>This setting allows you to define PPTP user accounts <a href="#">for authentication via local user accounts</a>. Click <b>Add</b> to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click  to delete the account in its corresponding row.</p>




## 19.7 Certificate Manager

Certificate Manager		
VPN Certificate	 No Certificate	<a href="#">Assign</a>
Web Admin SSL Certificate	 No Certificate	<a href="#">Assign</a>
Captive Portal SSL Certificate	No Certificate	<a href="#">Assign</a>

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

## 19.8 Service Forwarding

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

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

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

	after selecting <b>Enable</b> .
<b>Web Proxy Forwarding</b>	When this option is enabled, all outgoing connections destined for the proxy server specified in <b>Web Proxy Interception Settings</b> will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting <b>Enable</b> .
<b>DNS Forwarding</b>	When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down.
<b>Custom Service Forwarding</b>	When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number.

## 19.8.1 SMTP Forwarding

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

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

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

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

### Note

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule



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

## 19.8.2 Web Proxy Forwarding

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

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

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

## 19.8.3 DNS Forwarding

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

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

## 19.8.4 Custom Service Forwarding

The screenshot shows the 'Custom Service Forwarding Setup' configuration page. At the top, there is a section for 'Custom Service Forwarding' with an 'Enable' checkbox checked. Below this is the 'Settings' section, which contains a table with four columns: 'TCP Port', 'Server IP Address', 'Server Port', and a '+' button. The 'TCP Port' and 'Server Port' columns have text input fields, and the 'Server IP Address' column has a text input field.

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

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

## 19.9 Service Passthrough

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

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

(Registered trademarks are copyrighted by their respective owner)

Some Internet services need to be specially handled in a multi-WAN environment. Pepwave routers can handle these services such that Internet applications do not notice being behind a multi-WAN router. Settings for service passthrough support are available here.


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

to route the traffic to.

## 19.10 GPS Forwarding

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

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

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

## 20 AP Controller

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

### Special Note

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

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

### 20.1 Wireless SSID

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

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

### AP Controller

#### AP Management

The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, **CAPWAP Access Controller addresses** (field 138), will be added to the DHCP server. A local DNS record, **AP Controller**, will be added to the local DNS proxy.

#### Permitted AP

Access points to manage can be specified here. If **Any** is selected, the AP controller will manage any AP that reports to it. If **Approved List** is selected, only APs with serial numbers listed in the provided text box will be managed.

SSID	Security Policy	
PEPWAVE_8D1C	WPA/WPA2 - Personal	<input checked="" type="checkbox"/>

# Pepwave MAX and Surf User Manual

Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model.

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


- SSID Settings:** Contains fields for SSID (PEPWAVE\_8D1C), VLAN ID (LAN (No VLAN)), Broadcast SSID (checked), Data Rate (Auto selected), Multicast Filter (unchecked), Multicast Rate (MCS8/MCS0/6M), IGMP Snooping (unchecked), Layer 2 Isolation (unchecked), and Band Steering (Disable).
- Security Settings:** Contains a Security Policy dropdown menu set to "Open (No Encryption)".
- Access Control:** Contains a Restricted Mode dropdown menu set to "None".

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

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

# Pepwave MAX and Surf User Manual

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

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

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

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

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

Access Control	
<b>Restricted Mode</b>	The settings allow administrator to control access using MAC address filtering. Available options are <b>None</b> , <b>Deny all except listed</b> , <b>Accept all except listed</b> , and <b>RADIUS MAC Authentication</b> .  When <b>WPA/WPA2 - Enterprise</b> is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the <b>Shared Key</b> option should be disabled. When using

# Pepwave MAX and Surf User Manual

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

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

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

**MAC Address List** Connection coming from the MAC addresses in this list will be either denied or accepted based the option selected in the previous field.

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

## RADIUS Server Settings

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



## 20.2 Settings


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

AP Settings	
SSID	2.4 GHz 5 GHz Integrated AP supports 2.4 GHz only. PEPWAVE_8D1C
Operating Country	United States
Preferred Frequency	2.4 GHz 5 GHz Integrated AP supports 2.4 GHz only.
5 GHz Protocol	802.11n/ac
5 GHz Channel Width	Auto
5 GHz Channel	Auto Edit Channels: 36 40 44 48 ...
2.4 GHz Protocol	802.11ng
2.4 GHz Channel Width	20 MHz
2.4 GHz Channel	1 (2.412 GHz)
Management VLAN ID	LAN (No VLAN)
Power Boost	<input type="checkbox"/>
Output Power	Max
Beacon Rate	1Mbps Default
Beacon Interval	100ms
DTIM	1 Default
Slot Time	9 μs Default
ACK Timeout	48 μs Default
Frame Aggregation	<input checked="" type="checkbox"/>

AP Settings	
<b>SSID</b>	These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Pepwave router does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.
<b>Operating Country</b>	<p>This drop-down menu specifies the national/regional regulations which the AP should follow.</p> <ul style="list-style-type: none"> <li>If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).</li> <li>If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).</li> </ul> <p>NOTE: Users are required to choose an option suitable to local laws and regulations. Per FCC regulation, the country selection is not available on all models marketed in US. All US models are fixed to US channels only.</p>
<b>Preferred Frequency</b>	These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 2.4GHz and 5GHz frequencies.
<b>5 GHz Protocol</b>	This section displays the 5 GHz protocols your APs are using.
<b>5GHz Channel Width</b>	There are three options: <b>20 MHz</b> , <b>20/40 MHz</b> , and <b>40 MHz</b> . With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the

# Pepwave MAX and Surf User Manual

	performance of the Wi-Fi connection.
<b>5 GHz Channel</b>	This drop-down menu selects the 5 GHz 802.11 channel to be utilized. If <b>Auto</b> is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
<b>2.4 GHz Protocol</b>	This section displays the 2.4GHz protocols your APs are using.
<b>2.4 GHz Channel Width</b>	There are three options: <b>20 MHz</b> , <b>20/40 MHz</b> , and <b>40 MHz</b> . With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
<b>2.4 GHz Channel</b>	This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If <b>Auto</b> is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
<b>Management VLAN ID</b>	This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is <b>0</b> by default, meaning that no VLAN tagging will be applied. NOTE: change this value with caution as alterations may result in loss of connection to the AP controller.
<b>Power Boost<sup>A</sup></b>	With this option enabled, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to increased interference.
<b>Output Power<sup>A</sup></b>	<p>This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When <b>Dynamic</b> settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance.</p> <p>The <b>Dynamic: Auto</b> setting will set the AP to do this automatically. Otherwise, the <b>Dynamic: Manual</b> setting will set the AP to dynamically adjust only if instructed to do so. If you have set <b>Dynamic:Manual</b>, you can go to <b>AP&gt;Toolbox&gt;Auto Power Adj.</b> to give your AP further instructions.</p>
<b>Beacon Rate<sup>A</sup></b>	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are <b>1Mbps</b> , <b>2Mbps</b> , <b>5.5Mbps</b> , <b>6Mbps</b> , and <b>11Mbps</b> .
<b>Beacon Interval<sup>A</sup></b>	This drop-down menu provides the option to set the time between each beacon send. Available options are <b>100ms</b> , <b>250ms</b> , and <b>500ms</b> .
<b>DTIM<sup>A</sup></b>	This field provides the option to set the frequency for beacon to include delivery traffic indication messages (DTIM). The interval unit is measured in milliseconds.
<b>Slot Time<sup>A</sup></b>	This field provides the option to modify the unit wait time before it transmits. The default value is <b>9µs</b> .
<b>ACK Timeout<sup>A</sup></b>	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is <b>48µs</b> .
<b>Frame Aggregation<sup>A</sup></b>	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.

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


# Pepwave MAX and Surf User Manual

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

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

# Pepwave MAX and Surf User Manual

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

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

Wi-Fi Radio Settings	
Operating Country	United States
Wi-Fi Antenna	<input type="radio"/> Internal <input checked="" type="radio"/> External

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

## Wi-Fi Radio Settings

### Operating Country

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

### Wi-Fi Antenna

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

## Important Note

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

## Wi-Fi AP Settings

### Protocol

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

### Channel

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

### Channel Width

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

### Output Power

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

### Beacon Rate<sup>A</sup>

This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is

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


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

## 20.3 Toolbox

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



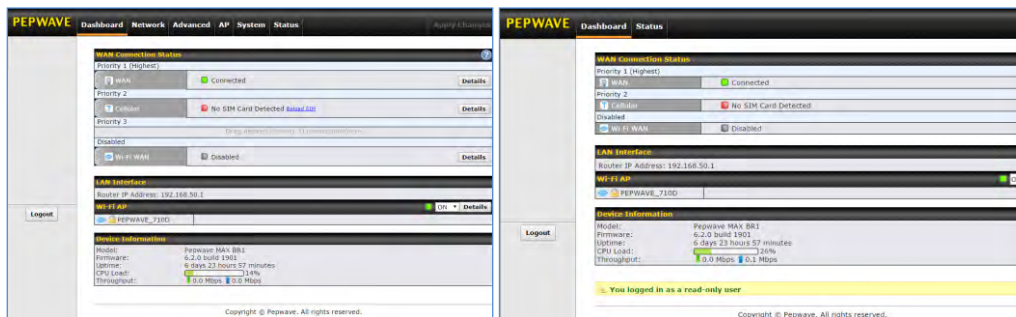
### Firmware Packs

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

## 21 System Settings

### 21.1 Admin Security

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



Admin account UI

User account UI

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

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

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

# Pepwave MAX and Surf User Manual

Admin Settings <span style="float: right;">?</span>		
Router Name	MAX_BR1_710D	hostname: max-br1-710d
Admin User Name	admin	
Admin Password	••••••••	
Confirm Admin Password	••••••••	
Read-only User Name	user	
User Password		
Confirm User Password		
Web Session Timeout	4	Hours 0 Minutes
Authentication by RADIUS	<input checked="" type="checkbox"/> Enable	
Auth Protocol	MS-CHAP v2	
Auth Server		Port <input type="text"/> <input type="button" value="Default"/>
Auth Server Secret		<input checked="" type="checkbox"/> Hide Characters
Auth Timeout	3 seconds	
Accounting Server		Port <input type="text"/> <input type="button" value="Default"/>
Accounting Server Secret		<input checked="" type="checkbox"/> Hide Characters
CLI SSH	<input checked="" type="checkbox"/> Enable	
CLI SSH Port	8822 <input type="button" value="Default"/>	
CLI SSH Access	LAN/WAN	
Security	HTTP	
Web Admin Port	80 <input type="button" value="Default"/>	
Web Admin Access	LAN Only	

Admin Settings	
<b>Router Name</b>	This field allows you to define a name for this Pepwave router. By default, <b>Router Name</b> is set as <b>MAX_XXXX</b> or <b>Surf_SOHO_XXXX</b> , where <b>XXXX</b> refers to the last 4 digits of the unit's serial number.
<b>Admin User Name</b>	<b>Admin User Name</b> is set as <i>admin</i> by default, but can be changed, if desired.
<b>Admin Password</b>	This field allows you to specify a new administrator password.
<b>Confirm Admin Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Read-only User Name</b>	<b>Read-only User Name</b> is set as <i>user</i> by default, but can be changed, if desired.
<b>User Password</b>	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
<b>Confirm User Password</b>	This field allows you to verify and confirm the new user password.
<b>Web Session Timeout</b>	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to <b>4 hours</b> .



# Pepwave MAX and Surf User Manual

<b>Authentication by RADIUS</b>	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.
<b>Auth Protocol</b>	This specifies the authentication protocol used. Available options are <b>MS-CHAP v2</b> and <b>PAP</b> .
<b>Auth Server</b>	This specifies the access address and port of the external RADIUS server.
<b>Auth Server Secret</b>	This field is for entering the secret key for accessing the RADIUS server.
<b>Auth Timeout</b>	This option specifies the time value for authentication timeout.
<b>Accounting Server</b>	This specifies the access address and port of the external accounting server.
<b>Accounting Server Secret</b>	This field is for entering the secret key for accessing the accounting server.
<b>Network Connection</b>	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
<b>CLI SSH</b>	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to <b>Section 21.16</b> .
<b>CLI SSH Port</b>	This field determines the port on which clients can access CLI SSH.
<b>CLI SSH Access</b>	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
<b>Security</b>	This option is for specifying the protocol(s) through which the web admin interface can be accessed: <ul style="list-style-type: none"><li>• HTTP</li><li>• HTTPS</li><li>• HTTP/HTTPS</li></ul>
<b>Web Admin Port</b>	This field is for specifying the port number on which the web admin interface can be accessed.
<b>Web Admin Access</b>	This option is for specifying the network interfaces through which the web admin interface can be accessed: <ul style="list-style-type: none"><li>• LAN only</li><li>• LAN/WAN</li></ul> If LAN/WAN is chosen, the <b>WAN Connection Access Settings</b> form will be displayed.

# Pepwave MAX and Surf User Manual

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

## 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.

## 21.2 Firmware

Pepwave router firmware is upgradeable through the web admin interface. Firmware upgrade functionality is located at **System>Firmware**.

The screenshot shows two sections of the web interface. The first section, 'Firmware Upgrade', has a dark header with a question mark icon. Below the header, it shows 'Current firmware version: 6.2.1' and 'Firmware check pending'. A 'Check for Firmware' button is centered below this section. The second section, 'Manual Firmware Upgrade', also has a dark header with a question mark icon. It contains a 'Firmware Image' label, a 'Choose File' button, and a text field with 'No file chosen'. A 'Manual Upgrade' button is centered below this section.

There are two ways to upgrade the unit. The first method is through an online download. The second method is to upload a firmware file manually.

To perform an online download, click on the **Check for Firmware** button. The Pepwave router will check online for new firmware. If new firmware is available, the Pepwave router will automatically download the firmware. The rest of the upgrade process will be automatically initiated.

You may also download a firmware image from the Peplink website and update the unit manually. To update using a firmware image, click **Choose File** to select the firmware file from the local computer, and then click **Manual Upgrade** to send the firmware to the Pepwave router. It will then automatically initiate the firmware upgrade process.

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

### Important Note

The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. 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 supported by Peplink. Upgrading the Pepwave router with an invalid firmware file will damage the unit and may void the warranty.

### Important Note

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

## 21.3 Time

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



Time Settings	
Time Zone	(GMT+07:00) Krasnoyarsk <input type="checkbox"/> Show all
Time Server	0.peplink.pool.ntp.org <span>Default</span>

Save

Time Settings	
<b>Time Zone</b>	This specifies the time zone (along with the corresponding Daylight Savings Time scheme). The <b>Time Zone</b> value affects the time stamps in the Pepwave router's event log and e-mail notifications. Check <b>Show all</b> to show all time zone options.
<b>Time Server</b>	This setting specifies the NTP network time server to be utilized by the Pepwave router.

## 21.4 Schedule

Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**

Schedule			
Enabled			
Name	Time	Used by	
Weekdays Only	Weekdays only	-	

New Schedule

Enable scheduling, and then click on your schedule name or on the **New Schedule** button to begin.

# Pepwave MAX and Surf User Manual

**Edit schedule profile** ✕

**Schedule Settings**

Enable	<input checked="" type="checkbox"/> The schedule function of those associated features will be lost if profile is disabled.
Name	<input type="text" value="Weekdays Only"/>
Schedule	<input type="text" value="Weekdays only"/>
Used by	You may go to supported feature settings page and set this profile as scheduler.

**Schedule Map**

	Midnight	4am	8am	Noon	4pm	8pm
Sunday	x	x	x	x	x	x
Monday	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓
Thursday	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓
Saturday	x	x	x	x	x	x

Edit Schedule Profile	
<b>Enabling</b>	Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.
<b>Name</b>	Enter your desired name for this particular schedule profile.
<b>Schedule</b>	Click the drop-down menu to choose pre-defined schedules as your starting point. Please note that upon selection, previous changes on the schedule map will be deleted.
<b>Schedule Map</b>	Click on the desired times to enable features at that time period. You can hold your mouse for faster entry.

## 21.5 Email Notification

Email notification functionality provides a system administrator with up-to-date information on network status. The settings for configuring email notifications are found at **System>Email Notification**.

# Pepwave MAX and Surf User Manual

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	smtp.mycompany.com <input checked="" type="checkbox"/> Require authentication
SSL Encryption	<input checked="" type="checkbox"/> (Note: any server certificate will be accepted)
SMTP Port	465 <input type="button" value="Default"/>
SMTP User Name	smtpuser
SMTP Password	••••••
Confirm SMTP Password	••••••
Sender's Email Address	idmin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Email Notification Settings	
<b>Email Notification</b>	This setting specifies whether or not to enable email notification. If <b>Enable</b> is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If <b>Enable</b> is not checked, email notification is disabled and the Pepwave router will not send email messages.
<b>SMTP Server</b>	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check <b>Require authentication</b> .
<b>SSL Encryption</b>	Check the box to enable SMTPS. When the box is checked, <b>SMTP Port</b> will be changed to <b>465</b> automatically.
<b>SMTP Port</b>	This field is for specifying the SMTP port number. By default, this is set to <b>25</b> ; when <b>SSL Encryption</b> is checked, the default port number will be set to <b>465</b> . You may customize the port number by editing this field. Click <b>Default</b> to restore the number to its default setting.
<b>SMTP User Name / Password</b>	This setting specifies the SMTP username and password while sending email. These options are shown only if <b>Require authentication</b> is checked in the <b>SMTP Server</b> setting.
<b>Confirm SMTP Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Sender's Email Address</b>	This setting specifies the email address the Pepwave router will use to send reports.
<b>Recipient's Email Address</b>	This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the enter key.

After you have finished setting up email notifications, you can click the **Test Email Notification** button to test the settings before saving. After **Test Email Notification** is

# Pepwave MAX and Surf User Manual

clicked, you will see this screen to confirm the settings:

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Click **Send Test Notification** to confirm. In a few seconds, you will see a message with detailed test results.

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

## Test Result

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

## 21.6 Event Log

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

Send Events to Remote Syslog Server	
Remote Syslog	<input checked="" type="checkbox"/>
Remote Syslog Host	<input type="text"/>

Push Events to Mobile Devices	
Push Events	<input checked="" type="checkbox"/>

## Event Log Settings

**Remote Syslog** This setting specifies whether or not to log events at the specified remote syslog server.

**Remote Syslog Host** This setting specifies the IP address or hostname of the remote syslog server.



# Pepwave MAX and Surf User Manual

The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature.

## Push Events



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

## 21.7 SNMP

SNMP or simple network management protocol is an open standard that can be used to collect information about the Pepwave router. SNMP configuration is located at **System>SNMP**.

**SNMP Settings**

SNMP Device Name	MAX_HD2_8D1C
SNMP Port	161 <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable

Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		
<input type="button" value="Add SNMP Community"/>		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		
<input type="button" value="Add SNMP User"/>		

SNMP Settings	
<b>SNMP Device Name</b>	This field shows the router name defined at <b>System&gt;Admin Security</b> .
<b>SNMP Port</b>	This option specifies the port which SNMP will use. The default port is <b>161</b> .
<b>SNMPv1</b>	This option allows you to enable SNMP version 1.
<b>SNMPv2</b>	This option allows you to enable SNMP version 2.
<b>SNMPv3</b>	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 is displayed:

**SNMP Community**

Community Name	My Company
Allowed Network	192.168.1.25 / 255.255.255.0 (/24) ▼

SNMP Community Settings	
<b>Community Name</b>	This setting specifies the SNMP community name.
<b>Allowed Source Subnet Address</b>	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., 192.168.1.0) and select the appropriate subnet mask.

To define a user name for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name**


SNMPv3 User	
User Name	SNMPUser
Authentication	SHA password
Privacy	DES privacypassword

Save Cancel

table, upon which the following screen is displayed:

SNMPv3 User Settings	
<b>User Name</b>	This setting specifies a user name to be used in SNMPv3.
<b>Authentication Protocol</b>	<p>This setting specifies via a drop-down menu one of the following valid authentication protocols:</p> <ul style="list-style-type: none"><li>• NONE</li><li>• MD5</li><li>• SHA</li></ul> <p>When MD5 or SHA is selected, an entry field will appear for the password.</p>
<b>Privacy Protocol</b>	<p>This setting specifies via a drop-down menu one of the following valid privacy protocols:</p> <ul style="list-style-type: none"><li>• NONE</li><li>• DES</li></ul> <p>When DES is selected, an entry field will appear for the password.</p>

## 21.8 InControl

InControl Management	
InControl Management 	<input checked="" type="checkbox"/> Allow InControl Management
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/>

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

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

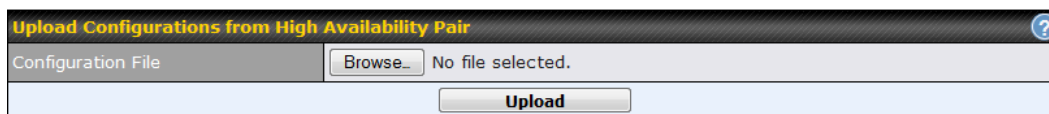
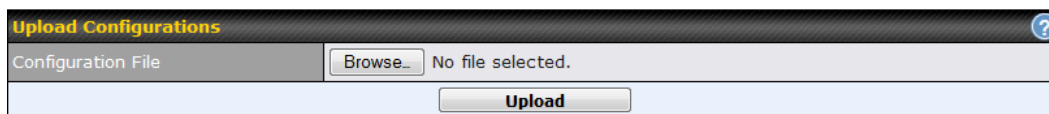
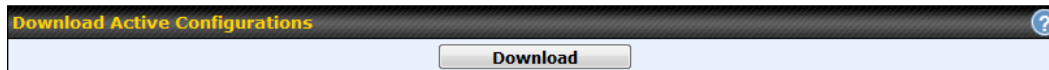
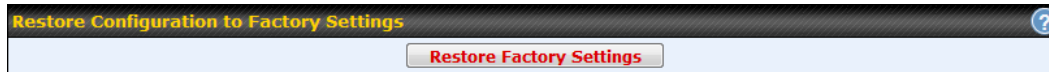
Alternately, you could also privately host InControl. Simply check the box beside the "Privately Host InControl" option, and enter the IP Address of your InControl Host.

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

## 21.9 Configuration

# Pepwave MAX and Surf User Manual

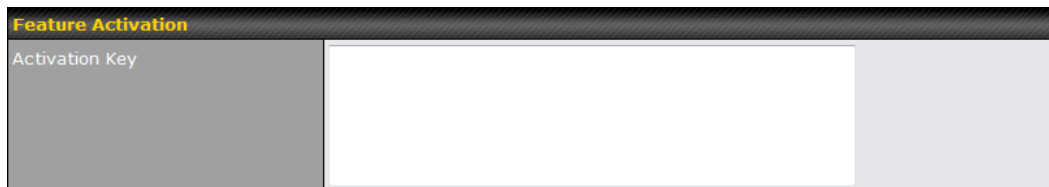
Backing up Pepwave router settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Pepwave router settings is found at **System>Configuration**. Note that available options vary by model.



Configuration	
<b>Restore Configuration to Factory Settings</b>	The <b>Restore Factory Settings</b> button is to reset the configuration to factory default settings. After clicking the button, you will need to click the <b>Apply Changes</b> button on the top right corner to make the settings effective.
<b>Download Active Configurations</b>	Click <b>Download</b> to backup the current active settings.
<b>Upload Configurations</b>	To restore or change settings based on a configuration file, click <b>Choose File</b> to locate the configuration file on the local computer, and then click <b>Upload</b> . The new settings can then be applied by clicking the <b>Apply Changes</b> button on the page header, or you can cancel the procedure by pressing <b>discard</b> on the main page of the web admin interface.
<b>Upload Configurations from High Availability Pair</b>	In a high availability (HA) configuration, a Pepwave router can quickly load the configuration of its HA counterpart. To do so, click the <b>Upload</b> button. After loading the settings, configure the LAN IP address of the Pepwave router so that it is different from the HA counterpart.

## 21.10 Feature Add-ons

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

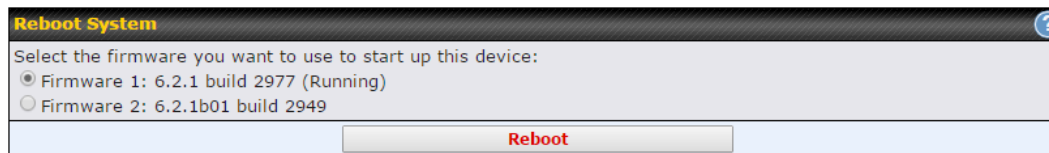


The screenshot shows a web interface titled "Feature Activation". It contains a label "Activation Key" on the left and a large, empty text input field on the right. The interface has a dark header bar with the title in yellow.

## 21.11 Reboot

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

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



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

## 21.12 Ping

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

The screenshot displays the 'Ping' utility interface. It features a configuration section with the following fields: 'Connection' set to 'WAN 1', 'Destination' set to '10.10.10.1', 'Packet Size' set to '56', and 'Number of times' set to '5'. Below these fields are 'Start' and 'Stop' buttons. The 'Results' section shows the output of the ping test, including a 'Clear Log' button. The results text is as follows:

```
PING 10.10.10.1 (10.10.10.1) from 10.88.3.158 56(84) bytes of data.  
64 bytes from 10.10.10.1: icmp_req=1 ttl=62 time=27.6 ms  
64 bytes from 10.10.10.1: icmp_req=2 ttl=62 time=26.5 ms  
64 bytes from 10.10.10.1: icmp_req=3 ttl=62 time=28.9 ms  
64 bytes from 10.10.10.1: icmp_req=4 ttl=62 time=28.3 ms  
64 bytes from 10.10.10.1: icmp_req=5 ttl=62 time=27.7 ms  
  
--- 10.10.10.1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 26.516/27.855/28.933/0.814 ms
```

### Tip

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



## 21.13 Traceroute Test

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

Traceroute	
Connection	WAN 1
Destination	64.233.189.99

Results		Clear Log
1	192.168.1.1	0
2	192.168.1.1	0
3	192.168.1.1	0
4	192.168.1.1	0
5	192.168.1.1	0
6	192.168.1.1	0
7	192.168.1.1	0
8	192.168.1.1	0
9	192.168.1.1	0
10	192.168.1.1	0
11	192.168.1.1	0
12	192.168.1.1	0
13	192.168.1.1	0
14	192.168.1.1	0
15	192.168.1.1	0
16	192.168.1.1	0
17	192.168.1.1	0
18	192.168.1.1	0
19	192.168.1.1	0
20	192.168.1.1	0
21	192.168.1.1	0
22	192.168.1.1	0
23	192.168.1.1	0
24	192.168.1.1	0
25	192.168.1.1	0
26	192.168.1.1	0
27	192.168.1.1	0
28	192.168.1.1	0
29	192.168.1.1	0
30	192.168.1.1	0
31	192.168.1.1	0
32	192.168.1.1	0
33	192.168.1.1	0
34	192.168.1.1	0
35	192.168.1.1	0
36	192.168.1.1	0
37	192.168.1.1	0
38	192.168.1.1	0
39	192.168.1.1	0
40	192.168.1.1	0
41	192.168.1.1	0
42	192.168.1.1	0
43	192.168.1.1	0
44	192.168.1.1	0
45	192.168.1.1	0
46	192.168.1.1	0
47	192.168.1.1	0
48	192.168.1.1	0
49	192.168.1.1	0
50	192.168.1.1	0
51	192.168.1.1	0
52	192.168.1.1	0
53	192.168.1.1	0
54	192.168.1.1	0
55	192.168.1.1	0
56	192.168.1.1	0
57	192.168.1.1	0
58	192.168.1.1	0
59	192.168.1.1	0
60	192.168.1.1	0
61	192.168.1.1	0
62	192.168.1.1	0
63	192.168.1.1	0
64	192.168.1.1	0
65	192.168.1.1	0
66	192.168.1.1	0
67	192.168.1.1	0
68	192.168.1.1	0
69	192.168.1.1	0
70	192.168.1.1	0
71	192.168.1.1	0
72	192.168.1.1	0
73	192.168.1.1	0
74	192.168.1.1	0
75	192.168.1.1	0
76	192.168.1.1	0
77	192.168.1.1	0
78	192.168.1.1	0
79	192.168.1.1	0
80	192.168.1.1	0
81	192.168.1.1	0
82	192.168.1.1	0
83	192.168.1.1	0
84	192.168.1.1	0
85	192.168.1.1	0
86	192.168.1.1	0
87	192.168.1.1	0
88	192.168.1.1	0
89	192.168.1.1	0
90	192.168.1.1	0
91	192.168.1.1	0
92	192.168.1.1	0
93	192.168.1.1	0
94	192.168.1.1	0
95	192.168.1.1	0
96	192.168.1.1	0
97	192.168.1.1	0
98	192.168.1.1	0
99	192.168.1.1	0
100	192.168.1.1	0

**Tip**

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

## 21.14 PepVPN Test

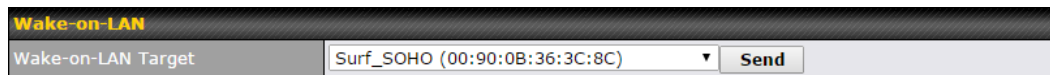
The **PepVPN Test** tool can help to test the throughput between different VPN peers. You can define the **Test Type**, **Direction**, and **Duration** of the test, and press **Go!** to perform the throughput test. The VPN test utility is located at **System>Tools>PepVPN Test**, illustrated as follows:

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

Results
(Empty)

## 21.15 Wake-on-LAN

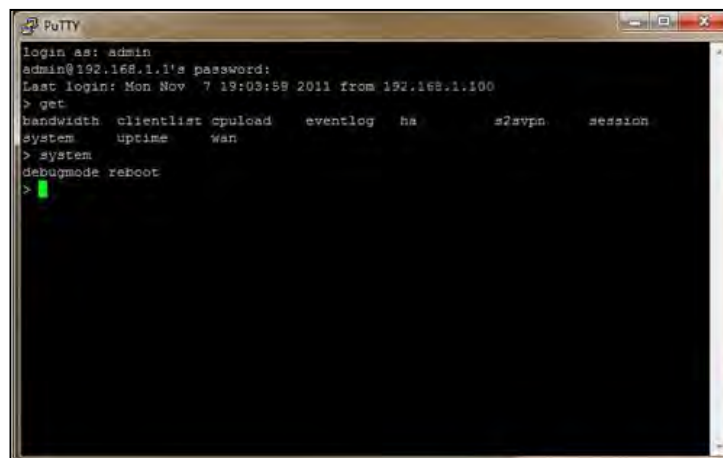
Peplink routers can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**



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

## 21.16 CLI (Command Line Interface Support)

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



## 22 Status

### 22.1 Device

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


System Information	
Router Name	MAX_HD2_8D1C
Model	Pepwave MAX HD2
Hardware Revision	2
Serial Number	2830-A48A-8D1C
Firmware	6.2.0 build 2891
PepVPN Version	4.0.0
Modem Support Version	1017 ( <a href="#">Modem Support List</a> )
Host Name	max-hd2-8d1c
Uptime	7 days 50 minutes
System Time	Mon Feb 23 11:14:13 WET 2015
Diagnostic Report	<a href="#">Download</a>
Remote Assistance	<a href="#">Turn on</a>

System Information	
<b>Router Name</b>	This is the name specified in the <b>Router Name</b> field located at <b>System&gt;Admin Security</b> .
<b>Model</b>	This shows the model name and number of this device.
<b>Product Code</b>	If your model uses a product code, it will appear here.
<b>Hardware Revision</b>	This shows the hardware version of this device.
<b>Serial Number</b>	This shows the serial number of this device.
<b>Firmware</b>	This shows the firmware version this device is currently running.
<b>PepVPN Version</b>	This shows the current PepVPN version.
<b>Modem Support Version</b>	This shows the modem support version. For a list of supported modems, click <b>Modem Support List</b> .
<b>Host Name</b>	The host name assigned to the Pepwave router appears here.
<b>Uptime</b>	This shows the length of time since the device has been rebooted.
<b>System Time</b>	This shows the current system time.
<b>Diagnostic Report</b>	The <b>Download</b> link is for exporting a diagnostic report file required for system investigation.

## Remote Assistance

Click **Turn on** to enable remote assistance.

Interface	MAC Address
LAN	00:1A:DD:BD:54:40
WAN 1	00:1A:DD:BD:54:41
WAN 2	00:1A:DD:BD:54:42

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

## Important Note

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

### 22.1.1 GPS Data

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

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

## 22.2 Active Sessions

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

Overview Search

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

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

Interface	Inbound Sessions	Outbound Sessions
<a href="#">WAN 1</a>	0	176
<a href="#">WAN 2</a>	0	32
<a href="#">Wi-Fi WAN</a>	0	51
<a href="#">Cellular 1</a>	0	64
<a href="#">Cellular 2</a>	0	0
<a href="#">USB</a>	0	0

**Top Clients**

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

This screen displays the number of sessions initiated by each application. Click on each service listing for additional information. This screen also indicates the number of sessions initiated by each WAN port. In addition, you can see which clients are initiating the most sessions.

# Pepwave MAX and Surf User Manual

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

Overview Search

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

IP / Subnet	Source or Destination	255.255.255.255 (/32)
Port	Source or Destination	
Protocol / Service	TCP	
Interface	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB <input type="checkbox"/> VPN	

Search

### Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

### Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

### Transit


Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

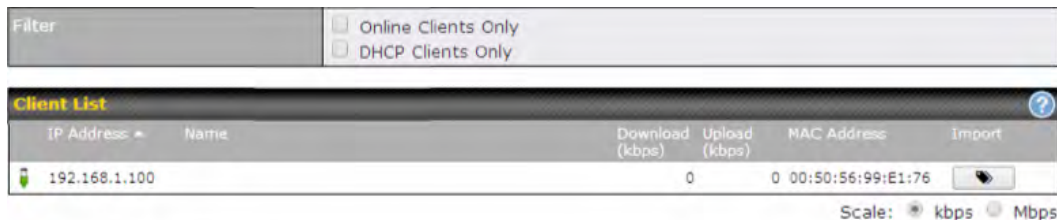
Total searched results: 0


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

## 22.3 Client List

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

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



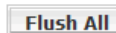
IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
192.168.1.100		0	0	00:50:56:99:E1:76	

Scale:  kbps  Mbps

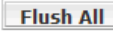
If the PPTP server (see **Section 19.2**), SpeedFusion™ (see **Section 12.1**), or AP controller (see **Section 20**) is enabled, you may see the corresponding connection name listed in the **Name** field.

## 22.4 WINS Client

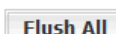
The WINS client list table is located at **Status>WINS Client**.




Name	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4



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



Name	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4





## 22.5 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 UPnP / NAT-PMP as mentioned in **Section 16.1.1**.

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

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

### Important Note

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

## 22.6 SpeedFusion Status

Current SpeedFusion™ status information is located at **Status>SpeedFusion™**. Details about SpeedFusion™ connection peers appears as below:

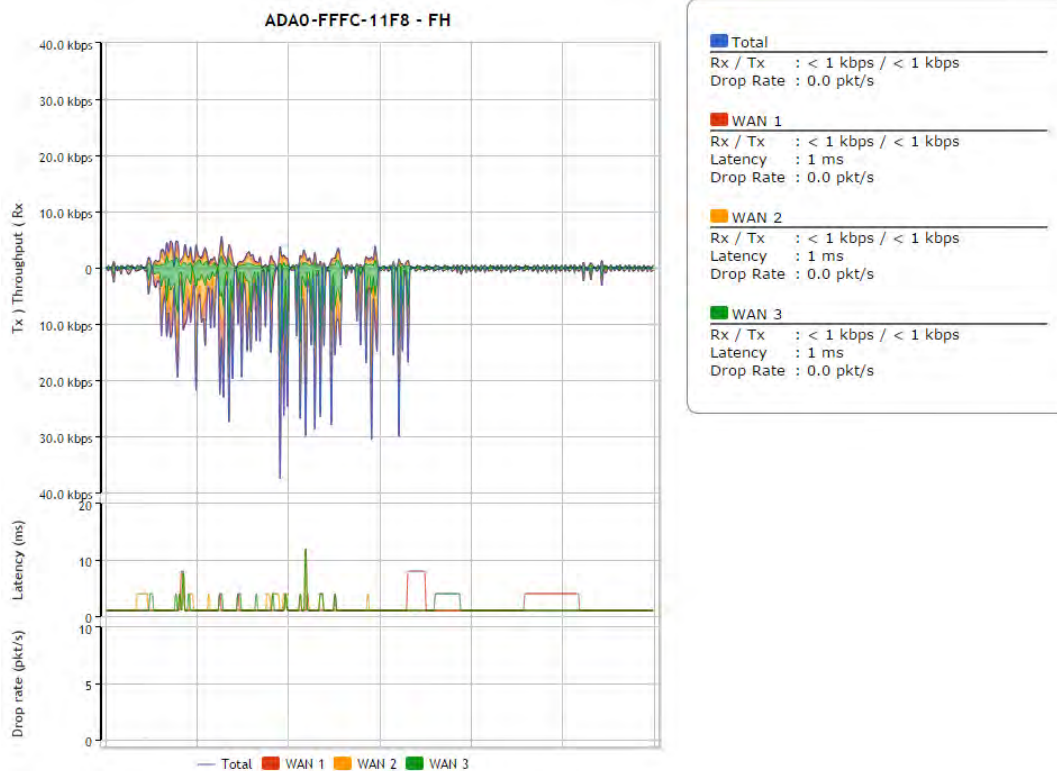
PepVPN with SpeedFusion - Remote Peer Details				<input type="checkbox"/> Show disconnected profiles	
Search		<input type="text"/>			
Remote Peer	Profile	Information			
▶ ADA0-FFFC-11F8	FH	192.168.77.0/24			
▶ 3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24			

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

# Pepwave MAX and Surf User Manual

Remote Peer	Profile	Information		
ADA0-FFFC-11F8	FH	192.168.77.0/24		
WAN 1	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms		
WAN 2	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms		
WAN 3	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms		
Total	Rx: < 1 kbps Tx: 1.1 kbps	Drop rate: 0.0 pkt/s		
3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24		
WAN 1	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms		
WAN 2	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms		
WAN 3	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms		
Total	Rx: 1.6 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s		


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




When pressing the button, the following menu will appear:

# Pepwave MAX and Surf User Manual

### PepVPN performance analysis - 9B0A-A29B-2931



**PepVPN Test:**  
Check the general TCP/UDP throughput.



**PepVPN Analyzer:**  
Check the uplink performance of each tunnel.

Warning: PepVPN Analyzer will temporarily interrupt VPN connectivity and will restore after test.

Close



**PepVPN Test:**  
Check the general TCP/UDP throughput.

After clicking the icon, the following menu appears:

#### Configuration

Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	Start
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download	
Duration	10 seconds (5 - 600)	

#### WAN Statistics

WAN 1	Rx: 2.5 kbps	Tx: 5.3 kbps	Drop rate: 0.0 pkt/s	Latency: 186 ms
WAN 3	Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a
WAN 4	Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a
Total	Rx: 2.5 kbps	Tx: 5.3 kbps	Drop rate: 0.0 pkt/s	Latency: 186 ms

Select the L2 protocol (TCP/UDP), direction, and duration and click the **Start** button to begin the general throughput test.

#### Results

0.1250 MB / 1.00 sec = 1.0485 Mbps
1.0000 MB / 1.00 sec = 8.3888 Mbps
1.3125 MB / 1.00 sec = 11.0098 Mbps
3.0000 MB / 1.00 sec = 25.1465 Mbps
5.6875 MB / 1.00 sec = 47.7473 Mbps
6.0625 MB / 1.00 sec = 50.8562 Mbps
4.9375 MB / 1.00 sec = 41.4188 Mbps
4.5000 MB / 1.00 sec = 37.7487 Mbps
5.0000 MB / 1.00 sec = 41.9438 Mbps
5.6875 MB / 1.00 sec = 47.7099 Mbps
37.3167 MB / 10.05 sec = 31.1504 Mbps 8 %TX 9 %RX 47 retrans 132.62 msRTT
TEST DONE

# Pepwave MAX and Surf User Manual



**PepVPN Analyzer:**  
Check the uplink performance of each tunnel.

The bandwidth bonding feature of PepVPN occurs when multiple WAN lines from one end merge with multiple WAN lines from the other end. For this to happen, each WAN line needs to form a connection with all the WAN lines on the opposite end. The function of the PepVPN analyzer is to report the throughput, packet loss, and latency of all possible combinations of connections. **Please note that the PepVPN Analyzer will temporarily interrupt VPN connectivity and will restore after test.**

After clicking the icon, the analyzer will require several minutes to perform its analysis depending the number of WAN links in the SpeedFusion™ Tunnel. Once the test the complete, the report will appear:

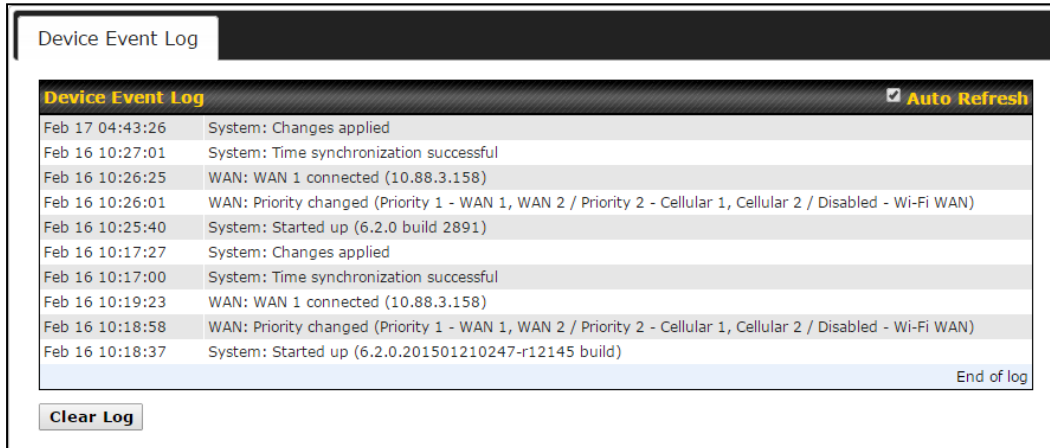
Results							
Estimated time: 150 s							
Time remaining: 0 s							
100%							
Local WAN1 > Remote WAN3	Local WAN1 > Remote WAN4	Local WAN1 > Remote WAN5	Local WAN1 > Remote WAN6	Tx Avg. (Mbps)	Tx Max. (Mbps)	Packet loss (%)	RTT (ms)
O				5.87	16.95	0.76	420.51
	O			20.72	26.39	1.59	29.89
		O		30.10	43.69	2.24	29.61
			O	45.01	55.93	2.16	28.24
O	O			24.87	33.56	0.86	49.86
O		O		19.30	31.28	0.01	49.78
	O	O		18.59	30.41	2.08	39.78
O	O	O		20.56	34.60	0.00	38.11
O			O	36.70	59.16	2.64	42.06
	O		O	19.98	30.40	4.40	38.01
O	O		O	31.63	42.99	0.72	37.99
		O	O	36.88	55.78	2.60	33.89
O		O	O	38.30	47.89	0.01	29.98
	O	O	O	33.21	55.23	2.69	30.48
O	O	O	O	30.02	46.66	3.77	28.68

"O" indicates that specific WAN / Tunnel is active for that particular test.

"Tx Avg." is the averaged throughput across the full 10 seconds time, while "Tx Max." is the averaged throughput of the fastest 30% of time.

## 22.7 Event Log

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



The screenshot shows the 'Device Event Log' interface. At the top, there is a tab labeled 'Device Event Log' and a checkbox for 'Auto Refresh' which is checked. Below this is a table of log entries. The entries are as follows:

Time	Event Description
Feb 17 04:43:26	System: Changes applied
Feb 16 10:27:01	System: Time synchronization successful
Feb 16 10:26:25	WAN: WAN 1 connected (10.88.3.158)
Feb 16 10:26:01	WAN: Priority changed (Priority 1 - WAN 1, WAN 2 / Priority 2 - Cellular 1, Cellular 2 / Disabled - Wi-Fi WAN)
Feb 16 10:25:40	System: Started up (6.2.0 build 2891)
Feb 16 10:17:27	System: Changes applied
Feb 16 10:17:00	System: Time synchronization successful
Feb 16 10:19:23	WAN: WAN 1 connected (10.88.3.158)
Feb 16 10:18:58	WAN: Priority changed (Priority 1 - WAN 1, WAN 2 / Priority 2 - Cellular 1, Cellular 2 / Disabled - Wi-Fi WAN)
Feb 16 10:18:37	System: Started up (6.2.0.201501210247-r12145 build)

At the bottom right of the log area, it says 'End of log'. Below the log area is a 'Clear Log' button.

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

## 22.8 Bandwidth

This section shows bandwidth usage statistics and is located at **Status>Bandwidth**. Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

## 22.8.1 Real-Time

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

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

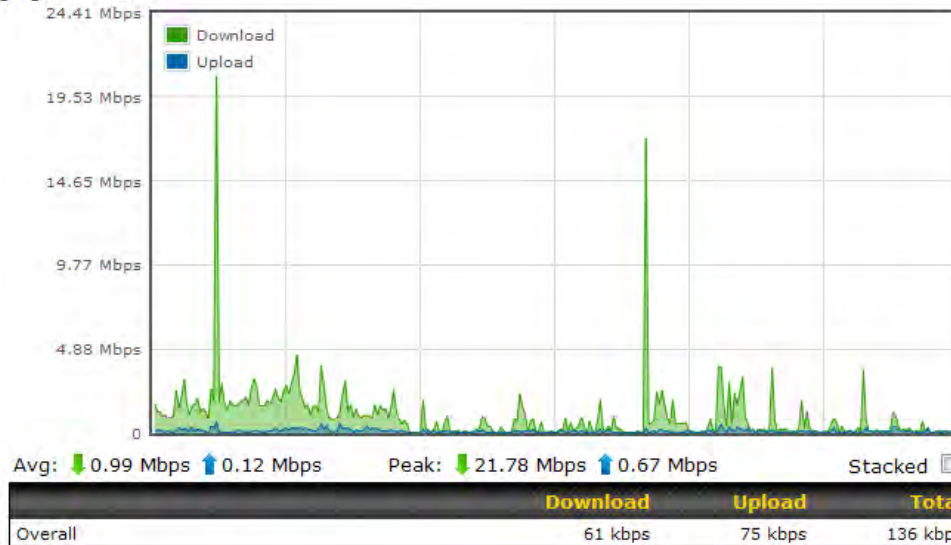
	Download	Upload	Total
All WAN Connections	216.68 GB	91.70 GB	308.38 GB

Data transferred since last reboot

[\[ Hide Details \]](#)

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

Aggregated Transfer



# Pepwave MAX and Surf User Manual

## 22.8.2 Hourly

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



## 22.8.3 Daily

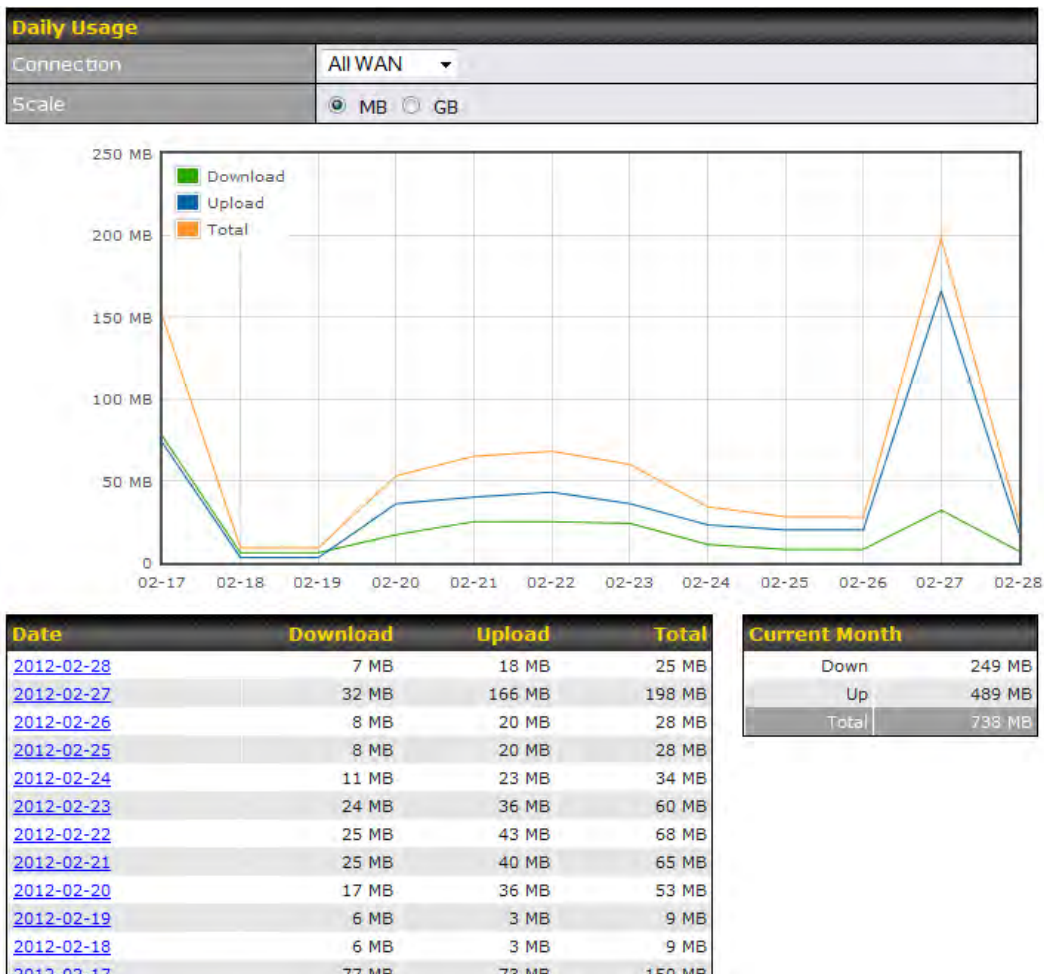


# Pepwave MAX and Surf User Manual

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

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

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).

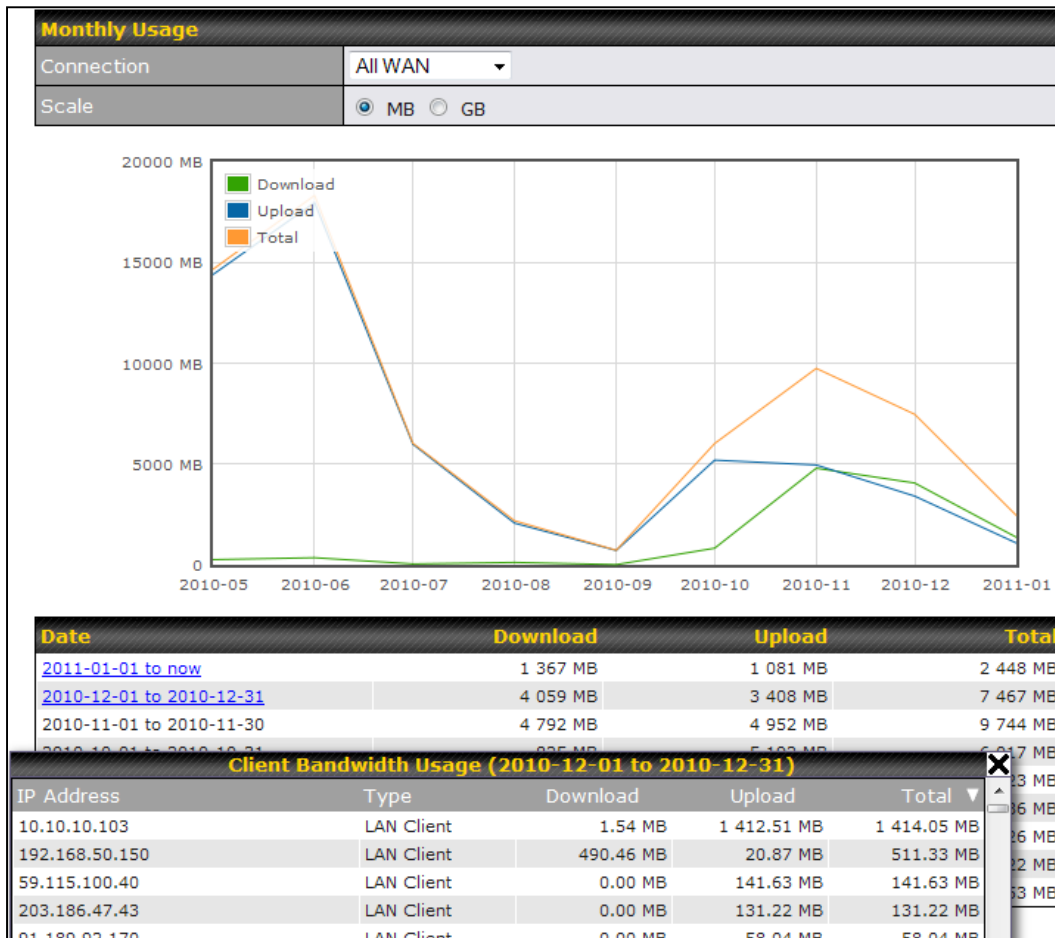


All WAN Daily Bandwidth Usage

## 22.8.4 Monthly

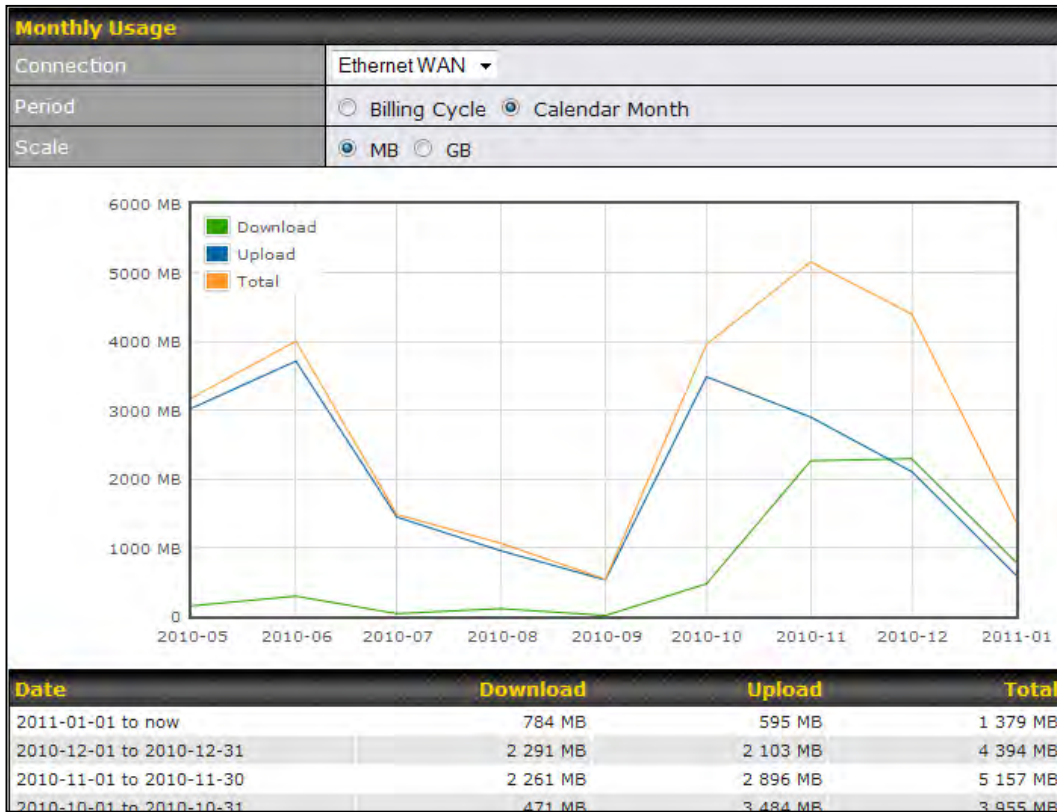
This page shows the monthly bandwidth usage for each WAN connection. If you have enabled the **Bandwidth Monitoring** feature, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

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



All WAN Monthly Bandwidth Usage

# Pepwave MAX and Surf User Manual



Ethernet WAN Monthly Bandwidth Usage

## Tip

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

## Appendix A. Restoration of Factory Defaults

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

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

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

### Important Note

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

## Appendix B. Case Studies

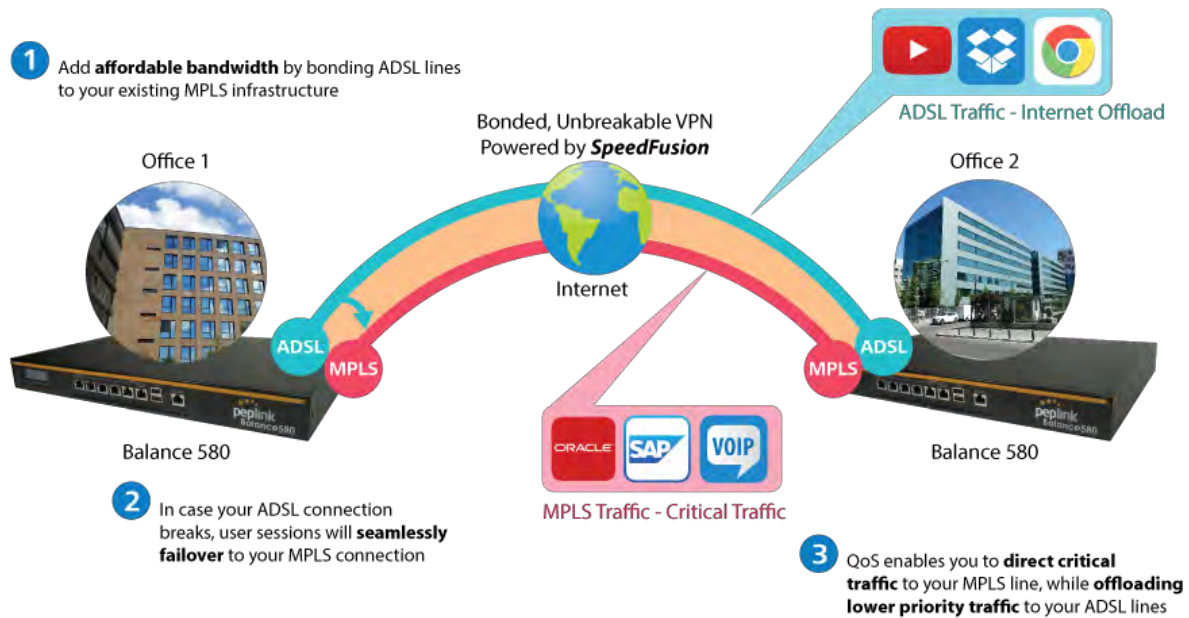
### MPLS Alternative

Our SpeedFusion enabled routers can be used to bond multiple low-cost/commodity Internet connections to replace an expensive managed business Internet connection, private leased line, MPLS, and frame relay without sacrificing reliability and availability.

Belows are typical deployment for using our Balance routers to replace expensive MPLS connection with commodity connections, such as ADSL, 3G, and 4G LTE links.

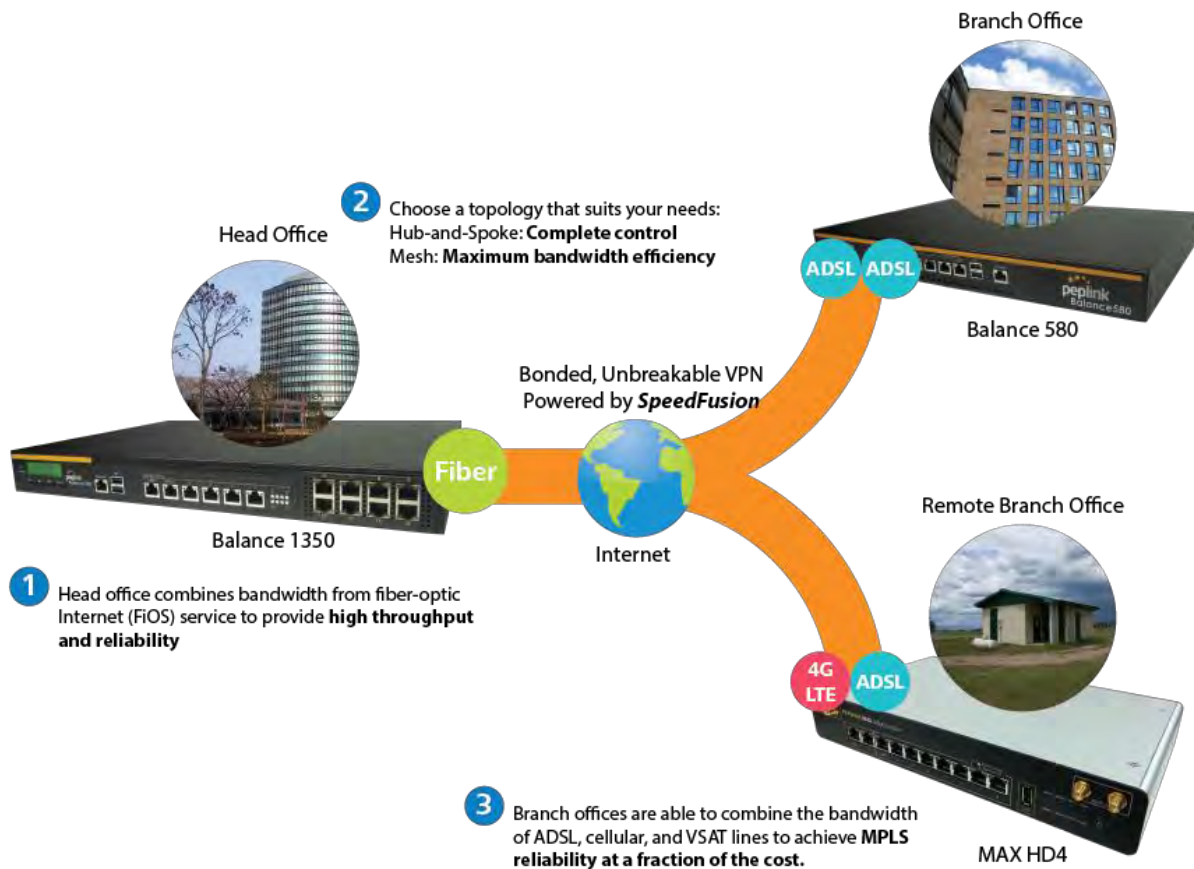
Our MAX HD4 routers are capable of connecting to four different wireless networks simultaneously.

## Option 1: MPLS Supplement



Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your network.

## Option 2: MPLS Alternative

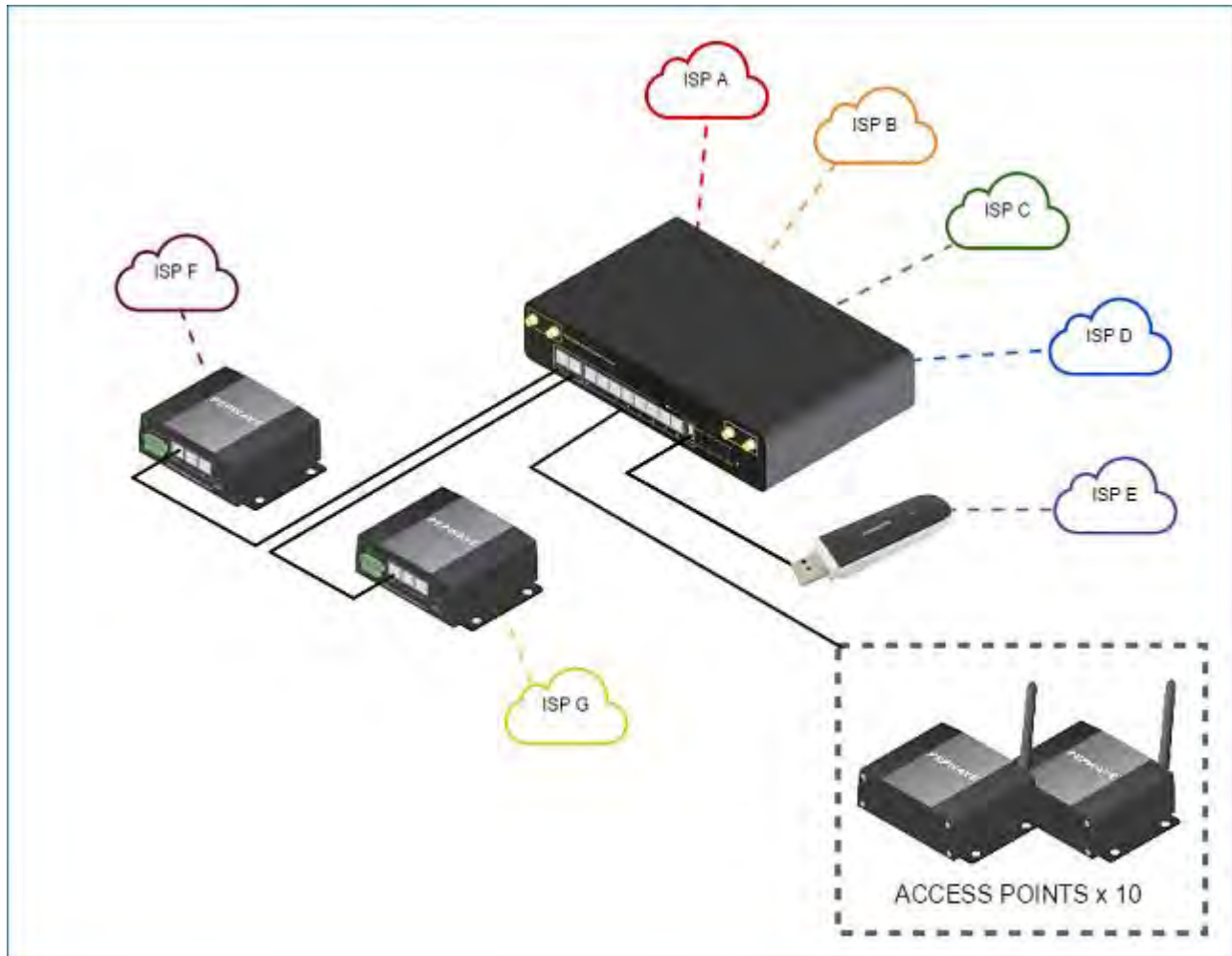


Achieve faster speeds and greater reliability while paying only 20% of MPLS costs by connecting multiple ADSL, 3G, and 4G LTE links. Choose a topology that suits your requirements: a hub-and-spoke topology maximizes control over your network, while a meshed topology can reduce your bandwidth overhead by enabling your devices to form Unbreakable VPN connections directly with each other.



## Network Traffic Distribution

How to distribute network traffic with 7 x LTE Cellular WANs simultaneously using a HD4



### Overview

Picture a coach full of some of the world's finest developers, programmers, hackers and technologists used as transportation between the company car park and corporate headquarters. Or perhaps a temporary office deployed rapidly for disaster recovery or whilst waiting for fixed line connectivity to be installed.

### Requirement:

- As much bandwidth as possible to share between bandwidth hungry users and their applications.
- The ability to use multiple cellular carriers, dependant on coverage (particularly if installed in a moving vehicle) and bandwidth allowance.



# Pepwave MAX and Surf User Manual

- Intelligent load balancing across all available connections and automatic WAN health/availability detection.
- In the case of a rapid site deployment - complete wireless network coverage of the building.

## **Solution Design:**

- A HD4 is installed as the local internet gateway. It has 4 active LTE cellular internet connections to the internet built in, and supports dual SIMs per connection (in an Active/Passive configuration for coverage or bandwidth allowance purposes).
- The HD4 has two BR1 LTE routers connected on its wired WAN ports. These also have an active cellular internet connection (with the same dual sim support as above).
- The HD4 also has a USB LTE cellular Dongle attached to provide another internet connection.
- Connected to the LAN of the HD4 are up to 10 Peplink Wi-Fi access points. 8 APs can be directly connected to the HD4 using the 8 physical LAN ports, any more are connected using an additional switch (not shown above).
- The HD4 acts as a AP Controller for the attached APs, providing centralised Wi-Fi configuration, firmware and security management.

## **Future Expansion:**

- The HD4 supports up to 8 SIM cards (with 4 actively used at any one time), the BR1s support two SIM cards each (with one actively used by each BR1). The additional SIMs can be added to take advantage of cellular data promotions, or to provide the highest number

## **Additional Options / Considerations**

- A Captive Portal can be deployed on the HD4 to allocate a bandwidth allowance per connected client to control bandwidth consumption
- External DNS providers (such as OpenDNS) can be used to restrict internet access destinations, blocking video streaming sites, OS update services and other high bandwidth activities.
- QoS can be applied to prioritise key applications (such as VoIP)
- SpeedFusion VPN and WAN Smoothing might be configured to provide a secure, high quality unbreakable VPN connection to corporate applications and resources improving staff productivity.

# Pepwave MAX and Surf User Manual

- Using a SpeedFusion VPN connection to the vehicle, wall boards and bulkhead mounted displays can show the vehicle location (using the HD4's inbuilt GPS) and other important corporate announcements pushed to the vehicle displays from a central corporate server.

**Devices Deployed: MAX HD4, BR1, AP One Series**

## Singapore National Day Parade 2015

Client: Singapore National Day Parade

Challenges:

- Security
- Bandwidth
- Connectivity
- Portability

Solution:

- MAX BR1 ENT
- MAX BR1 Slim
- MAX HD2
- MAX HD4
- Balance 2500
- SpeedFusion



August, 2015. Singapore held their largest ever National Day Parade to commemorate their 50th year of independence. The main display of the event – Singapore's Mobile Column comprised of more than 150 military vehicles and covered a distance of 20 KM along the Greater Marina Bay area.

This raised a multitude of security challenges and chief amongst which, was public safety. Road traffic, spectator safety, Mobile Column status, these were just a few of a long list of things that required real-time surveillance. This real-time data was to be fed constantly to the Core Command Group and various public safety agencies, so having rapidly deployable networks with huge amounts of bandwidth and top-notch reliability was of paramount importance.

The plan was to deploy a combination of HD pan tilt zoom (PTZ) CCTVs on high rise rooftops and roadside in the hundreds. But even with these super zoom-capable cameras, blind spots and blocked line of sights were inevitable. This was where the Mobile Rider

# Pepwave MAX and Surf User Manual

came in. An electronic self-balancing scooter fitted with 4 HD cameras, 4G/LTE Peplink BR1 Slim router and batteries to last for 6 hours covered the grounds that the fixed-locations CCTVs could not.

To enable their high definition monitoring and streaming throughout the parade stretch, the Event Committee appointed Peplink Partner iT-DnS PTE Ltd., who has a solid track record in rapidly deployable networking solutions for event surveillance, as well as years of experience in managing public safety monitoring for past National Day Parades. iT-DnS decided to deploy a Balance 2500 in order to achieve a SpeedFusion bonded network with 2Gbps of throughput. Scattered throughout the stretch was an assortment of surveillance cameras fitted with MAX BR1 ENTs and BR1 Slims. Public safety agencies that had access to the monitoring feed connected via MAX HD2s and HD4s. As for the Mobile Rider solution, the MAX BR1 Slim with its low power requirements and USB port allows it to run for 6 hours continuously with a 10,000mAh portable battery pack.

The Core Command Group was able to stream real time HD footage that allowed them to make decisions and respond to immediate threats. Multiple agencies also had simultaneous access to the feed elsewhere to monitor other safety and strategic concerns. Due to the on-ground effectiveness of the Mobile Rider vehicle, the number of surveillance cameras deployed were reduced by more than half, saving the organizers at least 50% in cost.

“Love it! The MAX series and SpeedFusion provided the flexibility and stability like we’ve never seen before!” -Melvin Lee, Operation Director. iT-DnS PTE Ltd.

# Pepwave MAX and Surf User Manual

## UNOLS (University-National Oceanographic Laboratory System)



“R/V Roger Revelle. A US Navy-owned research vessel operated by Scripps Institution of Oceanography as part of the wider UNOLS (University-National Oceanographic Laboratory System) fleet. We replaced our \$10,000+ Cisco router with a Peplink Balance 580 to load balance now three satellite connections (a proprietary system developed in-house, and two commercial systems from C-Bird and Inmarsat), and (if available) shore-based network connection and/or a 3g/4g cellular network. The 580 also administers several AP-One's deployed across the vessel.

We require a robust, and reliable internet link to shore in order for scientists onboard to conduct successful oceanographic research (downloading weather maps, downloading live data from equipment deployed in the ocean, live satellite imagery, outsourcing data processing at shore, outreach programs, etc...).

[Photo taken by me, in Keelung Harbor, Taiwan Oct 2014; as we're in between science deployments in and around the South China Sea. Notice the Seatel radome up on top using our proprietary HiSeasNet C-Band Satellite Internet System, and the smaller radome off the port side above the bridge, which is the Inmarsat FleetBroadBand system.]”

Daniel Yang – UNOLS



## KPKM Pioneers Bus Wi-Fi With Successful Peplink Deployment



The Municipal Enterprise of Public Transport, Ltd (KPKM), a privatized public bus company in Poland, had been looking for a way to differentiate itself and stand out from the competition. KPKM decided to do something that had never been attempted before: offering free Wi-Fi Internet to their passengers. With ACO Solutions' assistance, KPKM conducted lengthy trials and determined Peplink to be the best-performing solution. The ensuing installation for the entire fleet took just two weeks to complete, and KPKM gained more than just the ability to offer free Wi-Fi Internet.

### Requirements

- Offer quality Wi-Fi Internet to all bus passengers, for free
- A system that can simultaneously handle Internet access from all on-board passengers
- Display advanced Captive Portals with information for passengers or advertising.
- Integrated fleet management system, with the ability to export the collected data.

# Pepwave MAX and Surf User Manual

- 1 Free Internet is delivered to passengers via Wi-Fi, with Captive Portal controlling access and displaying ads on demand.



KPKM Bus fleet

- 2 The MAX BR1 is equipped with two SIM cards, each connects to a different network carrier.



MAX BR1

- 3 When the bus roams out of signal range of one carrier, it will automatically failover to the other network to continue delivering Internet service.

## Solution

- Pepwave MAX BR1
- InControl 2 Fleet Management
- Unbreakable Internet

## Benefits

- InControl 2's flexibility enabled the implementation of ACO Solutions' advertising system designed to bring in revenue and sustain the free Internet
- InControl 2's powerful API makes it possible for a third party systems to interface with Peplink devices. KPKM is able to collect user statistics and improve scheduling efficiency with the data
- Passengers enjoy stable, free Wi-Fi Internet
- The entire fleet's real-time location now available from InControl 2's fleet tracking and management
- Highly durable, operating between five and 122 degrees Fahrenheit, without issue
- System has laid the groundwork for future expansion, such as CCTV, bus tracking via mobile apps for users, and display of bus location on timetables
- Successfully set an example and provided proof of concept for the rest of the public transport sector in Poland

## Appendix C. Declarations

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

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

5.15 ~ 5.25GHZ is for indoor user only.

### IMPORTANT NOTE

#### FCC Radiation Exposure Statement (for MAX BR1 mini)

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

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

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

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

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

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

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



# Pepwave MAX and Surf User Manual

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

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

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

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

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

### **3. CE Statement for Pepwave Routers**

Europe – EU Declaration of Conformity

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

- EN 60950-1: 2006 + A11 : 2009+A1 : 2010+ A12: 2011  
Safety of Information Technology Equipment
- EN50385 : 2002 / Article 3(1)(a)  
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public  
  
EN 300 328 V1.7.1: 2006  
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 908-1 V5.2.1: 2011  
Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third-Generation cellular networks; Part 1: Harmonized EN for IMT-2000, introduction and common

# Pepwave MAX and Surf User Manual

requirements, covering essential requirements of article 3.2 of the R&TTE Directive

- EN 301 511 V9.0.2: 2003  
Global System for Mobile communications (GSM); Harmonized standard for mobile stations in the GSM 900 and DCS 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC)
- EN 301 489-1 V1.9.2: 2008  
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-7 V1.3.1: 2005  
ElectroMagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment ad services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
- EN 301 489-17 V2.2.1: 2012  
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment
- EN 301 489-24 V1.5.1: 2010  
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA) for Mobile and portable (UE) radio and ancillary equipment



Česky [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in

# Pepwave MAX and Surf User Manual

	compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente [ <i>nombre del fabricante</i> ] declara que el [ <i>clase de equipo</i> ] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [ <i>name of manufacturer</i> ] ΔΗΛΩΝΕΙ ΟΤΙ [ <i>type of equipment</i> ] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente [ <i>nom du fabricant</i> ] déclare que l'appareil [ <i>type d'appareil</i> ] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente [ <i>nome del costruttore</i> ] dichiara che questo [ <i>tipo di apparecchio</i> ] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo [ <i>name of manufacturer / izgatavotāja nosaukums</i> ] deklarē, ka [ <i>type of equipment / iekārtas tips</i> ] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [ <i>manufacturer name</i> ] deklaruoja, kad šis [ <i>equipment type</i> ] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart [ <i>naam van de fabrikant</i> ] dat het toestel [ <i>type van toestel</i> ] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, [ <i>isem tal-manifattur</i> ], jiddikjara li dan [ <i>il-mudel tal-prodott</i> ] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, [ <i>gyártó neve</i> ] nyilatkozom, hogy a [ <i>... típus</i> ]megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym [ <i>nazwa producenta</i> ] oświadczam, że [ <i>nazwa wyrobu</i> ] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	[ <i>Nome do fabricante</i> ] declara que este [ <i>tipo de equipamento</i> ] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	[ <i>Ime proizvajalca</i> ] izjavlja, da je ta [ <i>tip opreme</i> ] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[ <i>Meno výrobcu</i> ] týmto vyhlasuje, že [ <i>typ zariadenia</i> ]spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	[ <i>Valmistaja = manufacturer</i> ] vakuuttaa täten että [ <i>type of equipment = laiteen tyyppimerkintä</i> ] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar [ <i>företag</i> ] att denna [ <i>utrustningstyp</i> ] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

## **Appendix D. Product Datasheets**

# PEP WAVE

Broadband Possibilities

[www.pepwave.com](http://www.pepwave.com)

## **Contact Us:**

### **Sales**

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

### **Support**

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

### **Business Development and Partnerships**

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