



Pepwave MAX User Manual

Pepwave Products:

MAX BR2 Pro / BR2 Pro / MAX BR2 Pro LTE / MAX BR2 Pro LTEA / MAX -CX2-Mini / MAX CX2 Mini / CX2 Mini / MAX-BR2-PRO-LTE-E-T / MAX-BR2-PRO-LTE-US-T / MAX-BR2-PRO-LTEA-W-T / UBR LTE / UBR-LTE-US-T-PRM / MAX UBR LTE / MAX UBR / MAX UBR LTEA / UBR / Pismo941 / UBR-LTE / UBR-LTE-US-T / UBR-LTEA-W-T / UBR-LTEA-W-T-PRM / MAX BR1 Pro / MAX BR1 Pro LTE / MAX BR1 Pro LTEA / MAX-BR1-PRO-LTEA-W-T / MAX-BR1-LTE-US-T / UBR-LTE-EJ-T-PRM

Pepwave Firmware 8.0.0
August 2019

Copyright & Trademarks

Specifications are subject to change without notice. Copyright © 2019 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

| | |
|---|------------|
| Introduction and Scope | 7 |
| Glossary | 8 |
| Product Features | 9 |
| Supported Network Features | 9 |
| WAN | 9 |
| LAN | 10 |
| VPN | 10 |
| Firewall | 10 |
| Captive Portal | 10 |
| Outbound Policy | 10 |
| AP Controller | 11 |
| QoS | 11 |
| Other Supported Features | 11 |
| Pepwave MAX Mobile Router Overview | 134 |
| MAX BR2 Pro | 13 |
| Advanced Feature Summary | 16 |
| Drop-in Mode and LAN Bypass: Transparent Deployment | 16 |
| QoS: Clearer VoIP | 16 |
| Per-User Bandwidth Control | 17 |
| High Availability via VRRP | 17 |
| USB Modem and Android Tethering | 18 |
| Built-In Remote User VPN Support | 18 |
| SIM-card USSD support | 19 |
| Installation | 20 |
| Preparation | 20 |
| Constructing the Network | 20 |
| Configuring the Network Environment | 21 |
| Mounting the Unit | 21 |
| Wall Mount | 21 |
| Car Mount | 22 |
| IP67 Installation Guide | 22 |
| Connecting to the Web Admin Interface | 22 |
| Configuring the LAN Interface(s) | 24 |

| | |
|--|-----------|
| Basic Settings | 24 |
| Port Settings | 33 |
| Captive Portal | 34 |
| Configuring the WAN Interface(s) | 36 |
| Ethernet WAN | 37 |
| DHCP Connection | 40 |
| Static IP Connection | 440 |
| PPPoE Connection | 41 |
| L2TP Connection | 43 |
| Cellular WAN | 44 |
| Wi-Fi WAN | 549 |
| Creating Wi-Fi Connection Profiles | 57 |
| WAN Health Check | 58 |
| Dynamic DNS Settings | 60 |
| Advanced Wi-Fi Settings | 62 |
| ContentHub Configuration | 67 |
| ContentHub | 67 |
| Configuring the ContentHub | 67 |
| Configure a website to be published from the ContentHub | 68 |
| Configure an application to be published from the ContentHub | 69 |
| MediaFast Configuration | 71 |
| Setting Up MediaFast Content Caching | 72 |
| Scheduling Content Prefetching | 73 |
| Viewing MediaFast Statistics | 76 |
| Bandwidth Bonding SpeedFusion™ / PepVPN | 77 |
| PepVPN | 77 |
| The Pepwave Router Behind a NAT Router | 83 |
| SpeedFusion™ Status | 84 |
| IPsec VPN | 85 |
| IPsec VPN Settings | 85 |
| Outbound Policy Management | 89 |
| Outbound Policy | 89 |
| Custom Rules for Outbound Policy | 91 |
| Algorithm: Weighted Balance | 91 |
| Algorithm: Persistence | 92 |
| Algorithm: Enforced | 94 |

| | |
|--|--------------|
| Algorithm: Priority | 94 |
| Algorithm: Overflow | 94 |
| Algorithm: Least Used | 95 |
| Algorithm: Lowest Latency | 95 |
| Expert Mode | 96 |
| Inbound Access | 96 |
| Port Forwarding Service | 96 |
| UPnP / NAT-PMP Settings | 99 |
| NAT Mappings | 99 |
| QoS | 101 |
| User Groups | 10001 |
| Bandwidth Control | 10102 |
| Application | 10102 |
| Application Prioritization | 10102 |
| Prioritization for Custom Applications | 10103 |
| DSL/Cable Optimization | 10203 |
| Firewall | 10204 |
| Outbound and Inbound Firewall Rules | 10305 |
| Access Rules | 10305 |
| Apply Firewall Rules to PepVpn Traffic | 10608 |
| Intrusion Detection and DoS Prevention | 10608 |
| Content Blocking | 10709 |
| Application Blocking | 10709 |
| Web Blocking | 10709 |
| Customized Domains | 10810 |
| Exempted User Groups | 10810 |
| Exempted Subnets | 10810 |
| URL Logging | 10810 |
| OSPF & RIPv2 | 10810 |
| BGP | 11214 |
| Remote User Access | 11416 |
| L2TP with IPsec | 11517 |
| OpenVPN | 11517 |
| PPTP | 11618 |
| Authentication Methods | 11618 |
| Miscellaneous Settings | 11820 |

| | |
|---|--------------|
| High Availability | 11820 |
| Certificate Manager | 12123 |
| Service Forwarding | 12224 |
| SMTP Forwarding | 125 |
| Web Proxy Forwarding | 12326 |
| DNS Forwarding | 12426 |
| Custom Service Forwarding | 12426 |
| Service Passthrough | 12426 |
| UART | 12629 |
| GPS Forwarding | 12831 |
| Ignition Sensing | 12832 |
| Ignition Sensing installation | 12932 |
| GPIO Menu | 13134 |
| Grouped Networks | 13235 |
| SIM Toolkit | 13235 |
| AP - access point | 13538 |
| AP Controller | 13538 |
| Wireless SSID | 13538 |
| Settings | 13942 |
| AP Controller Status | 14447 |
| Info | 14447 |
| Access Point (Usage) | 146 |
| Wireless SSID | 14851 |
| Wireless Client | 14952 |
| Nearby Device | 15053 |
| Event Log | 15154 |
| Toolbox | 15255 |
| System Settings | 15356 |
| Admin Security | 15356 |
| Firmware | 15660 |
| Web admin interface : automatically check for updates | 15660 |
| Web admin interface : install updates manually | 15761 |
| The InControl method | 15862 |
| Time | 15962 |
| Schedule | 15963 |
| Email Notification | 16064 |
| Event Log | 166 |

| | |
|--------------------------------------|------------|
| SNMP | 166 |
| InControl | 168 |
| Configuration | 169 |
| Feature Add-ons | 170 |
| Reboot | 170 |
| Tools | 171 |
| Ping | 171 |
| Traceroute Test | 171 |
| PepVPN Test | 172 |
| Wake-on-LAN | 172 |
| CLI (Command Line Interface Support) | 173 |
| Status | 174 |
| Device | 174 |
| GPS Data | 175 |
| Active Sessions | 176 |
| Client List | 177 |
| WINS Client | 178 |
| UPnP / NAT-PMP | 178 |
| OSPF & RIPv2 | 179 |
| BGP | 179 |
| SpeedFusion Status | 180 |
| Event Log | 182 |
| WAN Quality | 184 |
| Usage Reports | 184 |
| Real-Time | 185 |
| 182 | 186 |
| Daily | 187 |
| Monthly | 188 |
| Appendix B: Declaration | 191 |

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!



<https://youtu.be/13M-JHRAICA>

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 |

2 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.

2.1 Supported Network Features

2.1.1 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

2.1.2 LAN

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

2.1.3 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

2.1.4 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

2.1.5 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

2.1.6 Outbound Policy

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

service

- Traffic prioritization and DSL optimization
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms

2.1.7 AP Controller

- Configure and manage Pepwave AP devices
- Review the status of connected APs

2.1.8 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

2.2 Other Supported Features

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

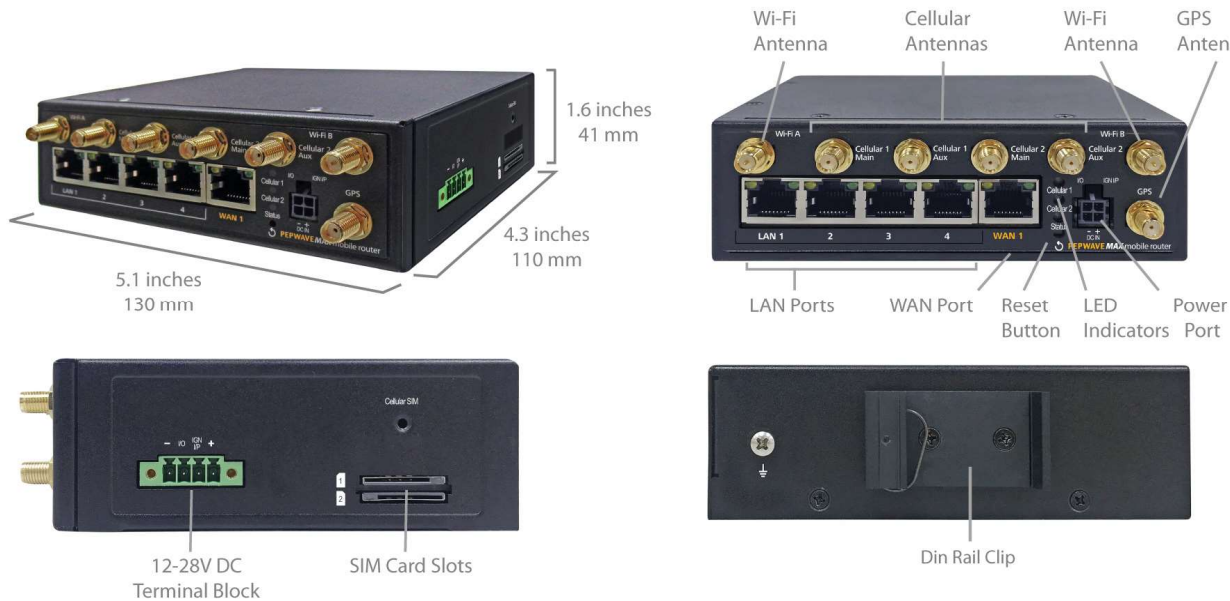
- IPv6 support
- Support USB tethering on Android 2.2+ phones

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

3 Pepwave MAX Mobile Router Overview

3.1 BR2 Pro

3.1.1 Panel Appearance



3.1.2 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 |
| | 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 | |

4 Advanced Feature Summary

4.1 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.

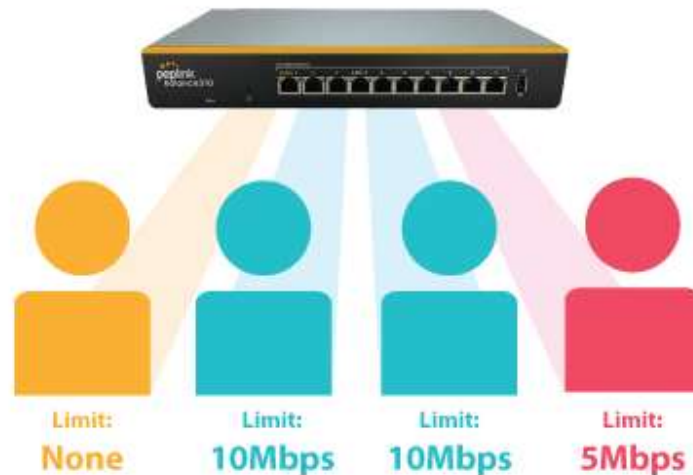
Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

4.2 QoS: Clearer VoIP



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

4.3 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.

4.4 High Availability via VRRP



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

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

4.5 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)

4.6 Built-In Remote User VPN Support

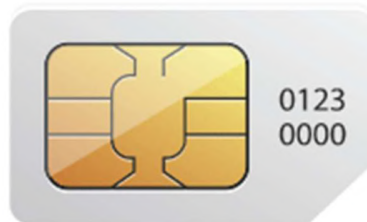


Use OpenVPN or L2TP with IPsec to safely and conveniently connect remote clients to your private network. L2TP with IPsec is supported by most devices, but legacy devices can also connect using PPTP.

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

[Click here for the full instructions on setting up OpenVPN connections](#)

4.7 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.](#)

5 Installation

The following section details connecting Pepwave routers to your network.

5.1 Preparation

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

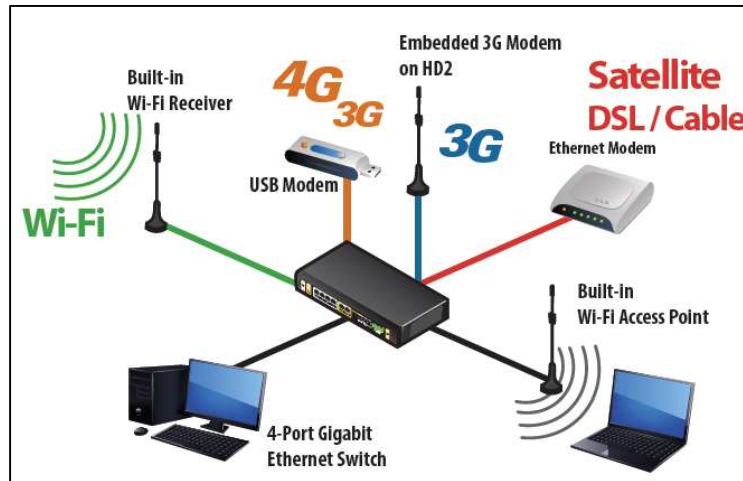
- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
 - **Ethernet WAN:** A 10/100/1000BaseT UTP cable with RJ45 connector
 - **USB:** A USB modem
 - **Embedded modem:** A SIM card for GSM/HSPA service
 - **Wi-Fi 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 11 or above, Mozilla Firefox 24 or above, Apple Safari 7 or above, and Google Chrome 18 or above.

5.2 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:



5.3 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.**

6 Mounting the Unit

6.1 Wall Mount

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

The Pepwave MAX BR1 requires four screws for wall mounting.

6.2 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.



6.3 IP67 Installation Guide

Installation instructions for IP67 devices can be found here:

http://download.peplink.com/manual/IP67_Installation_Guide.pdf

7 Connecting to the Web Admin Interface

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

`http://192.168.50.1`

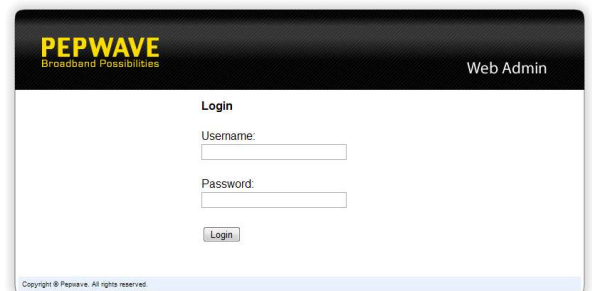
(This is the default LAN IP address for Pepwave routers.)

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

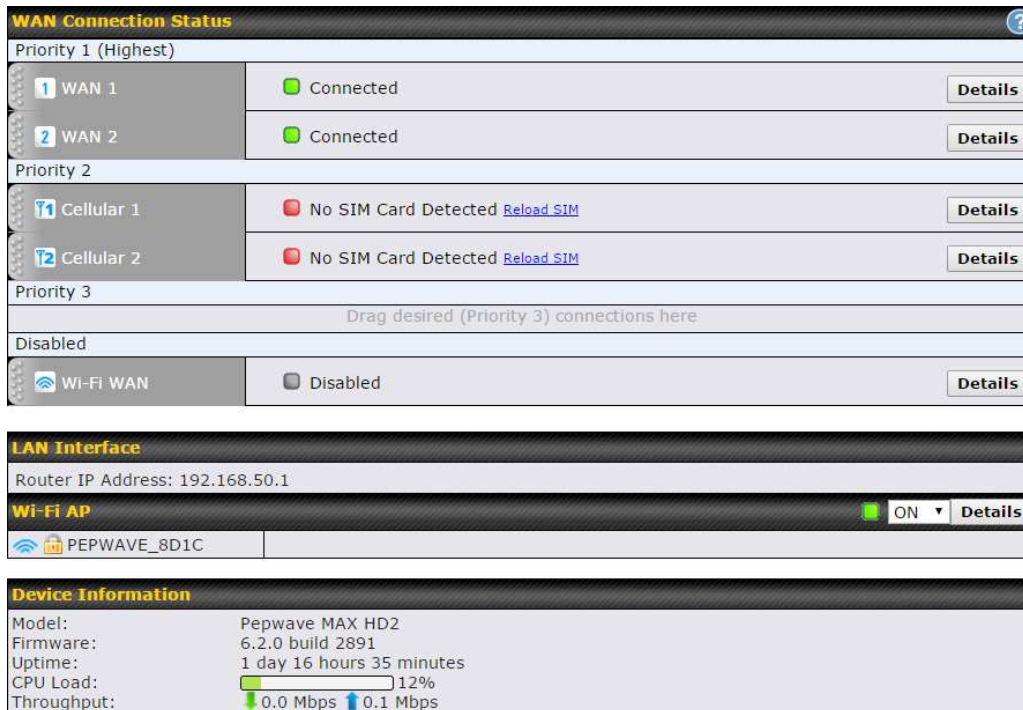
Username: admin

Password: admin

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



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



WAN Connection Status

Priority 1 (Highest)

| | | |
|---------|-----------|---------|
| 1 WAN 1 | Connected | Details |
| 2 WAN 2 | Connected | Details |

Priority 2

| | | |
|------------|---|---------|
| Cellular 1 | No SIM Card Detected Reload SIM | Details |
| Cellular 2 | No SIM Card Detected Reload SIM | Details |

Priority 3

Drag desired (Priority 3) connections here

Disabled

| | | |
|-----------|----------|---------|
| Wi-Fi WAN | Disabled | Details |
|-----------|----------|---------|

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP ON Details

PEPWAVE_8D1C

Device Information

| | |
|-------------|---|
| Model: | Pepwave MAX HD2 |
| Firmware: | 6.2.0 build 2891 |
| Uptime: | 1 day 16 hours 35 minutes |
| CPU Load: | <div style="width: 12%; background-color: green; border: 1px solid black;"></div> 12% |
| Throughput: | ↓ 0.0 Mbps ↑ 0.1 Mbps |

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

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

Important Note

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

8 Configuring the LAN Interface(s)

8.1 Basic Settings

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

| LAN | VLAN | Network | |
|-----------------------|------|-----------------|----------------------------------|
| LAN | None | 172.16.251.1/24 | |
| VLAN1 | 1 | 2.2.2.2/24 | <input type="button" value="X"/> |
| VLAN2 | 2 | 3.3.3.3/24 | <input type="button" value="X"/> |

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 on any of the existing LAN interfaces (or creating a new one) will show the following :

IP Settings

IP Address (/24) ▼

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

| Network Settings ? | |
|---|-------------------------------------|
| Name | <input type="text"/> |
| VLAN ID | <input type="text"/> |
| Inter-VLAN routing | <input checked="" type="checkbox"/> |



| 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. |

| Layer 2 PepVPN Bridging ? | |
|--|---|
| PepVPN Profiles to Bridge ? | No profile is available |
| Remote Network Isolation ? | <input type="checkbox"/> |
| Spanning Tree Protocol | <input type="checkbox"/> |
| DHCP Option 82 Injection | <input checked="" type="checkbox"/> |
| Override IP Address when bridge connected ? | <input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None |

| 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. |
| Remote Network Isolation | Enable this option if you want to block network traffic between the remote networks, this will not affect the connectivity between them and this local LAN. |
| Spanning Tree Protocol | Click the box will enable STP for this layer 2 profile bridge. |
| Override IP Address when bridge | Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up. If you choose to override IP address when the VPN is connected, the device will |

| | |
|-----------------------|--|
| connected | not act as a router, and most Layer 3 routing functions will cease to work. |
| DHCP Option 82 | <p>Click on the question Mark if you want to enable DHCP Option 82.</p> <p>This allows the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to a PepVPN peer, such that the DHCP Server can identify where the request originates from.</p> |

| 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. |
| DHCP Server Logging | Enable logging of DHCP events in the eventlog by selecting the checkbox. |
| 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 Servers | <p>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.</p> <p>When this unit is connected using SpeedFusion™, other VPN peers can share</p> |



| | |
|-----------------------------|--|
| | <p>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.</p> |
| BOOTP | <p>Check this box to enable BOOTP on older networks that still require it.</p> |
| Extended DHCP Option | <p>In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.</p> <p>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.</p> |
| DHCP Reservation | <p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p>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.</p> |

LAN Physical Settings

Speed

| LAN Physical Settings | |
|-----------------------|--|
| Speed | <p>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.</p> |

Static Route Settings

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

Static Route Settings

Static Route

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

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

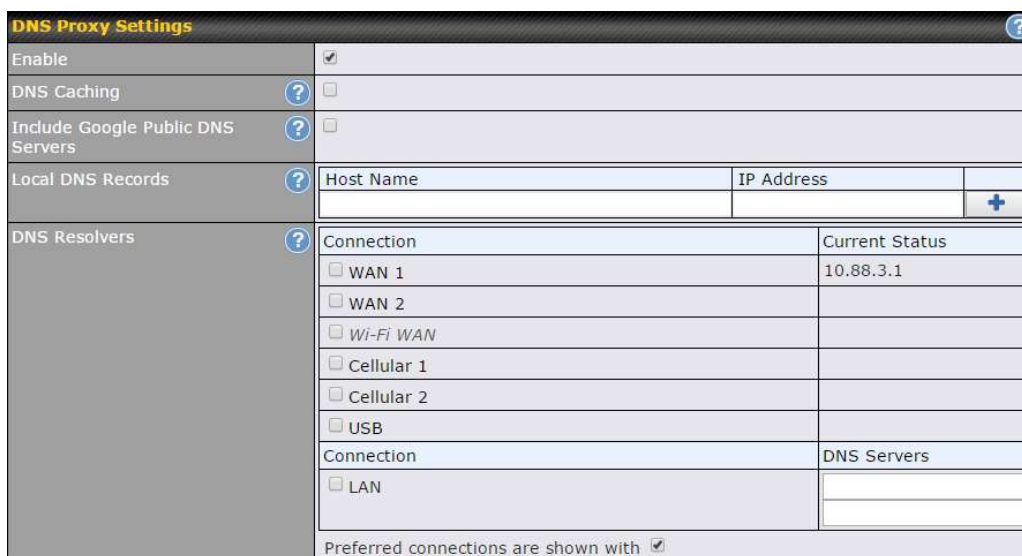
WINS Server Settings

Enable

WINS Server Settings

Enable

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



| 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. |

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.

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.

| LAN | VLAN | Network |
|--------------|------|-----------------|
| Untagged LAN | None | 192.168.50.1/24 |

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




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

| 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. |

| DHCP Server Settings | | | | | | | |
|--------------------------------|---|-----------|-------------|--------------------------------|--|------------|--|
| DHCP Server | <input checked="" type="checkbox"/> Enable | | | | | | |
| IP Range | <input type="text"/> - <input type="text"/> 255.255.255.0 (/24) | | | | | | |
| Lease Time | 1 Days 0 Hours 0 Mins | | | | | | |
| DNS Servers | <input checked="" type="checkbox"/> Assign DNS server automatically | | | | | | |
| WINS Servers | <input type="checkbox"/> Assign WINS server | | | | | | |
| BOOTP | <input type="checkbox"/> | | | | | | |
| Extended DHCP Option | <table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;"><i>No Extended DHCP Option</i></td> </tr> <tr> <td colspan="2" style="text-align: center;">Add</td> </tr> </tbody> </table> | Option | Value | <i>No Extended DHCP Option</i> | | Add | |
| Option | Value | | | | | | |
| <i>No Extended DHCP Option</i> | | | | | | | |
| Add | | | | | | | |
| DHCP Reservation | <table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> | Name | MAC Address | Static IP | | | |
| Name | MAC Address | Static IP | | | | | |
| | | | | | | | |

| 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 |

| | |
|-----------------------------------|---|
| | <p>prevent IP address collisions on the LAN.</p> <p>To enable DHCP bridge relay, please click the  icon on this menu item.</p> |
| 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 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 | <p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p>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.</p> |

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

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

| DHCP Relay Settings | |
|-------------------------------|--|
| 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 | DHCP 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.

8.2 Port Settings

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

| Port Settings | | | | | |
|---------------|-------------------------------------|--------|-------------------------------------|-----------|-------|
| Port Name | Enable | Speed | Advertise Speed | Port Type | VLAN |
| LAN Port 1 | <input checked="" type="checkbox"/> | | | Trunk ▾ | Any ▾ |
| LAN Port 2 | <input checked="" type="checkbox"/> | | | Trunk ▾ | Any ▾ |
| LAN Port 3 | <input checked="" type="checkbox"/> | Auto ▾ | <input checked="" type="checkbox"/> | Trunk ▾ | Any ▾ |
| LAN Port 4 | <input checked="" type="checkbox"/> | | | Trunk ▾ | Any ▾ |



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.





8.3 Captive Portal

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

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

| 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 | <p>This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:</p> <table border="1"> <tbody> <tr> <td>Authentication</td> <td>RADIUS Server</td> </tr> <tr> <td>Auth Server</td> <td><input type="text"/> Port 1812 Default</td> </tr> <tr> <td>Auth Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>CoA-DM</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Accounting Server</td> <td><input type="text"/> Port 1813 Default</td> </tr> <tr> <td>Accounting Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Accounting Interim Interval</td> <td><input type="text"/> seconds</td> </tr> </tbody> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p> | Authentication | RADIUS Server | Auth Server | <input type="text"/> Port 1812 Default | Auth Server Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | CoA-DM | <input type="checkbox"/> | Accounting Server | <input type="text"/> Port 1813 Default | Accounting Server Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | Accounting Interim Interval | <input type="text"/> seconds |
| Authentication | RADIUS Server | | | | | | | | | | | | | | |
| Auth Server | <input type="text"/> Port 1812 Default | | | | | | | | | | | | | | |
| Auth Server Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | |
| CoA-DM | <input type="checkbox"/> | | | | | | | | | | | | | | |
| Accounting Server | <input type="text"/> Port 1813 Default | | | | | | | | | | | | | | |
| Accounting Server Secret | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | |
| Accounting Interim Interval | <input type="text"/> seconds | | | | | | | | | | | | | | |
| LDAP Server | <p>This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:</p> <table border="1"> <tbody> <tr> <td>Authentication</td> <td>LDAP Server</td> </tr> <tr> <td>LDAP Server</td> <td><input type="text"/> Port 389 Default</td> </tr> <tr> <td></td> <td><input type="checkbox"/> Use DN/Password to bind to LDAP Server</td> </tr> <tr> <td>Base DN</td> <td><input type="text"/></td> </tr> <tr> <td>Base Filter</td> <td><input type="text"/></td> </tr> </tbody> </table> | Authentication | LDAP Server | LDAP Server | <input type="text"/> Port 389 Default | | <input type="checkbox"/> Use DN/Password to bind to LDAP Server | Base DN | <input type="text"/> | Base Filter | <input type="text"/> | | | | |
| Authentication | LDAP Server | | | | | | | | | | | | | | |
| LDAP Server | <input type="text"/> Port 389 Default | | | | | | | | | | | | | | |
| | <input type="checkbox"/> Use DN/Password to bind to LDAP Server | | | | | | | | | | | | | | |
| Base DN | <input type="text"/> | | | | | | | | | | | | | | |
| Base Filter | <input type="text"/> | | | | | | | | | | | | | | |

| | |
|-------------------------|---|
| | 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 | Add networks that can bypass the captive Portal in this field. 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. |
| Allowed Clients | Add MAC address and /or IP addresses for client devices that are allowed to bypass the Captive Portal. Clients accessing these domains and IP addresses will not be redirected to the splash page. |
| 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:  and . Clicking  displays a pop-up previewing the captive portal that your clients will see. Clicking  displays the following menu:

| Portal Customization | |
|----------------------|---|
| Logo Image | <input checked="" type="radio"/> No image [Use default Logo Image] <input type="radio"/> Choose File No file chosen <small>NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.</small> |
| Message | <div style="border: 1px solid #ccc; height: 100px;"></div> |
| Terms & Conditions | <div style="border: 1px solid #ccc; height: 150px;">[Use default Terms & Conditions]</div> |
| Custom Landing Page | <input checked="" type="checkbox"/> <input type="text" value="http://"/> |

| 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. |

9 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.

9.1 Ethernet WAN

| Health Check Settings | |
|-----------------------|---|
| Health Check Method | PING |
| PING Hosts | Host 1: 8.8.8.8 Host 2: <input type="text"/> <input type="checkbox"/> Use first two DNS servers as PING Hosts |
| Timeout | 5 second(s) |
| Health Check Interval | 5 second(s) |
| Health Check Retries | 3 |
| Recovery Retries | 3 |

Health Check Settings

Health Check Method This field specifies the Health Check method to be used for this WAN connection.

- Disabled - The WAN connection is always considered to be up and will not be treated as down for any IP routing errors.

| | |
|------------------------------|---|
| | <ul style="list-style-type: none"> • PING - ICMP PING packets will be issued to test connectivity with configurable target IP addresses or host names. • DNS Lookup - DNS lookups will be issued to test the connectivity with configurable target DNS server IP addresses. • HTTP - HTTP connections will be issued to test the connectivity with configurable URLs and strings to match. <p>Default: DNS Lookup</p> |
| PING Hosts | <p>These fields are for specifying the target IP addresses or host names where ICMP Ping packets will be sent to for health check.</p> <p>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.</p> <p>The connection is considered to be up if ping responses are received from any one of the ping hosts.</p> |
| 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. |

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

| Bandwidth Allowance Monitor Settings | |
|--------------------------------------|--|
| Bandwidth | Check the box <i>Enable</i> to enable bandwidth usage monitoring on this WAN |

| | |
|--------------------------|---|
| Allowance Monitor | 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 | <p>If Email Notification is enabled, you will receive an email notification when usage hits 75% and 95% of the monthly allowance.</p> <p>If the box Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume unless this option has been turned off or the usage has been reset when a new billing cycle starts.</p> |
| Start Day | This option allows you to select which day of the month a billing cycle starts. |
| Monthly Allowance | This field is to specify the bandwidth allowance for each billing cycle. |

Additional Public IP Settings

If you have access to status public IP addresses, you can assign them on this field.

Dynamic DNS Settings

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

Dynamic DNS Service Provider

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

Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.

9.1.1 DHCP Connection

There are four possible connection methods:

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

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

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

| DHCP Connection Settings | |
|---|---|
| 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. 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.

9.1.2 Static IP Connection

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

| | |
|-------------------|--|
| Connection Method | Static IP ▾ |
| Routing Mode | <input type="radio"/> NAT |
| IP Address | 10.88.3.158 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.88.3.253 |
| IP Address | <input type="text"/> |
| Subnet Mask | 255.255.255.0 (/24) ▾ |
| Default Gateway | <input type="text"/> |
| DNS Servers | <input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/> |

| Static IP Settings | |
|---|--|
| Routing Mode | NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it. |
| IP Address / Subnet Mask / Default Gateway | These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP. |
| DNS Servers | Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields. |

9.1.3 PPPoE Connection

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

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

| PPPoE Settings | |
|---|--|
| Routing Mode | NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it. |
| IP Address / Subnet Mask / Default Gateway | This information is obtained from the ISP automatically. |
| PPPoE Username / Password | Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP. |
| Confirm PPPoE Password | Verify your password by entering it again in this field. |
| Service Name (Optional) | Service name is provided by the ISP. Note: Leave this field blank unless it is provided by your ISP. |
| IP Address (Optional) | If your ISP provides a PPPoE IP address, enter it here. Note: Leave this field blank unless it is provided by your ISP. |
| DNS Servers | Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results 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. |

9.1.4 L2TP Connection

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

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

| L2TP Settings | |
|---------------------------------|--|
| L2TP Username / Password | Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP. |
| Confirm L2TP Password | Verify your password by entering it again in this field. |
| Server IP Address / Host | L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP. |
| Address Type | Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value. |
| DNS Servers | Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from |

the PPPoE server.)

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.

9.2 Cellular WAN



To access cellular WAN settings, click **Network>WAN>Details**.

Connection Details

| Cellular 1 Status | |
|-------------------|--------------------------------------|
| IMSI | (No SIM Card Detected) |
| MEID | A100001F7DC038 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. |

| Connection Settings | |
|----------------------------|--|
| WAN Connection Name | Indicate a name you wish to give this WAN connection |
| Enable | Click the checkbox to toggle the on and off state of this connection. |
| Routing Mode | <p>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.</p> <p>In the case if you need to choose IP Forwarding for your scenario. Click the button to enable IP Forwarding.</p> |
| Subnet Selection | <p>Choose between:</p> <p>Auto: The subnet mask will be set automatically.</p> <p>Force /31 Subnet: The subnet mask will be set as 255.255.255.254(/31), and the gateway IP address will be recalculated.</p> |
| Connection Priority | <p>This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only.</p> <p>If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections.</p> |

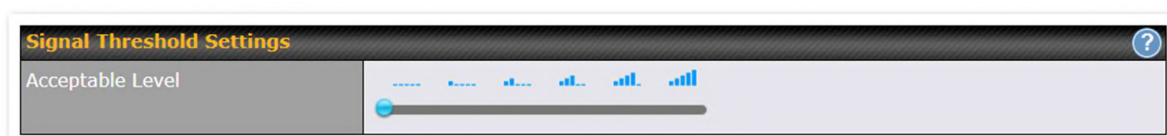
| | |
|-------------------------------------|---|
| | If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected. |
| Independent from Backup WANs | If this is checked, the connection will 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. |
| Idle Disconnect | If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default. |
| DNS Servers | Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by 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. |

| Cellular Settings ? | | |
|--|--|--|
| SIM Card | <input checked="" type="radio"/> Both SIMs <input type="radio"/> SIM A Only <input type="radio"/> SIM B Only | |
| Preferred SIM Card | <input checked="" type="radio"/> No Preference <input type="radio"/> SIM A <input type="radio"/> SIM B | |
| | SIM Card A | SIM Card B |
| Network Selection | <input checked="" type="radio"/> Auto <input type="radio"/> Manual | <input checked="" type="radio"/> Auto <input type="radio"/> Manual |
| LTE/3G | <input checked="" type="radio"/> LTE Only | <input checked="" type="radio"/> LTE Only |
| Optimal Network Discovery | <input type="checkbox"/> | <input type="checkbox"/> |
| Band Selection | Auto | Auto |
| Data Roaming | <input type="checkbox"/> | <input type="checkbox"/> |
| Authentication | Auto | Auto |
| Operator Settings | <input checked="" type="radio"/> Auto <input type="radio"/> Custom | <input checked="" type="radio"/> Auto <input type="radio"/> Custom |
| APN | <input type="text"/> | <input type="text"/> |
| Username | <input type="text"/> | <input type="text"/> |
| Password | <input type="text"/> | <input type="text"/> |
| Confirm Password | <input type="text"/> | <input type="text"/> |
| SIM PIN (Optional) | <input type="text"/> (Confirm) | <input type="text"/> (Confirm) |
| Bandwidth Allowance Monitor | <input checked="" type="checkbox"/> Enable | <input checked="" type="checkbox"/> Enable |
| Action | <input checked="" type="checkbox"/> Receive email notification <input type="checkbox"/> Reserve for management traffic when usage hits 100% <input type="checkbox"/> Disconnect when usage hits 100% | <input checked="" type="checkbox"/> Receive email notification <input type="checkbox"/> Reserve for management traffic when usage hits 100% <input type="checkbox"/> Disconnect when usage hits 100% |
| Start Day | On <input type="text"/> 26th of each month | On <input type="text"/> 21st of each month |
| Monthly Allowance | <input type="text"/> 4 GB | <input type="text"/> 22 GB |

| 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. |
| LTE/3G | This drop-down menu allows restricting cellular to particular band. Click the  button to enable the selection of specific bands. |
| Optimal Network Discovery | Cellular WAsN by default will only handover from 3G to LTE network when there is no active data traffic, enable this option will make it run the handover procedures after fallback to 3G for a defined effective period, even this may interrupt the connectivity for a short while. |
| Band Selection | When set to Auto , band selection allows for automatically connecting to available, supported bands (frequencies) . When set to Manual, you can manually select the bands (frequencies) the SIM will connect to. |
| Data Roaming | This checkbox enables data roaming on this particular SIM card. When data roaming is enabled this option allows you to select in which countries the SIM has a data connection. The option is configured by using MMC (country) codes. Please check your service provider's data roaming policy before proceeding. |
| Authentication | Choose from PAP Only or CHAP Only to use those authentication methods exclusively. Select Auto to automatically choose an authentication method. |
| Operator Settings | This setting 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. |

Signal Threshold Settings

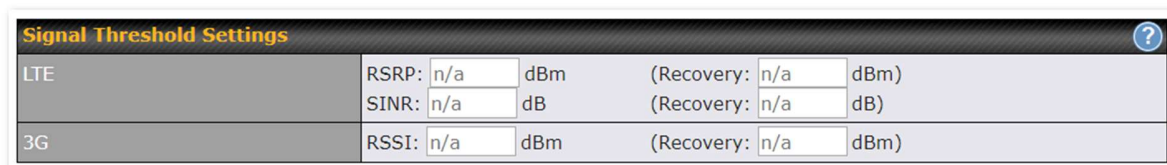


If signal threshold is defined, this connection will be treated as down when a weaker than threshold signal is determined.

The following values are used by the threshold scale:

| | 0 bars | 1 bar | 2 bars | 3 bars | 4 bars | 5 bars |
|-------------------|--------|-------|--------|--------|--------|--------|
| LTE / RSRP | -140 | -128 | -121 | -114 | -108 | -98 |
| 3G / RSSI | -120 | -100 | -95 | -90 | -85 | -75 |

To define the threshold manually using specific signal strength values, please click on the question Mark and the following field will be visible.



| 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 |

| 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 | Disabled |

| Dynamic DNS Settings | |
|-------------------------------------|---|
| Dynamic DNS Service Provider | <p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> <ul style="list-style-type: none"> • changeip.com • dyndns.org • no-ip.org |

- tzo.com
- DNS-O-Matic

Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.

| | | |
|-----|-----------------------------------|--|
| MTU | <input type="text" value="1428"/> | <input type="button" value="Default"/> |
|-----|-----------------------------------|--|

| 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. |

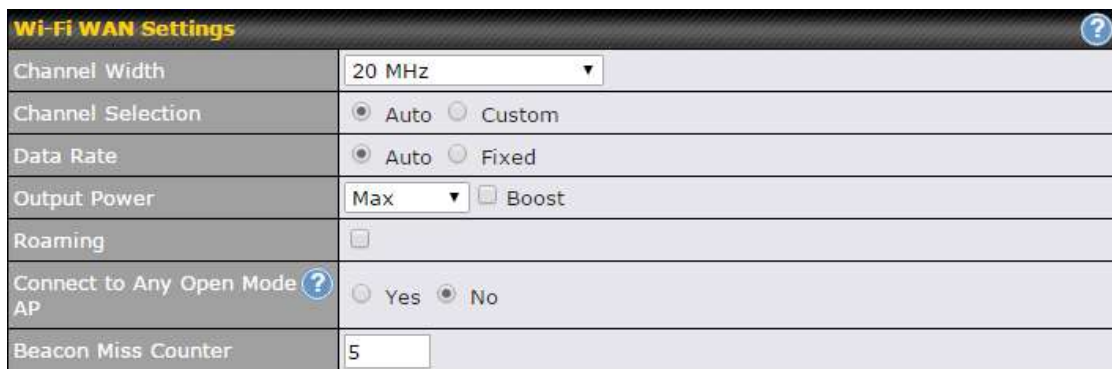
9.3 Wi-Fi WAN

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

| WAN Connection Settings | |
|---|--|
| WAN Connection Name | <input type="text" value="Wi-Fi WAN"/> <input type="button" value="Default"/> |
| Operating Schedule | Always on ▾ |
| Independent from Backup WANs <input type="checkbox"/> | <input type="checkbox"/> |
| Standby State | <input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected |
| MTU <input type="checkbox"/> | <input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: <input type="text" value="1500"/> <input type="button" value="Default"/> |
| Reply to ICMP PING <input type="checkbox"/> | <input checked="" type="radio"/> Yes <input type="radio"/> No |

| 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. |



| 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 | <p>Determine whether the channel will be automatically selected. If you select custom, the following table will appear:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Scan Channels</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">Scan Channels</th> <th>Clear</th> <th>All</th> </tr> </thead> <tbody> <tr> <td colspan="4">2.4GHz:</td> </tr> <tr> <td><input checked="" type="checkbox"/> 1</td> <td><input checked="" type="checkbox"/> 2</td> <td><input checked="" type="checkbox"/> 3</td> <td><input checked="" type="checkbox"/> 4</td> </tr> <tr> <td><input checked="" type="checkbox"/> 6</td> <td><input checked="" type="checkbox"/> 7</td> <td><input checked="" type="checkbox"/> 8</td> <td><input checked="" type="checkbox"/> 9</td> </tr> <tr> <td><input checked="" type="checkbox"/> 11</td> <td></td> <td></td> <td><input checked="" type="checkbox"/> 10</td> </tr> </tbody> </table> <p style="text-align: right; margin-top: 10px;">OK Cancel</p> </div> | Scan Channels | | Clear | All | 2.4GHz: | | | | <input checked="" type="checkbox"/> 1 | <input checked="" type="checkbox"/> 2 | <input checked="" type="checkbox"/> 3 | <input checked="" type="checkbox"/> 4 | <input checked="" type="checkbox"/> 6 | <input checked="" type="checkbox"/> 7 | <input checked="" type="checkbox"/> 8 | <input checked="" type="checkbox"/> 9 | <input checked="" type="checkbox"/> 11 | | | <input checked="" type="checkbox"/> 10 |
| Scan Channels | | Clear | All | | | | | | | | | | | | | | | | | | |
| 2.4GHz: | | | | | | | | | | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> 1 | <input checked="" type="checkbox"/> 2 | <input checked="" type="checkbox"/> 3 | <input checked="" type="checkbox"/> 4 | | | | | | | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> 6 | <input checked="" type="checkbox"/> 7 | <input checked="" type="checkbox"/> 8 | <input checked="" type="checkbox"/> 9 | | | | | | | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> 11 | | | <input checked="" type="checkbox"/> 10 | | | | | | | | | | | | | | | | | | |
| 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 exceed 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. |

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

| Bandwidth Allowance Monitor | |
|-----------------------------|--|
| Action | If Error! Reference source not found. is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts. |
| Start Day | This option allows you to define which day of the month each billing cycle begins. |
| Monthly Allowance | This field is for defining the maximum bandwidth usage allowed for the WAN connection each month. |

| Health Check Settings | |
|--------------------------|--|
| Health Check Method | DNS Lookup |
| Health Check DNS Servers | Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers |
| Timeout | 5 second(s) |
| Health Check Interval | 5 second(s) |
| Health Check Retries | 3 |
| Recovery Retries | 3 |

Health Check Settings

Method

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

Health Check Disabled

| Health Check Settings | |
|-----------------------|---|
| Health Check Method | Disabled <small>Health Check disabled. Network problem cannot be detected.</small> |

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

Health Check Method: PING

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

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

PING Hosts

This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup

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

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

Health Check DNS Servers

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

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

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

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

Health Check Method: HTTP

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

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

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

URL 2 **WAN Settings>WAN Edit>Health Check Settings>URL2**
 If **URL2** is also provided, a health check will pass if either one of the tests passed.

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 Retries | This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to 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 | DNS-O-Matic ▾ |
| Username | <input type="text"/> |
| Password | <input type="password"/> |
| Confirm Password | <input type="password"/> |
| Update All Hosts | <input type="checkbox"/> |
| Hosts / IDs | <input type="text"/> |

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

| | |
|----------------------------------|---|
| 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. |

Important Note

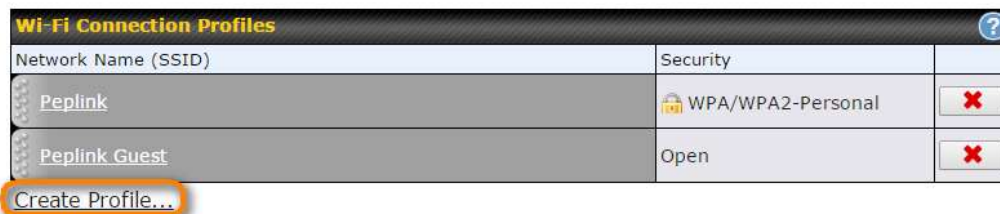
In order to use dynamic DNS services, appropriate hostname registration(s), as well as a valid account with a supported dynamic DNS service provider, are required.

A dynamic DNS update is performed whenever a WAN's IP address is changed, such as when an IP is changed after a DHCP IP refresh or reconnection.

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

9.3.1 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

Create Wi-Fi Connection Profile
✕

Wi-Fi Connection

| | |
|---------------------|---|
| Network Name (SSID) | <input style="width: 90%;" type="text"/> |
| Security | Open ▾ |
| IP Address | <input checked="" type="radio"/> Obtain an IP address automatically <input type="radio"/> Static |

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 | <p>This option allows you to select which security policy is used for this wireless network.</p> <p>Available options:</p> <ul style="list-style-type: none"> • Open <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr> <td style="width: 30%; padding: 2px;">Security</td> <td style="padding: 2px;">Open ▾</td> </tr> </table> <ul style="list-style-type: none"> • WEP <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr> <td style="width: 30%; padding: 2px;">Security</td> <td style="padding: 2px;">WEP ▾</td> </tr> <tr> <td style="padding: 2px;">Encryption Key ?</td> <td style="padding: 2px;"> <input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters </td> </tr> </table> <ul style="list-style-type: none"> • WPA/WPA2 – Personal <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr> <td style="width: 30%; padding: 2px;">Security</td> <td style="padding: 2px;">WPA/WPA2-Personal ▾</td> </tr> <tr> <td style="padding: 2px;">Shared Key ?</td> <td style="padding: 2px;"> <input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters </td> </tr> </table> <ul style="list-style-type: none"> • WPA/WPA2 – Enterprise <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Security</td> <td style="padding: 2px;">WPA/WPA2-Enterprise ▾</td> </tr> <tr> <td style="padding: 2px;">Login ID</td> <td style="padding: 2px;"><input style="width: 90%;" type="text"/></td> </tr> <tr> <td style="padding: 2px;">Password</td> <td style="padding: 2px;"><input style="width: 90%;" type="password"/></td> </tr> <tr> <td style="padding: 2px;">Confirm Password</td> <td style="padding: 2px;"><input style="width: 90%;" type="password"/></td> </tr> <tr> <td style="padding: 2px;">EAP Method</td> <td style="padding: 2px;">PEAP ▾</td> </tr> <tr> <td style="padding: 2px;">EAP Phase 2 Method</td> <td style="padding: 2px;">EAP/CHAP ▾</td> </tr> <tr> <td style="padding: 2px;">EAP outer authentication identity</td> <td style="padding: 2px;"> <input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input style="width: 60%;" type="text"/> </td> </tr> </table> | Security | Open ▾ | Security | WEP ▾ | Encryption Key ? | <input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters | Security | WPA/WPA2-Personal ▾ | Shared Key ? | <input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters | Security | WPA/WPA2-Enterprise ▾ | Login ID | <input style="width: 90%;" type="text"/> | Password | <input style="width: 90%;" type="password"/> | Confirm Password | <input style="width: 90%;" type="password"/> | EAP Method | PEAP ▾ | EAP Phase 2 Method | EAP/CHAP ▾ | EAP outer authentication identity | <input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input style="width: 60%;" type="text"/> |
| Security | Open ▾ | | | | | | | | | | | | | | | | | | | | | | | | |
| Security | WEP ▾ | | | | | | | | | | | | | | | | | | | | | | | | |
| Encryption Key ? | <input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | | | | | | | | | | | |
| Security | WPA/WPA2-Personal ▾ | | | | | | | | | | | | | | | | | | | | | | | | |
| Shared Key ? | <input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | | | | | | | | | | | |
| Security | WPA/WPA2-Enterprise ▾ | | | | | | | | | | | | | | | | | | | | | | | | |
| Login ID | <input style="width: 90%;" type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Password | <input style="width: 90%;" type="password"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Confirm Password | <input style="width: 90%;" type="password"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| EAP Method | PEAP ▾ | | | | | | | | | | | | | | | | | | | | | | | | |
| EAP Phase 2 Method | EAP/CHAP ▾ | | | | | | | | | | | | | | | | | | | | | | | | |
| EAP outer authentication identity | <input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input style="width: 60%;" type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |

9.4 WAN Health Check

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

| Health Check Settings | | | | | |
|--|--|---------------------|--|--|--|
| Method | This setting specifies the health check method for the WAN connection. This value can be configured as Disabled , PING , DNS Lookup , or HTTP . The default method is DNS Lookup . For mobile Internet connections, the value of Method can be configured as Disabled or SmartCheck . | | | | |
| Health Check Disabled | | | | | |
| <div style="border: 1px solid #ccc; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Health Check Method</td> <td style="padding: 2px;"> <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">Disabled</div> </div> </td> </tr> <tr> <td colspan="2" style="padding: 2px; font-size: 0.8em; color: #800000;">Health Check disabled. Network problem cannot be detected.</td> </tr> </table> </div> <p>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.</p> | | Health Check Method | <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">Disabled</div> </div> | Health Check disabled. Network problem cannot be detected. | |
| Health Check Method | <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">Disabled</div> </div> | | | | |
| Health Check disabled. Network problem cannot be detected. | | | | | |
| Health Check Method: PING | | | | | |
| <div style="border: 1px solid #ccc; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Health Check Method</td> <td style="padding: 2px;"> <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">PING</div> </div> </td> </tr> <tr> <td style="padding: 2px;">PING Hosts</td> <td style="padding: 2px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> ? Host 1: <input style="width: 150px;" type="text"/> Host 2: <input style="width: 150px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </div> </div> </td> </tr> </table> </div> <p>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.</p> | | Health Check Method | <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">PING</div> </div> | PING Hosts | <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> ? Host 1: <input style="width: 150px;" type="text"/> Host 2: <input style="width: 150px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </div> </div> |
| Health Check Method | <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">PING</div> </div> | | | | |
| PING Hosts | <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> ? Host 1: <input style="width: 150px;" type="text"/> Host 2: <input style="width: 150px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </div> </div> | | | | |
| 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 | | | | | |
| <div style="border: 1px solid #ccc; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Health Check Method</td> <td style="padding: 2px;"> <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">DNS Lookup</div> </div> </td> </tr> <tr> <td style="padding: 2px;">Health Check DNS Servers</td> <td style="padding: 2px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> ? Host 1: <input style="width: 150px;" type="text"/> Host 2: <input style="width: 150px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers </div> </div> </td> </tr> </table> </div> <p>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.</p> | | Health Check Method | <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">DNS Lookup</div> </div> | Health Check DNS Servers | <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> ? Host 1: <input style="width: 150px;" type="text"/> Host 2: <input style="width: 150px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers </div> </div> |
| Health Check Method | <div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">DNS Lookup</div> </div> | | | | |
| Health Check DNS Servers | <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> ? Host 1: <input style="width: 150px;" type="text"/> Host 2: <input style="width: 150px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers </div> </div> | | | | |
| Health Check DNS Servers | This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS lookup. | | | | |

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

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

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

Health Check Method: HTTP

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

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

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

URL 2 **WAN Settings>WAN Edit>Health Check Settings>URL2**
 If **URL2** is also provided, a health check will pass if either one of the tests passed.

| | |
|-----------------------|-----------------------------------|
| Timeout | 10 <input type="text"/> second(s) |
| Health Check Interval | 5 <input type="text"/> second(s) |
| Health Check Retries | 3 <input type="text"/> |
| Recovery Retries | 3 <input type="text"/> |

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 This setting specifies the time interval in seconds between ping or DNS lookup

| | |
|-----------------------------|--|
| Interval | 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. |

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.**

9.5 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 | <input type="text" value="changeip.com"/> |
| User ID | <input type="text"/> |
| Password | <input type="text"/> |
| Confirm Password | <input type="text"/> |
| Hosts | <input type="text"/> |

Dynamic DNS Settings

Dynamic DNS

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

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

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

Select **Disabled** to disable this feature.

Account Name / Email Address

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

Password / TZO Key

This setting specifies the password for the dynamic DNS service.

Hosts / Domain

This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

Important Note

In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN's IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service 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.

10 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 | <input type="checkbox"/> 2.4 GHz <input checked="" type="checkbox"/> 5 GHz <input type="checkbox"/> Integrated AP supports 2.4 GHz only. Testing |
| Operating Country | United States |
| Preferred Frequency | <input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz Integrated AP supports 2.4 GHz only. |


| AP Settings | |
|----------------------------|---|
| SSID | <p>You can select the wireless networks for 2.4 GHz or 5 GHz separately for each SSID.</p> |
| Operating Country | <p>This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow.</p> <ul style="list-style-type: none"> • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). <p>NOTE: Users are required to choose an option suitable to local laws and regulations.</p> |
| Preferred Frequency | <p>Indicate the preferred frequency to use for clients to connect.</p> |

| Important Note |
|--|
| <p>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.</p> |

| | 2.4 GHz | 5 GHz |
|----------------------------------|--|---|
| Protocol | 802.11ng | 802.11n/ac |
| Channel Width | 20 MHz | Auto |
| Channel | Auto <input type="button" value="Edit"/> Channels: 1 2 3 4 5 6 7 8 9 10 11 | Auto <input type="button" value="Edit"/> 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 <input checked="" type="checkbox"/> Wait until no active client associated | Daily at 03:00 <input checked="" type="checkbox"/> Wait until no active client associated |
| Output Power | Fixed: Max <input type="checkbox"/> Boost | Fixed: Max <input type="checkbox"/> 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**.

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

| 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. 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 Converter | Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout. |