# Pepwave MAX and Pepxim User Manual

**Pepwave Products:**
MAX 700/HD2/HD2 IP67/HD2 mini/HD4/Transit/CX4/BR1/BR1 Mini/BR1 Slim/BR1 ENT/BR1 Pro LTE/BR1 IP55/BR2 IP55//BR1 IP67/On-The-Go/MAX HD2/HD4 with MediaFast

**Pepxim Products:**
NPC/SD-PMU

Pepwave Firmware 7
January 2017

Copyright & Trademarks
Specifications are subject to change without notice. Copyright © 2017 Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Pepwave Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

# Table of Contents


**1 Introduction and Scope** 8

**2 Glossary** 9

**3 Product Features** 10

3.1 Supported Network Features 10

3.1.1 WAN 10

3.1.2 LAN 11

3.1.3 VPN 11

3.1.4 Firewall 11

3.1.5 Captive Portal 11

3.1.6 Outbound Policy 11

3.1.7 AP Controller 12

3.1.8 QoS 12

3.2 Other Supported Features 12

**4 Pepwave MAX Mobile Router Overview** 13

4.1 MAX 700 13

4.2 MAX HD2 15

4.3 MAX HD2 IP67 17

4.4 MAX HD2 Mini 18

4.5 MAX Transit 19

4.6 MAX CX4 20

4.7 MAX HD4 / HD2 and HD4 with MediaFast 21

4.8 MAX BR1 22

4.9 MAX BR1 MK2 24

4.10 MAX BR1 Slim 25

4.11 MAX BR1 ENT 25

4.12 MAX BR1 Pro LTE 27

4.13 MAX Hotspot 28

4.14 BR1 Mini 29


 Copyright @ 2017 Pepwave

4.15 MAX BR1/2 IP55 30
4.16 MAX BR1 IP67 32
4.17 MAX On-The-Go 32
4.18 NPC (Network Power Controller) 33
4.19 SD-PMU 34

5. **Advanced Feature Summary** 35
5.1 Drop-in Mode and LAN Bypass: Transparent Deployment 35
5.2 QoS: Clearer VoIP 35
5.3 Per-User Bandwidth Control 36
5.4 High Availability via VRRP 36
5.5 USB Modem and Android Tethering 37
5.6 Built-In Remote User VPN Support 38
5.7 SIM-card USSD support 39

6. **Installation** 40
6.1 Preparation 40
6.2 Constructing the Network 41
6.3 Configuring the Network Environment 41

7 **Mounting the Unit** 42
7.1 Wall Mount 42
7.2 Car Mount 42
7.3 IP67 Installation Guide 42

8 **Connecting to the Web Admin Interface** 43

9 **Configuring the LAN Interface(s)** 45
9.1 Basic Settings 45
9.2 Port Settings 55
9.3 Captive Portal 56

10 **Configuring the WAN Interface(s)** 59
10.1 Ethernet WAN 60
10.1.1 DHCP Connection 62

 Copyright @ 2017 Pepwave

10.1.2 Static IP Connection 63
10.1.3 PPPoE Connection 65
10.1.4 L2TP Connection 66
10.2 Cellular WAN 67
10.3 Wi-Fi WAN 73
10.3.1 Creating Wi-Fi Connection Profiles 79
10.4 WAN Health Check 80
10.5 Dynamic DNS Settings 83

**11 Advanced Wi-Fi Settings** 85

**12 MediaFast Configuration** 89
12.1 Setting Up MediaFast Content Caching 89
12.2 Scheduling Content Prefetching 90
12.3 Viewing MediaFast Statistics 92

**13 Bandwidth Bonding SpeedFusionTM / PepVPN** 93
13.1 PepVPN 93
13.2 The Pepwave Router Behind a NAT Router 100
13.3 SpeedFusionTM Status 101

**14 IPsec VPN** 102
14.1 IPsec VPN Settings 102

**15 Outbound Policy Management** 106
15.1 Outbound Policy 106
15.2 Custom Rules for Outbound Policy 107
15.2.1 Algorithm: Weighted Balance 108
15.2.2 Algorithm: Persistence 109
15.2.3 Algorithm: Enforced 110
15.2.4 Algorithm: Priority 111
15.2.5 Algorithm: Overflow 111
15.2.6 Algorithm: Least Used 112
15.2.7 Algorithm: Lowest Latency 112
15.2.8 Expert Mode 113

 Copyright @ 2017 Pepwave

**16 Inbound Access** 114
16.1 Port Forwarding Service 114
16.1.1 UPnP / NAT-PMP Settings 116

**17 NAT Mappings** 117

**18 QoS** 119
18.1 User Groups 119
18.2 Bandwidth Control 120
18.3 Application 120
18.3.1 Application Prioritization 120
18.3.2 Prioritization for Custom Applications 121
18.3.3 DSL/Cable Optimization 121

**19 Firewall** 121
19.1 Outbound and Inbound Firewall Rules 122
19.1.1 Access Rules 122
19.1.2 Apply Firewall Rules to PepVpn Traffic 125
19.1.3 Intrusion Detection and DoS Prevention 126
19.2 Content Blocking 127
19.2.1 Application Blocking 127
19.2.2 Web Blocking 128
19.2.3 Customized Domains 128
19.2.4 Exempted User Groups 128
19.2.5 Exempted Subnets 128
19.2.6 URL Logging 128

**20 OSPF & RIPv2** 129

**21 Remote User Access** 131

**Miscellaneous Settings** 133
21.1 High Availability 133
21.2 PPTP Server 137
21.3 Certificate Manager 139

 Copyright @ 2017 Pepwave

21.4 Service Forwarding 139
21.4.1 SMTP Forwarding 140
21.4.2 Web Proxy Forwarding 141
21.4.3 DNS Forwarding 141
21.4.4 Custom Service Forwarding 141
21.5 Service Passthrough 142
21.6 GPS Forwarding 143

**22 AP Controller** 144
22.1 Wireless SSID 144
22.2 Settings 148

**23 AP Controller Status** 154
23.1 Info 154
23.2 Access Point (Usage) 156
23.3 Wireless SSID 158
23.4 Wireless Client 159
23.5 Nearby Device 161
23.6 Event Log 162

**24 Toolbox** 163

**25 System Settings** 163
25.1 Admin Security 163
25.2 Firmware 168
25.3 Time 169
25.4 Schedule 169
25.5 Email Notification 171
25.6 Event Log 173
25.7 SNMP 173
25.8 InControl 176
25.9 Configuration 176
25.10 Feature Add-ons 178
25.11 Reboot 178

 Copyright @ 2017 Pepwave

**26 Tools** 178
26.1 Ping 178
26.2 Traceroute Test 179
26.3 PepVPN Test 180
26.4 Wake-on-LAN 181
26.5 CLI (Command Line Interface Support) 181

**27 Status** 182
27.1 Device 182
27.2 GPS Data 183
27.3 Active Sessions 183
27.4 Client List 185
27.5 WINS Client 186
27.6 UPnP / NAT-PMP 186
27.7 SpeedFusion Status 187
27.8 Event Log 191
28 Bandwidth Status 192
28.1 Real-Time 192
28.2 Hourly 193
28.3 Daily 194
28.4 Monthly 195

**Appendix A: Restoration of Factory Defaults** 197

**Appendix B: Declaration** 198

 Copyright @ 2017 Pepwave

# 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.

The MAX wireless SD-WAN router series has a wide range of products suitable for many different deployments and markets. Entry level SD-WAN models such as the MAX BR1 are suitable for SMEs or branch offices. High-capacity SD-WAN routers such as the MAX HD2 are suitable for larger organizations and head offices.

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

 Copyright @ 2017 Pepwave

# 2 Glossary

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

| Term | Definition |
|---|---|
| 3G | 3rd generation standards for wireless communications (e.g., HSDPA) |
| 4G | 4th generation standards for wireless communications (e.g., LTE) |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| EVDO | Evolution-Data Optimized |
| FQDN | Fully Qualified Domain Name |
| 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 |

 Copyright @ 2017 Pepwave

# 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.

## 3.1 Supported Network Features

### 3.1.1 WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- Built-in 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, dyndns.org, no-ip.org, tzo.com and DNS-O-Matic)
- Ping, DNS lookup, and HTTP-based health check

 Copyright @ 2017 Pepwave

### 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

 Copyright @ 2017 Pepwave

- 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

 Copyright @ 2017 Pepwave

- Support USB tethering on Android 2.2+ phones

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

# 4 Pepwave MAX Mobile Router Overview

## 4.1 MAX 700

### 4.1.1 Panel Appearance

### 4.1.2 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 |

 Copyright @ 2017 Pepwave

| | | |
|---|---|---|
| | Green | Ready |

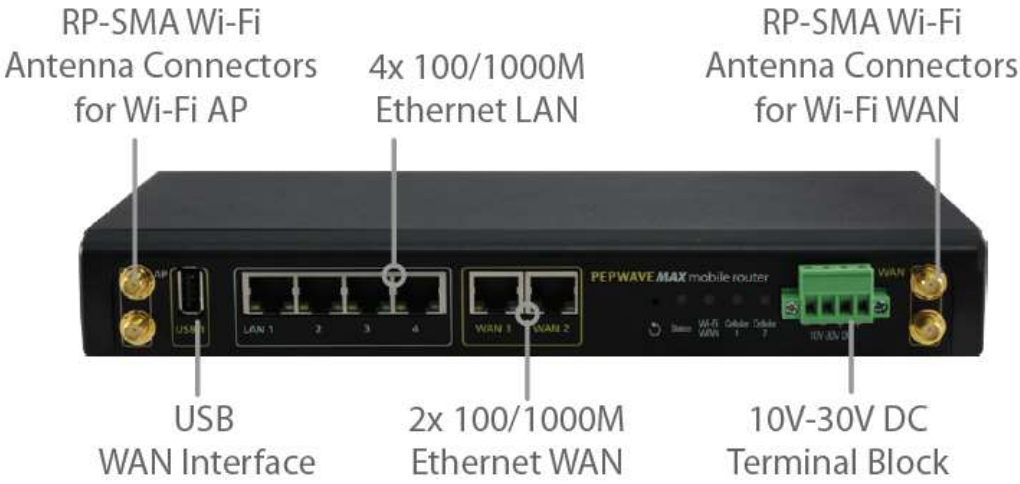
| Wi-Fi AP and Wi-Fi WAN Indicators | | |
|---|---|---|
| **Wi-Fi WAN** | OFF | Disconnected |
| | Blinking slowly | Connecting to network |
| | Blinking | Connected to network with traffic |
| | ON | Connected to network without traffic |
| **Wi-Fi AP** | OFF | Disabled |
| | Blinking slowly | Enabled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

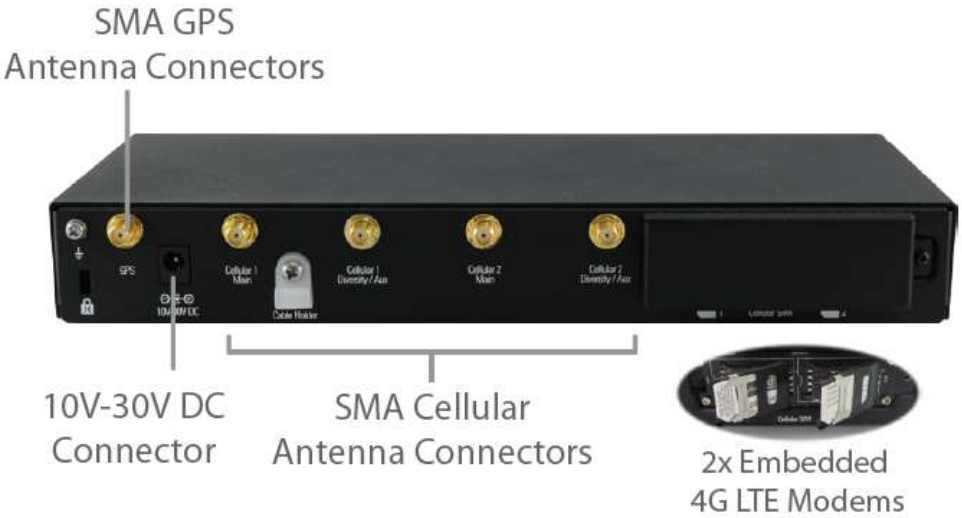
| LAN and Ethernet WAN Ports | | |
|---|---|---|
| **Green LED** | ON | 10 / 100/ 1000 Mbps |
| **Orange LED** | Blinking | Data is transferring |
| | OFF | No data is being transferred or port is not connected |
| **Port Type** | Auto MDI/MDI-X ports | |

 Copyright @ 2017 Pepwave

## 4.2 MAX HD2

### 4.2.1 Panel Appearance




 Copyright @ 2017 Pepwave

### 4.2.2 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 |

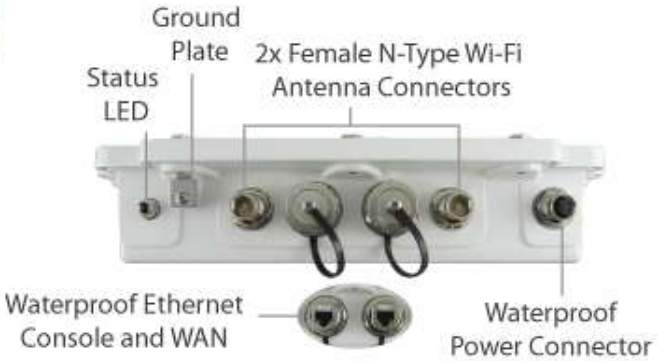
| Wi-Fi AP and Wi-Fi WAN Indicators | | |
|---|---|---|
| **Wi-Fi WAN / Cellular 1 / Cellular 2** | OFF | Disabled Intermittent |
| | Blinking slowly | Connecting to wireless network(s) |
| | Blinking | Connected to wireless network(s) with traffic |
| | ON | Connected to wireless network(s) without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

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

 Copyright @ 2017 Pepwave

## 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 |

 Copyright @ 2017 Pepwave

## 4.4 MAX HD2 mini

### 4.4.1 Panel Appearance

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

### 4.4.2 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 WAN Indicators** | | |
| **Cellular 1 / Cellular 2** | 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** | | |
| **Green LED** | ON | 10 / 100 / 1000 Mbps |
| **Orange LED** | Blinking | Data is transferring |
| | OFF | No data is being transferred or port is not connected |
| **Port Type** | Auto MDI/MDI-X ports | |

 Copyright @ 2017 Pepwave

## 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 | | |
|---|---|---|
| **Status** | OFF | System initializing |
| | Red | Booting up or busy |
| | Blinking red | Boot up error |
| | Green | Ready |

| Cellular WAN Indicators | | |
|---|---|---|
| **Cellular 1 / Cellular 2*** | 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 | | |
|---|---|---|
| **Green LED** | ON | 10 / 100 / 1000 Mbps |
| **Orange LED** | Blinking | Data is transferring |
| | OFF | No data is being transferred or port is not connected |
| **Port Type** | Auto MDI/MDI-X ports | |

 Copyright @ 2017 Pepwave

## 4.6 MAX CX4

### 4.6.1 Panel Appearance

### 4.6.2 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 |

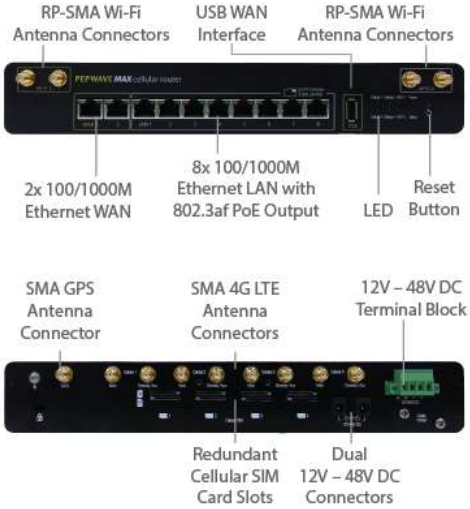
| Wi-Fi AP and Wi-Fi WAN Indicators | | |
|---|---|---|
| **Wi-Fi WAN / Cellular 1 / Cellular 2** | OFF | Disabled Intermittent |
| | Blinking slowly | Connecting to wireless network(s) |
| | Blinking | Connected to wireless network(s) with traffic |
| | ON | Connected to wireless network(s) without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

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

 Copyright @ 2017 Pepwave

## 4.7 MAX HD4 / HD2 and HD4 with MediaFast

### 4.7.1 Panel Appearance




### 4.7.2 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 AP and Wi-Fi WAN Indicators | | |
|---|---|---|
| **Wi-Fi WAN / Cellular 1 / Cellular 2** | 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 |

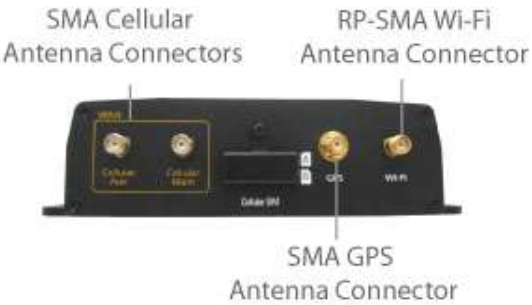
| LAN and Ethernet WAN Ports | | |
|---|---|---|
| **Green LED** | ON | 10 / 100 / 1000 Mbps |
| **Orange LED** | Blinking | Data is transferring |
| | OFF | No data is being transferred or port is not connected |
| **Port Type** | Auto MDI/MDI-X ports | |

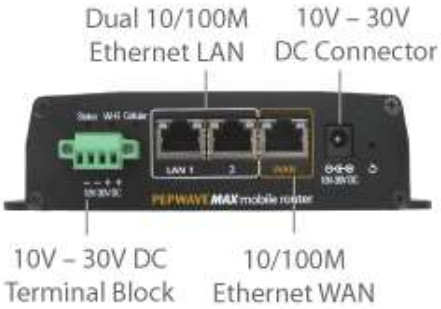
 Copyright @ 2017 Pepwave

# 4.8 MAX BR1

## 4.8.1 Panel Appearance

MAX-BR1-LTE Version




MAX-BR1 Version

## 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 |

 Copyright @ 2017 Pepwave

| 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 | |

 Copyright @ 2017 Pepwave

## 4.9 MAX BR1 MK2

### 4.9.1 Panel Appearance

### 4.9.2 LED Indicators

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

| Wi-Fi AP and Wi-Fi WAN Indicators | | |
|---|---|---|
| **Wi-Fi WAN / Cellular 1 / Cellular 2** | 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 | | |
|---|---|---|
| **Green LED** | ON | 10 / 100 / 1000 Mbps |
| **Orange LED** | Blinking | Data is transferring |
| | OFF | No data is being transferred or port is not connected |
| **Port Type** | Auto MDI/MDI-X ports | |

 Copyright @ 2017 Pepwave

## 4.10 MAX BR1 Slim

### 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 |

| 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 | | |
|---|---|---|
| **Green LED** | ON | 100 Mbps |
| | OFF | 10 Mbps |
| **Orange LED** | ON | Port is connected without traffic |

 Copyright @ 2017 Pepwave

| | | |
|---|---|---|
| | Blinking | Data is transferring |
| | OFF | Port is not connected |
| **Port Type** | Auto MDI/MDI-X ports | |

## 4.11 MAX BR1 ENT

### 4.11.1 Panel Appearance

### 4.11.2 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 | |

 Copyright @ 2017 Pepwave

## 4.12 MAX BR1 Pro LTE

### 4.12.1 Panel Appearance

### 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 |

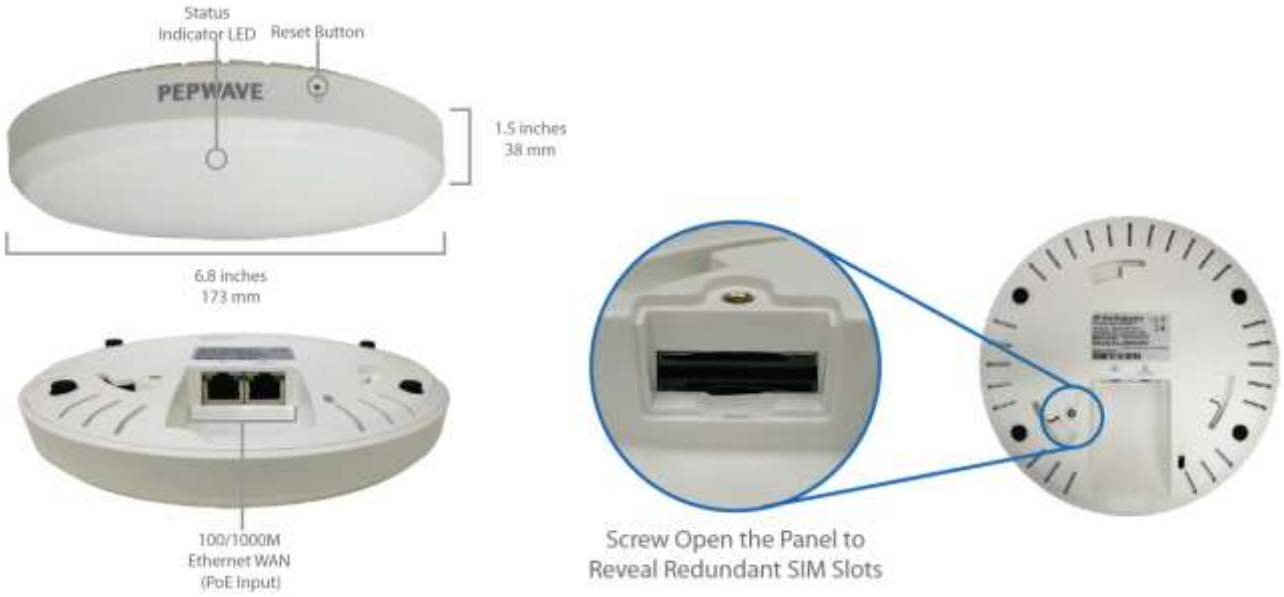
| Cellular Indicators | | |
|---|---|---|
| **Cellular** | OFF | Disabled or no SIM card inserted |
| | ON | Connecting or connected to network(s) |

| 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 | |

 Copyright @ 2017 Pepwave

## 4.13 MAX Hotspot

### 4.13.1 Panel Appearance



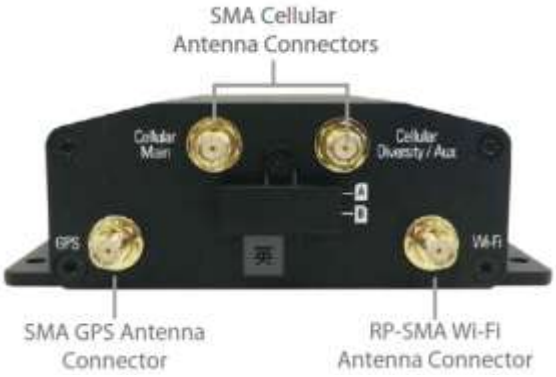

### 4.13.2 LED Indicators

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

 Copyright @ 2017 Pepwave

## 4.14 BR1 Mini

### 4.14.1 Panel Appearance




### 4.14.2 LED Indicators

| 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 | |

 Copyright @ 2017 Pepwave

## 4.15 MAX BR1/2 IP55

### 4.15.1 Panel Appearance

### 4.15.2 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 |

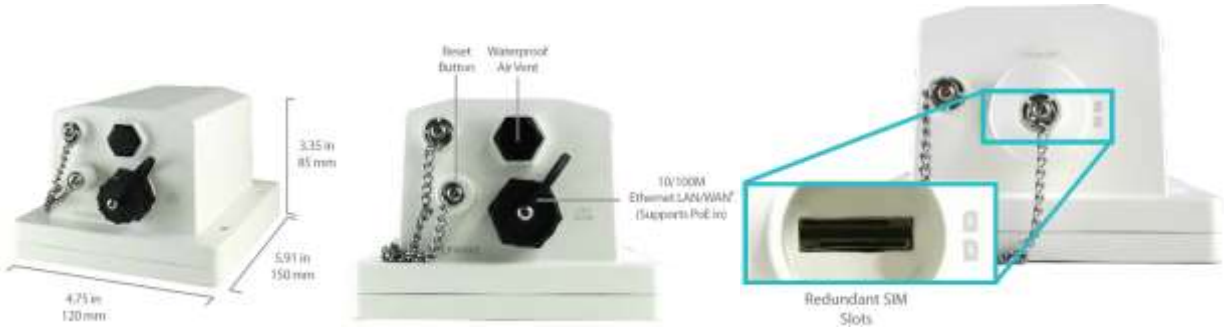
| Cellular Indicators | | |
|---|---|---|
| **Cellular** | OFF | Disabled or no SIM card inserted |
| | ON | Connecting or connected to network(s) |

 Copyright @ 2017 Pepwave

| 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 | |

## 4.16 MAX BR1 IP67

### 4.16.1 Panel Appearance




### 4.16.2 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 |

 Copyright @ 2017 Pepwave

## 4.17 MAX On-The-Go

### 4.17.1 Panel Appearance

### 4.17.2 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 |

 Copyright @ 2017 Pepwave

| 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 | |

## 4.18 NPC (Network Power Controller)

### 4.18.1 Panel Appearance

### 4.18.2 LED Indicators

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

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

| LAN 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 | |

 Copyright @ 2017 Pepwave

## 4.19 SD-PMU

### 4.19.1 Panel Appearance

### 4.19.2 LED Indicators

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

 Copyright @ 2017 Pepwave

# 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)

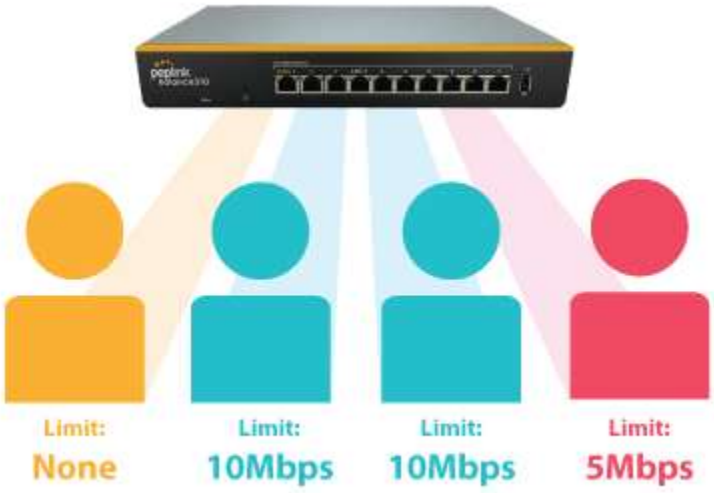
## 5.2 QoS: Clearer VoIP

VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP

 Copyright @ 2017 Pepwave

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

 Copyright @ 2017 Pepwave

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. Peplink 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)

 Copyright @ 2017 Pepwave

## 5.6 Built-In Remote User VPN Support

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.

 Copyright @ 2017 Pepwave

## 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.

 Copyright @ 2017 Pepwave

# 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.

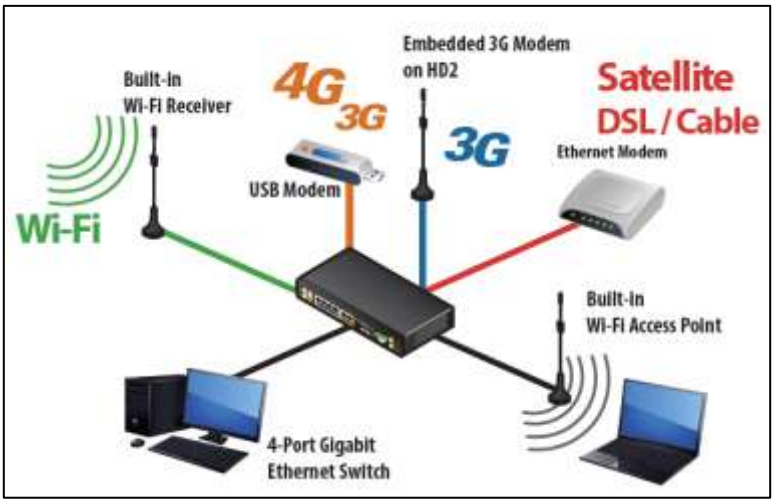
 Copyright @ 2017 Pepwave

## 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**.

 Copyright @ 2017 Pepwave

# 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. Recommeneded 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

 Copyright @ 2017 Pepwave

# 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

 Copyright @ 2017 Pepwave

displayed

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. |

 Copyright @ 2017 Pepwave

# 9 Configuring the LAN Interface(s)

## 9.1 Basic Settings

LAN interface settings are located at **Network>LAN>Network Settings**. Navigating to that page will result in the following dashboard:

| LAN | VLAN | Network | |
|---|---|---|---|
| LAN | None | 172.16.251.1/24 | |
| VLAN1 | 1 | 2.2.2.2/24 | ✖ |
| VLAN2 | 2 | 3.3.3.3/24 | ✖ |
| New LAN | | | |

This represents the LAN interfaces that are active on your router (including VLAN). A grey "X" means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the grey "X".

Alternatively, a red "X" means that there are no settings using the VLAN. You can delete that VLAN by clicking the red "X"

Clicking any of the existing LAN interfaces (or creating a new one) will result in the following

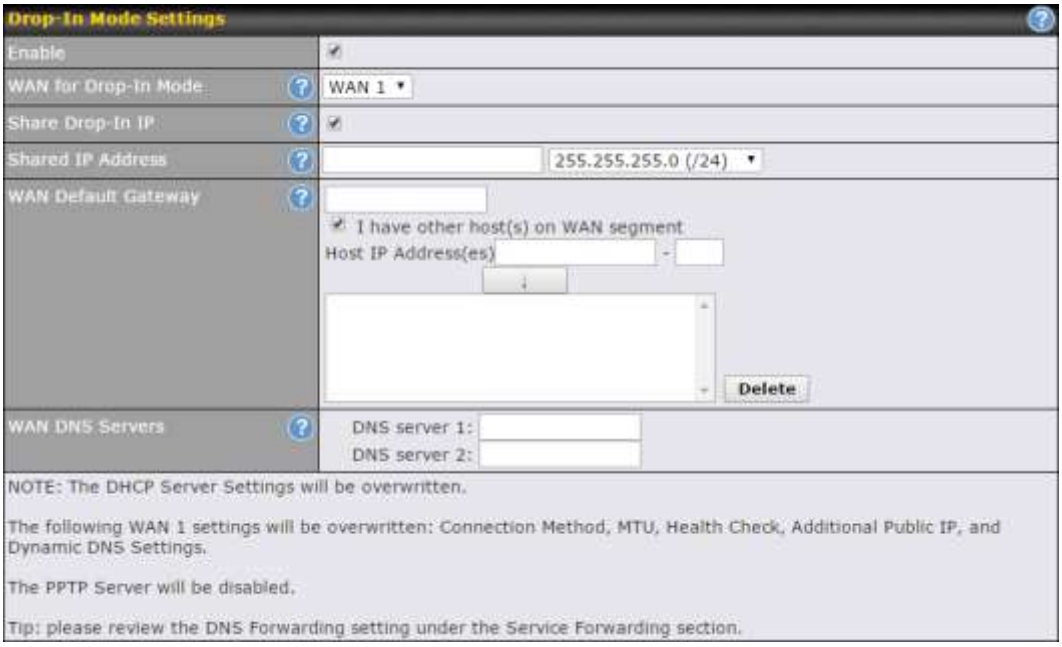
| IP Settings | | |
|---|---|---|
| IP Address | 192.168.50.1 | 255.255.255.0 (/24) |

| IP Settings | |
|---|---|
| **IP Address** | The IP address and subnet mask of the Pepwave router on the LAN. |

| Network Settings | |
|---|---|
| Name | |
| VLAN ID | |
| Inter-VLAN routing | ☑ |
| Captive Portal | ☐ |

 Copyright @ 2017 Pepwave

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




 Copyright @ 2017 Pepwave

| Drop-in Mode Settings | |
|---|---|
| **Enable** | 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. |
| **WAN for Drop-In Mode** | Select the WAN port to be used for drop-in mode. If **WAN 1 with LAN Bypass** is selected, the high availability feature will be disabled automatically. |
| **Share Drop-In IP[A]** | 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.).<br>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.). |
| **Shared IP Address[A]** | 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.) |
| **WAN Default Gateway** | 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 I **have other host(s) on WAN segment** box and enter the IP address of the hosts that need to access LAN devices or be accessed by others. |
| **WAN DNS Servers** | Enter the selected WAN's corresponding DNS server IP addresses. |

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

 Copyright @ 2017 Pepwave

| Layer 2 PepVPN Bridging | |
|---|---|
| **PepVPN Profiles to Bridge** | 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. |
| **Spanning Tree Protocol** | Click the box will enable STP for this layer 2 profile bridge. |
| **Override IP Address when bridge connected** | Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.<br><br>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. |

 Copyright @ 2017 Pepwave

| 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**.<br>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.<br>To define an extended DHCP option, click the **Add** button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only. |
| **DHCP Reservation** | 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.<br>**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.** |

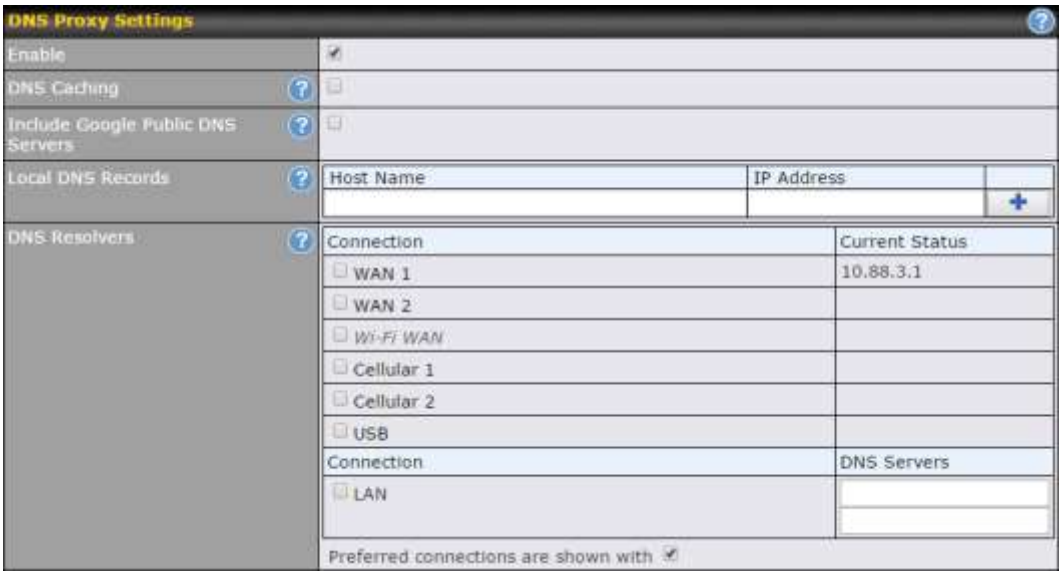
 Copyright @ 2017 Pepwave

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

 Copyright @ 2017 Pepwave




| DNS Proxy Settings | |
|---|---|
| **Enable** | To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN connection. |
| **DNS Caching** | 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, **DNS Caching** is disabled. |
| **Include Google Public DNS Servers** | When this option is **enabled**, 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. |
| **Local DNS Records** | 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 + to create a new record. Press ✖ to remove a record. |
| **DNS Resolvers** [A] | Check the box to enable the WINS server. A list of WINS clients will be displayed at **Network>LAN>DNS Proxy Settings>DNS Resolvers**. 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.<br>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. |

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

 Copyright @ 2017 Pepwave

Finally, if needed, configure Bonjour forwarding, Apple's zero configuration networking protocol. Once VLAN configuration is complete, click **Save** to store your changes.

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

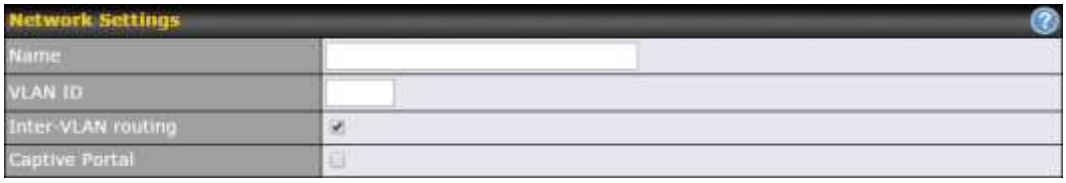
To enable VLAN configuration, click the button in the **IP Settings** section.

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.

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

 Copyright @ 2017 Pepwave

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




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

 Copyright @ 2017 Pepwave

| DHCP Server Settings | |
|---|---|
| **DHCP Server** | 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.<br><br>To enable DHCP bridge relay, please click the icon on this menu item. |
| **IP Range & Subnet Mask** | These settings allocate a range of IP address 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 **Lease Time**, the assigned IP address will no longer be valid and the IP address assignment must be renewed. |
| **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 Servers** | 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 **DHCP WINS Servers** 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 **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 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. |
| **DHCP Reservation** | 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.<br>**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 clients information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.** |

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

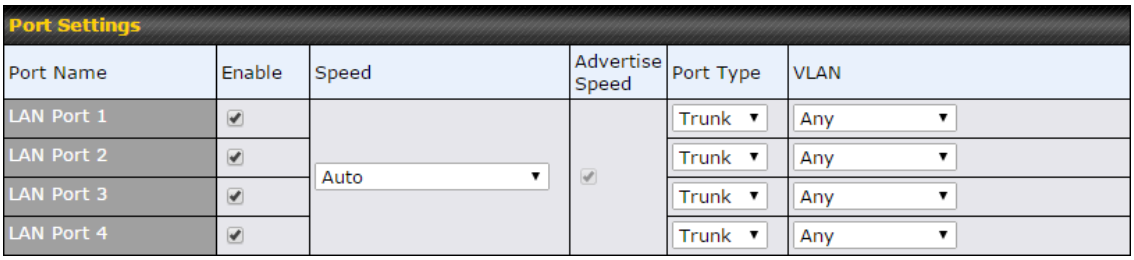
 Copyright @ 2017 Pepwave

| DHCP Relay Settings | |
|---|---|
| **Enable** | Check this box to turn on DHCP relay. Click the icon to disable DHCP relay. |
| **DHCP Server IP Address** | 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 **DHCP Server 1** and **DHCP Server 2.** |
| **DHCP Option 82** | 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 Port Settings

To configure port settings, navigate to **Network > Port Settings**

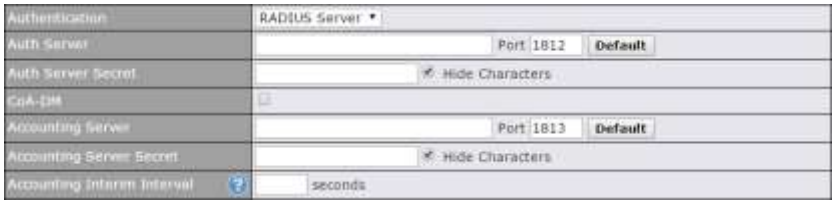



On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

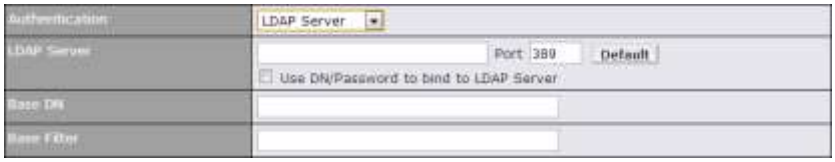
 Copyright @ 2017 Pepwave

## 9.3 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**.

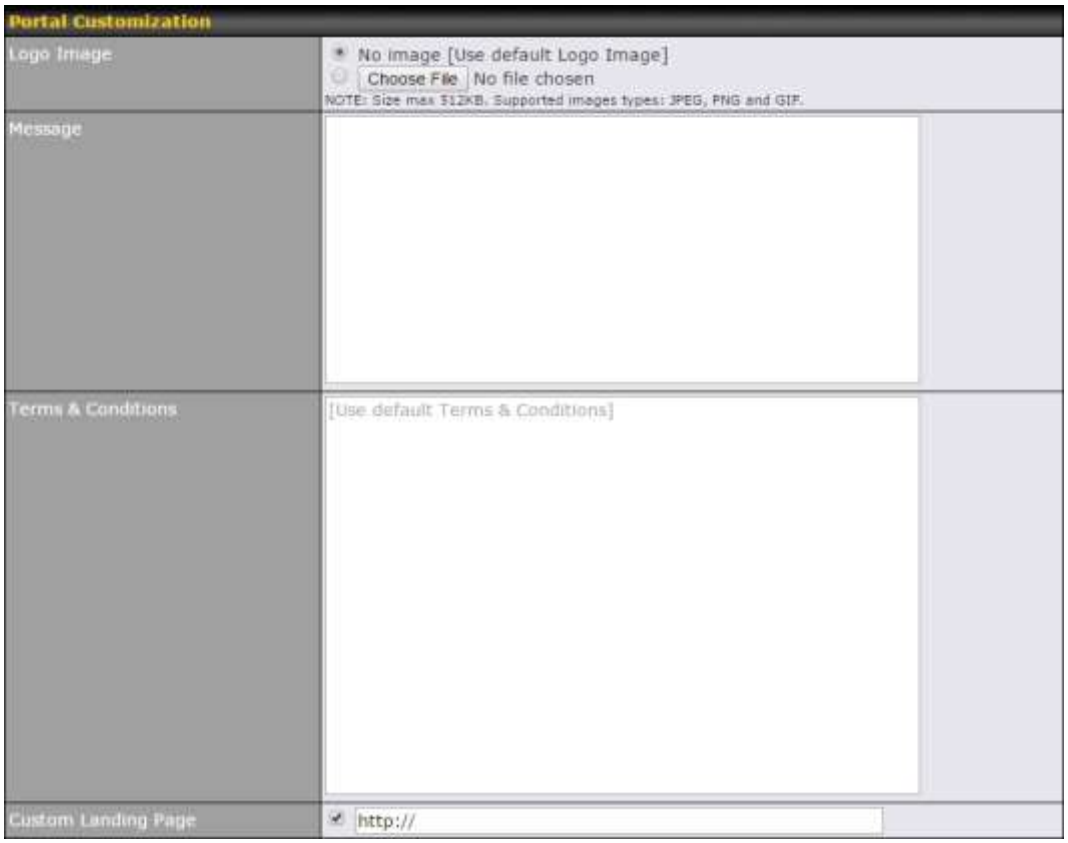
| Captive Portal Settings | |
|---|---|
| **Enable** | Check **Enable** and then, optionally, select the LANs/VLANs that will use the captive portal. |
| **Hostname** | To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click **Default**. |
| **Access Mode** | Click **Open Access** to allow clients to freely access your router. Click **User Authentication** to force your clients to authenticate before accessing your router. |
| **RADIUS Server** | This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:   Fill in the necessary information to complete your connection to the server and enable authentication. |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **LDAP Server** | This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:<br>  <br><br>Fill in the necessary information to complete your connection to the server and enable authentication. |
| **Access Quota** | Set a time and data cap to each user's Internet usage. |
| **Quota Reset Time** | This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached. |
| **Allowed Networks** | 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. |
| **Splash Page** | 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: [Preview] and [✎]. Clicking [Preview] displays a pop-up previewing the captive portal that your clients will see. Clicking [✎] displays the following menu:

 Copyright @ 2017 Pepwave




| Portal Customization | |
|---|---|
| **Logo Image** | Click the **Choose File** button to select a logo to use for the built-in portal. |
| **Message** | If you have any additional messages for your users, enter them in this field. |
| **Terms & Conditions** | 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. |
| **Custom Landing Page** | Fill in this field to redirect clients to an external URL. |

 Copyright @ 2017 Pepwave

# 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. |

 Copyright @ 2017 Pepwave

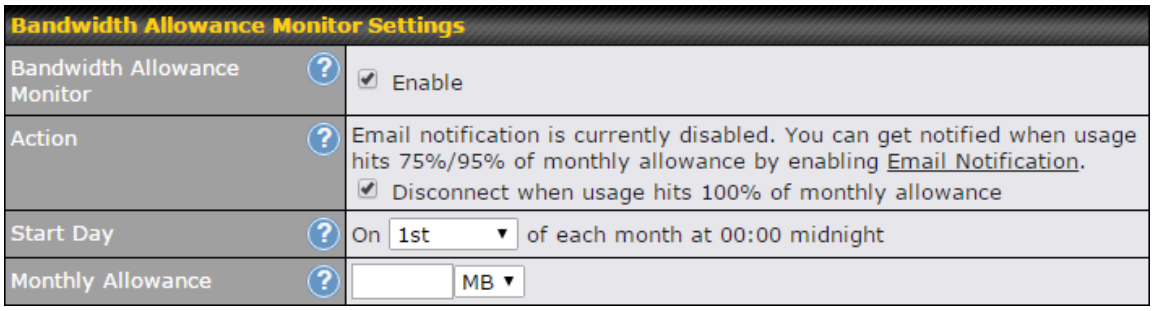
## 10.1 Ethernet WAN

| Health Check Settings | |
|---|---|
| Health Check Method | PING |
| PING Hosts | Host 1: 8.8.8.8<br>Host 2:<br>☐ 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 |

| Health Check Settings | |
|---|---|
| **Health Check Method** | This field specifies the Health Check method to be used for this WAN connection.<br>● Disabled - The WAN connection is always considered to be up and will not be treated as down for any IP routing errors.<br>● PING - ICMP PING packets will be issued to test connectivity with configurable target IP addresses or host names.<br>● DNS Lookup - DNS lookups will be issued to test the connectivity with configurable target DNS server IP addresses.<br>● HTTP - HTTP connections will be issued to test the connectivity with configurable URLs and strings to match.<br><br>Default: DNS Lookup |
| **PING Hosts** | These fields are for specifying the target IP addresses or host names where ICMP Ping packets will be sent to for health check.<br>If the box Use first two DNS servers as PING Hosts is checked, the first two DNS servers will be the ping 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.<br>The connection is considered to be up if ping responses are received from any one of the ping hosts. |
| **Timeout** | If a health check test cannot be completed within the specified amount of time, the test will be treated as failed. |
| **Health Check Interval** | This is the time interval between each health check test. |

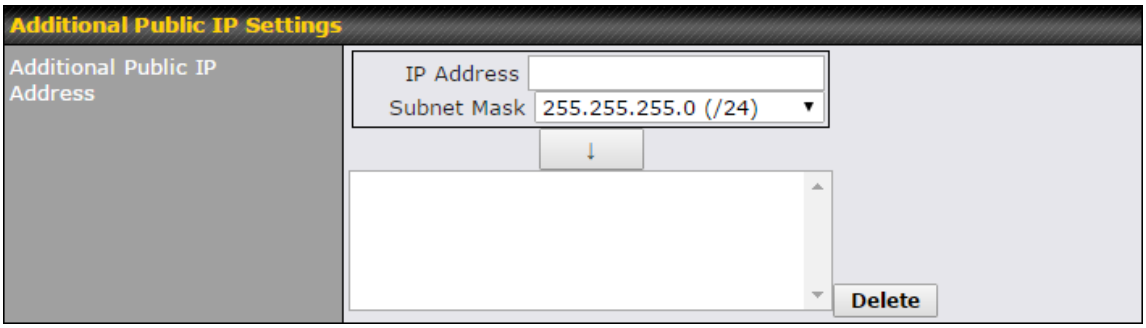
 Copyright @ 2017 Pepwave

| | |
|---|---|
| **Health Check Retries** | This is the number of consecutive check failures before treating a connection as down. |
| **Recovery Retries** | This is the number of responses required after a health check failure before treating a connection as up again. |




| Bandwidth Allowance Monitor Settings | |
|---|---|
| **Bandwidth Allowance Monitor** | 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. |
| **Action** | If Email Notification is enabled, you will receive an email notification when usage hits 75% and 95% of the monthly allowance.<br>If the box Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume 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 select which day of the month a billing cycle starts. |
| **Monthly Allowance** | This field is to specify the bandwidth allowance for each billing cycle. |

 Copyright @ 2017 Pepwave




| Additional Public IP Settings |
|---|
| If you have access to status public IP addresses,, you can assign them on this field. |

| Dynamic DNS Settings | |
|---|---|
| **Dynamic DNS Service Provider** | This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:<br>● changeip.com<br>● dyndns.org<br>● no-ip.org<br>● tzo.com<br>● DNS-O-Matic<br>Select **Disabled** to disable this feature. See **Section 9.5** for configuration details. |

### 10.1.1 DHCP Connection

There are four possible connection methods:

1. DHCP
2. Static IP
3. PPPoE

 Copyright @ 2017 Pepwave

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 | NAT |
| IP Address | 10.88.3.158 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.88.3.253 |
| Hostname (Optional) | Use custom hostname |
| DNS Servers | Obtain DNS server address automatically<br>10.88.3.1<br>Use the following DNS server address(es)<br>DNS Server 1:<br>DNS Server 2: |

| DHCP Connection 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. |
| **Hostname (Optional)** | 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. |
| **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.<br>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.)<br>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. |

### 10.1.2 Static IP Connection

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

 Copyright @ 2017 Pepwave

| | |
|---|---|
| Connection Method | Static IP |
| Routing Mode | NAT |
| IP Address | 10.88.3.158 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.88.3.253 |
| IP Address | |
| Subnet Mask | 255.255.255.0 (/24) |
| Default Gateway | |
| DNS Servers | Use the following DNS server address(es)<br>DNS Server 1:<br>DNS Server 2: |

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

 Copyright @ 2017 Pepwave

### 10.1.3 PPPoE Connection

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

| | |
|---|---|
| Connection Method | PPPoE |
| Routing Mode | NAT |
| IP Address | 10.88.3.158 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.88.3.253 |
| PPPoE User Name | |
| PPPoE Password | |
| Confirm PPPoE Password | |
| Service Name (Optional) | Leave it blank unless it is provided by ISP |
| IP Address (Optional) | Leave it blank unless it is provided by ISP |
| DNS Servers | Obtain DNS server address automatically<br>10.88.3.1<br>Use the following DNS server address(es)<br>DNS Server 1:<br>DNS Server 2: |

| 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.<br>**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.<br>**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 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. |

 Copyright @ 2017 Pepwave

### 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 | L2TP |
| Routing Mode | NAT |
| IP Address | 10.88.3.158 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.88.3.253 |
| L2TP User Name | |
| L2TP Password | |
| Confirm L2TP Password | |
| Server IP Address / Host | |
| Address Type | Dynamic IP Static IP |
| DNS Servers | Obtain DNS server address automatically<br>10.88.3.1<br>Use the following DNS server address(es)<br>DNS Server 1:<br>DNS Server 2: |

| L2TP Settings | |
|---|---|
| **L2TP User Name / Password** | Enter the required information in these fields in order to connect via L2TP to your ISP.<br>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.<br>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.<br><br>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.)<br><br>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. |

 Copyright @ 2017 Pepwave

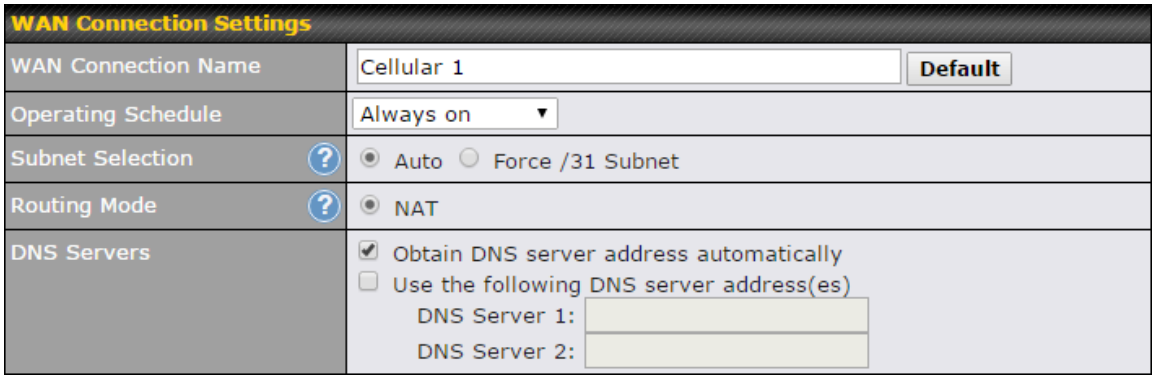
## 10.2 Cellular WAN

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

| Cellular 1 Status | |
|---|---|
| IMSI | (No SIM Card Detected) |
| MEID | A100001F7DC038<br>270113180708241208 |
| ESN | 8052FC8A |
| IMEI | 356144040031862 |

| Cellular Status | |
|---|---|
| **IMSI** | This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only. |
| **MEID** | 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. |
| **ESN** | This serves the same purpose as MEID HEX but uses an older format. |
| **IMEI** | This is the unique ID for identifying the modem in GSM/HSPA mode. |

 Copyright @ 2017 Pepwave




| WAN Connection Settings | |
|---|---|
| **WAN Connection Name** | Enter a name to represent this WAN connection. |
| **Operating Schedule** | Click the drop-down menu to apply a time schedule to this interface if needed. |
| **Subnet Selection** | Auto: The subnet mask will be set automatically.<br><br>Force /31 Subnet: The subnet mask will be set as 255.255.255.254(/31), and the gateway IP address will be recalculated. |
| **Routing Mode** | 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 **NAT** (network address translation) or **IP Forwarding**. Click the button to enable IP forwarding. |
| **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.<br><br>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.)<br><br>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. |

 Copyright @ 2017 Pepwave

| Cellular Settings | |
|---|---|
| SIM Card | Both SIMs / SIM A Only / SIM B Only |
| Preferred SIM Card | No Preference / SIM A / SIM B |
| 3G/2G | Auto |
| Authentication | Auto |
| Band Selection | WCDMA / HSDPA / HSUPA / HSPA+ (800 MHz)<br>WCDMA / HSDPA / HSUPA / HSPA+ (850 MHz)<br>WCDMA / HSDPA / HSUPA / HSPA+ (900 MHz)<br>WCDMA / HSDPA / HSUPA / HSPA+ (1700 MHz)<br>WCDMA / HSDPA / HSUPA / HSPA+ (1900 MHz)<br>WCDMA / HSDPA / HSUPA / HSPA+ (2100 MHz)<br>GSM / GPRS / EDGE (850 MHz)<br>GSM / GPRS / EDGE (900 MHz)<br>GSM / GPRS / EDGE (1800 MHz)<br>GSM / GPRS / EDGE (1900 MHz) |
| Data Roaming | |
| Operator Settings | Auto / Custom |
| APN | |
| Username | |
| Password | |
| Confirm Password | |
| SIM PIN (Optional) | (Confirm) |
| Bandwidth Allowance Monitor | Enable |
| Action | Disconnect when usage hits 100%<br>Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. |
| Start Day | On 1st of each month |
| Monthly Allowanace | MB |

 Copyright @ 2017 Pepwave

| Cellular Settings | |
|---|---|
| **SIM Card** | Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards. |
| **Preferred SIM Card** | If both cards were enabled on the above field, then you can designate the priority of the SIM card slots here. |
| **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. |
| **Operator Settings** | 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 **Auto** 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 **Custom** to enter your carrier's **APN**, **Login**, **Password**, and **Dial Number** settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**. |
| **APN / Login / Password / SIM PIN** | When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP. |
| **Bandwidth Allowance Monitor** | 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. |
| **Action** | If email notification 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. |

 Copyright @ 2017 Pepwave

| General Settings | |
|---|---|
| Independent from Backup WANs | ☐ |
| Standby State | ◉ Remain connected ○ Disconnected |
| Idle Disconnect | ☐ |

| General Settings | |
|---|---|
| **Independent from Backup WANs** | If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available. |
| **Standby State** | 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 **Remain connected** is chosen, bringing up this WAN connection to active makes it immediately available for use. |
| **Idle Disconnect** | 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 | SmartCheck |
| Timeout | 5 second(s) |
| Health Check Interval | 10 second(s) |
| Health Check Retries | 3 |
| Recovery Retries | 3 |

 Copyright @ 2017 Pepwave

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

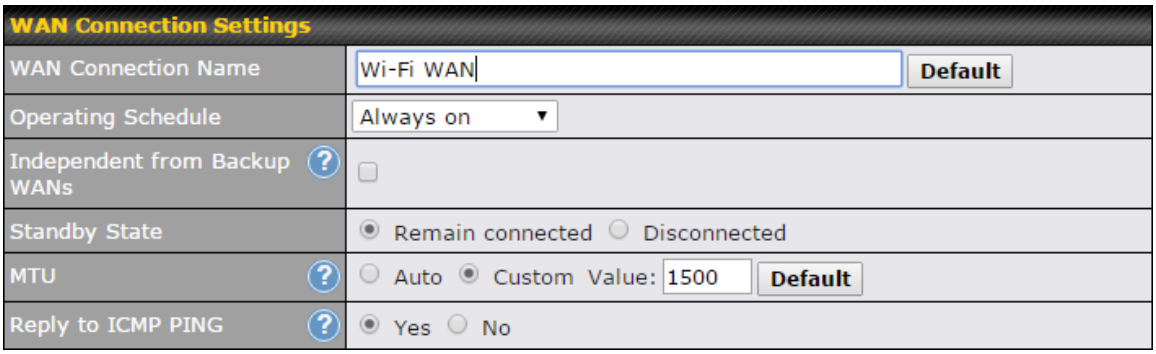
| Dynamic DNS Settings | |
|---|---|
| **Dynamic DNS Service Provider** | This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:<br>● changeip.com<br>● dyndns.org<br>● no-ip.org<br>● tzo.com<br>● DNS-O-Matic<br>Select **Disabled** to disable this feature. See **Section 9.5** for configuration details. |

| MTU | |
|---|---|
| **MTU** | This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value. |

 Copyright @ 2017 Pepwave

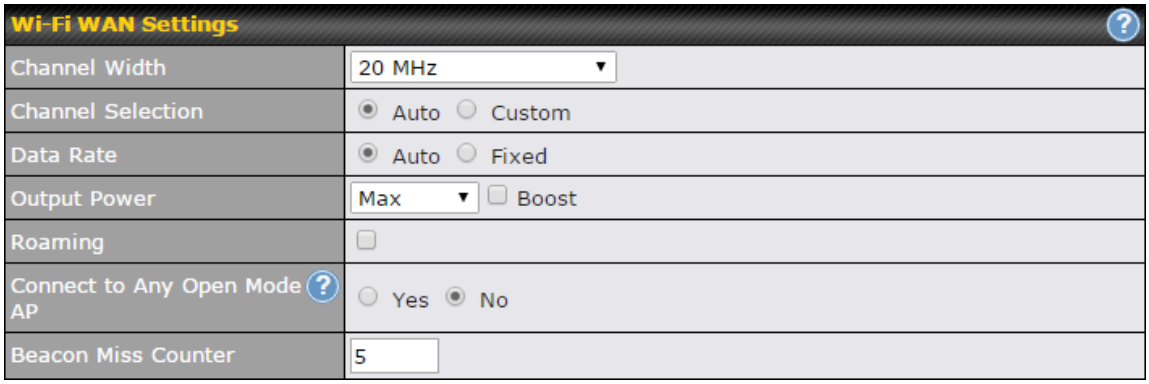
## 10.3 Wi-Fi WAN

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




| WAN Connection Settings | |
|---|---|
| **WAN Connection Name** | Enter a name to represent this WAN connection. |
| **Operating Schedule** | Click the drop-down menu to apply a time schedule to this interface. |
| **Independent from Backup WANs** | If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available. |
| **Standby State** | This setting specifies the state of the WAN connection while in standby. The available options are **Remain Connected** (hot standby) and **Disconnect** (cold standby). |
| **MTU** | This setting specifies the maximum transmission unit. By default, MTU is set to **Custom 1440**. You may adjust the MTU value by editing the text field. Click **Default** to restore the default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes |
| **Reply to ICMP PING** | If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled. |

 Copyright @ 2017 Pepwave




| Wi-Fi WAN Settings | |
|---|---|
| **Channel Width** | Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz |
| **Channel Selection** | Determine whether the channel will be automatically selected. If you select custom, the following table will appear: |
| **Data Rate** | Selecting Auto will enable the router to automatically determine the best data rate, while manually selecting a rate will force devices to connect using the fixed rate. |
| **Output Power** | If you are setting up a network with many Wi-Fi devices in close proximity, then you can configure the output power here. Click the "boost" button for additional power. However, with that option ticked, output power may exced local regulatory limits. |
| **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. |
| **Beacon Miss Counter** | This sets the threshold for the number of missed beacons. |

 Copyright @ 2017 Pepwave

| Bandwidth Allowance Monitor | |
|---|---|
| Bandwidth Allowance Monitor | ☑ Enable |
| Action | Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification.<br>☑ Disconnect when usage hits 100% of monthly allowance |
| Start Day | On 1st ▾ of each month at 00:00 midnight |
| Monthly Allowance | 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.<br>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. |

| Health Check Settings | |
|---|---|
| Health Check Method | DNS Lookup ▾ |
| Health Check DNS Servers | Host 1:<br>Host 2:<br>☑ Use first two DNS servers as Health Check DNS Servers<br>☐ Include public DNS servers |
| Timeout | 5 ▾ second(s) |
| Health Check Interval | 5 ▾ second(s) |
| Health Check Retries | 3 ▾ |
| Recovery Retries | 3 ▾ |

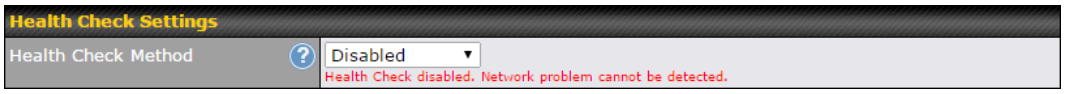
 Copyright @ 2017 Pepwave

## Health Check Settings

**Method**

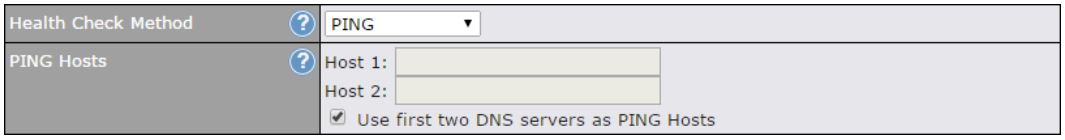
This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

### Health Check Disabled




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

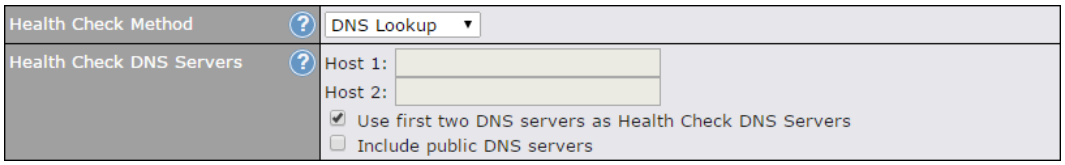



ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

**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




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

 Copyright @ 2017 Pepwave

| | |
|---|---|
| | treated as down only if there is also no response received from the public DNS servers.<br>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 | HTTP |
| URL 1 | http:// <br> Matching String: |
| URL 2 | http:// <br> Matching String: |

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

| | |
|---|---|
| **URL1** | **WAN Settings>WAN Edit>Health Check Settings>URL1**<br>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**<br>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 |

| | |
|---|---|
| **Timeout** | This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**. |
| **Health Check Interval** | This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**. |
| **Health Check** | This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **Retries** | Balance will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts. |
| **Recovery Retries** | 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, **Recover Retries** is set to **3**. 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** | This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:<br>● changeip.com<br>● dyndns.org<br>● no-ip.org<br>● tzo.com<br>● DNS-O-Matic<br>Select **Disabled** to disable this feature. |
| **User ID / User / Email** | This setting specifies the registered user name for the dynamic DNS service. |
| **Password / Pass / TZO Key** | This setting specifies the password for the dynamic DNS service. |
| **Update All Hosts** | Check this box to automatically update all hosts. |
| **Hosts / Domain** | This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection. |

 Copyright @ 2017 Pepwave

**Important Note**

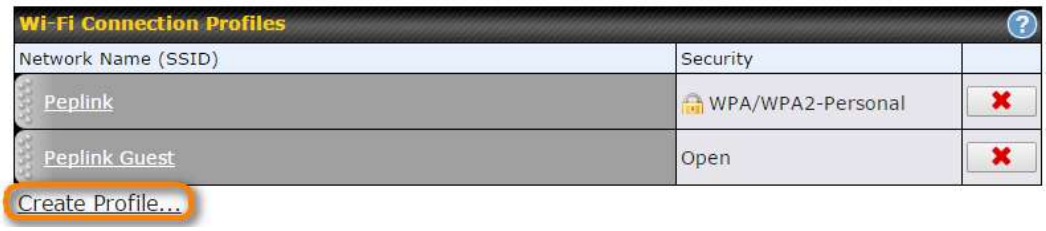
In order to use dynamic DNS services, appropriate hostname registration(s), as well as a valid account with a supported dynamic DNS service provider, are required.

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.

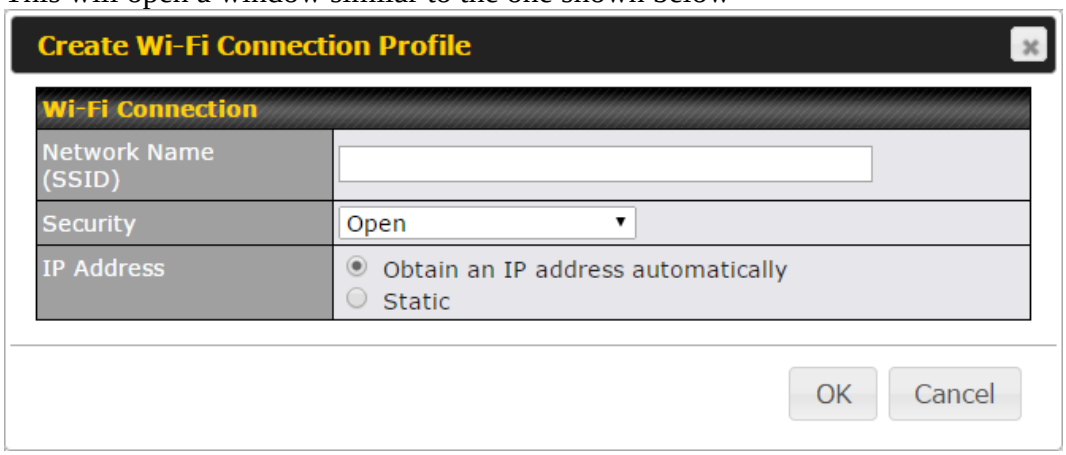
Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been not updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a WAN's IP address did not change.

### 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




 Copyright @ 2017 Pepwave

| 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. |
| **Security** | This option allows you to select which security policy is used for this wireless network.<br>Available options:<br>● **Open**<br>● **WEP**<br>● **WPA/WPA2 – Personal**<br>● **WPA/WPA2 – Enterprise** |

**Open**

| | |
|---|---|
| Security | Open |

**WEP**

| | |
|---|---|
| Security | WEP |
| Encryption Key | Hide Characters |

**WPA/WPA2 – Personal**

| | |
|---|---|
| Security | WPA/WPA2-Personal |
| Shared Key | Hide Characters |

**WPA/WPA2 – Enterprise**

| | |
|---|---|
| Security | WPA/WPA2-Enterprise |
| Login ID | |
| Password | |
| Confirm Password | |
| EAP Method | PEAP |
| EAP Phase 2 Method | EAP/CHAP |
| EAP outer authentication identity | Anonymous<br>User Credentials<br>Other: |

## 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**.

 Copyright @ 2017 Pepwave

## Health Check Settings

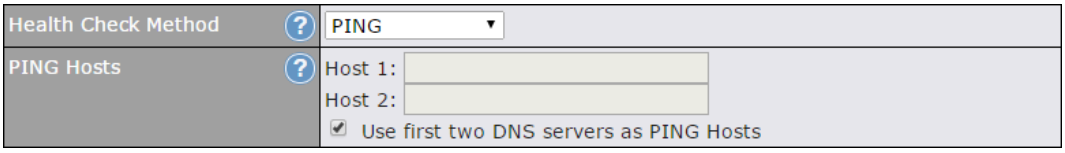
**Method**

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

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

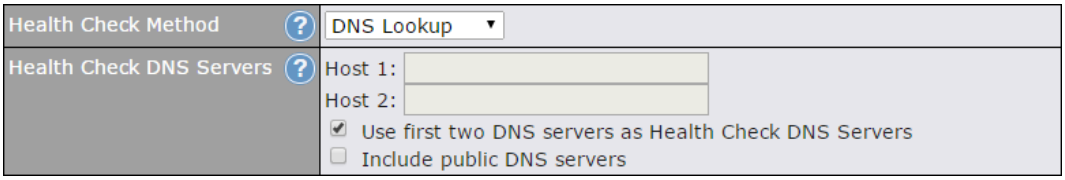



ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

**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




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

 Copyright @ 2017 Pepwave

| | |
|---|---|
| | of the WAN connection are used as the health check DNS servers. |

## Health Check Method: HTTP

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

| | |
|---|---|
| Health Check Method | HTTP |
| URL 1 | http:// <br> Matching String: |
| URL 2 | http:// <br> Matching String: |

| | |
|---|---|
| **URL1** | **WAN Settings>WAN Edit>Health Check Settings>URL1**<br>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**<br>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 | |
|---|---|
| **Timeout** | This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**. |
| **Health Check Interval** | This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**. |
| **Health Check Retries** | 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 **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts. |
| **Recovery Retries** | 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, **Recover Retries** is set to **3**. 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. |

 Copyright @ 2017 Pepwave

| 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 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 | changeip.com |
| User ID | |
| Password | |
| Confirm Password | |
| Hosts | |

 Copyright @ 2017 Pepwave

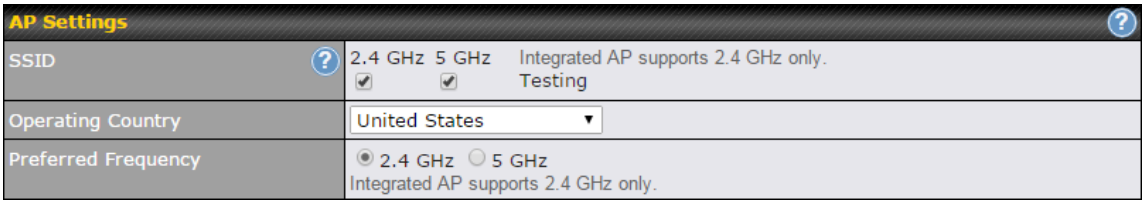
| Dynamic DNS Settings | |
|---|---|
| **Dynamic DNS** | This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:<br>● changeip.com<br>● dyndns.org<br>● no-ip.org<br>● tzo.com<br>● DNS-O-Matic<br>● Others…<br>Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.<br>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 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. |

 Copyright @ 2017 Pepwave

# 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.




| AP Settings | |
|---|---|
| **SSID** | You can select the wireless networks for 2.4 GHz or 5 GHz seperately for each SSID. |
| **Operating Country** | This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow.<br>● 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).<br>● If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).<br>NOTE: Users are required to choose an option suitable to local laws and regulations. |
| **Preferred Frequency** | Indicate the preferred frequency to use for clients to connect. |

| 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. |

 Copyright @ 2017 Pepwave

| | 2.4 GHz | 5 GHz |
|---|---|---|
| Protocol | 802.11ng | 802.11n/ac |
| Channel Width | 20 MHz | Auto |
| Channel | Auto Edit<br>Channels: 1 2 3 4 5 6 7 8 9 10 11 | Auto Edit<br>Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165 |
| Auto Channel Update | Daily at 03 :00<br>Wait until no active client associated | Daily at 03 :00<br>Wait until no active client associated |
| Output Power | Fixed: Max Boost | Fixed: Max Boost |
| Client Signal Strength Threshold | 0 -95 dBm (0: Unlimited) | 0 -95 dBm (0: Unlimited) |
| Maximum number of clients | 0 (0: Unlimited) | 0 (0: Unlimited) |

| AP Settings (part 2) | |
|---|---|
| **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 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. |
| **Channel** | This option allows you to select which 802.11 RF channel will be utilized. **Channel 1 (2.412 GHz)** is selected by default. |
| **Auto Channel Update** | Indicate the time of day at which update automatic channel selection. |
| **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. |
| **Client Signal Strength Threshold** | This setting determines the maximum strength at which the Wi-Fi AP can broadcast |
| **Maximum number of clients** | This setting determines the maximum number of clients that can connect to this Wi-Fi frequency. |

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**.

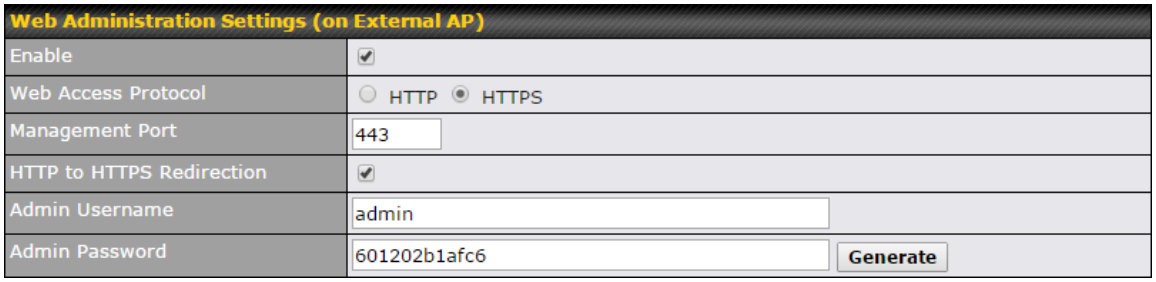
 Copyright @ 2017 Pepwave

| | |
|---|---|
| Management VLAN ID | Untagged LAN (No VLAN) |
| Operating Schedule | Always on |
| Beacon Rate | 1 Mbps 6 Mbps will be used for 5 GHz radio |
| Beacon Interval | 100 ms |
| DTIM | 1 Default |
| RTS Threshold | 0 Default |
| Fragmentation Threshold | 0 (0: Disable) Default |
| Distance / Time Converter | 4050 m<br>Note: Input distance for recommended values |
| Slot Time | Auto Custom 9 µs Default |
| ACK Timeout | 48 µs Default |
| Frame Aggregation | |

| Advanced AP Settings | |
|---|---|
| **Management VLAN ID** | This field specifies the VLAN ID to tag to management traffic, such as communication traffic between the AP and the AP Controller. The value is zero by default, which means that no VLAN tagging will be applied.<br>NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller. |
| **Operating Schedule** | Choose from the schedules that you have defined in System>Schedule. Select the schedule for the integrated AP to follow from the drop-down menu. |
| **Beacon Rate** [A] | This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected. |
| **Beacon Interval** [A] | This option is for setting the time interval between each beacon. By default, **100ms** is selected. |
| **DTIM** [A] | This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to **1 ms**. |
| **RTS Threshold** [A] | The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500. |
| **Fragmentation Threshold** [A] | This setting determines the maximum size of a packet before it gets fragmented into multiple pieces. |
| **Distance / Time Convertor** | Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout. |
| **Slot Time** [A] | This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to **9 µs**. |
| **ACK Timeout** [A] | This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to **48 µs**. |
| **Frame Aggregation** [A] | This option allows you to enable frame aggregation to increase transmission throughput. |

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

 Copyright @ 2017 Pepwave




| Web Administration Settings | |
|---|---|
| **Enable** | Ticking this box enables web admin access for APs located on the WAN. |
| **Web Access Protocol** | Determines whether the web admin portal can be accessed thorugh HTTP or HTTPS |
| **Management Port** | Determines the port at which the management UI can be accessed. |
| **Admin Username** | Determines the username to be used for logging into the web admin portal |
| **Admin Password** | Determines the password for the web admin portal on external AP. |

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** | 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. |

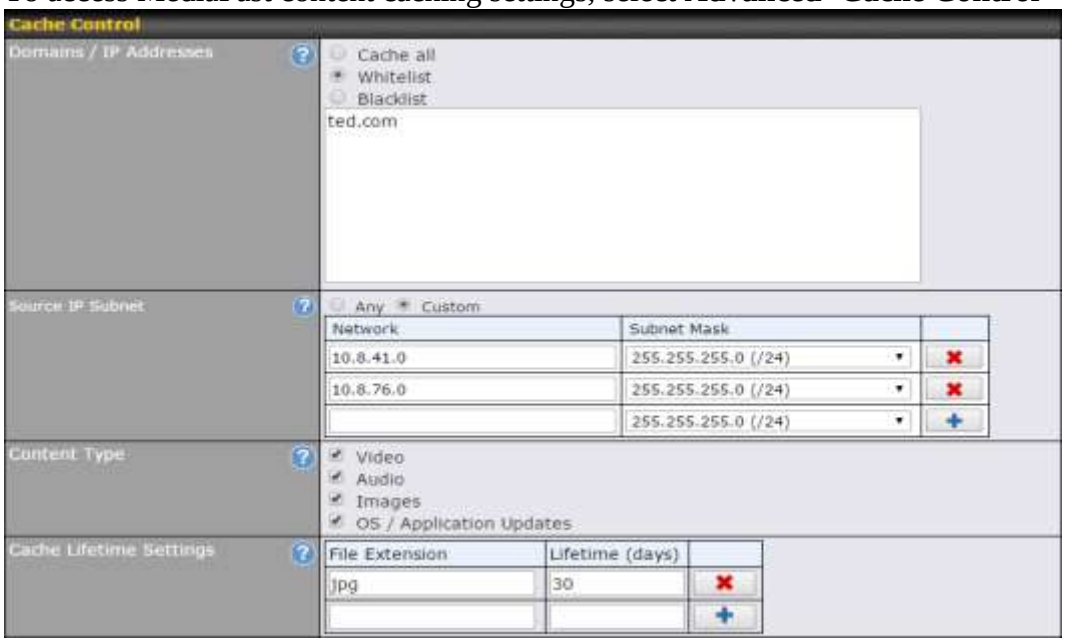
 Copyright @ 2017 Pepwave

# 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**

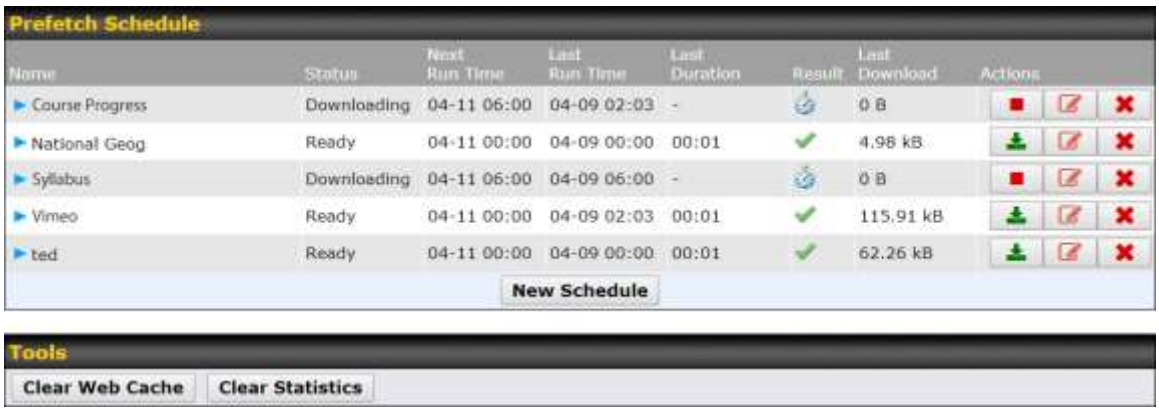



| Cache Control Settings | |
|---|---|
| **Domain** | Choose to **Cache on all domains**, or enter domain names and then choose either **Cache the specified domains only** or **Do not cache the specified domains**. |
| **Source IP Subnet** | This setting allows caching to be applied to the user-specified IP subnets. If "Any" is selected, then caching will apply to all subnets. |
| **Content Type** | Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types. |
| **Cache Lifetime Settings** | 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. |

 Copyright @ 2017 Pepwave

## 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 Settings | |
|---|---|
| **Name** | This field displays the name given to the scheduled download. |
| **Status** | Check the status of your scheduled download here. |
| **Next Run Time/Last Run Time** | These fields display the date and time of the next and most recent occurrences of the scheduled download. |
| **Last Duration** | 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. |
| **Result** | This field indicates whether downloads are in progress ( ) or complete ( ). |
| **Last Download** | 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 . |

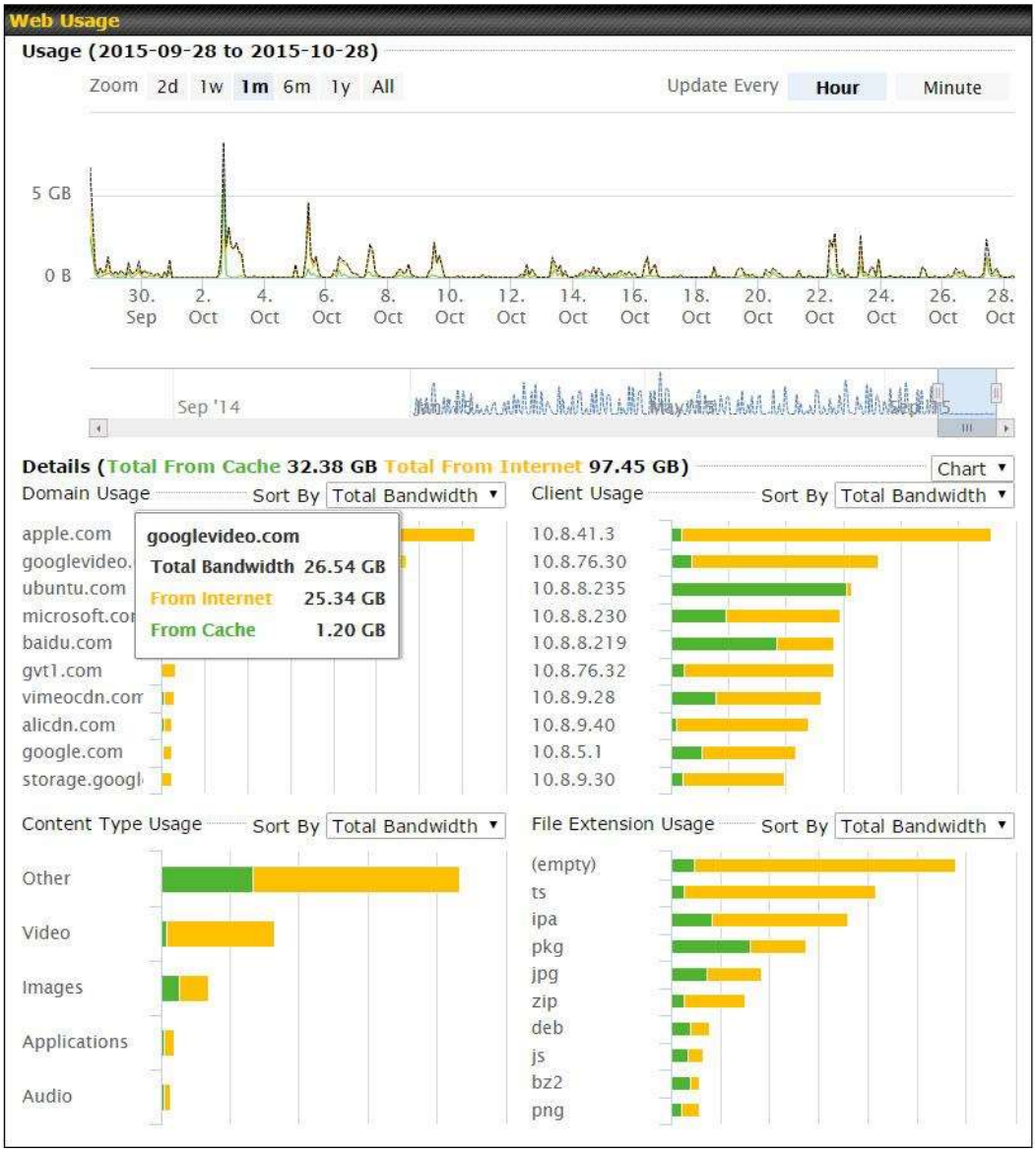
 Copyright @ 2017 Pepwave

| | |
|---|---|
| | To cancel a scheduled download, click ■.<br>To edit a scheduled download, click ✎.<br>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:<br> <br><br>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. |

 Copyright @ 2017 Pepwave

## 12.3 Viewing MediaFast Statistics

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




 Copyright @ 2017 Pepwave

# 13 Bandwidth Bonding SpeedFusion™ / PepVPN

Pepwave bandwidth bonding SpeedFusionTM 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.

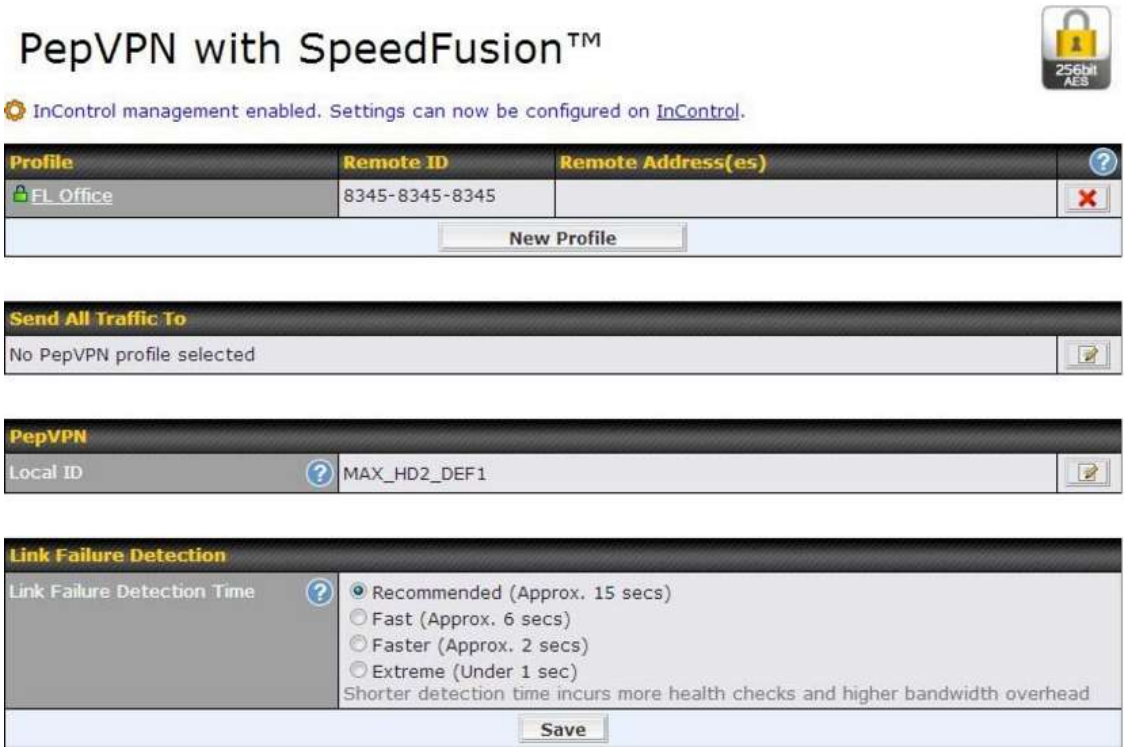
Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.

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**.

 Copyright @ 2017 Pepwave

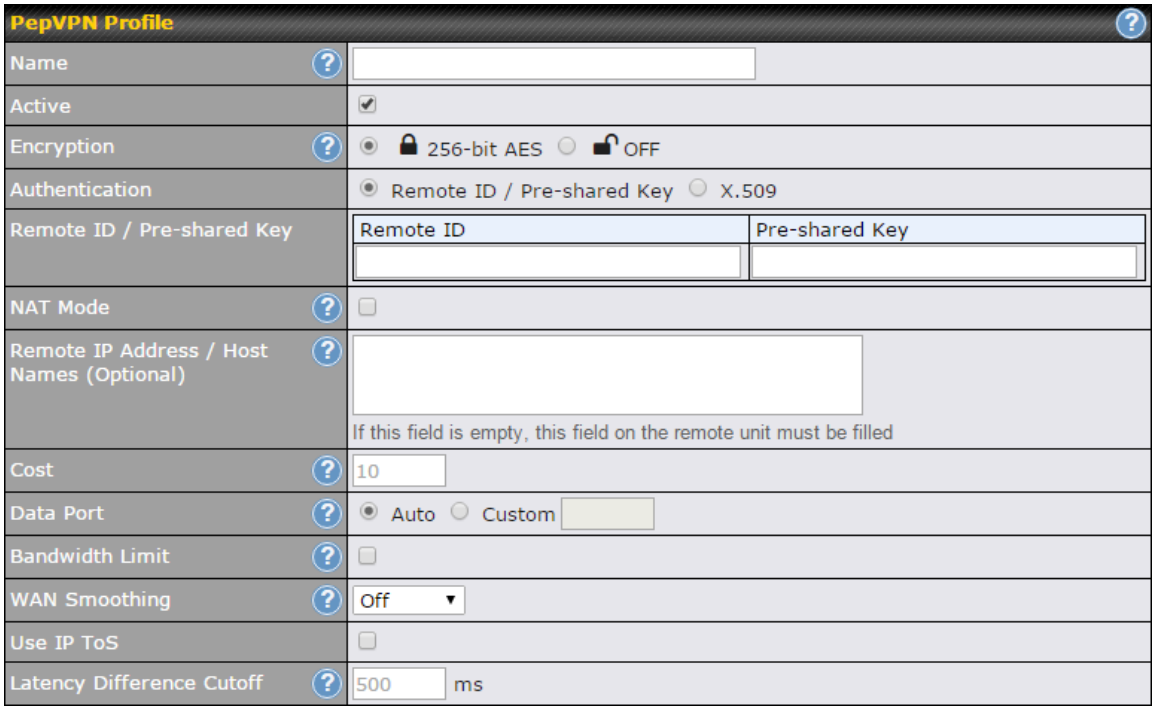



The local LAN subnet and subnets behind the LAN (defined under **Static Route** on the LAN settings page) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to local subnets.
Note that all LAN subnets and the subnets behind them must be unique. Otherwise, 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 acesss 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.

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.

 Copyright @ 2017 Pepwave




| PepVPN Profile Settings | |
|---|---|
| **Name** | 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 ( ). |
| **Active** | When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled. |
| **Encryption** | By default, VPN traffic is encrypted with **256-bit AES**. If **Off** is selected on both sides of a VPN connection, no encryption will be applied. |
| **Authentication** | Select from **By Remote ID Only**, **Preshared Key**, or **X.509** to specify the method the Peplink Balance will use to authenticate peers. When selecting **By Remote ID Only**, be sure to enter a unique peer ID number in the **Remote ID** field. |
| **Remote ID / Pre-shared Key** | This optional field becomes available when **Remote ID / Pre-shared Key** is selected as the Peplink Balance's VPN **Authentication** method, as explained above. **Pre-shared Key** 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.<br><br>Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| | you wish to paste a CSV, click the icon next to the "Remote ID / Preshared Key" setting. |
| **Remote ID/Remote Certificate** | These optional fields become available when **X.509** 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 **Show Details** link below the field. |
| **Allow Shared Remote ID** | When this option is enabled, the router will allow multiple peers to run using the same remote ID. |
| **NAT Mode** | Check this box to allow the local DHCP server to assign an IP address to the remote peer. When **NAT Mode** is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation. |
| **Remote IP Address / Host Names (Optional)** | If **NAT Mode** 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.<br><br>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. |
| **Cost** | Define path cost for this profile.<br>OSPF will determine the best route through the network using the assigned cost.<br>Default: 10 |
| **Data Port** | This field is used to specify a UDP port number for transporting outgoing VPN data. If **Default** 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 **Custom** is selected, enter an outgoing port number from 1 to 65535. |
| **Bandwidth Limit** | Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above. |
| **Cost** | Define path cost for this profile.<br>OSPF will determine the best route through the network using the assigned cost.<br>Default: 10 |
| **WAN Smoothing**[A] | Select the degree to which WAN Smoothing will be implemented across your WAN links. |
| **Use IP ToS** | Checking this button enables the use of IP ToS header field. |
| **Latency Difference Cutoff** | Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used) |

 Copyright @ 2017 Pepwave

[A] - 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

**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.<br><br>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:

 Copyright @ 2017 Pepwave

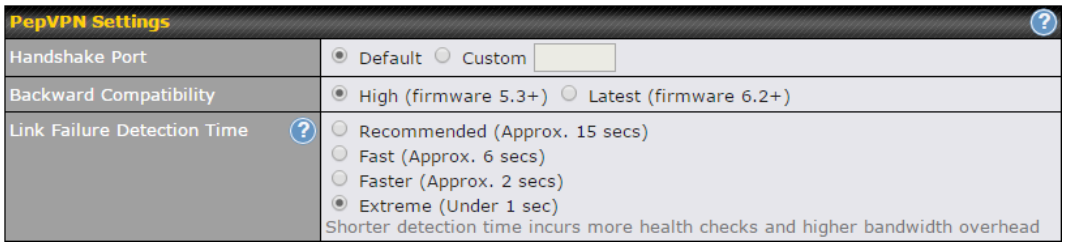
You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main PepVPN connection fail.

## 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.

## 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**.




## PepVPN Settings

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

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **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.<br>When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds.<br>When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds.<br>When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds.<br>When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second. |

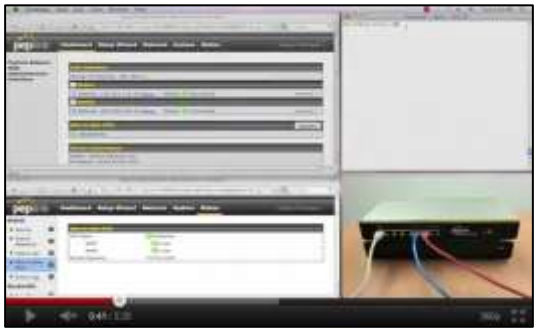
[A] - Advanced feature, please click the button on the top right-hand corner to activate.

**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/TLQgdpPSY88

 Copyright @ 2017 Pepwave

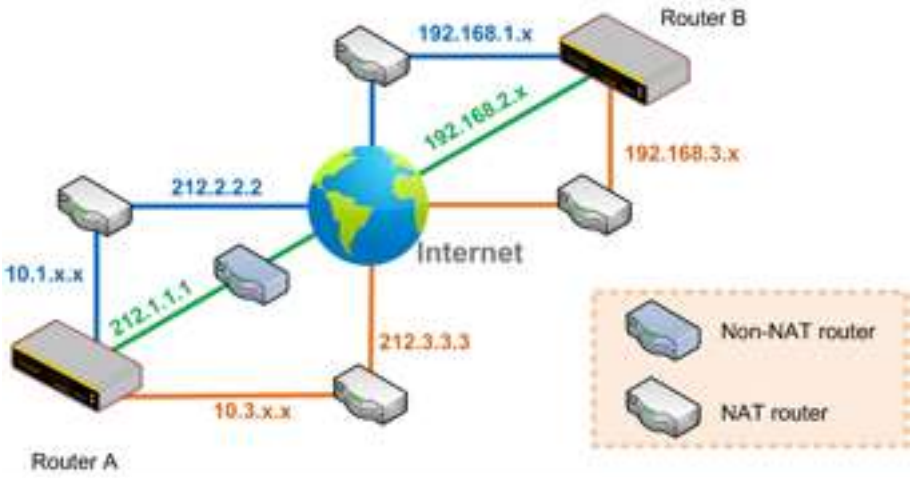
## 13.2 The Pepwave Router Behind a NAT Router

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.

 Copyright @ 2017 Pepwave

## 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. |

 Copyright @ 2017 Pepwave

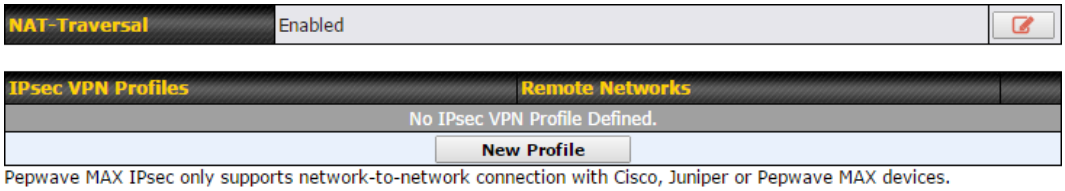
# 14 IPsec VPN

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.**




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.

 Copyright @ 2017 Pepwave

| | |
|---|---|
| Name | Profile 1 |
| Active | ☑ |
| Connect Upon Disconnection of | ☑ WAN 2 |
| Remote Gateway IP Address / Host Name | 12.12.12.12 |
| Local Networks | Propose the following networks to remote gateway:<br>☐ *172.16.1.1/24*<br>☐ 172.16.2.1/24<br>☐ 172.16.3.1/24<br>☑ 10.10.0.1/32<br>☑ 192.168.10.0/24<br>☑ 192.168.11.0/24<br>☐ |
| | Apply the following NAT policies:<br>☑ 172.16.1.0/24 → 192.168.10.0/24<br>☑ 172.16.2.0/24 → 10.10.0.1/32<br>☑ 172.16.3.11/32 → 192.168.11.101/32<br>☑ 172.16.3.21/32 → 192.168.11.201/32<br>☐ Local Network → NAT Network |
| Remote Networks | Network: 192.167.11.193 / Subnet Mask: 255.255.255.0 (/24) ✚ |
| Authentication | ◉ Preshared Key ○ X.509 Certificate |
| Mode | ◉ Main Mode (All WANs need to have Static IP)<br>○ Aggressive Mode |
| Force UDP Encapsulation | ☐ |
| Preshared Key | ••••••••••••<br>☑ Hide Characters |
| Local ID | |
| Remote ID | |
| Phase 1 (IKE) Proposal | 1 AES-256 & SHA1<br>2 ----- |
| Phase 1 DH Group | ☑ Group 2: MODP 1024<br>☐ Group 5: MODP 1536 |
| Phase 1 SA Lifetime | 3600 seconds Default |
| Phase 2 (ESP) Proposal | 1 AES-256 & SHA1<br>2 ----- |
| Phase 2 PFS Group | ◉ None<br>○ Group 2: MODP 1024<br>○ Group 5: MODP 1536 |
| Phase 2 SA Lifetime | 28800 seconds 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 will be disabled. |
| **Connect Upon Disconnection of** | Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected. |
| **Remote Gateway IP Address / Host Name** | Enter the remote peer's public IP address. For **Aggressive Mode**, this is optional. |
| **Local Networks** | Enter the local LAN subnets here. If you have defined static routes, they will be shown here.<br><br>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.<br><br>Two types of NAT policies can be defined:<br><br>One-to-One NAT policy: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 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.<br><br>Many-to-One NAT policy: 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 > 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. |
| **Remote Networks** | Enter the LAN and subnets that are located at the remote site here. |
| **Authentication** | To access your VPN, clients will need to authenticate by your choice of methods. Choose between the **Preshared Key** and **X.509 Certificate** methods of authentication. |
| **Mode** | Choose **Main Mode** if both IPsec peers use static IP addresses. Choose **Aggressive Mode** if one of the IPsec peers uses dynamic IP addresses. |
| **Force UDP Encapsulation** | For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox. |
| **Pre-shared Key** | 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. |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **Remote Certificate (pem encoded)** | Available only when **X.509 Certificat**e is chosen as the **Authentication** method, this field allows you to paste a valid X.509 certificate. |
| **Local ID** | In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN. |
| **Remote ID** | In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN. |
| **Phase 1 (IKE) Proposal** | In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In **Aggressive Mode**, only one selection is permitted. |
| **Phase 1 DH Group** | 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.<br>**Group 2**: **1024-bit** is the default value.<br>**Group 5**: **1536-bit** is the alternative option. |
| **Phase 1 SA Lifetime** | This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at **3600** seconds. |
| **Phase 2 (ESP) Proposal** | In **Main Mode**, 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 **Aggressive Mode**, only one selection is permitted. |
| **Phase 2 PFS Group** | 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.<br>**None** - 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.<br>**Group 2**: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security.<br>**Group 5**: **1536-bit** is the third option. |
| **Phase 2 SA Lifetime** | This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds. |

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

 Copyright @ 2017 Pepwave

# 15 Outbound Policy Management

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

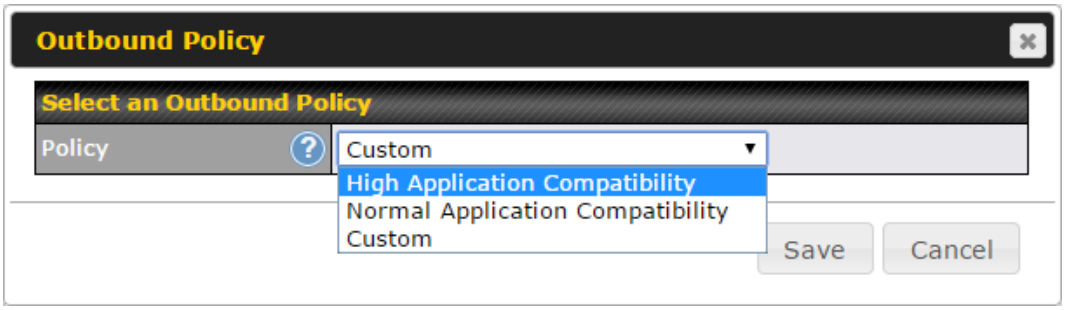
| Important Note |
| --- |
| Outbound policy is applied only when more than one WAN connection is active. |

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

## 15.1 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at

**Network>Outbound Policy>** or **Advanced>PepVPN>Outbound Policy.**




There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

 Copyright @ 2017 Pepwave

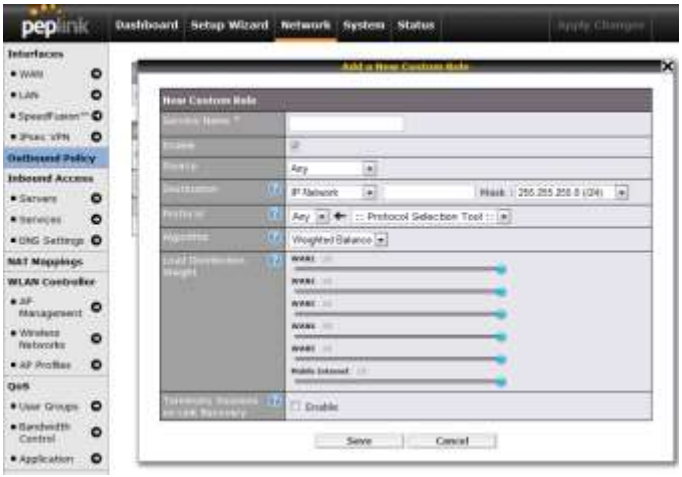
Note that some Pepwave routers provide only the **Send All Traffic To** setting here. See **Section 12.1** for details.

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

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

**Tip**

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

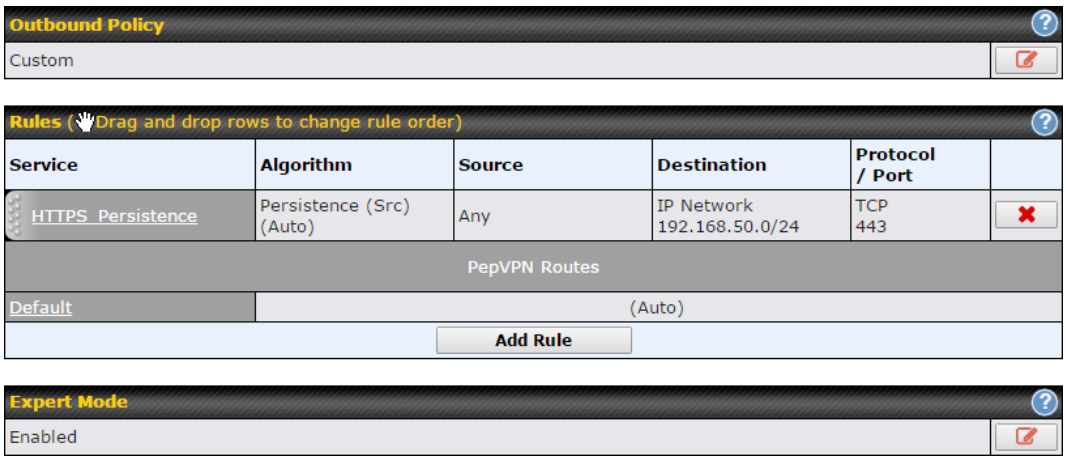



http://youtu.be/rKH4AS_bQnE

 Copyright @ 2017 Pepwave

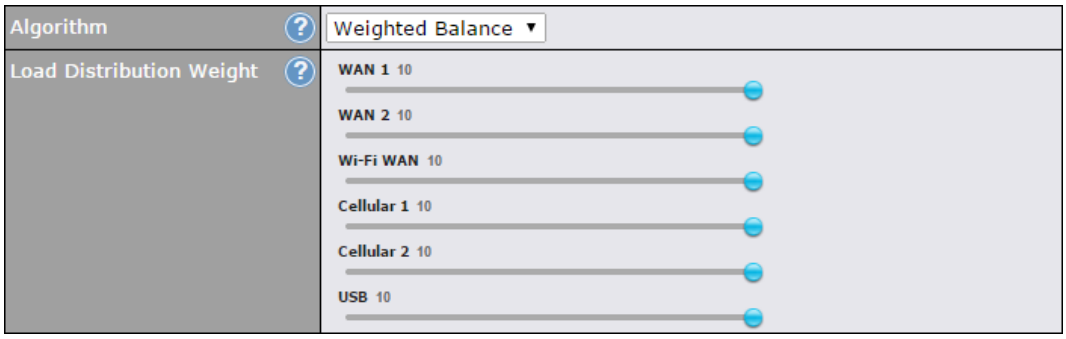
## 15.2 Custom Rules for Outbound Policy

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




### 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**.




 Copyright @ 2017 Pepwave

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

For example, with the following weight settings:

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

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

Matching traffic distributed to Ethernet WAN1 is 16.7% = (10 / 60 x 100%.

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

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

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

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

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

### 15.2.2 Algorithm: Persistence

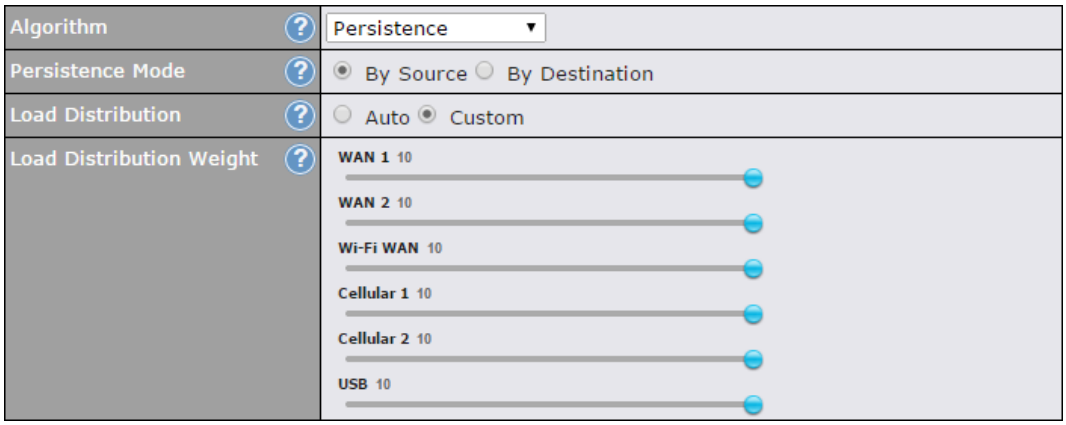
The configuration of persistent services is the solution to the few situations where link load distribution for Internet services is undesirable. For example, for security reasons, many e-banking and other secure websites terminate the session when the client computer's Internet IP address changes mid-session.

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

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

 Copyright @ 2017 Pepwave

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.



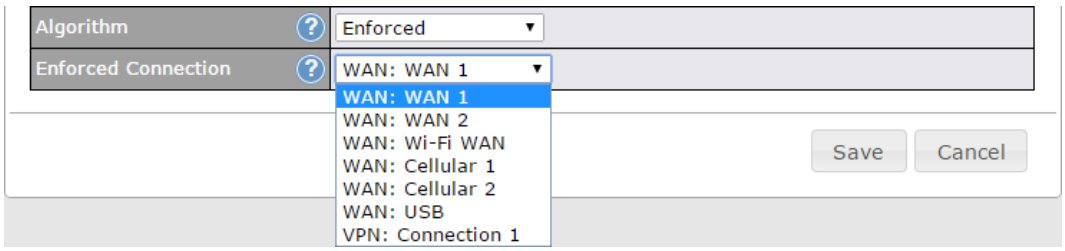

There are two persistent modes: **By Source** and **By Destination**.

| | |
|---|---|
| **By Source:** | The same WAN connection will be used for traffic matching the rule and originating from the same machine, regardless of its destination. This option will provide the highest level of application compatibility. |
| **By Destination:** | The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute 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**.

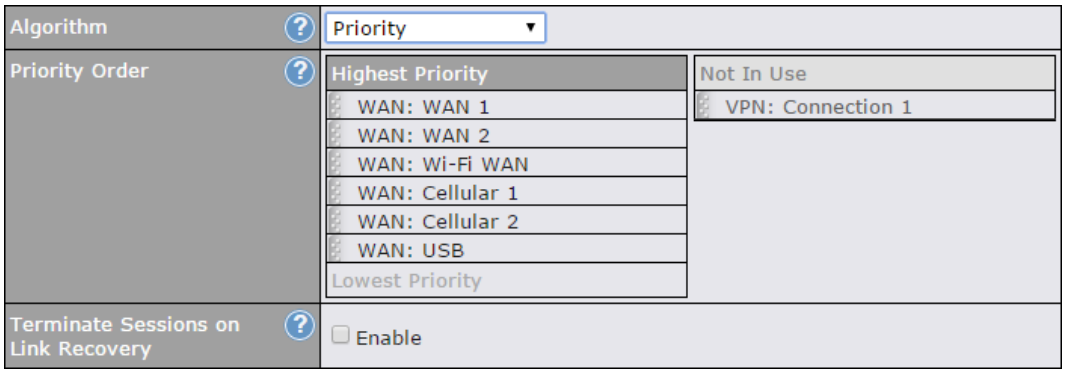



 Copyright @ 2017 Pepwave

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.



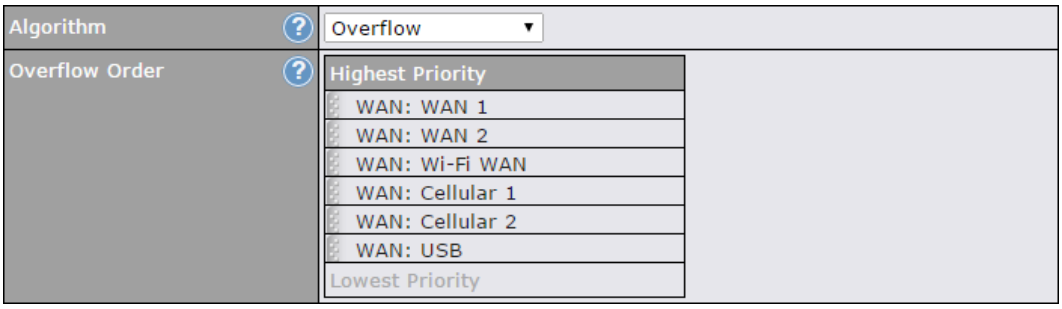

Starting from Firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion™ connection(s). By default, VPN connections are not included in the priority list.

| Tip |
| --- |
| Configure multiple distribution rules to accommodate different kinds of services. |

### 15.2.5 Algorithm: Overflow

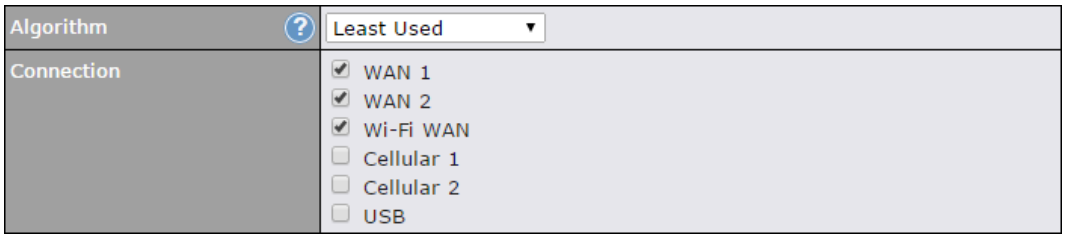
The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.

 Copyright @ 2017 Pepwave



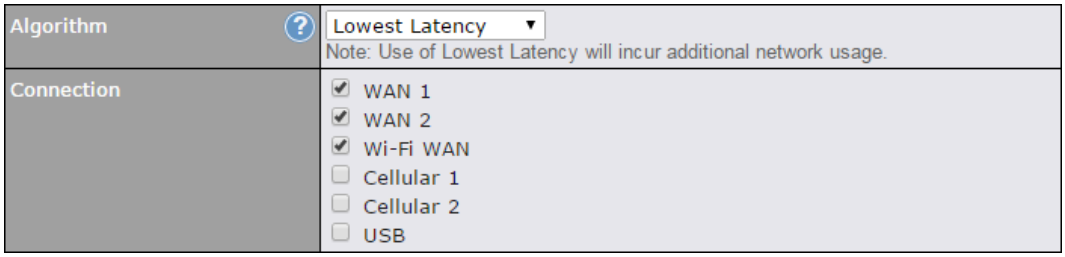

Drag and drop to specify the order of WAN connections to be used for routing traffic. Only the highest priority healthy connection that is not in full load will be used.

### 15.2.6 Algorithm: Least Used




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

### 15.2.7 Algorithm: Lowest Latency




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.

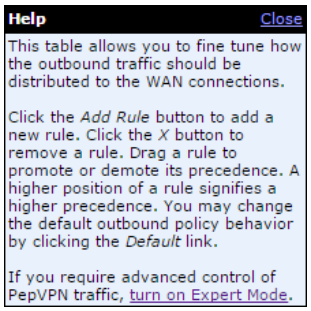
 Copyright @ 2017 Pepwave

**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.

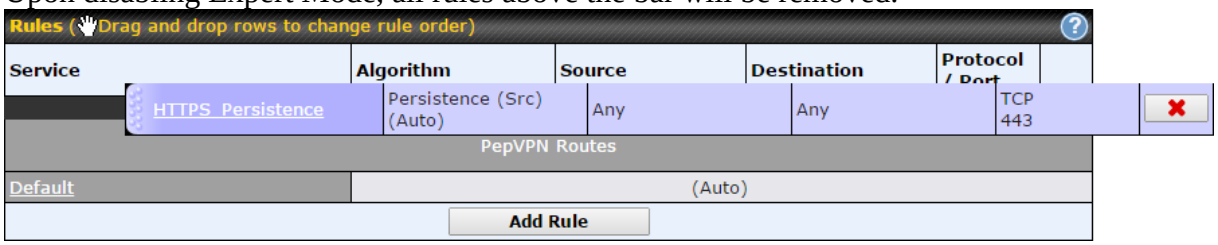
### 15.2.8 Expert Mode




**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.

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



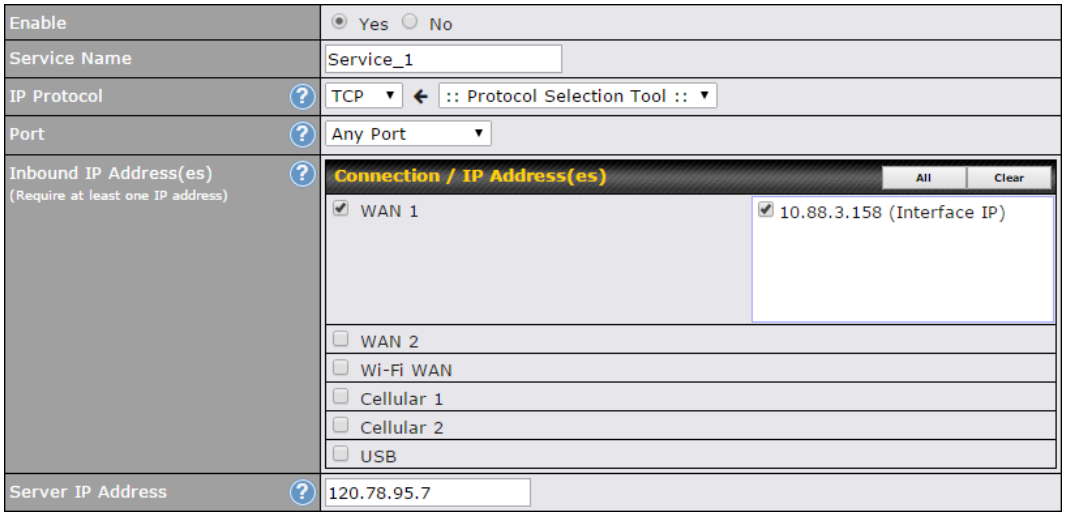

 Copyright @ 2017 Pepwave

# 16 Inbound Access

## 16.1 Port Forwarding Service

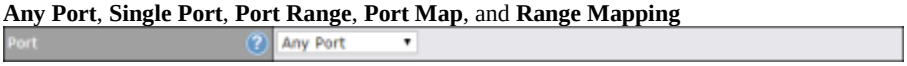
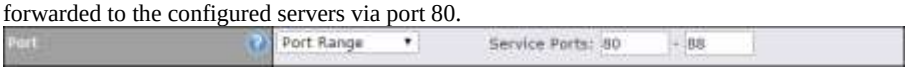
Pepwave routers can act as a firewall that blocks, by default, all inbound access from the Internet. By using port forwarding, Internet users can access servers behind the Pepwave router. Inbound port forwarding rules can be defined at **Advanced>Port Forwarding**.

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




| Port Forwarding Settings | |
|---|---|
| **Enable** | This setting specifies whether the inbound service takes effect. When **Enable** is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule. |
| **Service Name** | This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore "_" characters. |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **IP Protocol** | The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable. |
| **Port** | The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:<br>**Any Port**, **Single Port**, **Port Range**, **Port Map**, and **Range Mapping**<br>  <br><br>**Any Port**: all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.<br> <br><br>**Single Port**: traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.<br>  <br><br>**Port Range**: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.<br> <br><br>**Port Mapping**: traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting.<br>For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88.<br>(Please see below for details on the **Servers** setting.)<br> <br><br>**Range Mapping**: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting. |
| **Inbound IP Address(es)** | This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed. |
| **Server IP Address** | This setting specifies the LAN IP address of the server that handles the requests for the service. |

 Copyright @ 2017 Pepwave

### 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.

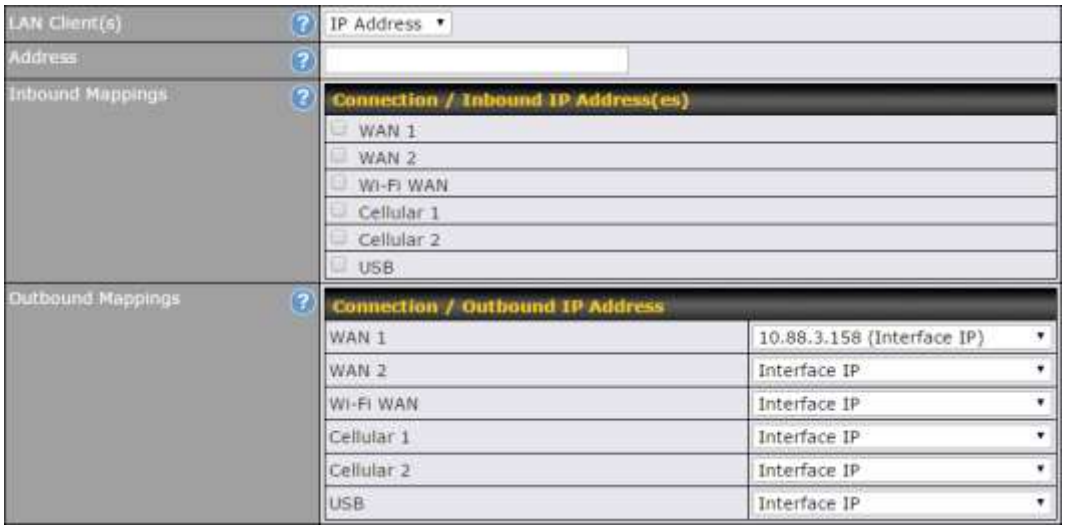
When the options are enabled, a table listing all the forwarded ports under these two protocols can be found at **Status>UPnP / NAT-PMP**.

 Copyright @ 2017 Pepwave

# 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**.

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




 Copyright @ 2017 Pepwave

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

 Copyright @ 2017 Pepwave

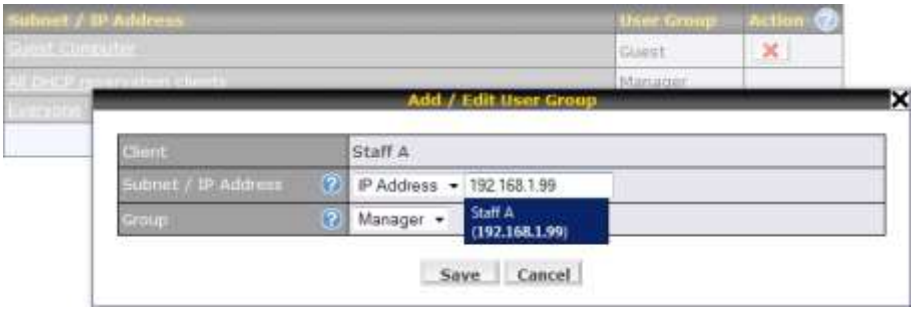
# 18 QoS

## 18.1 User Groups

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

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

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



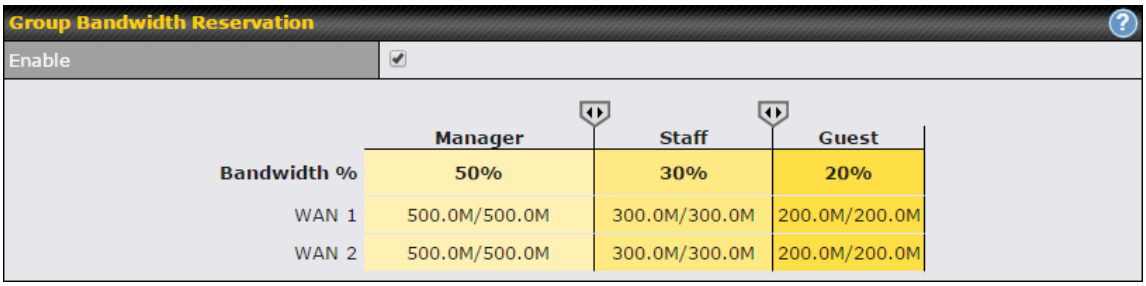

| Add / Edit User Group | |
|---|---|
| **Subnet / IP Address** | From the drop-down menu, choose whether you are going to define the client(s) by an **IP Address** or a **Subnet**. If **IP Address** is selected, enter a name defined in DHCP reservation table or a LAN client's IP address. If **Subnet**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

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

 Copyright @ 2017 Pepwave

## 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**).

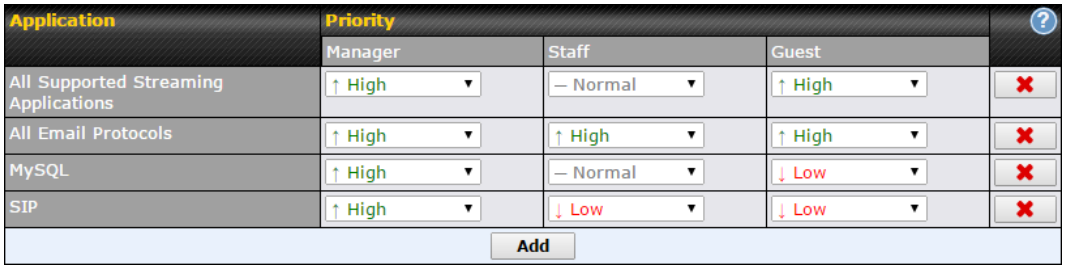



## 18.3 Application

### 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.

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.

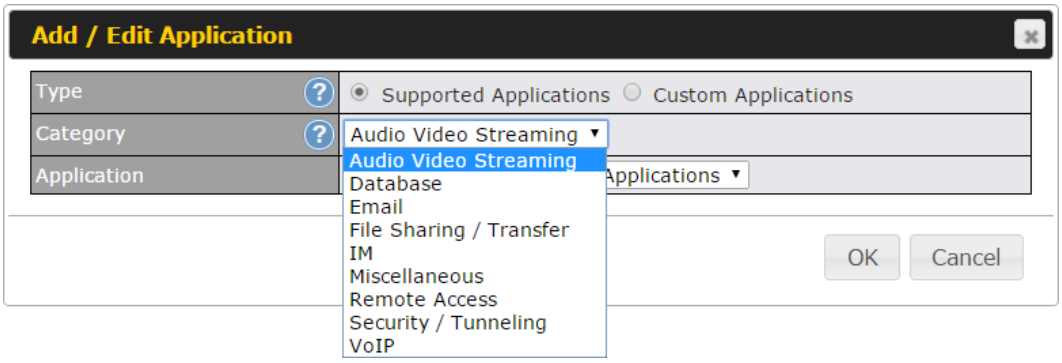



 Copyright @ 2017 Pepwave

### 18.3.2 Prioritization for Custom Applications

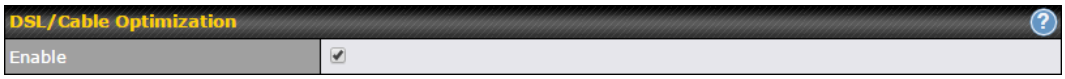
Click the **Add** button to define a custom application. Click the button ✖ in the **Action** column to delete the custom application in the corresponding row.

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:

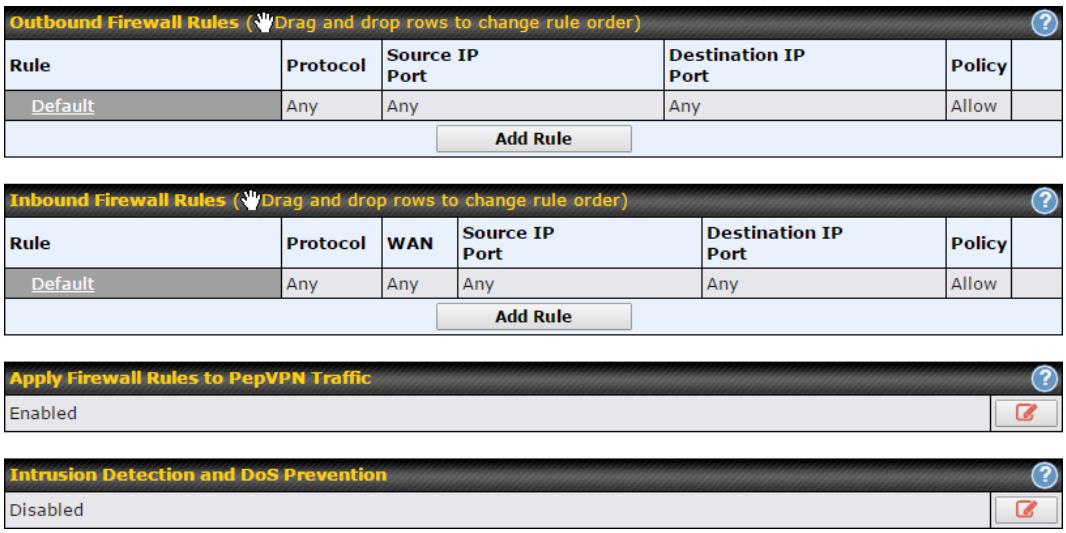
 Copyright @ 2017 Pepwave

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

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

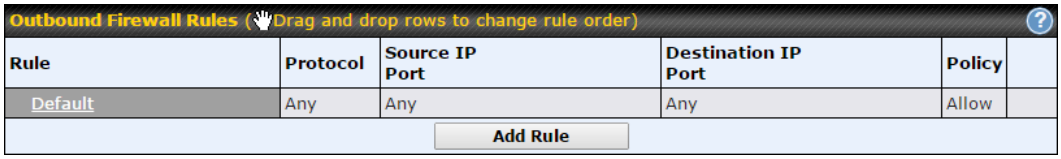
With SpeedFusion™ enabled, the firewall rules also apply to VPN tunneled traffic.




## 19.1 Outbound and Inbound Firewall Rules

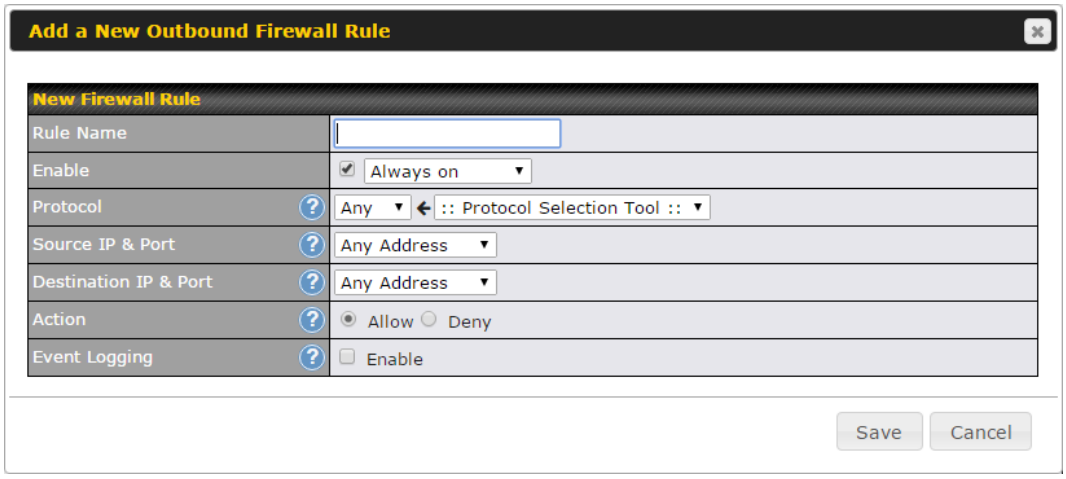
### 19.1.1 Access Rules

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



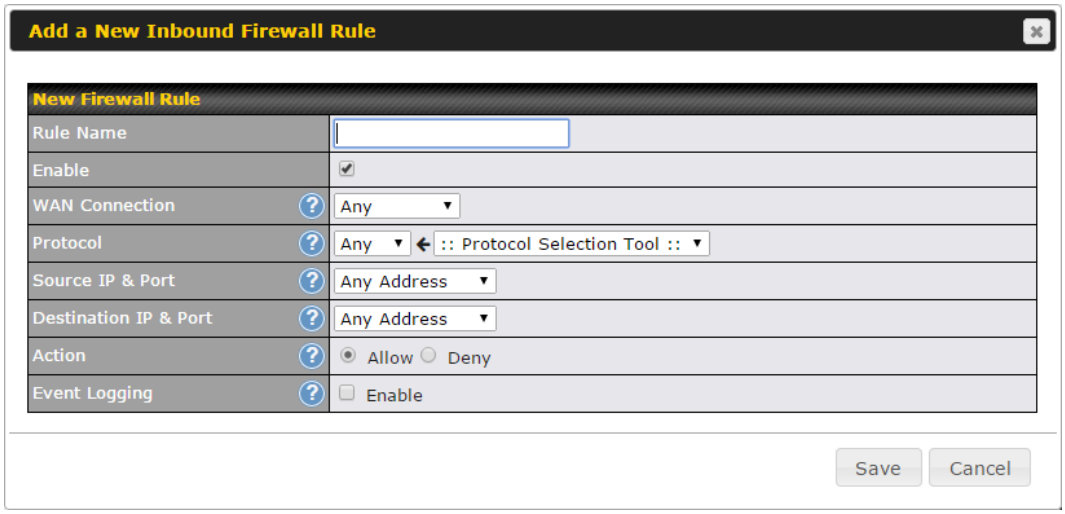

Click **Add Rule** to display the following screen:

 Copyright @ 2017 Pepwave




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

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




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

 Copyright @ 2017 Pepwave

| Inbound / Outbound Firewall Settings | |
|---|---|
| **Rule Name** | This setting specifies a name for the firewall rule. |
| **Enable** | 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.<br><br>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule. |
| **WAN Connection (Inbound)** | Select the WAN connection that this firewall rule should apply to. |
| **Protocol** | This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:<br>● **TCP**<br>● **UDP**<br>● **ICMP**<br>● **IP**<br>Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)<br>After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable. |
| **Source IP & Port** | This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Source IP & Port** setting, as indicated by the following screenshot:<br> <br><br>In addition, a single port, or a range of ports, can be specified for the **Source IP & Port** settings. |
| **Destination IP & Port** | This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Destination IP & Port** setting, as indicated by the following screenshot:<br> <br><br>In addition, a single port, or a range of ports, can be specified for the **Destination IP & Port** settings. |
| **Action** | This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:<br>● Source IP & port<br>● Destination IP & port<br>With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| | routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded). |
| **Event Logging** | This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows:<br>Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1<br>DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80<br>● **CONN:** The connection where the log entry refers to<br>● **SRC:** Source IP address<br>● **DST:** Destination IP address<br>● **LEN:** Packet length<br>● **PROTO:** Protocol<br>● **SPT:** Source port<br>● **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.

 Copyright @ 2017 Pepwave

### 19.1.3 Intrusion Detection and DoS Prevention

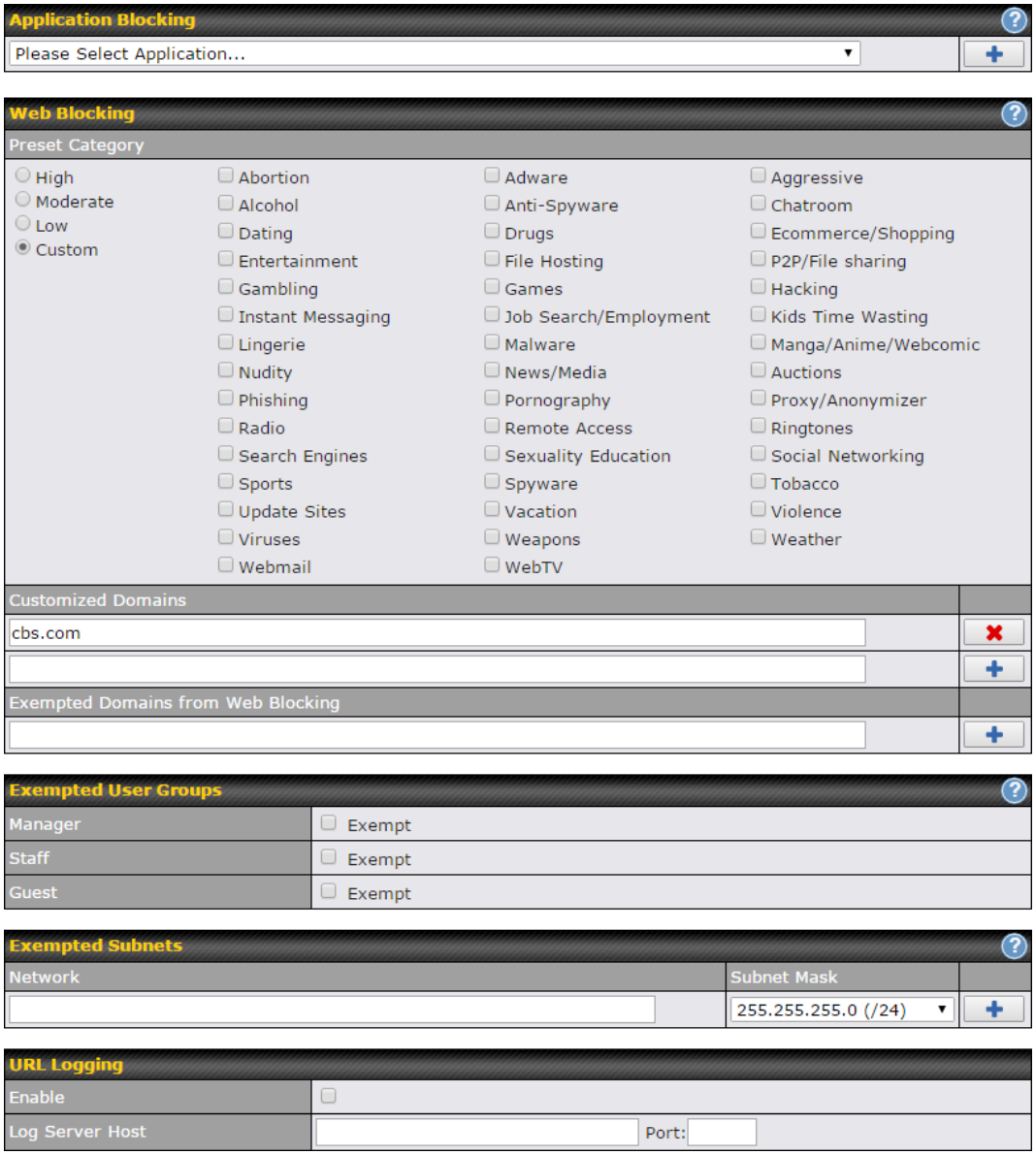
Pepwave routers can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click , check the **Enable** check box, and press the **Save** button.

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

 Copyright @ 2017 Pepwave

## 19.2 Content Blocking




### 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.

 Copyright @ 2017 Pepwave

### 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/SpeedFusionTM 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 the enter the ip address and port (if applicable) where your remote syslog server is located.

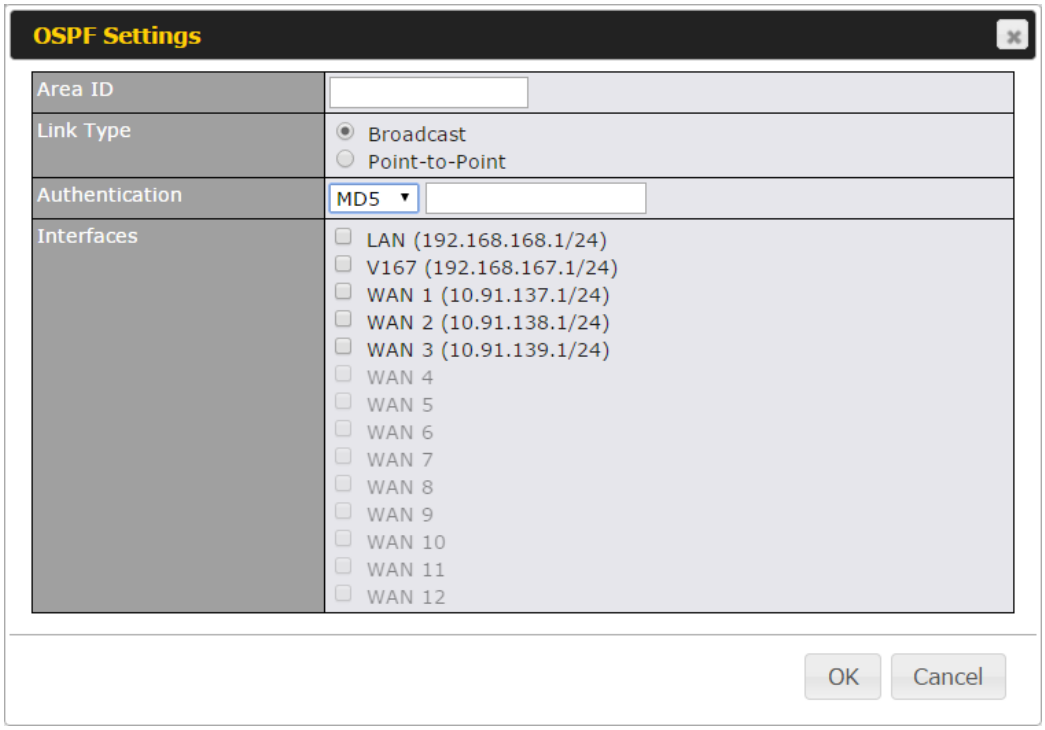
 Copyright @ 2017 Pepwave

# 20 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:

| 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 ✖ . |

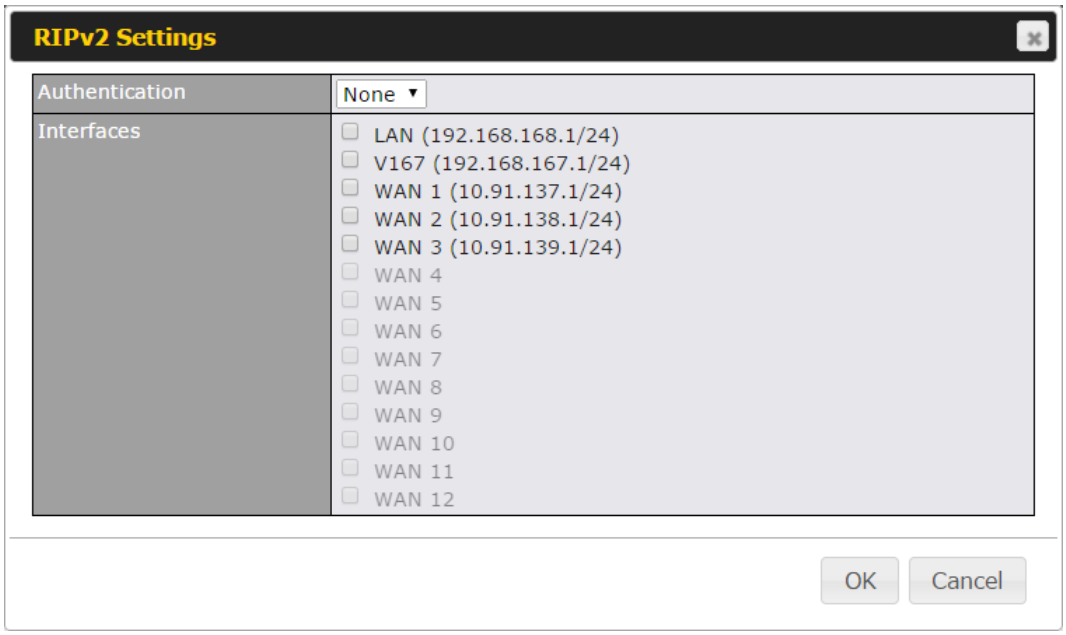
 Copyright @ 2017 Pepwave




| 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 .

 Copyright @ 2017 Pepwave

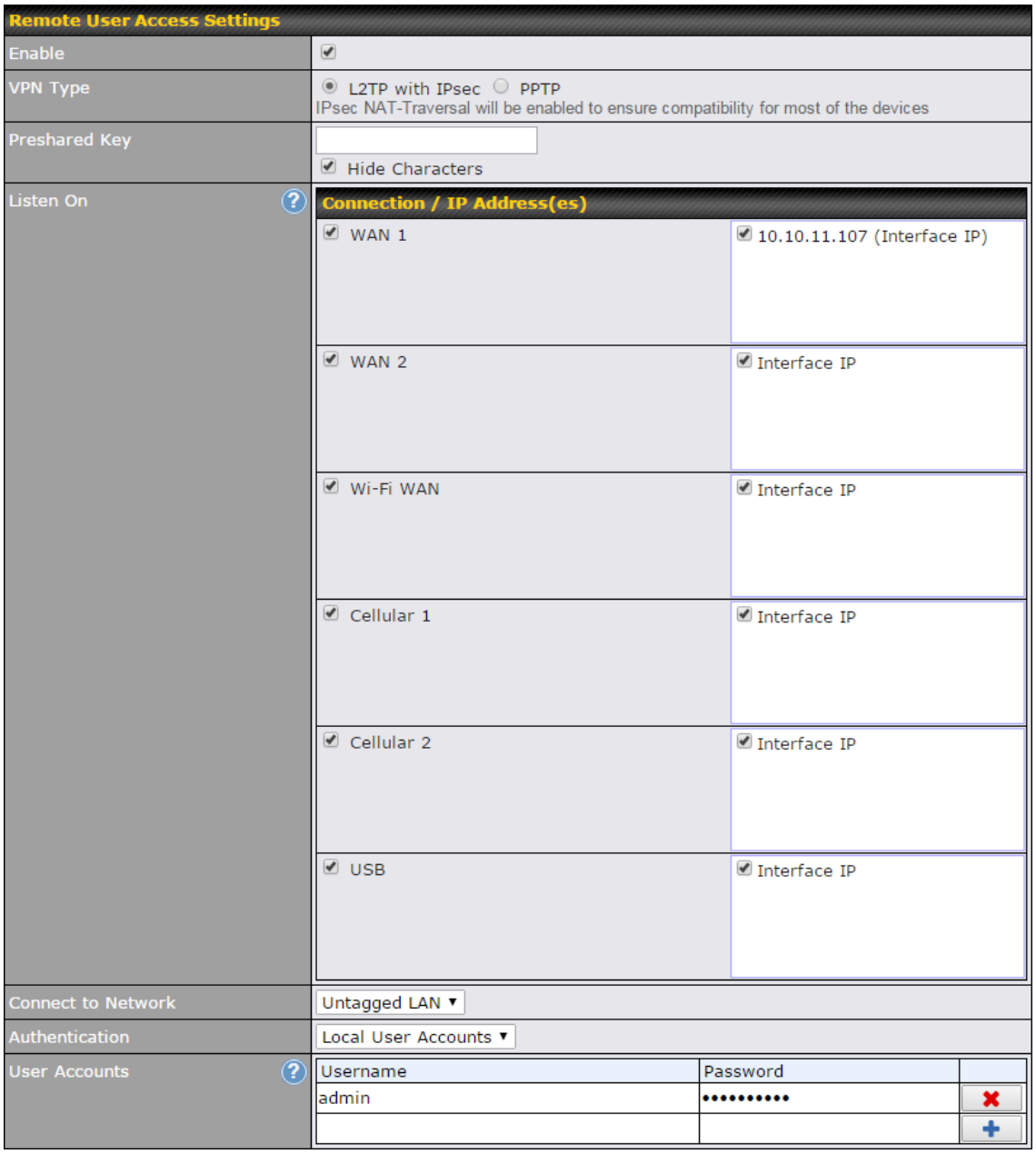



| RIPv2 Settings | |
|---|---|
| **Authentication** | Choose an authentication method, if one is used, from this drop-down menu. Available options are **MD5** and **Text**. Enter the authentication key next to the drop-down menu. |
| **Interfaces** | Determine which interfaces this group will use to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

# 21 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**

 Copyright @ 2017 Pepwave




| Remote User Access Settings | |
|---|---|
| **Enable** | Click the checkbox to enable Remote User Access. |

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

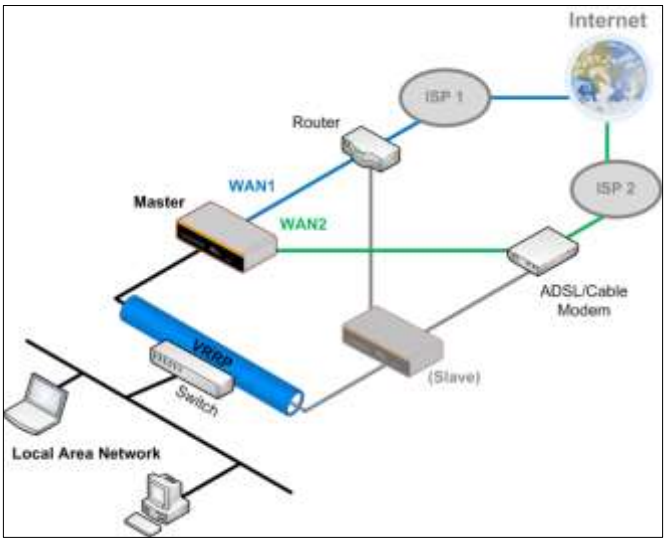
# Miscellaneous Settings

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

## 21.1 High Availability

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

 Copyright @ 2017 Pepwave




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.

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

 Copyright @ 2017 Pepwave

Interface for Master Router

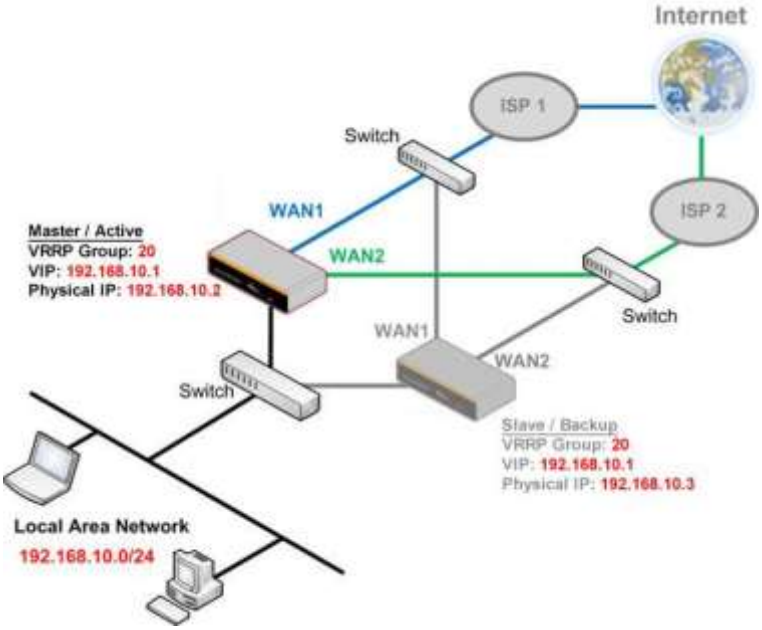
Interface for Slave Router

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

 Copyright @ 2017 Pepwave

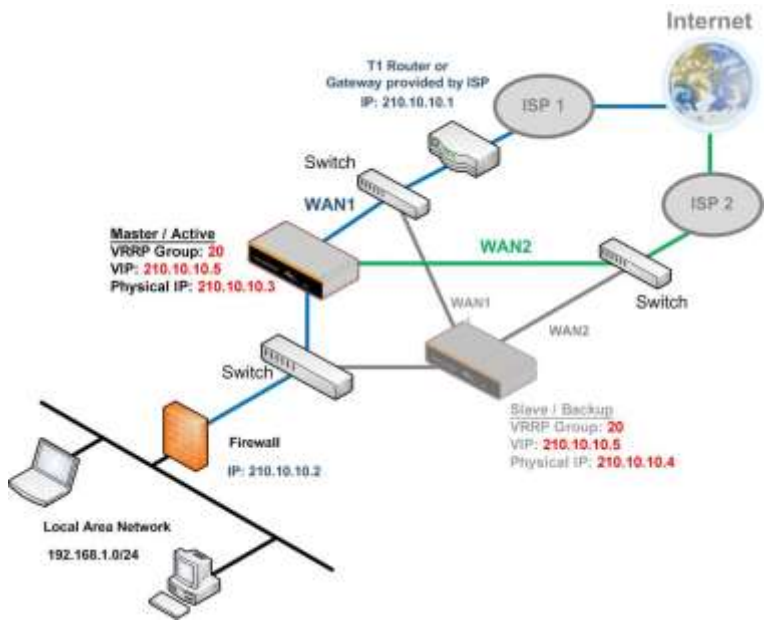
## Important Note

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.

 Copyright @ 2017 Pepwave



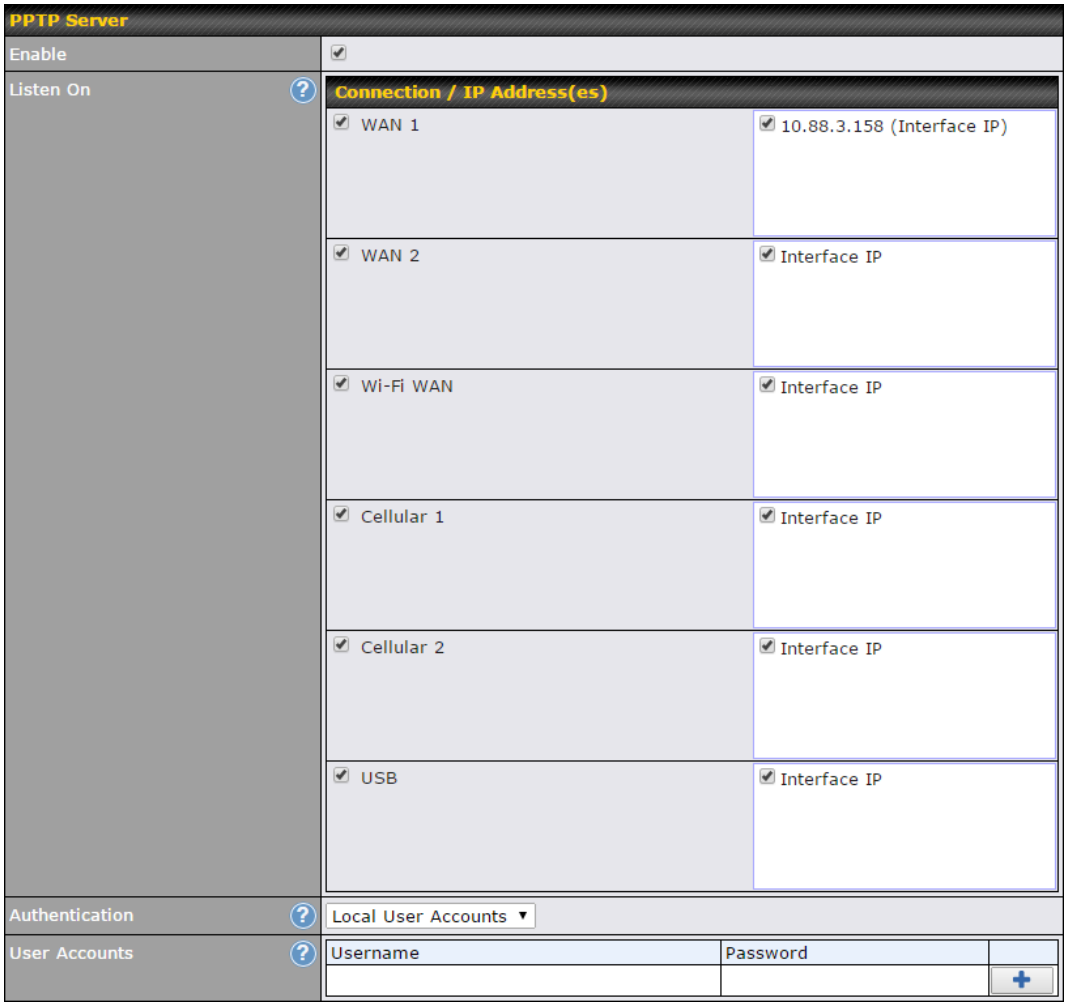

Please note that the drop-in WAN cannot be configured as a LAN bypass port while it is configured for high availability.

## 21.2 PPTP Server

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

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

 Copyright @ 2017 Pepwave




| PPTP Server Settings | |
|---|---|
| **Listen On** | This setting is for specifying the WAN connection(s) and IP address(es) that the PPTP server should listen on. |
| **Authentication** | This setting is for specifying the user database source for PPTP authentication. Three sources can be selected: **Local User Accounts, LDAP Server,** or **RADIUS Server**.<br>**Local User Accounts** - User accounts are stored in the Pepwave router locally. You can add/modify/delete accounts in the **User Accounts** table.<br>**LDAP Server** - Authenticate with an external LDAP server. This has been tested with Open LDAP servers where passwords are NTLM hashed. Active Directory is not supported. (You can choose to use RADIUS to authenticate with a Windows server.)<br>**RADIUS Server** - Authenticate with an external RADIUS server. This has been tested with Microsoft Windows Internet Authentication Service and FreeRADIUS servers where passwords are |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| | NTLM hashed or in plain text. |
| **User Accounts** | This setting allows you to define PPTP user accounts for authentication via local user accounts. Click **Add** to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click ✖ to delete the account in its corresponding row. |

## 21.3 Certificate Manager

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.

## 21.4 Service Forwarding

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

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

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **DNS Forwarding** | When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down. |
| **Custom Service Forwarding** | When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number. |

### 21.4.1 SMTP Forwarding

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

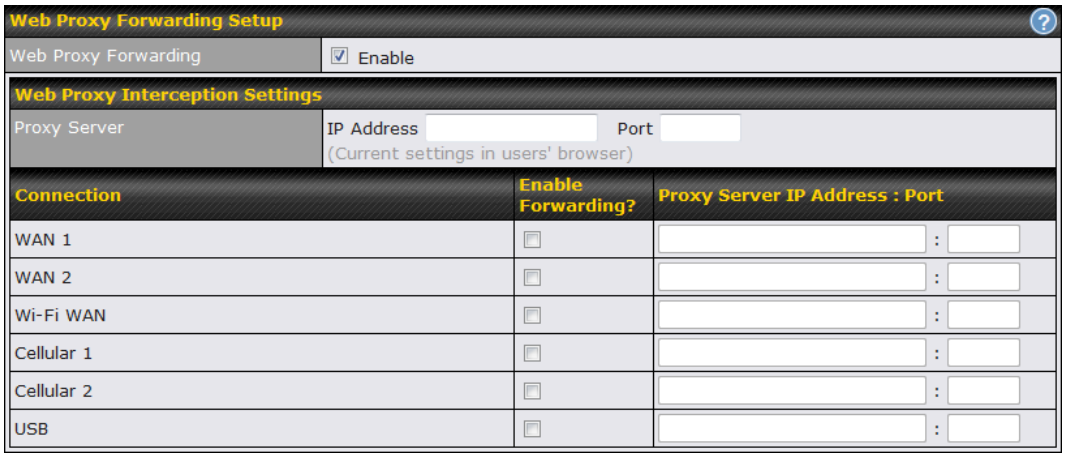
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

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**). |

 Copyright @ 2017 Pepwave

### 21.4.2 Web Proxy Forwarding




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.

### 21.4.3 DNS Forwarding

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

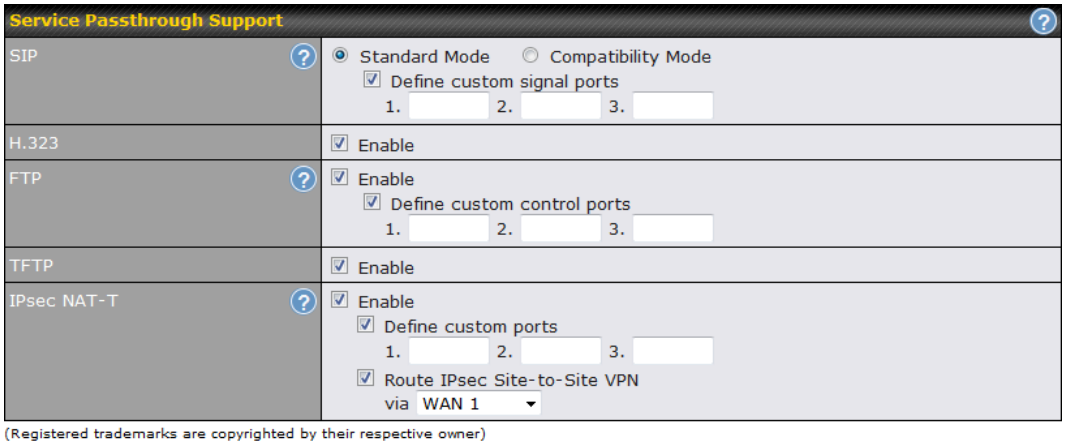
### 21.4.4 Custom Service Forwarding

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.

 Copyright @ 2017 Pepwave

## 21.5 Service Passthrough

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



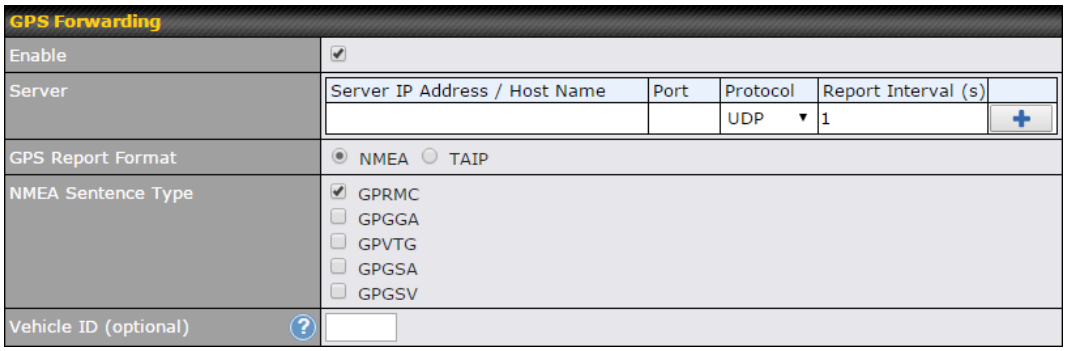

Some Internet services need to be specially handled in a multi-WAN environment. Pepwave routers can handle these services such that Internet applications do not notice being behind a multi-WAN router. Settings for service passthrough support are available here.

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

 Copyright @ 2017 Pepwave

## 21.6 GPS Forwarding

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




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

 Copyright @ 2017 Pepwave

# 22 AP Controller

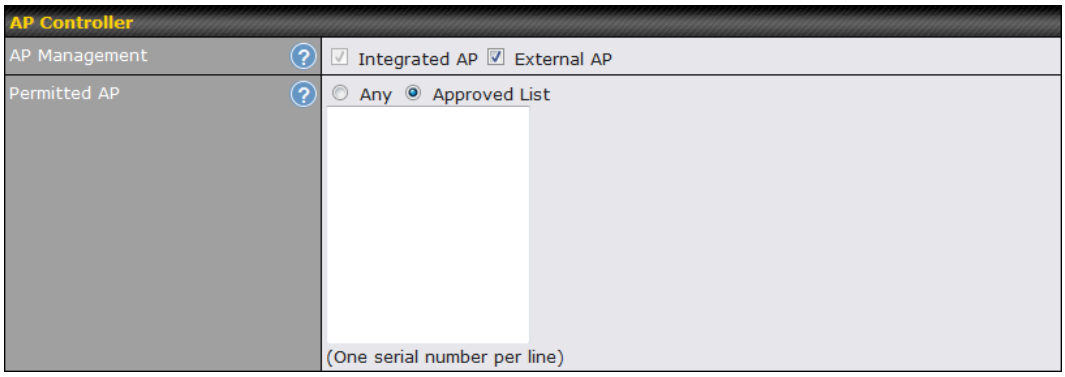
The AP controller acts as a centralized controller of Pepwave AP devices. With this feature, users can customize and manage multiple APs from a single Pepwave router interface.

| 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.

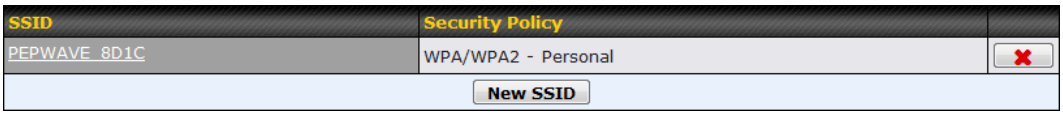
## 22.1 Wireless SSID

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.

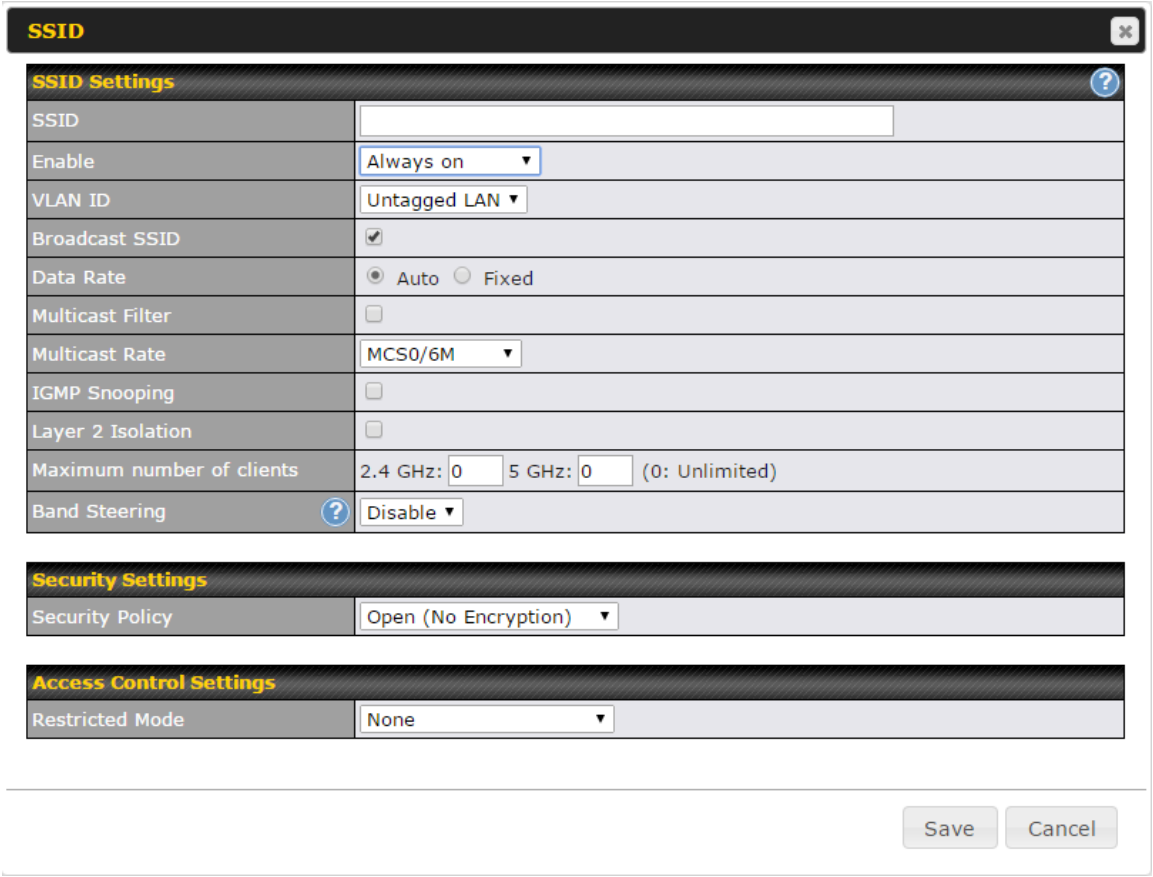



| AP Controller | |
| --- | --- |
| **AP Management** | The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for 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. |

 Copyright @ 2017 Pepwave




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.




 Copyright @ 2017 Pepwave

| SSID Settings | |
|---|---|
| **SSID** | This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients. |
| **Enable** | Click the drop-down menu to apply a time schedule to this interface |
| **VLAN ID** | This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is **0**, which means VLAN tagging is disabled (instead of tagged with zero). |
| **Broadcast SSID** | This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. **Broadcast SSID** is enabled by default. |
| **Data Rate** [A] | Select **Auto** to allow the Pepwave router to set the data rate automatically, or select **Fixed** and choose a rate from the displayed drop-down menu. |
| **Multicast Filter**[A] | This setting enables the filtering of multicast network traffic to the wireless SSID. |
| **Multicast Rate**[A] | This setting specifies the transmit rate to be used for sending multicast network traffic. The selected **Protocol** and **Channel Bonding** settings will affect the rate options and values available here. |
| **IGMP Snooping** [A] | To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option. |
| **DHCP Option 82** [A] | If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network. |
| **Network Priority (QoS)** [A] | Select from **Gold**, **Silver**, and **Bronze** to control the QoS priority of this wireless network's traffic. |
| **Layer 2 Isolation** [A] | **Layer 2** refers to the second layer in the ISO Open System Interconnect model.<br>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. |
| **Maximum Number of Clients** | Indicate the maximum number of clients that should be able to connect to each frequency. |
| **Band Steering** [A] | Band steering allows the Pepwave router to steer AP clients from the 2.4GHz band to the 5GHz band for better usage of bandwidth. To make steering mandatory, select **Enforce**. To cause the Pepwave router to preferentially choose steering, select **Prefer**. The default for this setting is **Disable**. |

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

 Copyright @ 2017 Pepwave

| Security Settings | |
|---|---|
| Security Policy | WPA2 - Personal |
| Encryption | AES:CCMP |
| Shared Key | •••••••• <br> ☑ Hide Characters |

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

| Access Control | |
|---|---|
| Restricted Mode | Deny all except listed |
| MAC Address List | |

| Access Control | |
|---|---|
| **Restricted Mode** | The settings allow administrator to control access using MAC address filtering. Available options are **None**, **Deny all except listed**, **Accept all except listed**, and **RADIUS MAC Authentication**.<br><br>When **WPA/WPA2 - Enterprise** is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the **Shared Key** option should be disabled. When using this method, select the appropriate version using the **V1**/**V2** controls. The security level of this method is known to be very high.<br>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.<br>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. |

 Copyright @ 2017 Pepwave

| RADIUS Server Settings | Primary Server | Secondary Server |
|---|---|---|
| Host | | |
| Secret | | |
| Authentication Port | 1812 Default | 1812 Default |
| Accounting Port | 1813 Default | 1813 Default |

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

## 22.2 Settings

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

 Copyright @ 2017 Pepwave

| AP Settings | | |
|---|---|---|
| SSID | 2.4 GHz ☑ 5 GHz ☑ Integrated AP supports 2.4 GHz only. Testing | |
| Operating Country | United States | |
| Preferred Frequency | ◉ 2.4 GHz ○ 5 GHz<br>Integrated AP supports 2.4 GHz only. | |
| | 2.4 GHz | 5 GHz |
| Protocol | 802.11ng | 802.11n/ac |
| Channel Width | 20 MHz | Auto |
| Channel | Auto Edit<br>Channels: 1 2 3 4 5 6 7 8 9 10 11 | Auto Edit<br>Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165 |
| Auto Channel Update | Daily at 03 :00<br>☑ Wait until no active client associated | Daily at 03 :00<br>☑ Wait until no active client associated |
| Output Power | Fixed: Max ☐ Boost | Fixed: Max ☐ Boost |
| Client Signal Strength Threshold | 0 -95 dBm (0: Unlimited) | 0 -95 dBm (0: Unlimited) |
| Maximum number of clients | 0 (0: Unlimited) | 0 (0: Unlimited) |
| Management VLAN ID | Untagged LAN (No VLAN) | |
| Operating Schedule | Always on | |
| Beacon Rate | 1 Mbps 6 Mbps will be used for 5 GHz radio | |
| Beacon Interval | 100 ms | |
| DTIM | 1 Default | |
| RTS Threshold | 0 Default | |
| Fragmentation Threshold | 0 (0: Disable) Default | |
| Distance / Time Converter | 4050 m<br>Note: Input distance for recommended values | |
| Slot Time | ○ Auto ◉ Custom 9 µs Default | |
| ACK Timeout | 48 µs Default | |
| Frame Aggregation | ☐ | |

 Copyright @ 2017 Pepwave

| AP Settings | |
|---|---|
| **SSID** | These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Peplink Balance does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP. |
| **Operating Country** | This drop-down menu specifies the national / regional regulations which the AP should follow.<br>● 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).<br>● If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).<br>NOTE: Users are required to choose an option suitable to local laws and regulations.<br>Per FCC regulation, the country selection is not available on all models marketed in US. All US models are fixed to US channels only. |
| **Preferred Frequency** | These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies. |
| **Protocol** | This section displays the 2.4 GHz protocols your APs are using. |
| **Channel Width** | There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection. |
| **Channel** | This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If **Auto** is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically. |
| **Auto Channel Update** | Indicate the time of day at which update automatic channel selection. |
| **Output Power**[A] | This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When **Dynamic** settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance.<br>The **Dynamic: Auto** setting will set the AP to do this automatically. Otherwise, the **Dynamic: Manual** setting will set the AP to dynamically adjust only of instructed to do so. If you have set **Dynamic:Manual**, you can go to **AP>Toolbox>Auto Power Adj.** to give your AP further instructions.<br><br>If you click the **Boost** checkbox, 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. |

 Copyright @ 2017 Pepwave

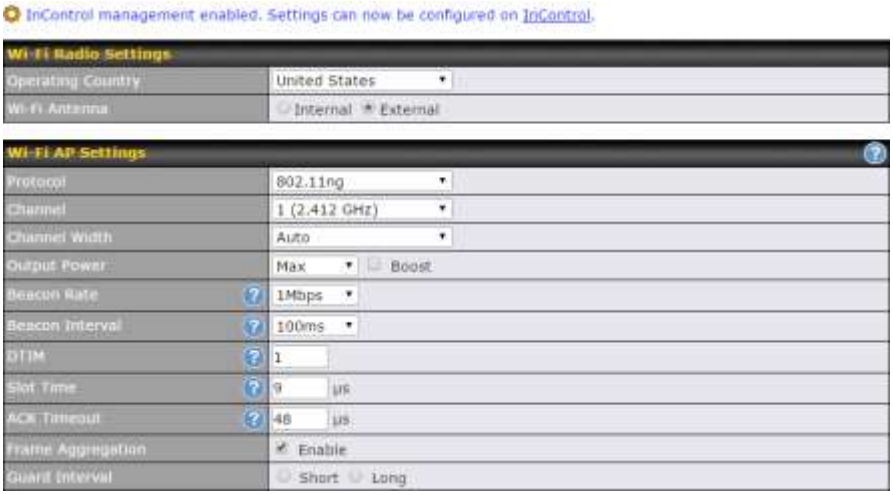
| | |
|---|---|
| **Client Signal Strength Threshold[A]** | This field determines that maximum signal strength each individual client will receive. The measurment unit is megawatts. |
| **Max number of Clients[A]** | This field determines the maximum clients that can be connected to APs under this profile. |
| **Management VLAN ID** | This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is **0** by default, meaning that no VLAN tagging will be applied. NOTE: change this value with caution as alterations may result in loss of connection to the AP controller. |
| **Operating Schedule** | Choose from the schedules that you have defined in **System>Schedule**. Select the schedule for the integrated AP to follow from the drop-down menu. |
| **Beacon Rate[A]** | This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are **1Mbps**, **2Mbps**, **5.5Mbps**, **6Mbps**, and **11Mbps**. |
| **Beacon Interval[A]** | This drop-down menu provides the option to set the time between each beacon send. Available options are **100ms**, **250ms**, and **500ms**. |
| **DTIM[A]** | This field provides the option to set the frequency for beacon to include delivery traffic indication messages (DTIM). The interval unit is measured in milliseconds. |
| **RTS Threshold[A]** | This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting **0** disables this feature. |
| **Fragmentation Threshold[A]** | Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation. |
| **Distance/Time Converter[A]** | Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended. |
| **Slot Time[A]** | This field provides the option to modify the unit wait time before it transmits. The default value is **9µs**. |
| **ACK Timeout[A]** | This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is **48µs**. |
| **Frame Aggregation[A]** | With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission. |
| **Frame Length** | This field is only available when **Frame Aggregation** is enabled. It specifies the frame length for frame aggregation. By default, it is set to **50000**. |

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

 Copyright @ 2017 Pepwave

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

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




 Copyright @ 2017 Pepwave

| Wi-Fi Radio Settings | |
|---|---|
| **Operating Country** | This option sets the country whose regulations the Pepwave router follows. |
| **Wi-Fi Antenna** | Choose from the router's internal or optional external antennas, if so equipped. |

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

| Wi-Fi AP Settings | |
|---|---|
| **Protocol** | This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, **802.11ng** is selected. |
| **Channel** | This option allows you to select which 802.11 RF channel will be used. **Channel 1 (2.412 GHz)** is selected by default. |
| **Channel Width** | **Auto (20/40 MHz)** and **20 MHz** are available. The default setting is **Auto (20/40 MHz),** which allows both widths to be used simultaneously. |
| **Output Power** | This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country. |
| **Beacon Rate[A]** | This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected. |
| **Beacon Interval[A]** | This option is for setting the time interval between each beacon. By default, **100ms** is selected. |
| **DTIM[A]** | This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to **1 ms**. |
| **Slot Time[A]** | This field is for specifying the wait time before the Router transmits a packet. By default, this field is set to **9 µs**. |
| **ACK Timeout[A]** | This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to **48 µs**. |
| **Frame Aggregation[A]** | This option allows you to enable frame aggregation to increase transmission throughput. |
| **Guard Interval[A]** | This setting allows choosing a short or long guard period interval for your transmissions. |

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

 Copyright @ 2017 Pepwave

# 23 AP Controller Status

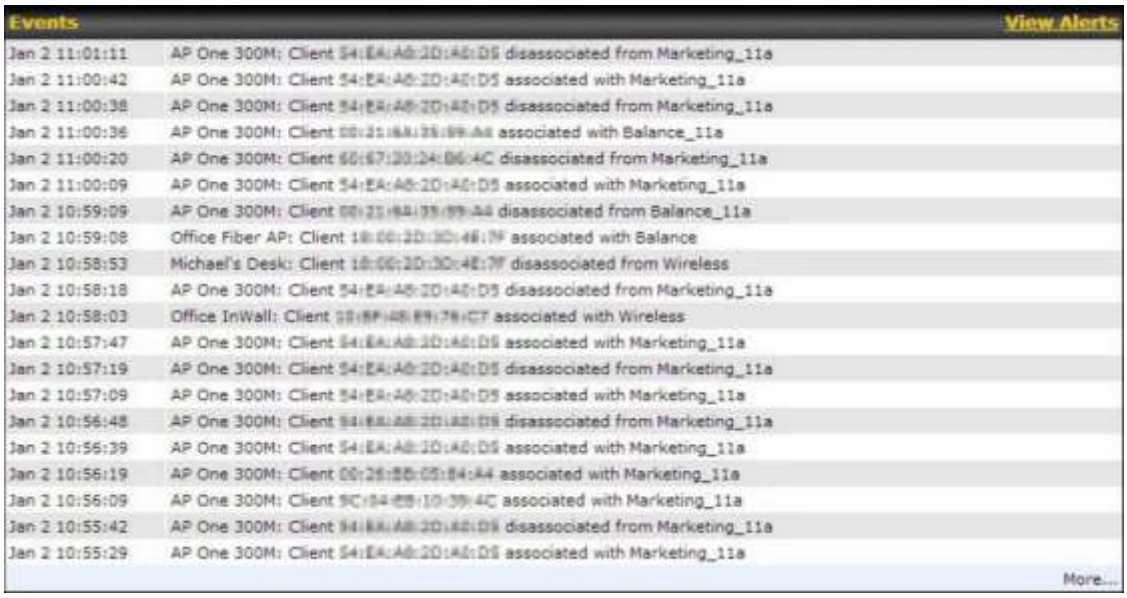
## 23.1 Info

A comprehensive overview of your AP can be accessed by navigating to **AP > Controller Status > Info**.

| AP Controller | |
|---|---|
| **License Limit** | This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage. |
| **Frequency** | Underneath, there are two check boxes labeled **2.4 Ghz** and **5 Ghz**. Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies. |
| **SSID** | The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs. |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **No. of APs** | This pie chart and table indicates how many APs are online and how many are offline. |
| **No.of Clients** | This graph displays the number of clients connected to each network at any given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time. |
| **Data Usage** | This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to **Zoom** to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale. |



| Events | View Alerts |
|---|---|
| Jan 2 11:01:11 | AP One 300M: Client 54:EA:A6:2D:A6:D5 disassociated from Marketing_11a |
| Jan 2 11:00:42 | AP One 300M: Client 54:EA:A6:2D:A6:D5 associated with Marketing_11a |
| Jan 2 11:00:38 | AP One 300M: Client 54:EA:A6:2D:A6:D5 disassociated from Marketing_11a |
| Jan 2 11:00:36 | AP One 300M: Client 00:21:6A:35:99:A8 associated with Balance_11a |
| Jan 2 11:00:20 | AP One 300M: Client 60:67:20:24:D6:4C disassociated from Marketing_11a |
| Jan 2 11:00:09 | AP One 300M: Client 54:EA:A6:2D:A6:D5 associated with Marketing_11a |
| Jan 2 10:59:09 | AP One 300M: Client 00:21:6A:35:99:A8 disassociated from Balance_11a |
| Jan 2 10:59:08 | Office Fiber AP: Client 10:00:2D:3D:4E:7F associated with Balance |
| Jan 2 10:58:53 | Michael's Desk: Client 10:00:2D:3D:4E:7F disassociated from Wireless |
| Jan 2 10:58:18 | AP One 300M: Client 54:EA:A6:2D:A6:D5 disassociated from Marketing_11a |
| Jan 2 10:58:03 | Office InWall: Client 10:BF:48:89:78:C7 associated with Wireless |
| Jan 2 10:57:47 | AP One 300M: Client 54:EA:A6:2D:A6:D5 associated with Marketing_11a |
| Jan 2 10:57:19 | AP One 300M: Client 54:EA:A6:2D:A6:D5 disassociated from Marketing_11a |
| Jan 2 10:57:09 | AP One 300M: Client 54:EA:A6:2D:A6:D5 associated with Marketing_11a |
| Jan 2 10:56:48 | AP One 300M: Client 54:EA:A6:2D:A6:D5 disassociated from Marketing_11a |
| Jan 2 10:56:39 | AP One 300M: Client 54:EA:A6:2D:A6:D5 associated with Marketing_11a |
| Jan 2 10:56:19 | AP One 300M: Client 00:26:B6:05:84:A4 associated with Marketing_11a |
| Jan 2 10:56:09 | AP One 300M: Client 9C:54:B5:10:39:4C associated with Marketing_11a |
| Jan 2 10:55:42 | AP One 300M: Client 54:EA:A6:2D:A6:D5 disassociated from Marketing_11a |
| Jan 2 10:55:29 | AP One 300M: Client 54:EA:A6:2D:A6:D5 associated with Marketing_11a |
| | More... |

## Events

This event log displays all activity on your AP network, down to the client level. Click **View Alerts** to see only alerts, and click the **More…** link for additional records.

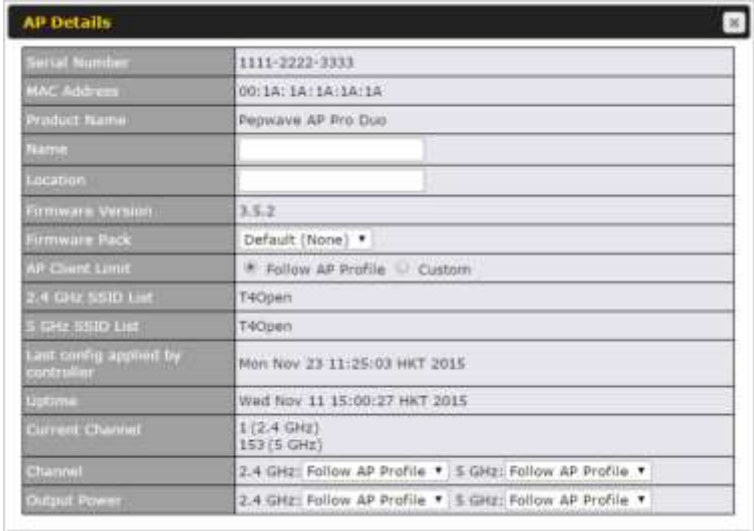
 Copyright @ 2017 Pepwave

## 23.2 Access Point (Usage)

A detailed breakdown of data usage for each AP is available at **AP > Controller Status > Access Point**.

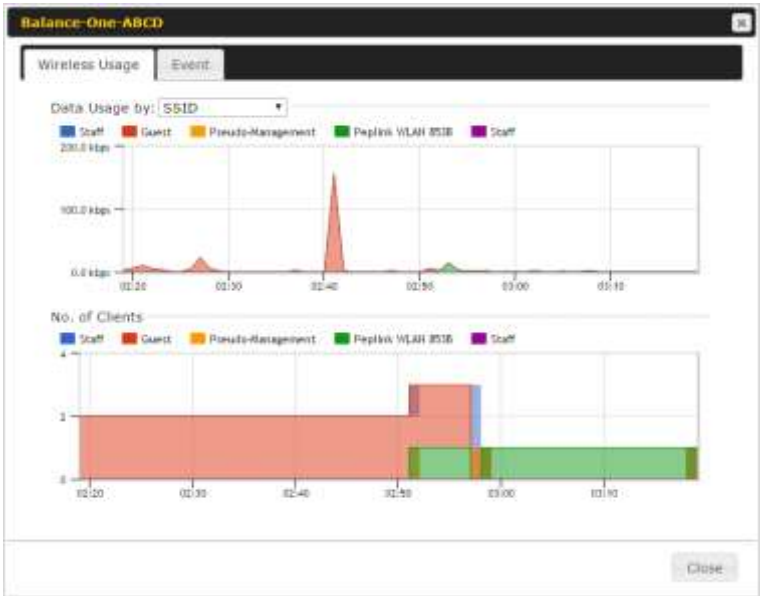
| Usage | |
|---|---|
| **AP Name/Serial Number** | This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported. |
| **Online Status** | This button toggles whether your search will include offline devices. |
| **Managed Wireless Devices** | This table shows the detailed information on each AP, including channel, number of clients, upload traffic, and download traffic. Click the blue arrows at the left of the table to expand and collapse information on each device group. You could also expand and collapse all groups by using the Expand Collapse buttons.<br>On the right of the table, you will see the following icons: .<br>Click the icon to see a usage table for each client:<br> <br><br>Click the icon to configure each client |

 Copyright @ 2017 Pepwave




For easier network management, you can give each client a name and designate its location. You can also designate which firmware pack (if any) this client will follow, as well as the channels on which the client will broadcast.

Click the icon to see a graph displaying usage:



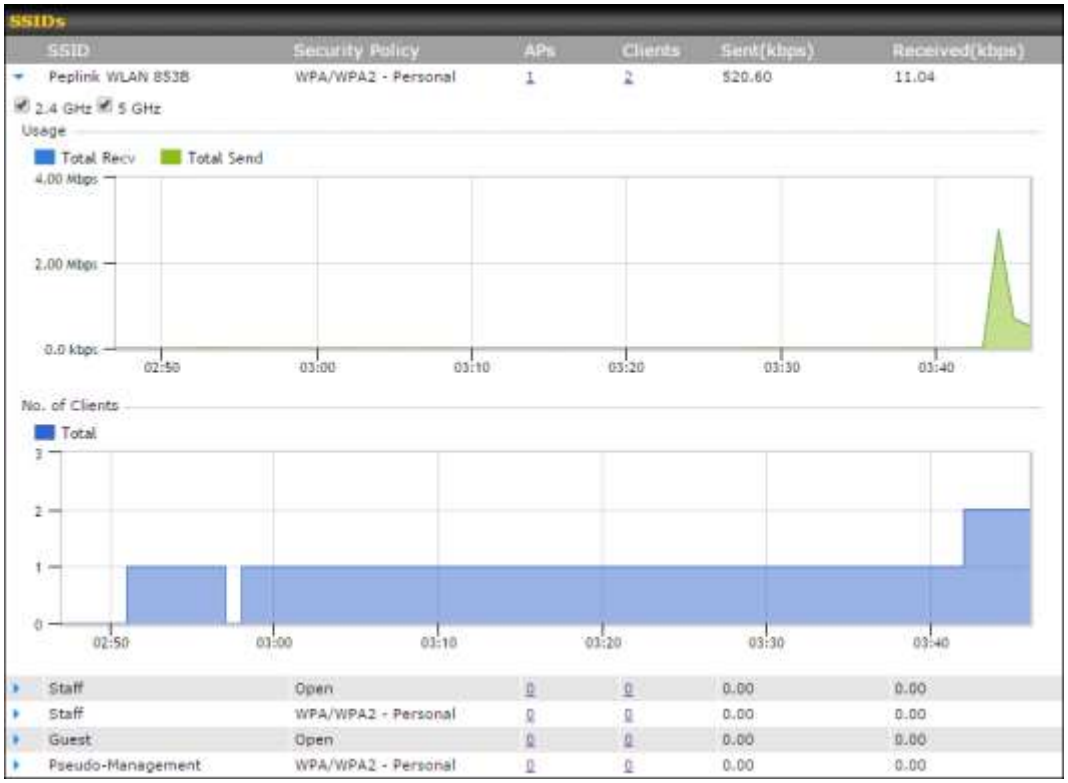

Click any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can display the information by SSID or by AP send/receive rate.

Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:

 Copyright @ 2017 Pepwave

## 23.3 Wireless SSID

In-depth SSID reports are available under **AP > Controller Status > Wireless SSID**.

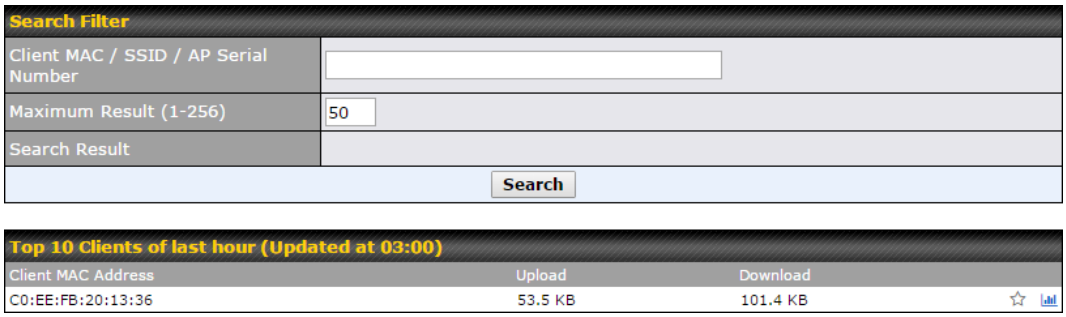



Click the blue arrow on any SSID to obtain more detailed usage information on each SSID.

 Copyright @ 2017 Pepwave

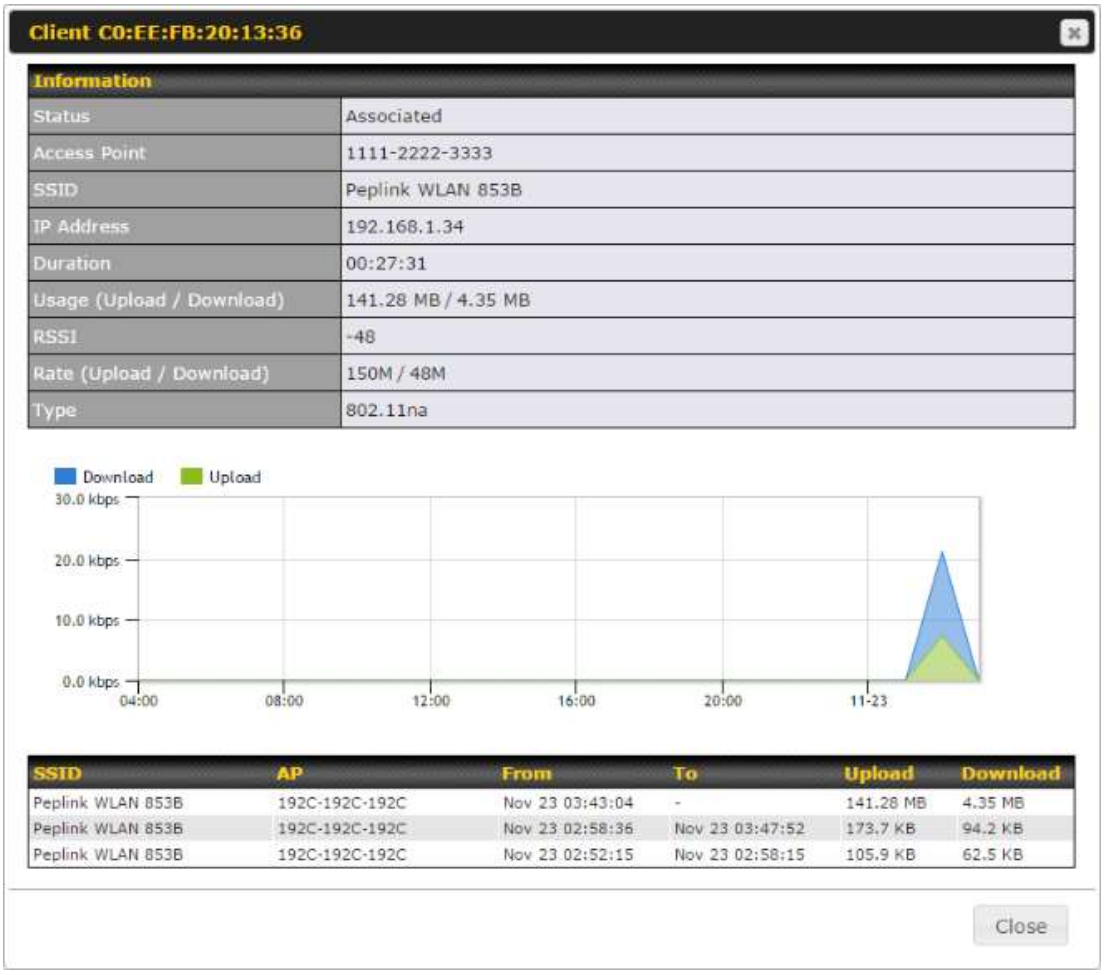
## 23.4 Wireless Client

You can search for specific Wi-Fi users by navigating to **AP > Controller Status > Wireless Client**.




Here, you will be able to see your network's heaviest users as well as search for specific users. Click the ☆ icon to bookmark specific users, and click the icon for additional details about each user:

 Copyright @ 2017 Pepwave




 Copyright @ 2017 Pepwave

## 23.5 Nearby Device

A listing of near devices can be accessed by navigating to **AP > Controller Status > Nearby Device**.

**Suspected Rogue APs**

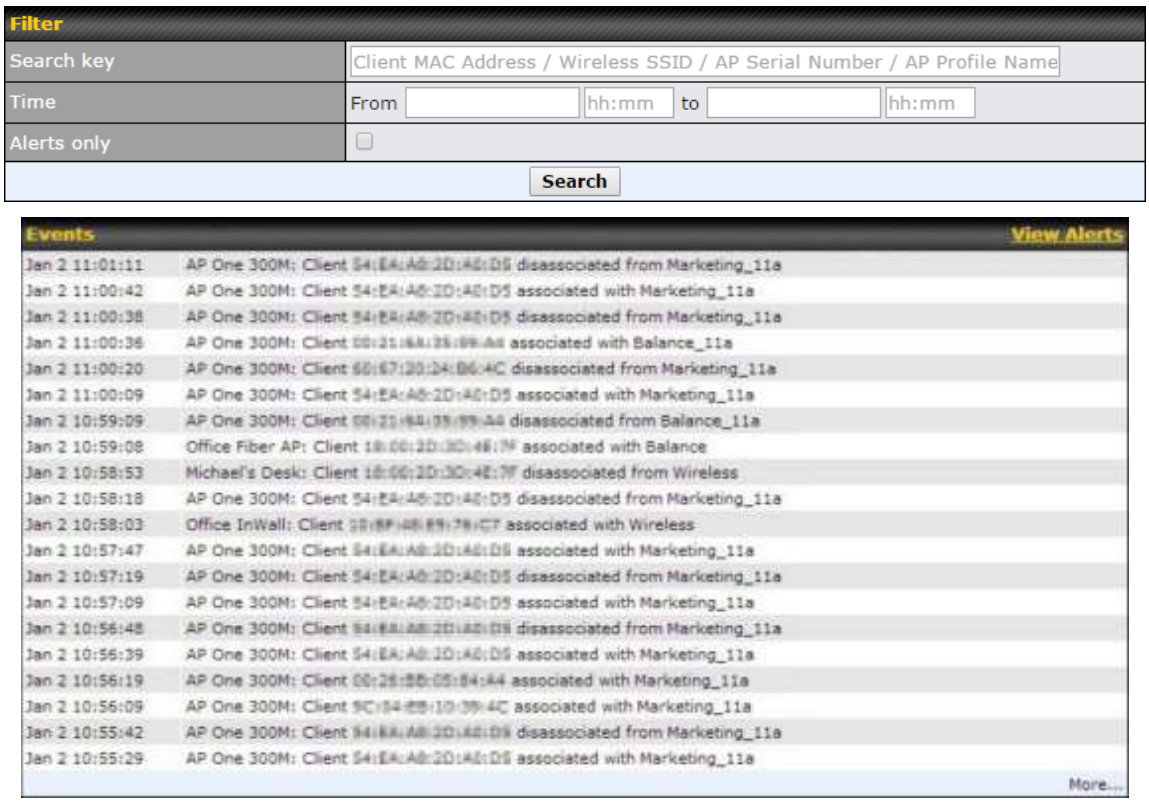
| BSSID | SSID | Channel | Encryption | Last Seen | Mark as |
|---|---|---|---|---|---|
| [illegible] | Wireless | 11 | WPA2 | 10 hours ago | |
| [illegible] | Accounting | 11 | WPA2 | 10 hours ago | |
| [illegible] | Marketing | 11 | WPA2 | 11 hours ago | |
| [illegible] | MYB1PUSH | 1 | WPA & WPA2 | 11 minutes ago | |
| [illegible] | MYB1 | 1 | WPA2 | 15 minutes ago | |
| [illegible] | PEPWAVE_CB7E | 1 | WPA & WPA2 | 5 minutes ago | |
| [illegible] | Micro_S1_1 | 6 | WPA & WPA2 | 1 hour ago | |
| [illegible] | MAX HD2 Gobi | 11 | WPA & WPA2 | 2 minutes ago | |
| [illegible] | PEPLINK_05B5 | 4 | WPA & WPA2 | 1 minute ago | |
| [illegible] | LK_05B5 | 4 | WPA2 | 1 minute ago | |
| [illegible] | LK_05B5_VLAN22 | 4 | WPA2 | 1 minute ago | |
| [illegible] | dev_captive_portal_test | 1 | WPA & WPA2 | 3 minutes ago | |
| [illegible] | PEPWAVE_7052 | 11 | WPA & WPA2 | 2 hours ago | |
| [illegible] | dev_captive_portal_test | 6 | WPA & WPA2 | 6 minutes ago | |
| [illegible] | ssid_test | 8 | WPA & WPA2 | 2 minutes ago | |
| [illegible] | SSID New | 8 | WPA & WPA2 | 2 minutes ago | |
| [illegible] | Guest SSID | 9 | WPA2 | 2 minutes ago | |
| [illegible] | PEPWAVE_67B8 | 1 | WPA & WPA2 | 5 minutes ago | |
| [illegible] | G BR1 Portal | 2 | WPA2 | 2 minutes ago | |
| [illegible] | ssid_test | 8 | WPA & WPA2 | 2 hours ago | |

| Suspected Rogue Devices |
|---|
| Hovering over the device MAC address will result in a popup with information on how this device was detected. Click the icons and the device will be moved to the bottom table of identified devices. |

 Copyright @ 2017 Pepwave

## 23.6 Event Log

You can access the AP Controller Event log by navigating to **AP > Controller Status > Event Log**.




| Events |
| --- |
| This event log displays all activity on your AP network, down to the client level. Use to filter box to search by MAC address, SSID, AP Serial Number, or AP Profile name. Click **View Alerts** to see only alerts, and click the **More…** link for additional records. |

 Copyright @ 2017 Pepwave

# 24 Toolbox

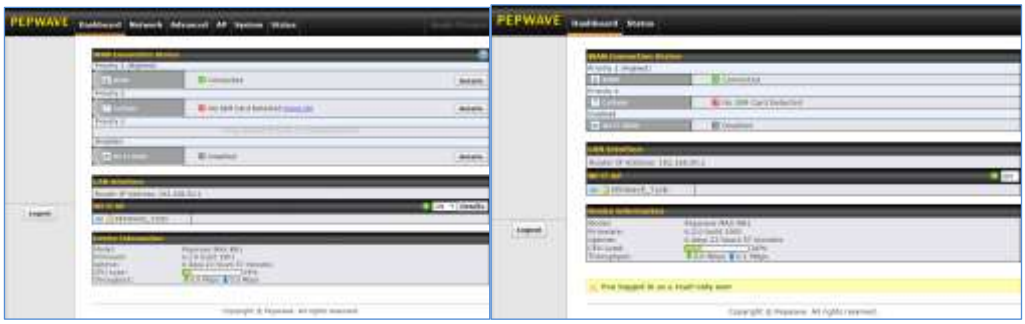
Tools for managing firmware packs can be found at **AP>Toolbox**.

| 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. |

# 25 System Settings

## 25.1 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.



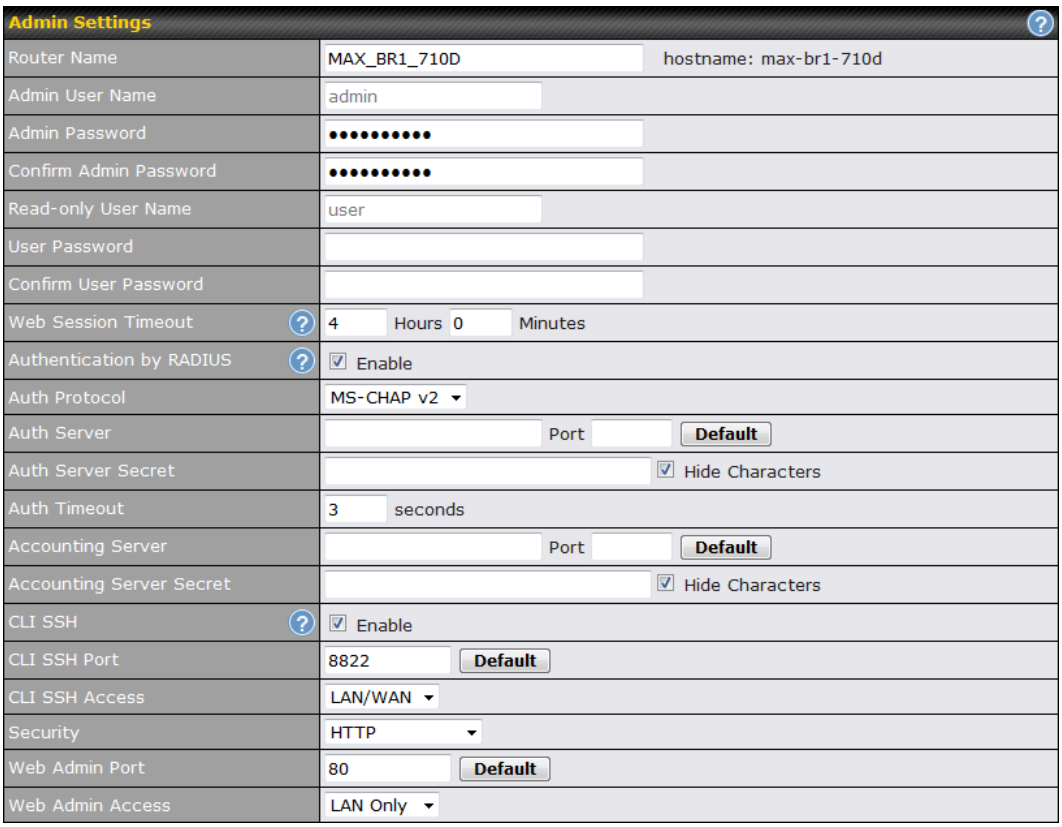
Admin account UI User account UI

 Copyright @ 2017 Pepwave

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**.



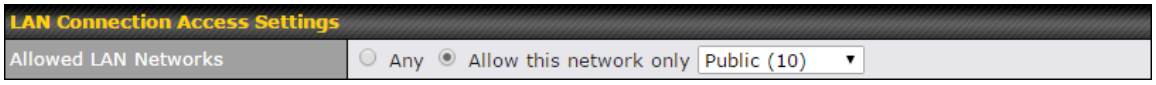
| Admin Settings | |
|---|---|
| Router Name | MAX_BR1_710D hostname: max-br1-710d |
| Admin User Name | admin |
| Admin Password | •••••••••• |
| Confirm Admin Password | •••••••••• |
| Read-only User Name | user |
| User Password | |
| Confirm User Password | |
| Web Session Timeout | 4 Hours 0 Minutes |
| Authentication by RADIUS | ☑ Enable |
| Auth Protocol | MS-CHAP v2 |
| Auth Server | Port Default |
| Auth Server Secret | ☑ Hide Characters |
| Auth Timeout | 3 seconds |
| Accounting Server | Port Default |
| Accounting Server Secret | ☑ Hide Characters |
| CLI SSH | ☑ Enable |
| CLI SSH Port | 8822 Default |
| CLI SSH Access | LAN/WAN |
| Security | HTTP |
| Web Admin Port | 80 Default |
| Web Admin Access | LAN Only |

 Copyright @ 2017 Pepwave

| Admin Settings | |
|---|---|
| **Router Name** | This field allows you to define a name for this Pepwave router. By default, **Router Name** is set as **MAX_XXXX**, where *XXXX* refers to the last 4 digits of the unit's serial number. |
| **Admin User Name** | **Admin User Name** is set as *admin* by default, but can be changed, if desired. |
| **Admin Password** | This field allows you to specify a new administrator password. |
| **Confirm Admin Password** | This field allows you to verify and confirm the new administrator password. |
| **Read-only User Name** | **Read-only User Name** is set as *user* by default, but can be changed, if desired. |
| **User Password** | This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled. |
| **Confirm User Password** | This field allows you to verify and confirm the new user password. |
| **Web Session Timeout** | This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to **4 hours**. |
| **Authentication by RADIUS** | 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. |
| **Auth Protocol** | This specifies the authentication protocol used. Available options are **MS-CHAP v2** and **PAP**. |
| **Auth Server** | This specifies the access address and port of the external RADIUS server. |
| **Auth Server Secret** | This field is for entering the secret key for accessing the RADIUS server. |
| **Auth Timeout** | This option specifies the time value for authentication timeout. |
| **Accounting Server** | This specifies the access address and port of the external accounting server. |
| **Accounting Server Secret** | This field is for entering the secret key for accessing the accounting server. |
| **Network** | This option is for specifying the network connection to be used for authentication. Users can |

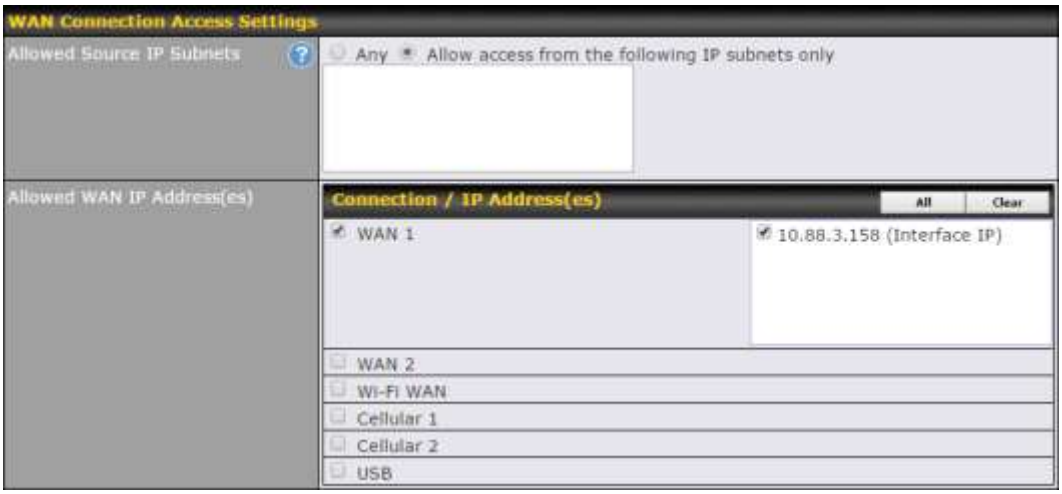
 Copyright @ 2017 Pepwave

| | |
|---|---|
| **Connection** | choose from LAN, WAN, and VPN connections. |
| **CLI SSH** | The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to **Section 21.16**. |
| **CLI SSH Port** | This field determines the port on which clients can access CLI SSH. |
| **CLI SSH Access** | This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only. |
| **Security** | This option is for specifying the protocol(s) through which the web admin interface can be accessed:<br>● HTTP<br>● HTTPS<br>● HTTP/HTTPS |
| **Web Admin Port** | This field is for specifying the port number on which the web admin interface can be accessed. |
| **Web Admin Access** | This option is for specifying the network interfaces through which the web admin interface can be accessed:<br>● LAN only<br>● LAN/WAN<br>If LAN/WAN is chosen, the **WAN Connection Access Settings** form will be displayed. |




| LAN Connection Access Settings | |
|---|---|
| **Allowed LAN Networks** | This field allows you to permit only specific networks or VLANs to access the Web UI. |

 Copyright @ 2017 Pepwave

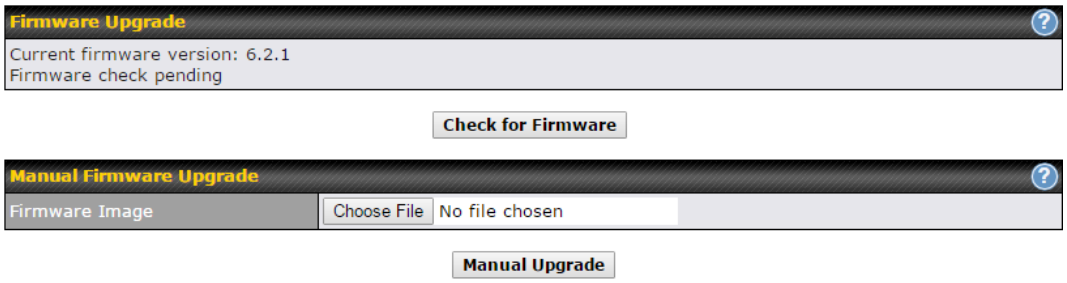



| WAN Connection Access Settings | |
|---|---|
| **Allowed Source IP Subnets** | This field allows you to restrict web admin access only from defined IP subnets.<br>● **Any** - Allow web admin accesses to be from anywhere, without IP address restriction.<br>● **Allow access from the following IP subnets only** - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:<br>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*).<br>To define multiple subnets, separate each IP subnet one in a line. For example:<br>● 192.168.0.0/24<br>● 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. |

 Copyright @ 2017 Pepwave

## 25.2 Firmware

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




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.

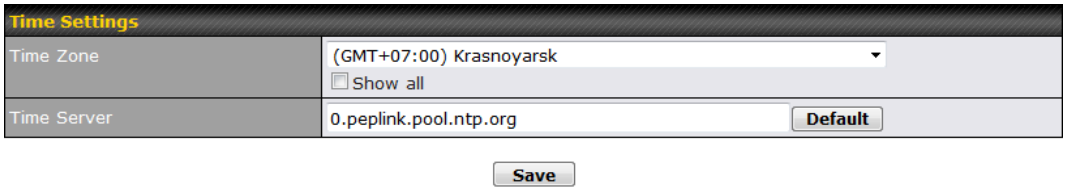
| Important Note |
| --- |
| The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. Do not disconnect the power during firmware upgrade process. 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. |

 Copyright @ 2017 Pepwave

## 25.3 Time

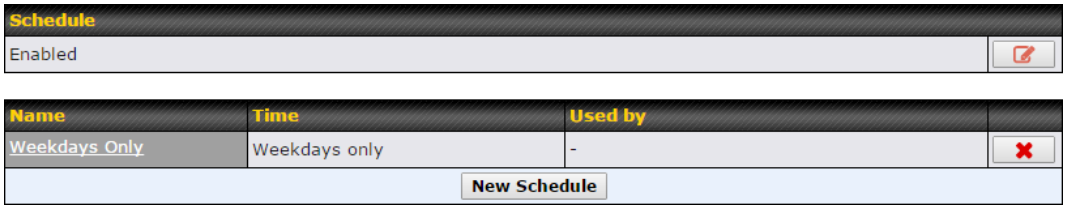
**Time Settings** enables the system clock of the Pepwave router to be synchronized with a specified time server. Time settings are located at **System>Time**.




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

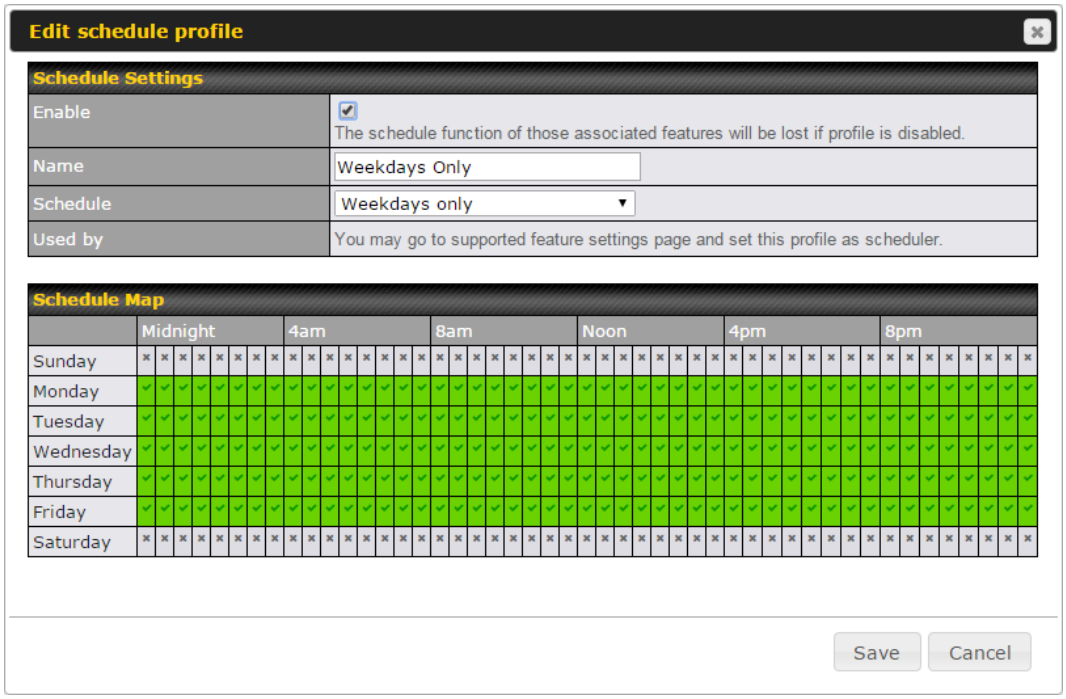
## 25.4 Schedule

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**




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

 Copyright @ 2017 Pepwave

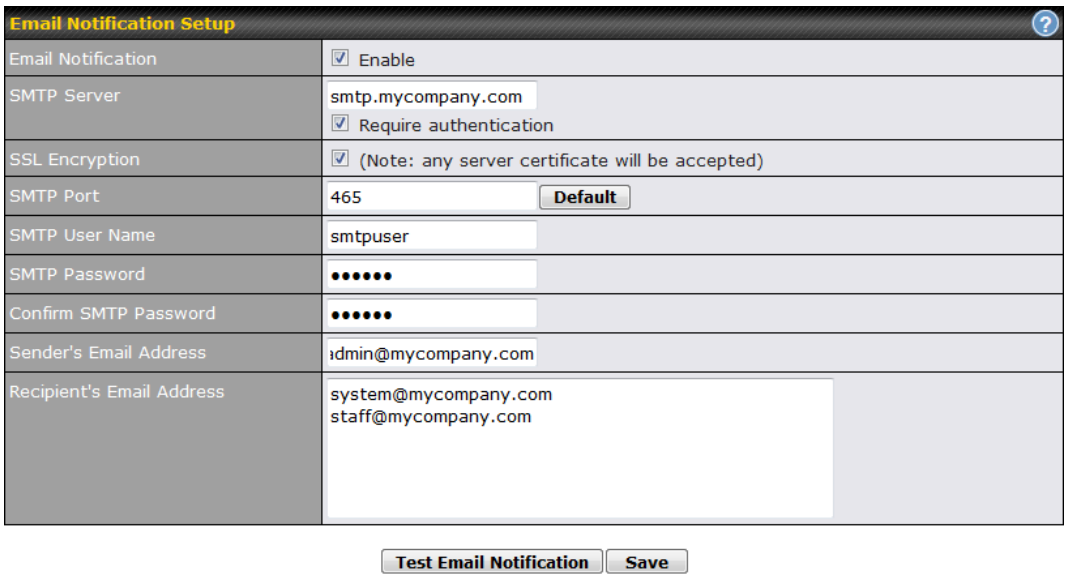



| Edit Schedule Profile | |
|---|---|
| **Enabling** | Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled. |
| **Name** | Enter your desired name for this particular schedule profile. |
| **Schedule** | 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. |
| **Schedule Map** | Click on the desired times to enable features at that time period. You can hold your mouse for faster entry. |

 Copyright @ 2017 Pepwave

## 25.5 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**.




| Email Notification Settings | |
|---|---|
| **Email Notification** | This setting specifies whether or not to enable email notification. If **Enable** is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If **Enable** is not checked, email notification is disabled and the Pepwave router will not send email messages. |
| **SMTP Server** | This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check **Require authentication**. |
| **SSL Encryption** | Check the box to enable SMTPS. When the box is checked, **SMTP Port** will be changed to **465** automatically. |
| **SMTP Port** | This field is for specifying the SMTP port number. By default, this is set to **25**; when **SSL Encryption** is checked, the default port number will be set to **465**. You may customize the port number by editing this field. Click **Default** to restore the number to its default setting. |
| **SMTP User Name / Password** | This setting specifies the SMTP username and password while sending email. These options are shown only if **Require authentication** is checked in the **SMTP Server** setting. |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **Confirm SMTP Password** | This field allows you to verify and confirm the new administrator password. |
| **Sender's Email Address** | This setting specifies the email address the Pepwave router will use to send reports. |
| **Recipient's Email Address** | 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 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<br>staff@mycompany.com |

Send Test Notification | Cancel

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.**

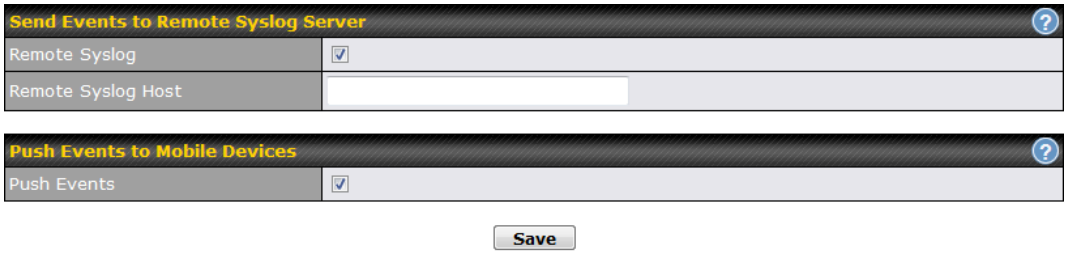
**Test Result**

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

 Copyright @ 2017 Pepwave

## 25.6 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**.




| 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. |
| **Push Events** | 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. |
| | For more information on the Router Utility, go to: HYPERLINK "http://www.peplink.com/products/router-utility" www.peplink.com/products/router-utility |

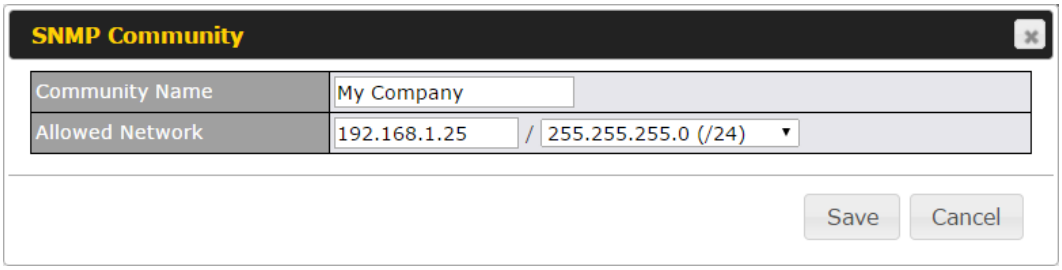
## 25.7 SNMP

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**.

 Copyright @ 2017 Pepwave

| SNMP Settings | |
|---|---|
| **SNMP Device Name** | This field shows the router name defined at **System>Admin Security**. |
| **SNMP Port** | This option specifies the port which SNMP will use. The default port is **161**. |
| **SNMPv1** | This option allows you to enable SNMP version 1. |
| **SNMPv2** | This option allows you to enable SNMP version 2. |
| **SNMPv3** | This option allows you to enable SNMP version 3. |

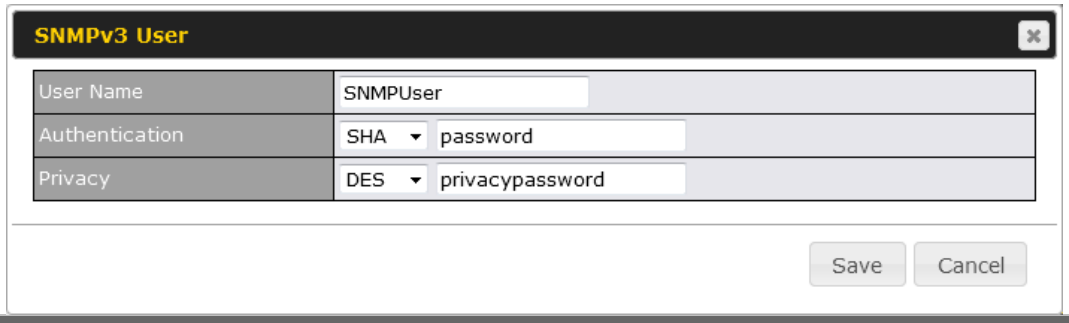
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:




 Copyright @ 2017 Pepwave

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

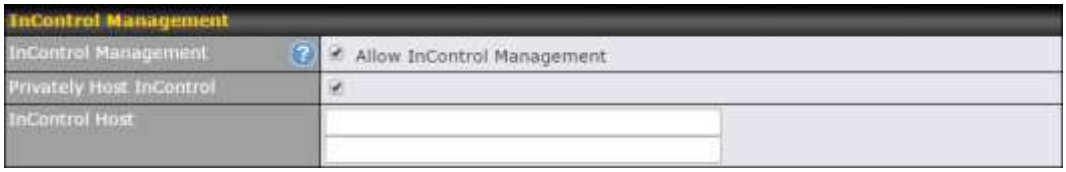
To define a user name for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:




| SNMPv3 User Settings | |
|---|---|
| **User Name** | This setting specifies a user name to be used in SNMPv3. |
| **Authentication Protocol** | This setting specifies via a drop-down menu one of the following valid authentication protocols:<br>● NONE<br>● MD5<br>● SHA<br>When MD5 or SHA is selected, an entry field will appear for the password. |
| **Privacy Protocol** | This setting specifies via a drop-down menu one of the following valid privacy protocols:<br>● NONE<br>● DES<br>When DES is selected, an entry field will appear for the password. |

 Copyright @ 2017 Pepwave

## 25.8 InControl




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.

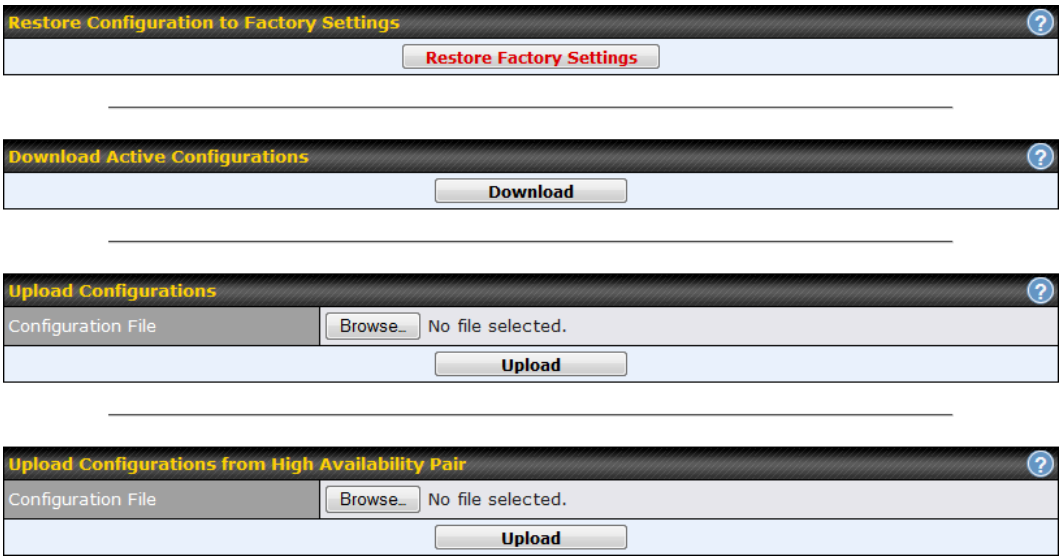
Alternately, you could also privately host InControl. Simply check the box beside the “Privately Host InControl” open, and enter the IP Address of your InControl Host.

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.

## 25.9 Configuration

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.

 Copyright @ 2017 Pepwave




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

 Copyright @ 2017 Pepwave

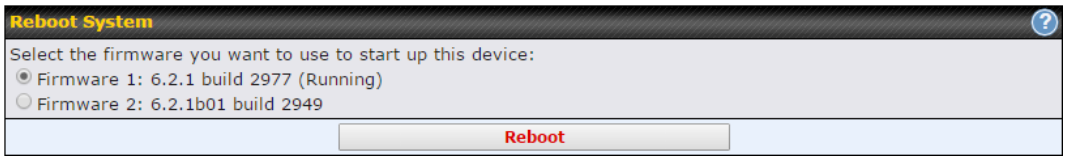
## 25.10 Feature Add-ons

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**.

## 25.11 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.**

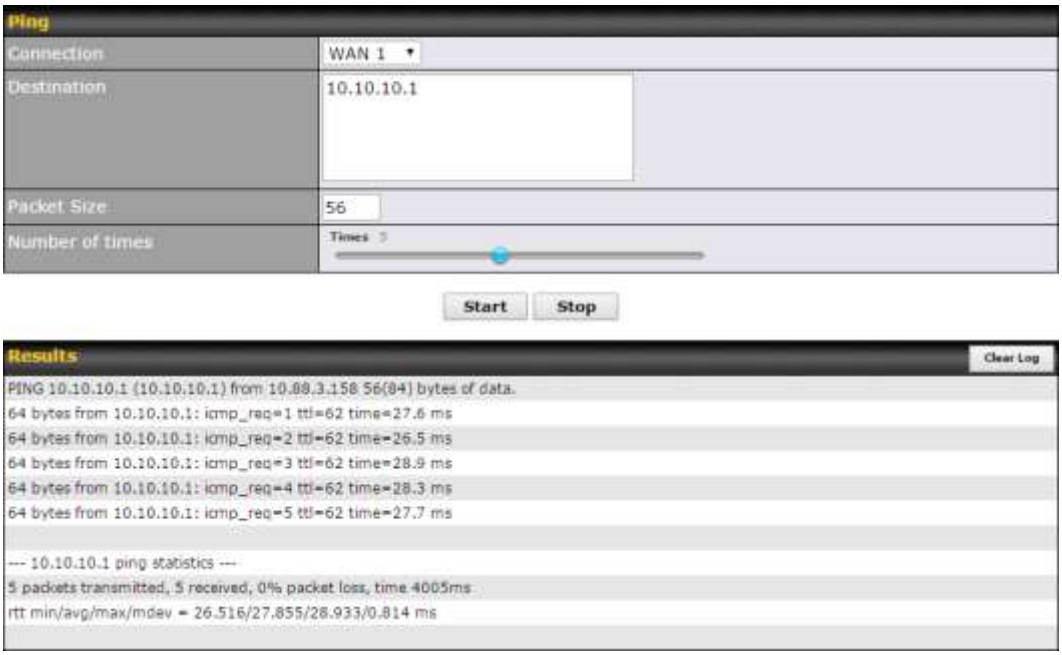



# 26 Tools

## 26.1 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:

 Copyright @ 2017 Pepwave

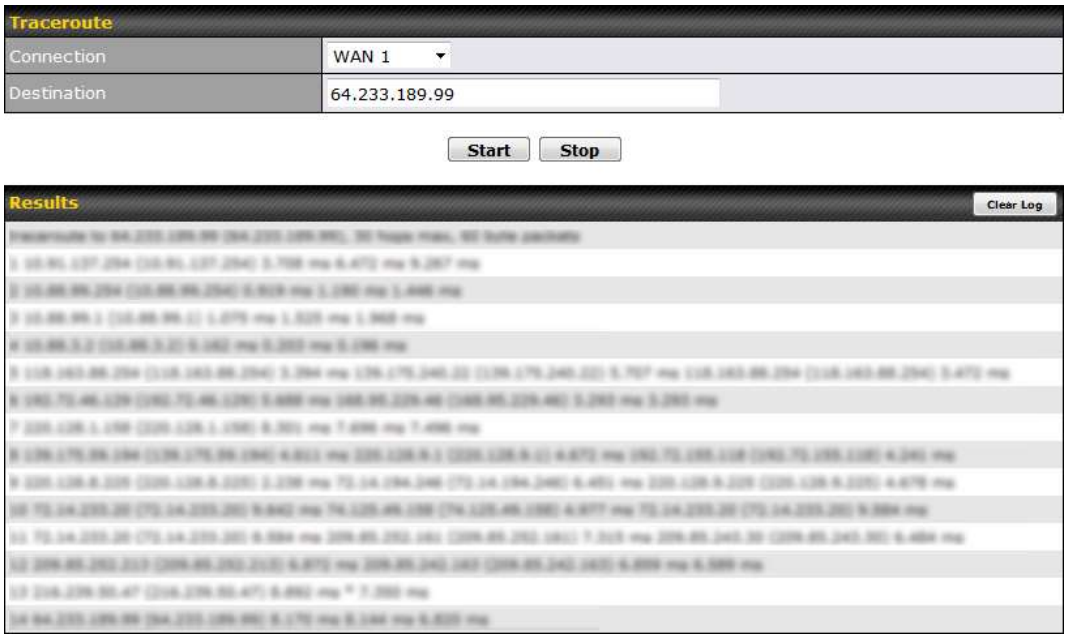



| Tip |
| --- |
| A system administrator can use the ping utility to manually check the connectivity of a particular LAN/WAN connection. |

## 26.2 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**.

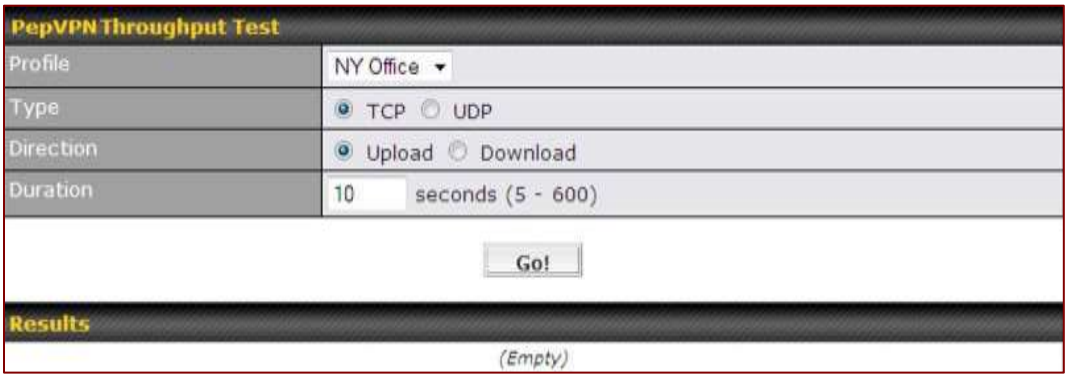
 Copyright @ 2017 Pepwave




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

## 26.3 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:



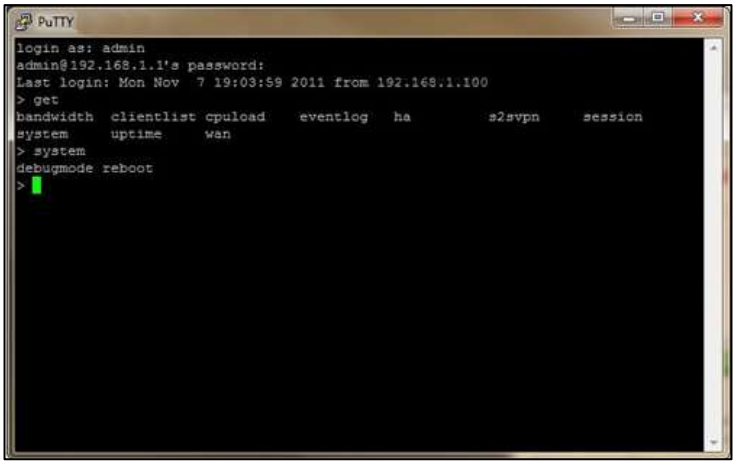
## 26.4 Wake-on-LAN

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”

## 26.5 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.




 Copyright @ 2017 Pepwave

# 27 Status

## 27.1 Device

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

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

| System Information | |
|---|---|
| **Router Name** | This is the name specified in the **Router Name** field located at **System>Admin Security**. |
| **Model** | This shows the model name and number of this device. |
| **Product Code** | If your model uses a product code, it will appear here. |
| **Hardware Revision** | This shows the hardware version of this device. |
| **Serial Number** | This shows the serial number of this device. |
| **Firmware** | This shows the firmware version this device is currently running. |
| **PepVPN Version** | This shows the current PepVPN version. |
| **Modem Support Version** | This shows the modem support version. For a list of supported modems, click **Modem Support List**. |
| **Host Name** | The host name assigned to the Pepwave router appears here. |

 Copyright @ 2017 Pepwave

| | |
|---|---|
| **Uptime** | This shows the length of time since the device has been rebooted. |
| **System Time** | This shows the current system time. |
| **Diagnostic Report** | The **Download** 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.<br>In Firmware 5.1 or before, the diagnostic report file can be obtained at **System>Reboot.** |

## 27.2 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.

## 27.3 Active Sessions

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

 Copyright @ 2017 Pepwave

Overview | Search

Session data captured within one minute. Refresh

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

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

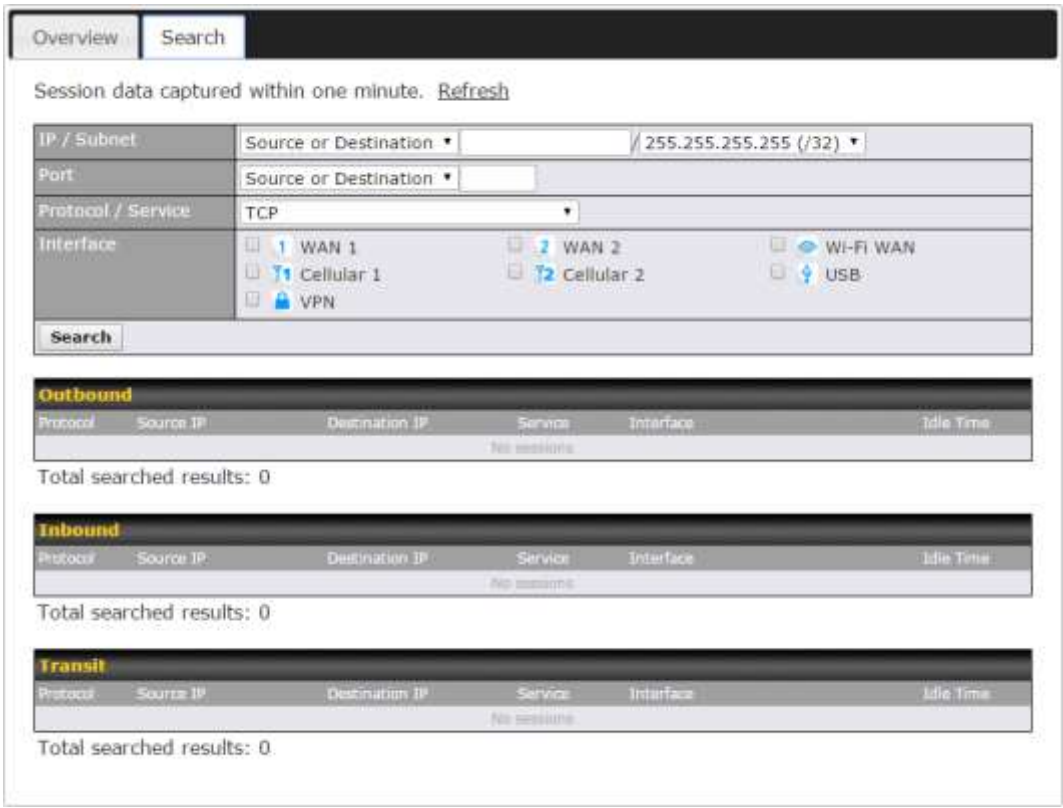
**Top Clients**

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

This screen displays the number of sessions initiated by each application. Click on each service 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.

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**.

 Copyright @ 2017 Pepwave



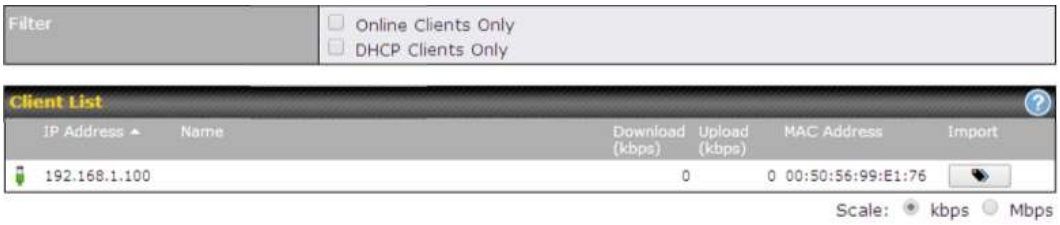

This **Active Sessions** section displays the active inbound/outbound sessions of each WAN connection on the Pepwave router. A filter is available to sort active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering.

## 27.4 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**.

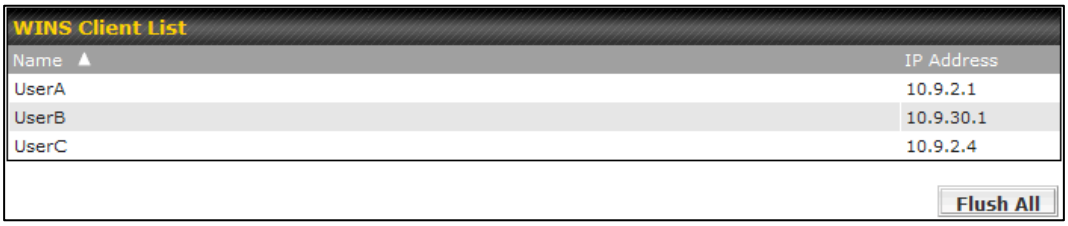
 Copyright @ 2017 Pepwave



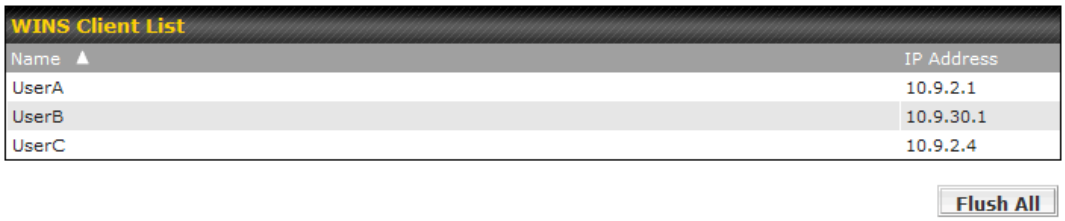

If the PPTP server (see **Section 19.2),** SpeedFusion™ (see **Section 12.1**), or AP controller (see **Section 20**) is enabled, you may see the corresponding connection name listed in the **Name** field.

## 27.5 WINS Client

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



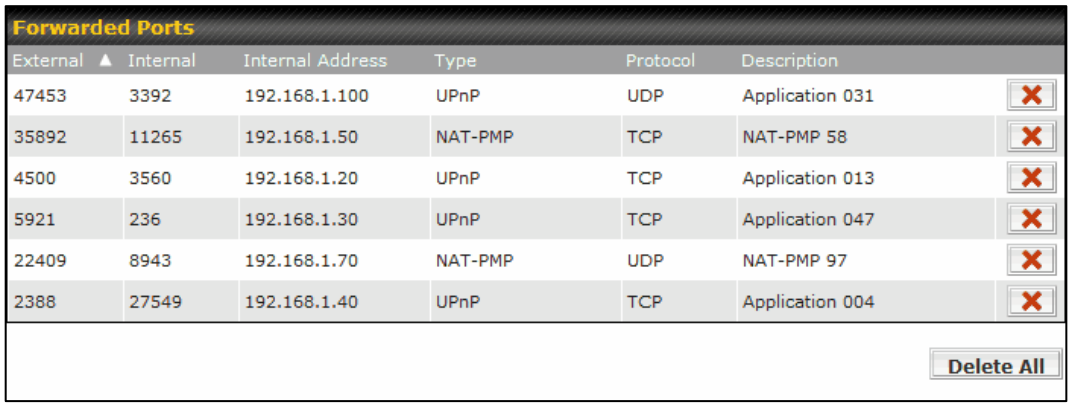

The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server (navigation: **Network>Interfaces>LAN**). The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush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




## 27.6 UPnP / NAT-PMP

The table that shows the forwarded ports under UPnP and NAT-PMP protocols is located at **Status>UPnP/NAT-PMP**. This section appears only if you have enabled UPnP / NAT-PMP as mentioned in **Section 16.1.1**.

 Copyright @ 2017 Pepwave



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 |

Delete All

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**.

## 27.7 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  Show disconnected profiles

Search

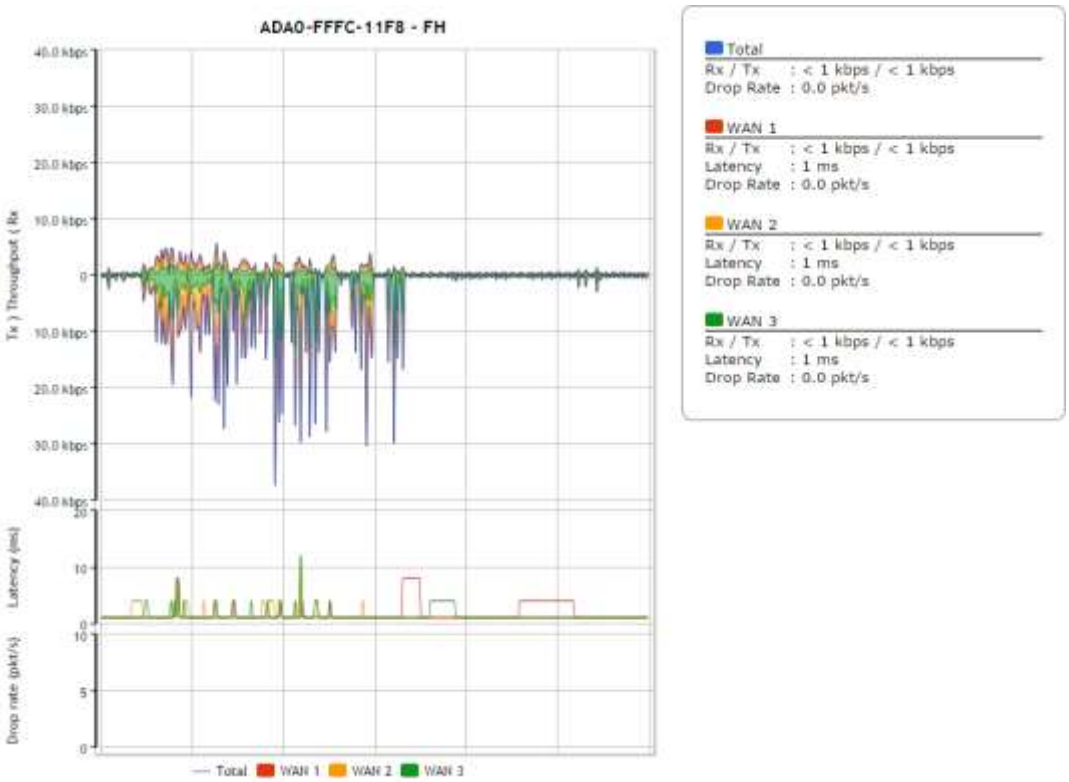
| Remote Peer | Profile | Information |
|---|---|---|
| FFFC-FFFC-FFFC | FH | 192.168.77.0/24 |
| 3ED2-3ED2-3ED2 | 380-5 - NO NAT | 192.168.3.0/24 |

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

 Copyright @ 2017 Pepwave

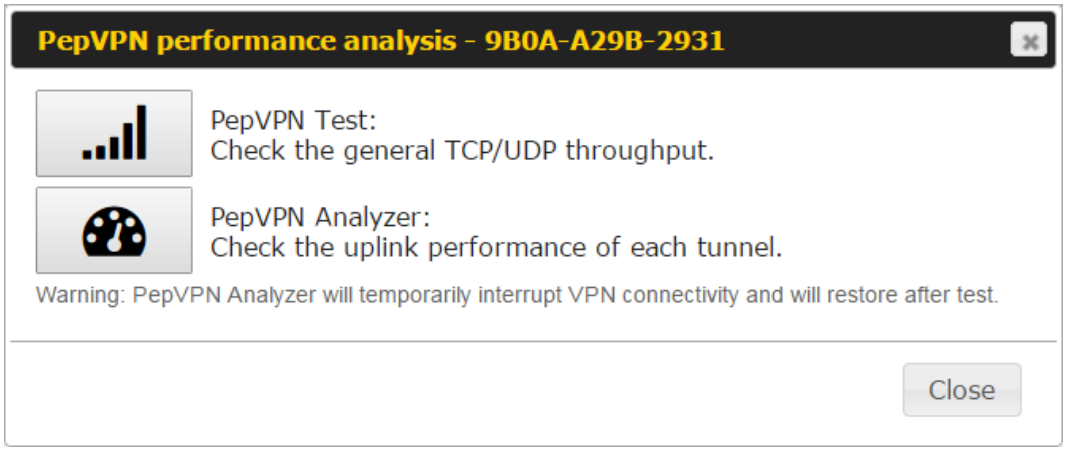
| Remote Peer | Profile | | | Information | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| FFFC-FFFC-FFFC | FH | | | 192.168.77.0/24 | | | | | |
| WAN 1 | Rx: | < 1 kbps | Tx: | < 1 kbps | Drop rate: | 0.0 pkt/s | Latency: | 1 ms | |
| WAN 2 | Rx: | < 1 kbps | Tx: | < 1 kbps | Drop rate: | 0.0 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 | | | |
| 3ED2-3ED2-3ED2 | 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 | | | |

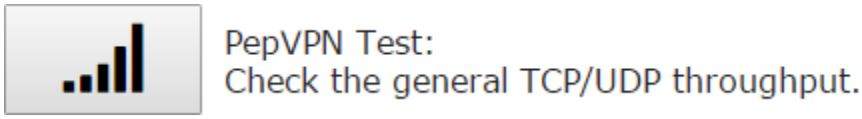
Click the button for a chart displaying real-time throughput, latency, and drop-rate information for each WAN connection.



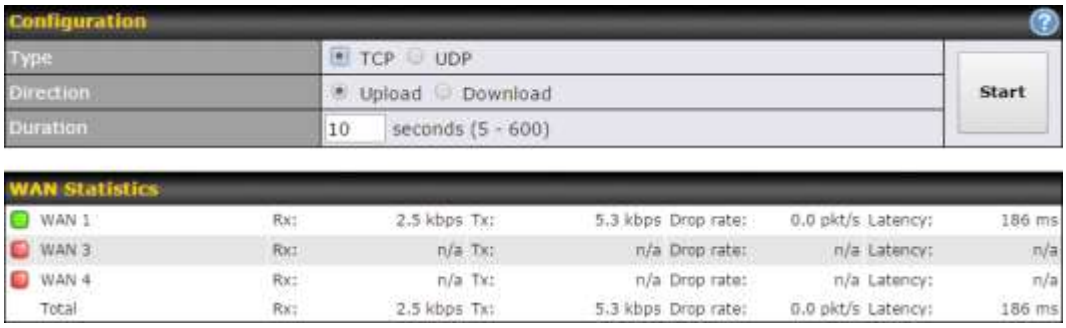

When pressing the button, the following menu will appear:

 Copyright @ 2017 Pepwave




After clicking the icon, the following menu appears:




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

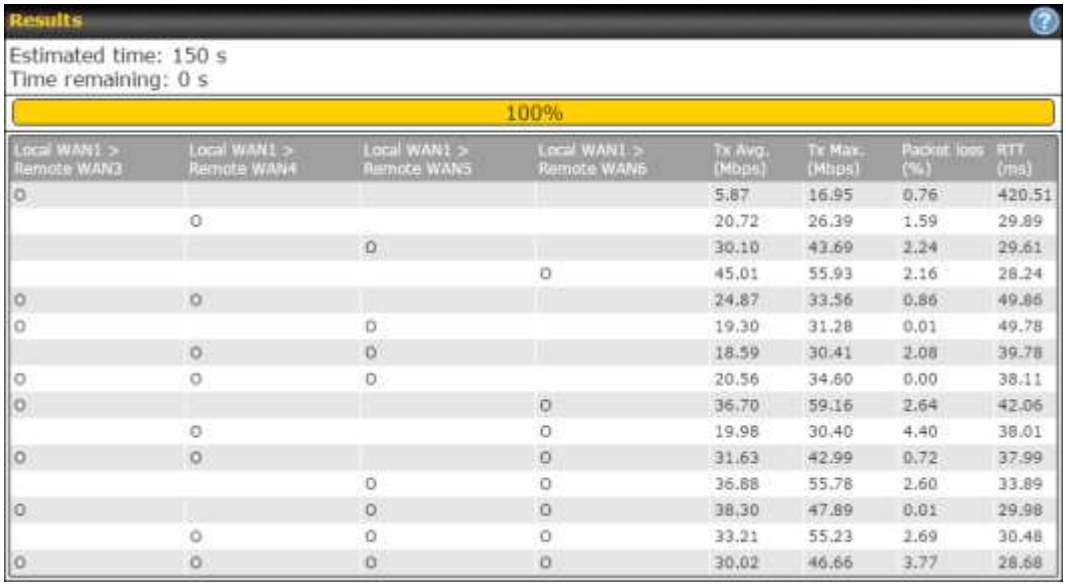
 Copyright @ 2017 Pepwave

## 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:

 Copyright @ 2017 Pepwave



Results

Estimated time: 150 s
Time remaining: 0 s

100%

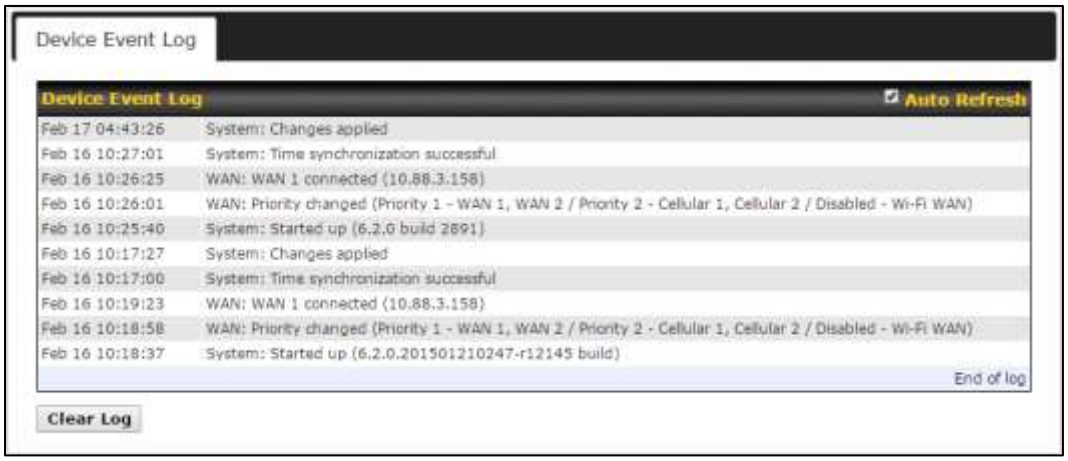
| Local WAN1 > Remote WAN3 | Local WAN1 > Remote WAN4 | Local WAN1 > Remote WAN5 | Local WAN1 > Remote WAN6 | Tx Avg. (Mbps) | Tx Max. (Mbps) | Packet loss (%) | RTT (ms) |
|---|---|---|---|---|---|---|---|
| O | | | | 5.87 | 16.95 | 0.76 | 420.51 |
| | O | | | 20.72 | 26.39 | 1.59 | 29.89 |
| | | O | | 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.

## 27.8 Event Log

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



Device Event Log

Device Event Log — Auto Refresh

| | |
|---|---|
| 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) |

End of log

Clear Log

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.

 Copyright @ 2017 Pepwave

# 28 Bandwidth Status

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.

## 28.1 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.

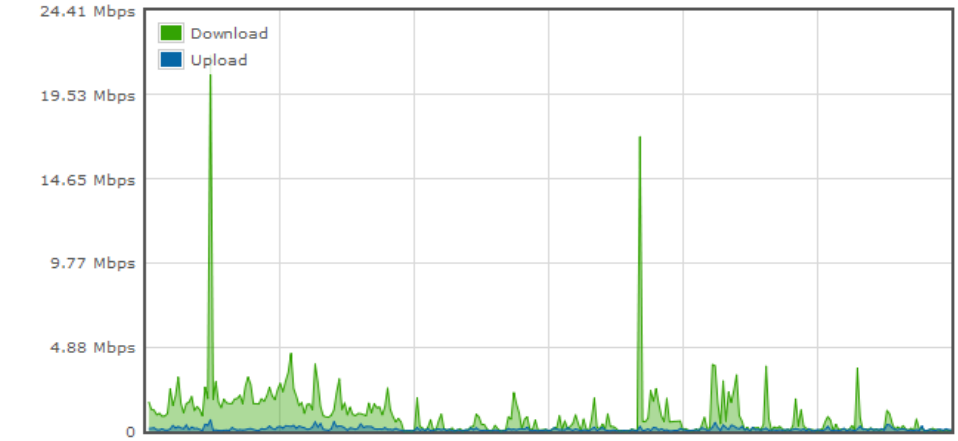
Data transferred since installation (Sun Oct 10 05:56:02 PST 2010)

| | 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




Avg: 0.99 Mbps 0.12 Mbps Peak: 21.78 Mbps 0.67 Mbps Stacked

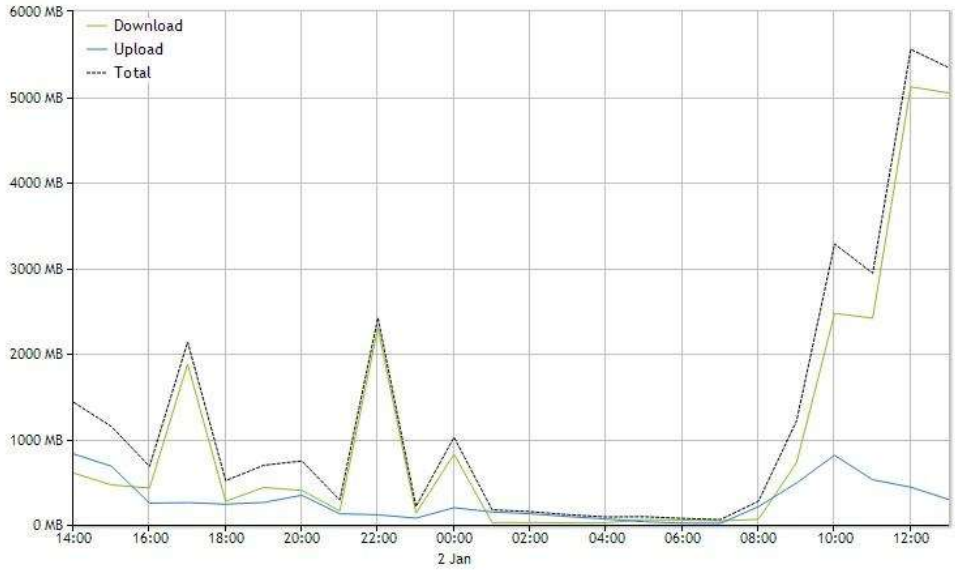
| | Download | Upload | Total |
|---|---|---|---|
| Overall | 61 kbps | 75 kbps | 136 kbps |

 Copyright @ 2017 Pepwave

## 28.2 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.

| Hourly Usage | |
|---|---|
| Connection | All WAN |
| Scale | MB GB |




| Date | Download | Upload | Total |
|---|---|---|---|
| 13:00 | 5 047 MB | 295 MB | 5 342 MB |
| 12:00 | 5 117 MB | 439 MB | 5 556 MB |
| 11:00 | 2 414 MB | 526 MB | 2 940 MB |
| 10:00 | 2 470 MB | 812 MB | 3 282 MB |
| 09:00 | 725 MB | 488 MB | 1 213 MB |
| 08:00 | 64 MB | 211 MB | 275 MB |

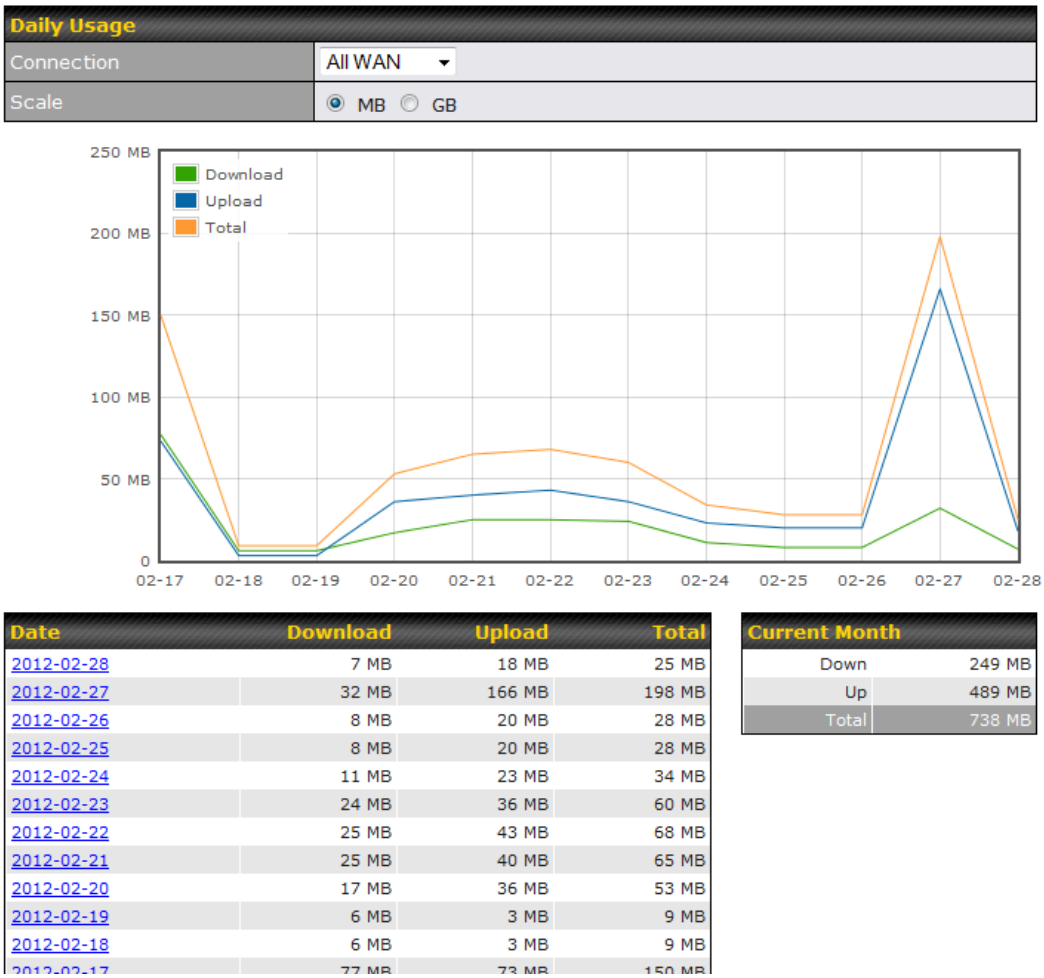
 Copyright @ 2017 Pepwave

## 28.3 Daily

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**).



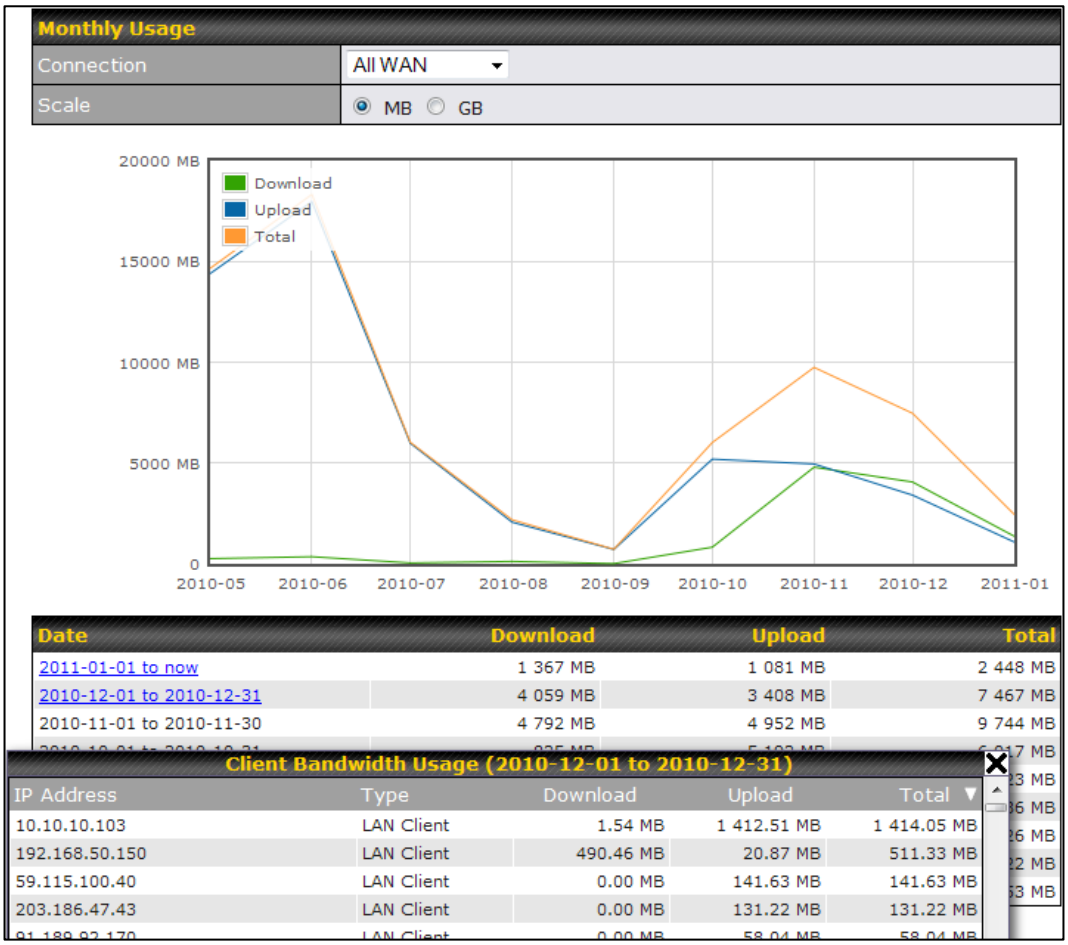

All WAN Daily Bandwidth Usage

 Copyright @ 2017 Pepwave

## 28.4 Monthly

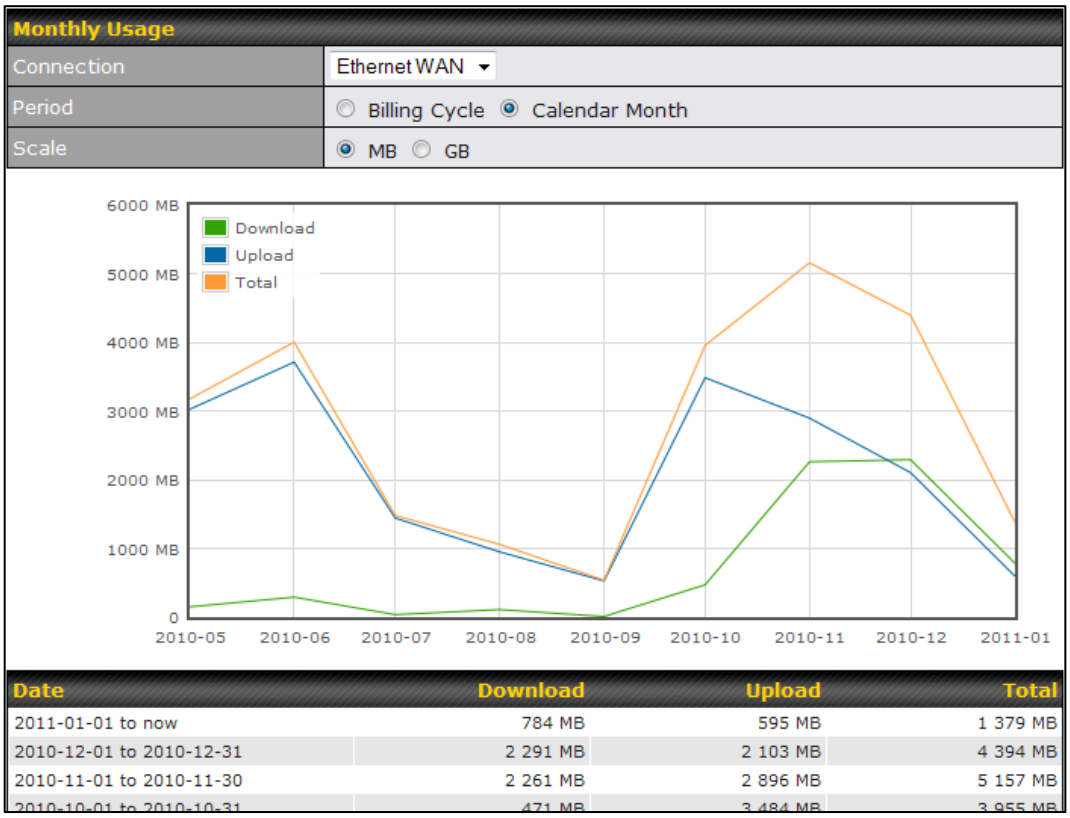
This page shows the monthly bandwidth usage for each WAN connection. If you have enabled the **Bandwidth Monitoring** feature, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

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

 Copyright @ 2017 Pepwave




Ethernet WAN Monthly Bandwidth Usage

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

 Copyright @ 2017 Pepwave

# 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. |

 Copyright @ 2017 Pepwave

# Appendix B: Declaration

1. **The device supports time division technology**

2. **Federal Communication Commission Interference Statement**

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

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

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help. FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

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

 Copyright @ 2017 Pepwave

# IMPORTANT NOTE

FCC Radiation Exposure Statement (for MAX BR1 MK2)
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm 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 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 25cm 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/ Surf SOHO)
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

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

1. 20cm minimum when the product is operated alone without co-transmitting with a plug-in 3G USB dongle device.

2. 65cm minimum when the product is operated with a plug-in 3G USB device which has maximum of 7W ERP output power.
3. For co-transmission scenario which is not covered above, please consult the RF technician or device supplier.

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

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.

 Copyright @ 2017 Pepwave

**3. Industry Canada Statement (for MAX BR1 MK2)**

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

**To maintain compliance with the RF exposure guidelines, place the unit at least 30cm from nearby persons.**

Mise en garde_: Pour assurer la conformité aux directives relatives à l'exposition aux fréquences radio, le jouet doit êtreplacé à au moins 30_cm des personnes à proximité.

**Caution:**

(i) The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel Mobile Satellite systems;

(ii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p limits specified for point-to-point and non-point-to-point operation as appropriate; and

(iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

**Avertissement:**

(i) Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

(ii) Le gain maximal d'antenne permis (pour les dispositifs utilisant les bandes 5250 à 5850) doit se conformer à la limite de p.i.r.e. Le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5825 MHz) doit être conforme à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;

(iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

 Copyright @ 2017 Pepwave

**Industry Canada Statement (for MAX Hotspot/ Surf SOHO/ MAX HD2 / MAX BR1 mini)**

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

***Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.***

To maintain compliance with the RF exposure guidelines, place the unit at least 20cm from nearby persons.

***Mise en garde_: Pour assurer la conformité aux directives relatives à l'exposition aux fréquences radio, le jouet doit êtreplacé à au moins 20_cm des personnes à proximité.***

**Caution :**

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
(ii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
(iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

**Avertissement:**

***(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;***
***(ii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;***
***(iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.***
***Radiation Exposure Statement: (For MAX BR1 Mini)***
***This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25cm between the radiator & your body.***

***Déclaration d'exposition aux radiations:***
***Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 25 cm de distance entre la source de rayonnement et votre corps.***

 Copyright @ 2017 Pepwave

## 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:

This device complies with the essential requirements of the Radio Equipment Directive 2014/53/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the RE Directive 2014/53/EU:

- EN 60950-1: 2006 + A11: 2009+A1: 2010+ A12: 2011+A12: 2013
  Safety of Information Technology Equipment
- EN50385 : 2002
  Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
  EN 300 328 V1.7.1: 2006
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 908-1 V5.2.1: 2011
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third-Generation cellular networks; Part 1: Harmonized EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive
- EN 301 511 V9.0.2: 2003
  Global System for Mobile communications (GSM); Harmonized standard for mobile stations in the GSM 900 and DCS 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC)
- EN 301 489-1 V1.9.2: 2008
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-7 V1.3.1: 2005
  ElectroMagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment ad services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
- EN 301 489-17 V2.2.1: 2012
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment
- EN 301 489-24 V1.5.1: 2010
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA) for Mobile and portable (UE) radio and ancillary equipment

**Recycling** - Our product bears this selective sorting symbol for Waste Electrical and Electronic Equipment (**WEEE**) Directive 2012/19/EU. This means this product must be handled according to this Directive. Old electrical appliance **must not be disposed of together with the residual waste**, but have to be disposed of separately. The disposal at the communal collecting point via private persons is for free. The owner of old appliances is responsible to bring the appliances to these collecting points.

 Copyright @ 2017 Pepwave

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

 Copyright @ 2017 Pepwave

## 4. NCC for Pepwave Routers

For MAX Transit, MAX BR1 MK2, MAX BR1 MK2 LTE

**WLAN**

[警語]

「電磁波曝露量 MPE 標準值 1mW/cm2，本產品使用時建議應距離人體 24 cm」

電磁波

「**減少電磁波影響，請妥適使用**」。

[警語內容]

(1) 電磁波警語標示：「減少電磁波影響，請妥適使用」。 標示方式：必須標示於設備本體適當位置及設備外包裝及使用說明書上。

**低功率電波輻射性電機管理辦法**

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本行動寬頻設備的行動寬頻頻段(LTE900/LTE1800)

警告使用者:

此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

 Copyright @ 2017 Pepwave

## 5. Compliance (For MAX BR1 mini & MAX BR1 & BR1 MK2)

Please observe the following instructions:

5.1 Ex marking:

CLASS I, DIVISION 2, GROUP C AND D

5.2 Warning：

5.2.2 The Antenna shall not be disconnected while the power is connected.
5.2.3 The front panel presents an electrostatic hazard. Clean only by using a damp cloth.
5.3.3 Provision shall be made to prevent the rated voltage being exceeded by the transient disturbances of more than 140% of the peak rated voltage.
5.3.4 Explosion Hazard. Do not connect or disconnect when energized.

5.2 Mise en garde：

5.2.2 L'antenne ne doit pas être déconnectée quand le matériel est toujours sous tension
5.2.3 Le panneau avant présente un risque électrostatique. Utiliser un chiffon humide.
5.3.3 Des dispositions doivent être mises en place contre les perturbations passagères entrainant un dépassement de la tension assignée de plus de 140% du pic pouvant être atteint.
5.3.4 Risque d'explosion. Ne connectez ou ne déconnectez pas le produit quand celle-ci est sous tension.

5.3 Temperature class

Temperature class is T4.

 Copyright @ 2017 Pepwave

## 5. Compliance (Important Information and Safety Compliance for MAX HD4 / MAX HD4 LTE / MAX HD4 LTEA / Pismo 803AC)

Please observe the following instructions:

5.1 User should pay attention to use manufacturer supplied power adapter:

ADAPTER TECH.

AC ADAPTER

INPUT: 100-240V~ 50-60Hz, 1.2A MAX,

OUTPUT: 12V 4.2A LPS

FOR INDOOR USE ONLY

5.2 USB port output rating：5VDC, 2A

5.3 Temperature suitable for use: ambient temp. Maximum 40 °C.

 Copyright @ 2017 Pepwave

# Additional information

Module information:

LTEA module: MC7455 (FCC ID: N7NMC7455) or

LTE module: MC7354 (FCC ID: N7NMC7355)

Operating frequency for the Pepwave MAX Mobile Router:

| Model: | Operating frequency: |
|---|---|
| 4.1 MAX 700 | 2.4GHz + 5GHz |
| 4.2 MAX HD2 | 2.4GHz + 5GHz |
| 4.3 MAX HD2 IP67 | 3G/4G cellular network, no Wi-Fi for MAX HD2 IP67 (Contains FCC ID: MC7455 / Contains FCC ID: MC7354) / 698-960MHz, 1710-2170MHz, 2500-2700MHz (Cellular Antenna) |
| 4.4 MAX HD2 Mini | 3G/4G cellular network, no Wi-Fi for MAX HD2 mini (Contains FCC ID: MC7455 / Contains FCC ID: MC7354 ) / 698-960MHz, 1710-2170MHz, 2500-2700MHz (Cellular Antenna) |
| 4.5 MAX Transit | 2.4GHz + 5GHz |
| 4.6 MAX CX4 | No Wi-Fi for CX4, 2.4GHz + 5GHz for MAX Transit Quad (U8G-P1817) still in testing stage, not certified |
| 4.7 MAX HD4/ HD2 and HD4 with MediaFast | 2.4GHz + 5GHz |
| 4.8 MAX BR1 | 2.4GHz only |
| 4.9 MAX BR1 MK2 | 2.4GHz + 5GHz |
| 4.10 MAX BR1 Slim | 3G/4G cellular network, no Wi-Fi for MAX BR1 Slim (Contains FCC ID: MC7455 / Contains FCC ID: MC7354) / 698-960MHz, 1710-2170MHz, 2500-2700MHz (Cellular Antenna) |
| 4.11 MAX BR1 ENT | 3G/4G cellular network, no Wi-Fi for MAX BR1 ENT (Contains FCC ID: MC7455 / Contains FCC ID: MC7354) / 698-960MHz, 1710-2170MHz, 2500-2700MHz (Cellular Antenna) |
| 4.12 MAX BR1 Pro LTE | 2.4GHz only |
| 4.13 MAX Hotspot | 2.4GHz + 5GHz |
| 4.14 BR1 Mini | 2.4GHz only |
| 4.15 MAX BR1/2 IP55 | 2.4GHz only |

| | |
|---|---|
| 4.16 MAX BR1 IP67 | 2.4GHz only |
| 4.17 MAX On-The Go | 2.4GHz + 5GHz |
| 4.18 NPC (Network Power Controller) | no wireless function for existing version of NPC |
| 4.19 SD-PMU | no wireless function for existing version of SD-PMU |

Remark: FCC ID of Item 4.16 MAX BR1 IP67 is U8G-P193067