



Pepwave MAX User Manual

Pepwave Products:

MAX 700 / HD2 / HD2 IP67 / HD2 mini / HD4 / Transit / MAX Transit Mini / Max transit Mini / MAX-Transit-Mini / MAX Transit Mini LTE / Max Transit Mini LTE / MAX Transit Mini LTEA / Max Transit Mini LTEA / BR1 Classic / BR1 MK2 / BR1 Slim / BR1 ENT / MAX BR1 M2M / MAX BR1 Mini / Max BR1 Mini / MAX BR1 Mini LTE / MAX BR1 Mini LTEA / MAX-BR1-MINI-LTE-US / MAX-BR1-MINI-LTE-US-T / BR1 Pro LTE / BR1 IP55 / BR2 IP55 / On-The-Go / MAX HD2 / HD4 with MediaFast / SpeedFusion Engine / Pismo 930 LITE / Pismo930 LITE / Pismo930LITE / Pismo 930 Lite / Pismo930LITER5 / Pismo 930LITER5

Pepwave Firmware 7.1.1

December 2018

Copyright & Trademarks

Specifications are subject to change without notice. Copyright © 2018 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 | 11 |
| AP Controller | 11 |
| QoS | 11 |
| Other Supported Features | 11 |
| Pepwave MAX Mobile Router Overview | 13 |
| MAX 700 | 13 |
| MAX HD2 | 15 |
| MAX HD2 IP67 | 17 |
| MAX HD2 mini | 18 |
| MAX Transit | 20 |
| MAX Transit Mini | 21 |
| MAX HD4 / HD2 and HD4 with MediaFast | 23 |
| MAX BR1 Classic | 24 |
| MAX BR1 MK2 | 26 |
| MAX BR1 Slim | 28 |
| MAX BR1 Mini | 30 |
| MAX BR1 M2M | 31 |
| MAX BR1 ENT | 33 |
| MAX BR1 Pro LTE | 34 |
| MAX Hotspot | 36 |
| MAX BR1/2 IP55 | 36 |
| MAX On-The-Go | 38 |
| SpeedFusion Engine | 40 |
| Advanced Feature Summary | 40 |

| | |
|---|----|
| Drop-in Mode and LAN Bypass: Transparent Deployment | 40 |
| QoS: Clearer VoIP | 41 |
| Per-User Bandwidth Control | 41 |
| High Availability via VRRP | 42 |
| USB Modem and Android Tethering | 42 |
| Built-In Remote User VPN Support | 43 |
| SIM-card USSD support | 43 |
| Installation | 44 |
| Preparation | 44 |
| Constructing the Network | 44 |
| Configuring the Network Environment | 45 |
| Mounting the Unit | 45 |
| Wall Mount | 45 |
| Car Mount | 46 |
| IP67 Installation Guide | 46 |
| Connecting to the Web Admin Interface | 46 |
| Configuring the LAN Interface(s) | 49 |
| Basic Settings | 49 |
| Port Settings | 59 |
| Captive Portal | 59 |
| Configuring the WAN Interface(s) | 62 |
| Ethernet WAN | 63 |
| DHCP Connection | 66 |
| Static IP Connection | 67 |
| PPPoE Connection | 68 |
| L2TP Connection | 69 |
| Cellular WAN | 70 |
| Wi-Fi WAN | 76 |
| Creating Wi-Fi Connection Profiles | 82 |
| WAN Health Check | 84 |
| Dynamic DNS Settings | 86 |
| Advanced Wi-Fi Settings | 88 |
| MediaFast Configuration | 93 |
| Setting Up MediaFast Content Caching | 93 |
| Scheduling Content Prefetching | 94 |

| | |
|--|-----|
| Viewing MediaFast Statistics | 95 |
| Bandwidth Bonding SpeedFusion™ / PepVPN | 96 |
| PepVPN | 97 |
| The Pepwave Router Behind a NAT Router | 103 |
| SpeedFusion™ Status | 104 |
| IPsec VPN | 104 |
| IPsec VPN Settings | 104 |
| Outbound Policy Management | 109 |
| Outbound Policy | 109 |
| Custom Rules for Outbound Policy | 111 |
| Algorithm: Weighted Balance | 111 |
| Algorithm: Persistence | 112 |
| Algorithm: Enforced | 113 |
| Algorithm: Priority | 114 |
| Algorithm: Overflow | 114 |
| Algorithm: Least Used | 115 |
| Algorithm: Lowest Latency | 115 |
| Expert Mode | 116 |
| Inbound Access | 116 |
| Port Forwarding Service | 116 |
| UPnP / NAT-PMP Settings | 118 |
| NAT Mappings | 119 |
| QoS | 121 |
| User Groups | 121 |
| Bandwidth Control | 122 |
| Application | 122 |
| Application Prioritization | 122 |
| Prioritization for Custom Applications | 122 |
| DSL/Cable Optimization | 123 |
| Firewall | 123 |
| Outbound and Inbound Firewall Rules | 124 |
| Access Rules | 124 |
| Apply Firewall Rules to PepVpn Traffic | 127 |
| Intrusion Detection and DoS Prevention | 127 |
| Content Blocking | 128 |

| | |
|-------------------------------|-----|
| Application Blocking | 128 |
| Web Blocking | 128 |
| Customized Domains | 129 |
| Exempted User Groups | 129 |
| Exempted Subnets | 129 |
| URL Logging | 129 |
| OSPF & RIPv2 | 129 |
| BGP | 133 |
| Remote User Access | 135 |
| Miscellaneous Settings | 137 |
| High Availability | 137 |
| PPTP Server | 141 |
| Certificate Manager | 143 |
| Service Forwarding | 143 |
| SMTP Forwarding | 144 |
| Web Proxy Forwarding | 145 |
| DNS Forwarding | 145 |
| Custom Service Forwarding | 145 |
| Service Passthrough | 145 |
| GPS Forwarding | 147 |
| AP Controller | 147 |
| Wireless SSID | 148 |
| Settings | 152 |
| AP Controller Status | 157 |
| Info | 157 |
| Access Point (Usage) | 159 |
| Wireless SSID | 162 |
| Wireless Client | 162 |
| Nearby Device | 163 |
| Event Log | 164 |
| Toolbox | 165 |
| System Settings | 166 |
| Admin Security | 166 |
| Firmware | 170 |
| Time | 171 |

| | |
|--------------------------------------|-----|
| Schedule | 171 |
| Email Notification | 172 |
| Event Log | 174 |
| SNMP | 175 |
| InControl | 178 |
| Configuration | 178 |
| Feature Add-ons | 179 |
| Reboot | 179 |
| Tools | 180 |
| Ping | 180 |
| Traceroute Test | 180 |
| PepVPN Test | 181 |
| Wake-on-LAN | 182 |
| CLI (Command Line Interface Support) | 182 |
| Status | 183 |
| Device | 183 |
| GPS Data | 184 |
| Active Sessions | 184 |
| Client List | 186 |
| WINS Client | 187 |
| UPnP / NAT-PMP | 187 |
| SpeedFusion Status | 188 |
| Event Log | 191 |
| Bandwidth Status | 192 |
| Real-Time | 193 |
| Hourly | 193 |
| Daily | 193 |
| Monthly | 194 |
| Appendix B: Declaration | 198 |

1 Introduction and Scope

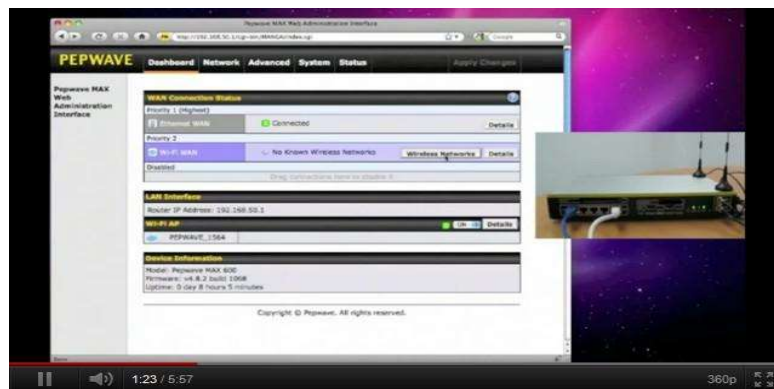
Pepwave routers provide link aggregation and load balancing across multiple WAN connections, allowing a combination of technologies like 3G HSDPA, EVDO, 4G LTE, Wi-Fi, external WiMAX dongle, and satellite to be utilized to connect to the Internet.

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

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

Tips

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



<http://youtu.be/UckVQThLKO4>

2 Glossary

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

| Term | Definition |
|-------------|--|
| 3G | 3rd generation standards for wireless communications (e.g., HSDPA) |
| 4G | 4th generation standards for wireless communications (e.g., LTE) |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| EVDO | Evolution-Data Optimized |
| FQDN | Fully Qualified Domain Name |
| HSDPA | High-Speed Downlink Packet Access |
| HTTP | Hyper-Text Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IP | Internet Protocol |
| LAN | Local Area Network |
| MAC Address | Media Access Control Address |
| MTU | Maximum Transmission Unit |
| MSS | Maximum Segment Size |
| NAT | Network Address Translation |
| PPPoE | Point to Point Protocol over Ethernet |
| QoS | Quality of Service |
| SNMP | Simple Network Management Protocol |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |

| | |
|------|------------------------------------|
| VPN | Virtual Private Network |
| VRRP | Virtual Router Redundancy Protocol |
| WAN | Wide Area Network |
| WINS | Windows Internet Name Service |
| WLAN | Wireless Local Area Network |

3 Product Features

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

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

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

3.1 Supported Network Features

3.1.1 WAN

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

tzo.com and DNS-O-Matic)

- Ping, DNS lookup, and HTTP-based health check

3.1.2 LAN

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

3.1.3 VPN

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

3.1.4 Firewall

- Outbound (LAN to WAN) firewall rules
- Inbound (WAN to LAN) firewall rules per WAN connection
- Intrusion detection and prevention
- Specification of NAT mappings
- Outbound firewall rules can be defined by destination domain name

3.1.5 Captive Portal

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

3.1.6 Outbound Policy

- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
- Traffic prioritization and DSL optimization
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms

3.1.7 AP Controller

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

3.1.8 QoS

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

3.2 Other Supported Features

- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Time server synchronization
- SNMP
- Email notification
- Read-only user for web admin
- Shared IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Built-in WINS servers*
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Event log

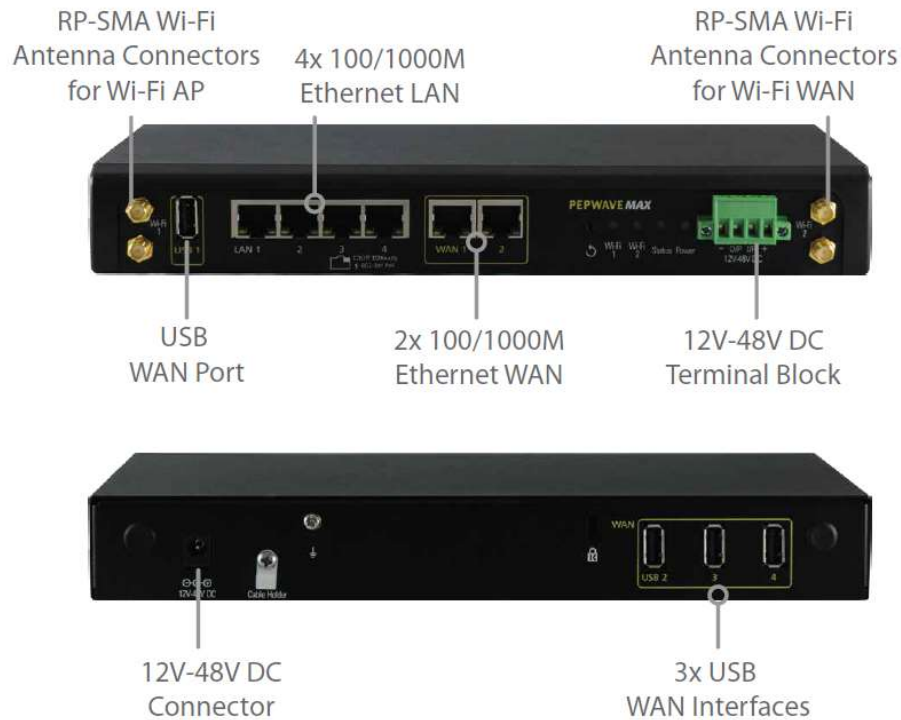
- Active sessions
- Client list
- WINS client list *
- UPnP / NAT-PMP
- Real-time, hourly, daily, and monthly bandwidth usage reports and charts
- IPv6 support
- Support USB tethering on Android 2.2+ phones

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

4 Pepwave MAX Mobile Router Overview

4.1 MAX 700

4.1.1 Panel Appearance



4.1.2 LED Indicators

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

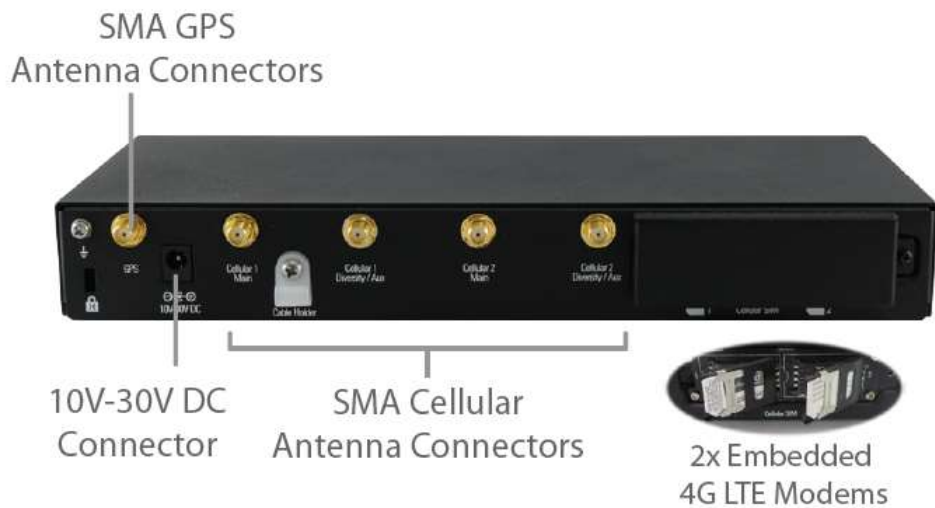
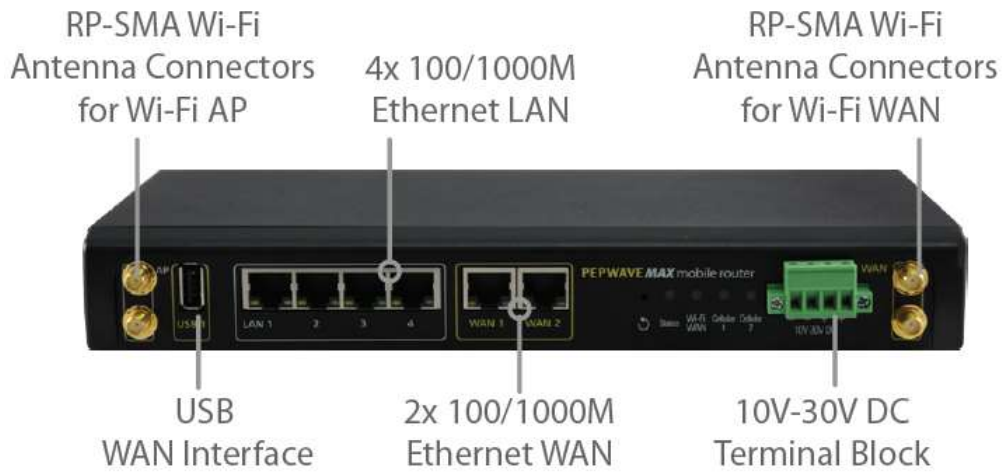
| Status Indicators | | |
|-------------------|--------------|---------------------|
| Status | OFF | System initializing |
| | Red | Booting up or busy |
| | Blinking red | Boot up error |
| | Green | Ready |

| 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 | |

4.2 MAX HD2

4.2.1 Panel Appearance



4.2.2 LED Indicators

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

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

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

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

4.3 MAX HD2 IP67

4.3.1 Panel Appearance

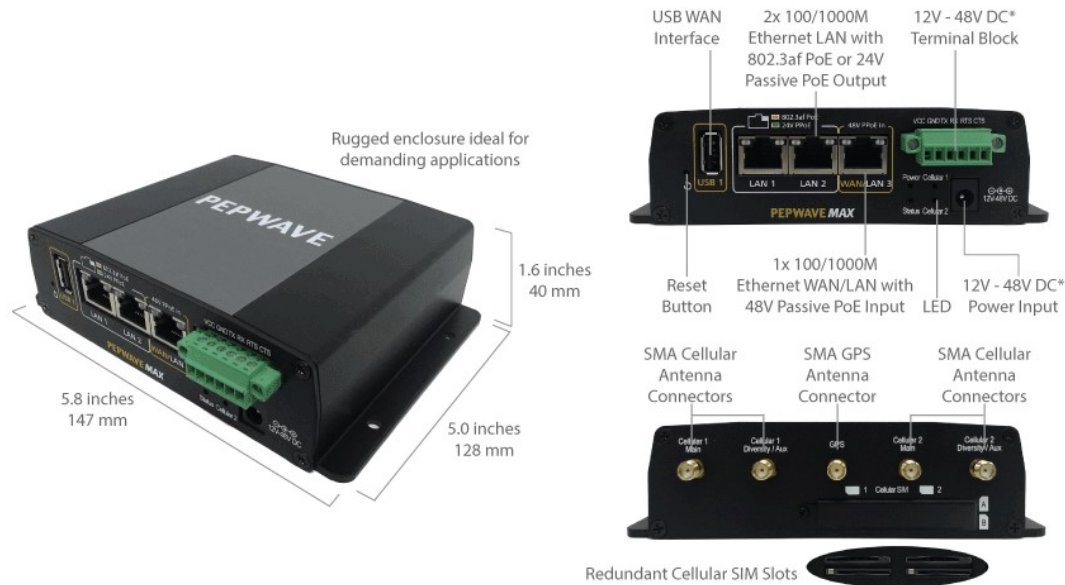


The statuses indicated by the front panel LEDs are as follows:

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

4.4 MAX HD2 mini

4.4.1 Panel Appearance



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

4.4.2 LED Indicators

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

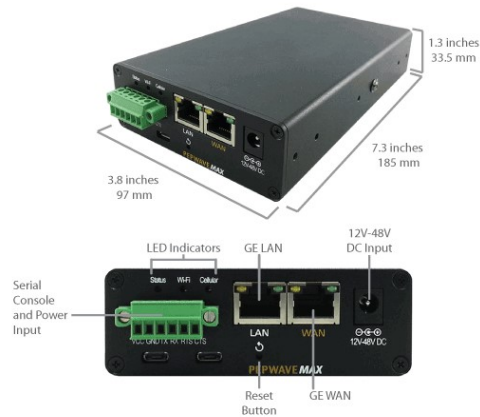
| Status Indicators | | |
|-------------------|--------------|---------------------|
| Status | OFF | System initializing |
| | Red | Booting up or busy |
| | Blinking red | Boot up error |
| | Green | Ready |

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

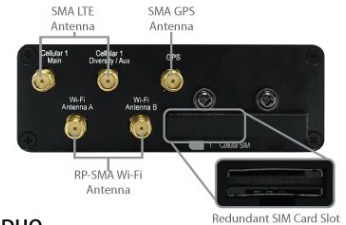
| LAN and Ethernet WAN Ports | | |
|----------------------------|----------------------|---|
| Green LED | ON | 10 / 100 / 1000 Mbps |
| Orange LED | Blinking | Data is transferring |
| | OFF | No data is being transferred or port is not connected |
| Port Type | Auto MDI/MDI-X ports | |

4.5 MAX Transit

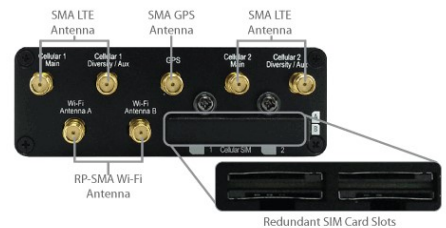
4.5.1 Panel Appearance



MAX-TST



MAX-TST-DUO



4.5.2 LED Indicators

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

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

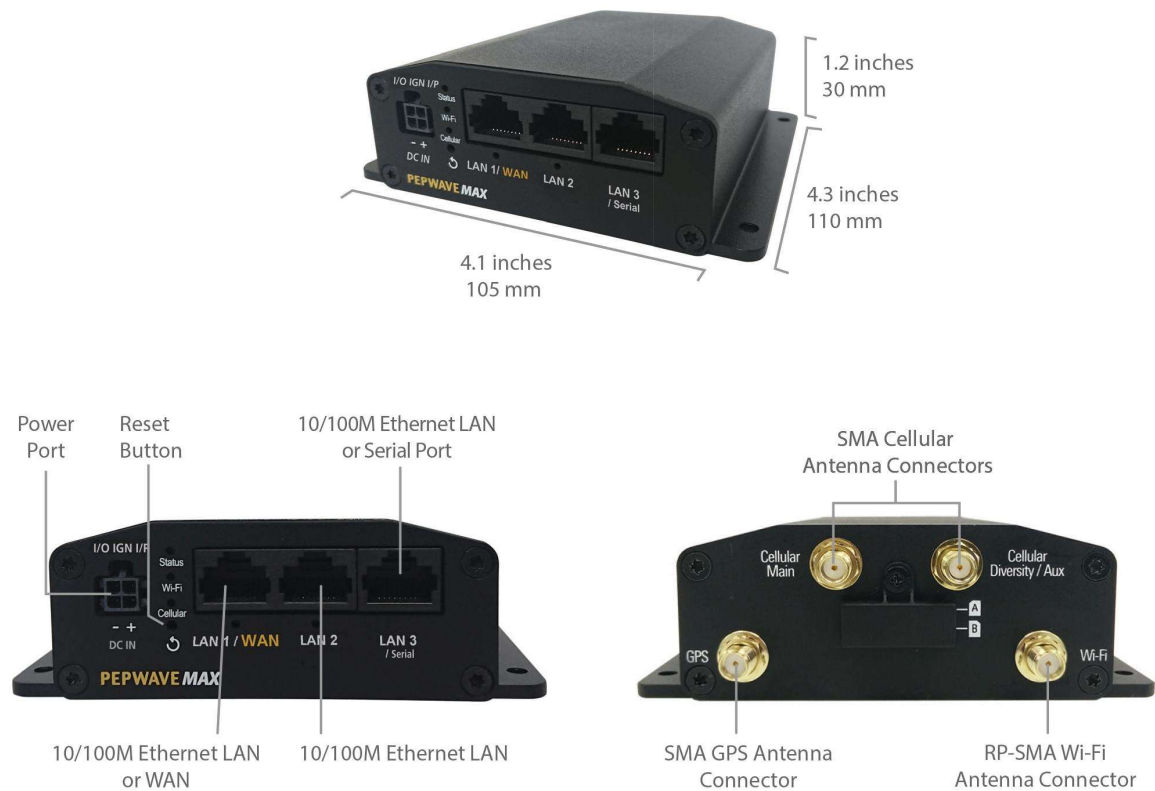
| Cellular WAN Indicators | | |
|--------------------------|-----------------|--|
| Cellular 1 / Cellular 2* | OFF | Disabled intermittent |
| | Blinking slowly | Connecting to wireless network(s) |
| | Blinking | Connected to wireless network(s) with traffic |
| | ON | Connected to wireless network(s)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

* For MAX-TST_DUO

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

4.6 MAX Transit Mini

4.6.1 Panel Appearance



4.6.2 LED Indicators

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

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

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

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

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

4.7 MAX HD4 / HD2 and HD4 with MediaFast

4.7.1 Panel Appearance



4.7.2 LED Indicators

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

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

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

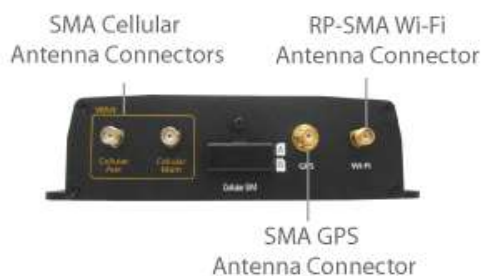
| LAN and Ethernet WAN Ports | | |
|----------------------------|----------------------|---|
| Green LED | ON | 10 / 100 / 1000 Mbps |
| | Blinking | Data is transferring |
| Orange LED | OFF | No data is being transferred or port is not connected |
| | ON | |
| Port Type | Auto MDI/MDI-X ports | |

4.8 MAX BR1 Classic

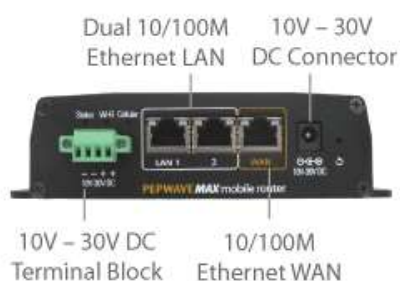
4.8.1 Panel Appearance



MAX-BR1-LTE Version



MAX-BR1 Version



4.8.2 LED Indicators

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

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

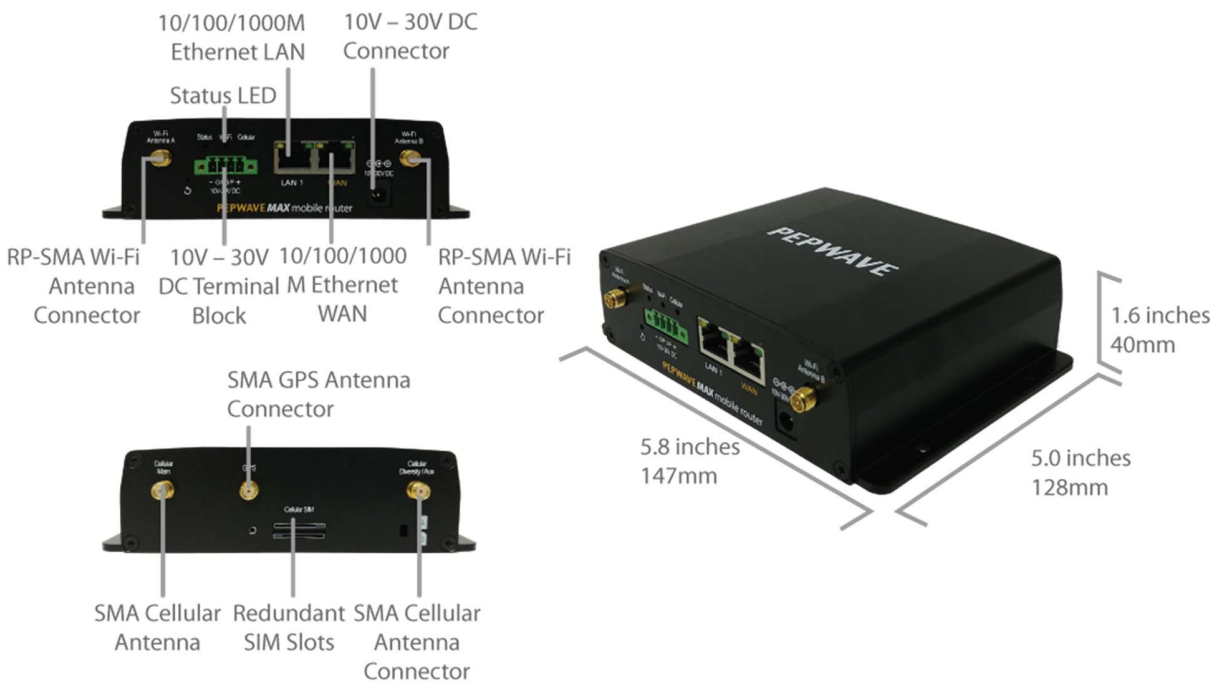
| Wi-Fi Indicators | | |
|------------------|-----------------|--|
| Wi-Fi | OFF | Disabled intermittent |
| | Blinking slowly | Connecting to wireless network(s) |
| | Blinking | Connected to wireless network(s) with traffic |
| | ON | Connected to wireless network(s) without traffic |

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

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

4.9 MAX BR1 MK2

4.9.1 Panel Appearance



4.9.2 LED Indicators

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

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

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

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

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

4.10 MAX BR1 Slim

4.10.1 Panel Appearance



4.10.2 LED Indicators

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

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

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

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

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

4.11 MAX BR1 Mini

4.11.1 Panel Appearance



4.11.2 LED Indicators

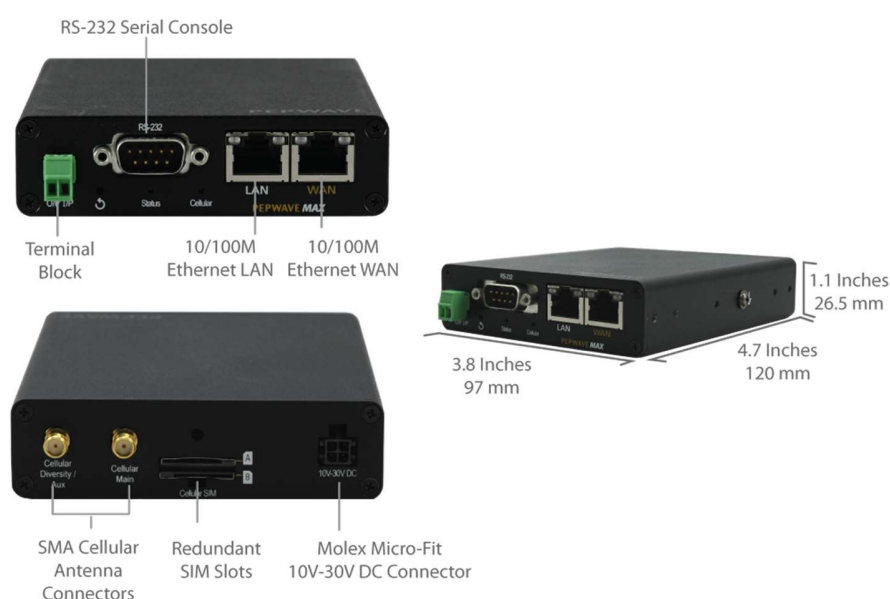
| Status Indicators | | |
|-------------------|--------------|---------------------|
| Status | OFF | System initializing |
| | Red | Booting up or busy |
| | Blinking red | Boot up error |
| | Green | Ready |

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

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

4.12 MAX BR1 M2M

4.12.1 Panel Appearance



4.12.2 LED Indicators

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

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

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

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

4.13 MAX BR1 ENT

4.13.1 Panel Appearance



4.13.2 LED Indicators

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

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

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

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

4.14 MAX BR1 Pro LTE

4.14.1 Panel Appearance



4.14.2 LED Indicators

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

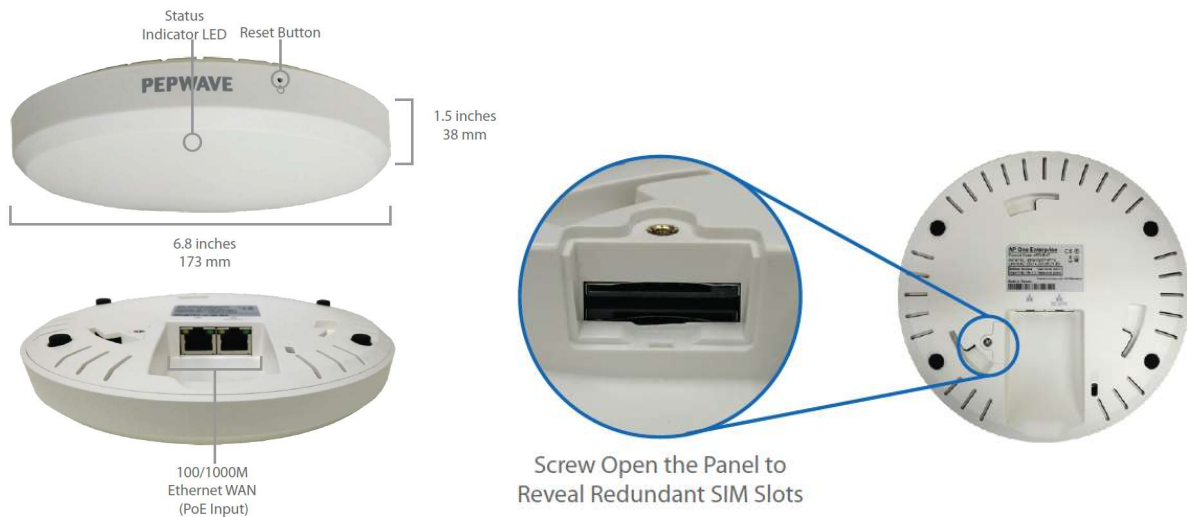
| Status Indicators | | |
|-------------------|--------------|---------------------|
| Status | OFF | System initializing |
| | Red | Booting up or busy |
| | Blinking red | Boot up error |
| | Green | Ready |

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

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

4.15 MAX Hotspot

4.15.1 Panel Appearance

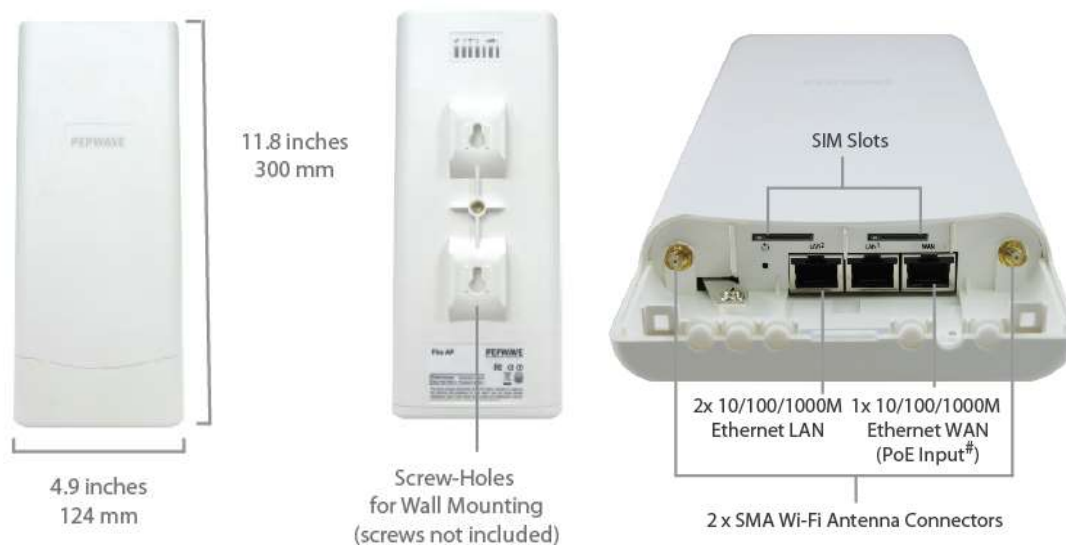


4.15.2 LED Indicators

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

4.16 MAX BR1/2 IP55

4.16.1 Panel Appearance



4.16.2 LED Indicators

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

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

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

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

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

4.17 MAX On-The-Go

4.17.1 Panel Appearance



4.17.2 LED Indicators

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

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

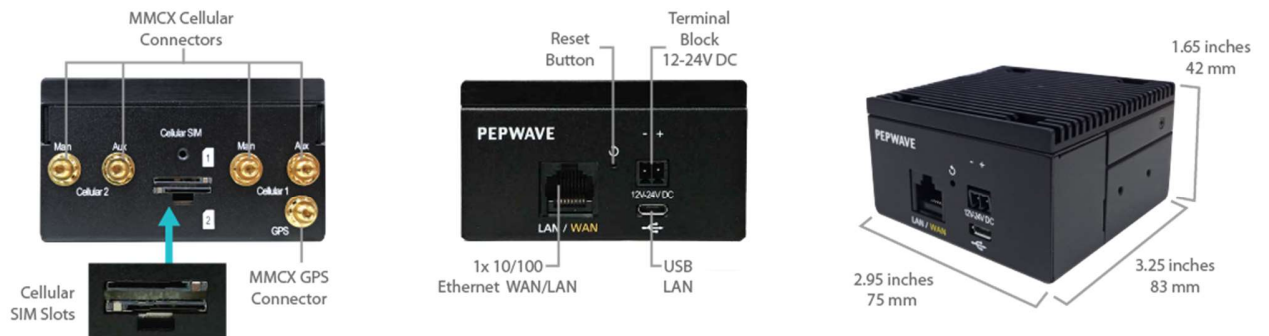
| Wi-Fi Indicators | | |
|------------------|-------|----------------------|
| Wi-Fi | OFF | Disconnected from AP |
| | Green | Connected to AP |

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

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

4.18 SpeedFusion Engine

4.18.1 Panel Appearance



5 Advanced Feature Summary

5.1 Drop-in Mode and LAN Bypass: Transparent Deployment



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

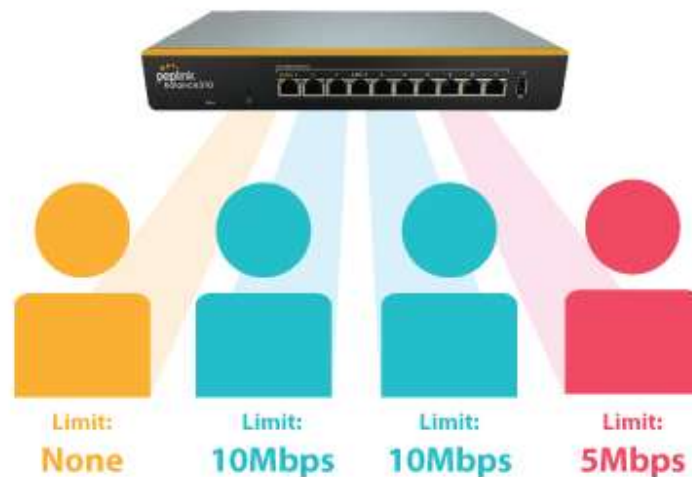
Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

5.2 QoS: Clearer VoIP



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

5.3 Per-User Bandwidth Control



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

5.4 High Availability via VRRP



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

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

5.5 USB Modem and Android Tethering



For increased WAN diversity, plug in a USB LTE modem as backup. 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)

5.6 Built-In Remote User VPN Support



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

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

5.7 SIM-card USSD support



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

6 Installation

The following section details connecting Pepwave routers to your network.

6.1 Preparation

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

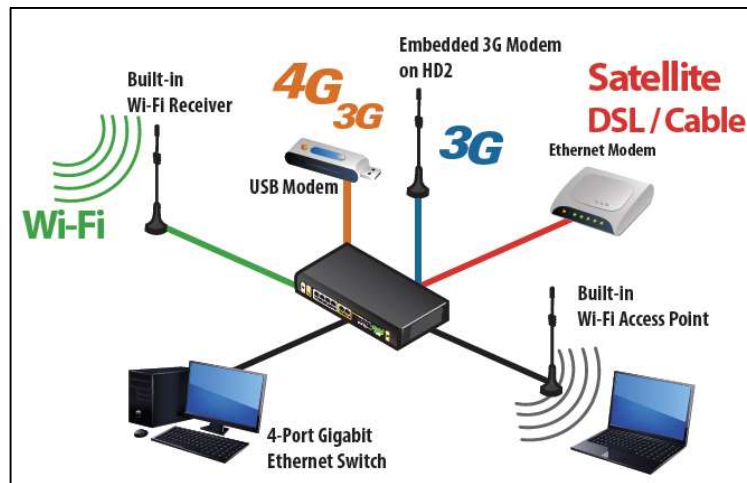
- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
 - **Ethernet WAN:** A 10/100/1000BaseT UTP cable with RJ45 connector
 - **USB:** A USB modem
 - **Embedded modem:** A SIM card for GSM/HSPA service
 - **Wi-Fi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

6.2 Constructing the Network

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

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

The following figure schematically illustrates the resulting configuration:



6.3 Configuring the Network Environment

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

- LAN configuration
For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.
For advanced configuration, go to **Section 9, Configuring the LAN Interface(s)**.
- WAN configuration
For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.
For advanced configuration, go to **Section 9.2, Captive Portal**.

7 Mounting the Unit

7.1 Wall Mount

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

The Pepwave MAX BR1 requires four screws for wall mounting.

7.2 Car Mount

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



7.3 IP67 Installation Guide

Installation instructions for IP67 devices can be found here:
http://download.peplink.com/manual/IP67_Installation_Guide.pdf

8 Connecting to the Web Admin Interface

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

http://192.168.50.1

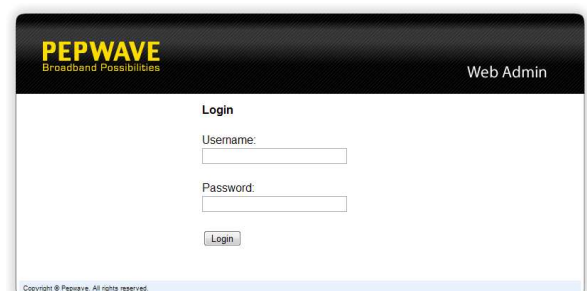
(This is the default LAN IP address for Pepwave routers.)

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


Username: admin

Password: admin

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



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

WAN Connection Status 

Priority 1 (Highest)

1 WAN 1

Connected

Details

2 WAN 2

Connected

Details

Priority 2

1 Cellular 1

No SIM Card Detected [Reload SIM](#)

Details

2 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:

12%

Throughput:

0.0 Mbps

0.1 Mbps

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

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

Important Note

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

9 Configuring the LAN Interface(s)

9.1 Basic Settings

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

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

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

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

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

IP Settings

IP Address

192.168.50.1

255.255.255.0 (/24) ▾

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

| Network Settings | |
|--------------------|-------------------------------------|
| Name | <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. |

| Drop-In Mode Settings | |
|---|--|
| Enable | <input checked="" type="checkbox"/> |
| WAN for Drop-In Mode | <input type="button" value="WAN 1"/> |
| Share Drop-In IP | <input checked="" type="checkbox"/> |
| Shared IP Address | <input type="text"/> 255.255.255.0 (/24) |
| WAN Default Gateway | <input type="text"/> <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) <input type="text"/> - <input type="text"/> <input type="button" value="↓"/> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <input type="button" value="Delete"/> |
| WAN DNS Servers | DNS server 1: <input type="text"/> DNS server 2: <input type="text"/> |
| <p>NOTE: The DHCP Server Settings will be overwritten.</p> <p>The following WAN 1 settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.</p> <p>The PPTP Server will be disabled.</p> <p>Tip: please review the DNS Forwarding setting under the Service Forwarding section.</p> | |

Drop-in Mode Settings

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

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



| Layer 2 PepVPN Bridging | |
|---|---|
| PepVPN Profiles to Bridge |  Connection 1 |
| Spanning Tree Protocol | <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. |
| Spanning Tree Protocol | Click the box will enable STP for this layer 2 profile bridge. |
| Override IP Address when bridge connected | <p>Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.</p> <p>If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.</p> |

| DHCP Server Settings | | | | | | | | | | | |
|-------------------------|-------------|---|---|--------|-------------|-------------------------|--|-----|--|--|---|
| DHCP Server | | <input checked="" type="checkbox"/> Enable | | | | | | | | | |
| IP Range | | 192.168.50.10 - 192.168.50.250 | | | | | | | | | |
| Subnet Mask | | 255.255.255.0 (/24) | | | | | | | | | |
| Lease Time | | 1 Days 0 Hours 0 Mins | | | | | | | | | |
| DNS Servers | | <input checked="" type="checkbox"/> Assign DNS server automatically | | | | | | | | | |
| WINS Server | | <input checked="" type="checkbox"/> Assign WINS server <input checked="" type="radio"/> Built-in <input type="radio"/> External | | | | | | | | | |
| BOOTP | | <input checked="" type="checkbox"/> Server IP Address: <input type="text"/> Boot File: <input type="text"/> Server Name: <input type="text"/> (Optional) | | | | | | | | | |
| Extended DHCP Option | | <table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;">Add</td> </tr> </tbody> </table> | | Option | Value | No Extended DHCP Option | | Add | | | |
| Option | Value | | | | | | | | | | |
| No Extended DHCP Option | | | | | | | | | | | |
| Add | | | | | | | | | | | |
| DHCP Reservation | | <table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td style="text-align: center;">+</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 DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN. |
| IP Range & Subnet Mask | These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server. |
| Lease Time | This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required. |

| | |
|-----------------------------|--|
| DNS Servers | <p>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.</p> |
| WINS Server | <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 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 | Auto |

| LAN Physical Settings | |
|-----------------------|--|
| Speed | This is the port speed of the LAN interface. It should be set to the same speed as the connected device to avoid port negotiation problems. When a static speed is |

set, you may choose whether to advertise its speed to the peer device. **Auto** is selected by default. You can choose not to advertise the port speed if the port has difficulty negotiating with the peer device.

Static Route Settings

Static Route

?

| Destination Network | Subnet Mask | Gateway | |
|---------------------|---------------------|---------|--------------|
| | 255.255.255.0 (/24) | | <div>+</div> |

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**.

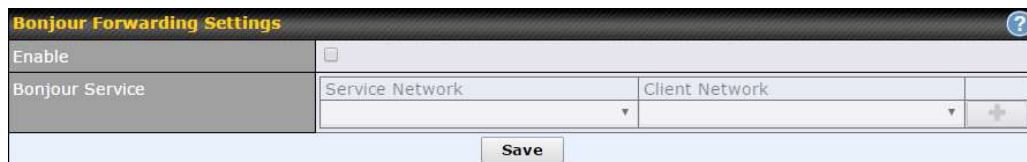
| DNS Proxy Settings | | | | | | | | | | | | | | | | | | | | | | |
|--|---|--|------------|----------------|--------------------------------|-----------|--------------------------------|--|------------------------------------|--|-------------------------------------|--|-------------------------------------|--|------------------------------|--|------------|--|---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



| 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  . |

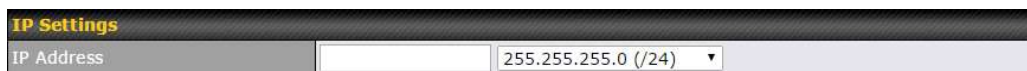
To enable VLAN configuration, click the  button in the **IP Settings** section.



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.



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 | <input type="text"/> Days <input type="text"/> Hours <input type="text"/> 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">No Extended DHCP Option</td> </tr> <tr> <td colspan="2">Add</td> </tr> </tbody> </table> | | | Option | Value | No Extended DHCP Option | | Add | | | |
| Option | Value | | | | | | | | | | |
| No Extended DHCP Option | | | | | | | | | | | |
| Add | | | | | | | | | | | |
| DHCP Reservation | <input type="checkbox"/> | <table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td>+</td> </tr> </tbody> </table> | | Name | MAC Address | Static IP | | | | | + |
| Name | MAC Address | Static IP | | | | | | | | | |
| | | | + | | | | | | | | |


DHCP Server Settings

| | |
|-----------------------------------|---|
| DHCP Server | <p>When this setting is enabled, the Pepwave router's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collisions on the LAN.</p> <p>To enable DHCP bridge relay, please click the  icon on this menu item.</p> |
| IP Range & Subnet Mask | These settings allocate a range of IP address that will be assigned to LAN computers by the Pepwave router's DHCP server. |
| Lease Time | This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of Lease Time , the assigned IP address will no longer be valid and the IP address assignment must be renewed. |
| DNS Servers | This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered. |
| WINS Servers | This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP WINS Servers setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at Status>WINS Clients . |
| BOOTP | Check this box to enable BOOTP on older networks that still require it. |
| Extended DHCP Option | In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the Add button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only. |
| DHCP Reservation | <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.

9.2 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"/> | Auto <input type="text"/> | <input checked="" type="checkbox"/> | Trunk <input type="text"/> | Any <input type="text"/> |
| LAN Port 2 | <input checked="" type="checkbox"/> | | | Trunk <input type="text"/> | Any <input type="text"/> |
| LAN Port 3 | <input checked="" type="checkbox"/> | | | Trunk <input type="text"/> | Any <input type="text"/> |
| LAN Port 4 | <input checked="" type="checkbox"/> | | | Trunk <input type="text"/> | Any <input type="text"/> |

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.

9.3 Captive Portal

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

| Captive Portal Settings | |
|-------------------------|---|
| Enable | <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"/> <input type="button" value="+"/> |
| Allowed Clients | <input type="text" value="MAC / IP Address"/> <input type="button" value="+"/> |
| Splash Page | <input checked="" type="radio"/> Built-in <input type="radio"/> External, URL: <input type="text" value="http://"/> |

Captive Portal Settings

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.

This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:



RADIUS Server



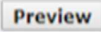

| | | | |
|-----------------------------|--------------------------|---|----------------|
| Authentication | RADIUS Server ▾ | | |
| Auth Server | <input type="text"/> | Port 1812 | Default |
| Auth Server Secret | <input type="text"/> | <input checked="" type="checkbox"/> Hide Characters | |
| CoA-DM | <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 | |

Fill in the necessary information to complete your connection to the server and enable authentication.

LDAP Server

This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:

| | |
|-------------------------|---|
| | <div> <div>Authentication</div> <div>LDAP Server</div> </div> <div> <div>LDAP Server</div> <div> <input type="text"/> <div>Port 389</div> <div>Default</div> </div> <div><input type="checkbox"/> Use DN/Password to bind to LDAP Server</div> </div> <div> <div>Base DN</div> <div><input type="text"/></div> </div> <div> <div>Base Filter</div> <div><input type="text"/></div> </div> |
| | Fill in the necessary information to complete your connection to the server and enable authentication. |
| Access Quota | Set a time and data cap to each user's Internet usage. |
| Quota Reset Time | This menu determines how your usage quota resets. Setting it to Daily will reset it at a specified time every day. Setting a number of minutes after quota reached establish a timer for each user that begins after the quota has been reached. |
| Allowed Networks | To whitelist a network, enter the domain name / IP address here and click  . To delete an existing network from the list of allowed networks, click the  button next to the listing. |
| Splash Page | Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define. |

The **Portal Customization** menu has two options:  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 | |
| Terms & Conditions | [Use default Terms & Conditions] |
| 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. |

10 Configuring the WAN Interface(s)

WAN Interface settings are located at **Network>WAN**. To reorder WAN priority, drag on the appropriate WAN by holding the left mouse button, move it to the desired priority (the first one would be the highest priority, the second one would be lower priority, and so on), and drop it by

releasing the mouse button.



The image shows two screenshots of a network configuration interface. The top screenshot is titled "WAN Connection Status" and displays a list of connections organized by priority. Priority 1 (Highest) includes WAN 1 and WAN 2, both marked as "Connected" with green status icons and "Details" buttons. Priority 2 includes Cellular 1 and Cellular 2, both marked as "No SIM Card Detected" with red status icons and "Reload SIM" links, along with "Details" buttons. Priority 3 is currently empty, with a prompt to "Drag desired (Priority 3) connections here". Below the priorities is a "Disabled" section containing a "Wi-Fi WAN" connection, which is marked as "Disabled" with a grey status icon and a "Details" button. The bottom screenshot shows the "IPv6" settings, which are currently "Disabled" with a red status icon and a "Details" button.

| WAN Connection Status | | |
|--|---|---------|
| Priority 1 (Highest) | | |
| 1 WAN 1 | Connected | Details |
| 2 WAN 2 | Connected | Details |
| Priority 2 | | |
| 1 Cellular 1 | No SIM Card Detected Reload SIM | Details |
| 2 Cellular 2 | No SIM Card Detected Reload SIM | Details |
| Priority 3 | | |
| Drag desired (Priority 3) connections here | | |
| Disabled | | |
| Wi-Fi WAN | Disabled | Details |

| IPv6 | |
|----------|---------|
| Disabled | Details |

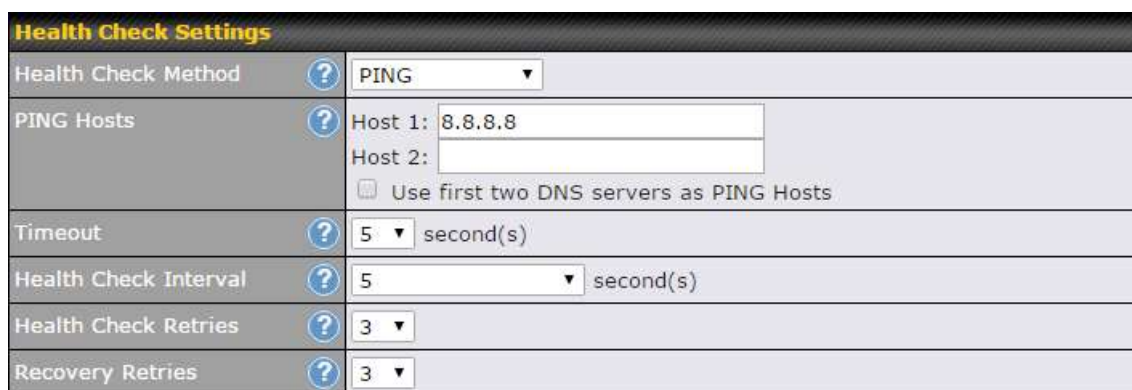
To disable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it the **Disabled** row, and drop it by releasing the mouse button.

You can also set priorities on the **Dashboard**. Click the **Details** button in the corresponding row to modify the connection setting.

Important Note

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

10.1 Ethernet WAN



The image shows the "Health Check Settings" interface. It contains several configuration fields: "Health Check Method" is set to "PING"; "PING Hosts" shows "Host 1" as "8.8.8.8" and "Host 2" as an empty field, with a checkbox for "Use first two DNS servers as PING Hosts"; "Timeout" is set to "5 second(s)"; "Health Check Interval" is set to "5 second(s)"; "Health Check Retries" is set to "3"; and "Recovery Retries" is set to "3". Each field has a help icon (question mark) to its left.

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

| Health Check Settings | |
|------------------------------|--|
| Health Check Method | <p>This field specifies the Health Check method to be used for this WAN connection.</p> <ul style="list-style-type: none"> • Disabled - The WAN connection is always considered to be up and will not be treated as down for any IP routing errors. • 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 | <p>If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.</p> |
| Health Check Interval | <p>This is the time interval between each health check test.</p> |
| Health Check Retries | <p>This is the number of consecutive check failures before treating a connection as down.</p> |
| Recovery Retries | <p>This is the number of responses required after a health check failure before treating a connection as up again.</p> |

| 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 Allowance Monitor | Check the box <i>Enable</i> 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 | <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 | |
|-------------------------------|--|
| Additional Public IP Address | <div> <div>IP Address</div> <div>Subnet Mask 255.255.255.0 (/24)</div> <div>↓</div> <div></div> <div>Delete</div> </div> |

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

| Dynamic DNS Settings | |
|------------------------------|------------|
| Dynamic DNS Service Provider | Disabled ▼ |



| Dynamic DNS Settings | |
|---|---|
| <p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> | |
| Dynamic DNS Service Provider | <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. |

10.1.1 DHCP Connection

There are four possible connection methods:

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

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

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

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

10.1.2 Static IP Connection

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

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

Static IP Settings

Routing Mode

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

**IP Address /
Subnet Mask /
Default**

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.



Gateway

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.

10.1.3 PPPoE Connection

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

| | |
|-------------------------|--|
| Connection Method |  PPPoE |
| Routing Mode |  <input checked="" type="radio"/> NAT |
| IP Address | 10.88.3.158 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.88.3.253 |
| PPPoE User Name | <input type="text"/> |
| PPPoE Password | <input type="password"/> |
| Confirm PPPoE Password | <input type="password"/> |
| Service Name (Optional) | <input type="text"/> <small>Leave it blank unless it is provided by ISP</small> |
| IP Address (Optional) | <input type="text"/> <small>Leave it blank unless it is provided by ISP</small> |
| 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.

| | |
|---------------------------------|---|
| 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 | <p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)</p> <p>When Use the following DNS server address(es) is selected, you can enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p> |

10.2 Cellular WAN



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


Connection Details ✕

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


| Cellular Status | |
|-----------------|--|
| 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. |

| WAN Connection Settings | |
|---------------------------------|--|
| WAN Connection Name | Cellular 1 Default |
| Operating Schedule | Always on ▼ |
| Subnet Selection ? | <input checked="" type="radio"/> Auto <input type="radio"/> Force /31 Subnet |
| Routing Mode ? | <input checked="" type="radio"/> NAT |
| DNS Servers | <input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/> |

WAN Connection Settings

| | |
|----------------------------|---|
| WAN Connection Name | Enter a name to represent this WAN connection. |
| Operating Schedule | Click the drop-down menu to apply a time schedule to this interface if needed. |
| Subnet Selection | <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> |
| Routing Mode | This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (network address translation) or IP Forwarding . Click the  button to enable IP forwarding. |
| DNS Servers | <p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)</p> <p>When Use the following DNS server address(es) is selected, you can enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p> |

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






| Cellular Settings | |
|---------------------------|---|
| SIM Card | Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards. |
| Preferred SIM Card | If both cards were enabled on the above field, then you can designate the priority of the SIM card slots here. |
| 3G/2G | This drop-down menu allows restricting cellular to particular band. Click the  |

| | |
|---|---|
| | button to enable the selection of specific bands. |
| Authentication | Choose from PAP Only or CHAP Only to use those authentication methods exclusively. Select Auto to automatically choose an authentication method. |
| Data Roaming | This checkbox enables data roaming on this particular SIM card. Please check your service provider's data roaming policy before proceeding. |
| Operator Settings | This setting applies to 3G/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems. This allows you to configure the APN settings of your connection. If Auto is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select Custom to enter your carrier's APN , Login , Password , and Dial Number settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto . |
| APN / Login / Password / SIM PIN | When Auto is selected, the information in these fields will be filled automatically. Select Custom to customize these parameters. The parameter values are determined by and can be obtained from the ISP. |
| Bandwidth Allowance Monitor | Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken. |
| Action | If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts. |
| Start Day | This option allows you to define which day of the month each billing cycle begins. |
| Monthly Allowance | This field is for defining the maximum bandwidth usage allowed for the WAN connection each month. |

| General Settings | |
|------------------------------|--|
| Independent from Backup WANs | <input type="checkbox"/> |
| Standby State | <input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected |
| Idle Disconnect | <input type="checkbox"/> |

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 | |
|--|--|
| <p>Dynamic DNS Service Provider</p> | <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 <p>Select Disabled to disable this feature. See Section 9.5 for configuration details.</p> |

| | | | |
|-----|---|------|---------|
| MTU |  | 1428 | Default |
|-----|---|------|---------|

| MTU | |
|-------------------|--|
| <p>MTU</p> | <p>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.</p> |



10.3 Wi-Fi WAN

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

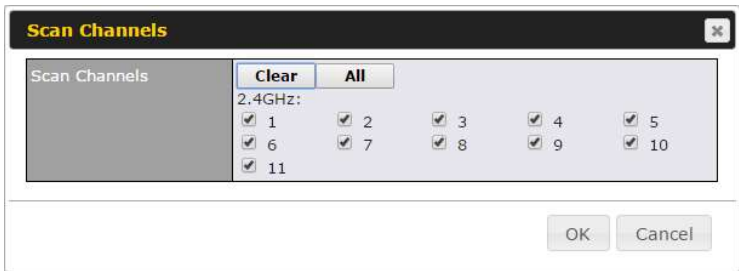

| WAN Connection Settings | |
|--|---|
| WAN Connection Name | Wi-Fi WAN Default |
| Operating Schedule | Always on ▼ |
| Independent from Backup WANs  |  |
| Standby State | <input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected |
| MTU  | <input type="radio"/> Auto <input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

| WAN Connection Settings | |
|-----------------------------------|---|
| <p>WAN Connection Name</p> | <p>Enter a name to represent this WAN connection.</p> |

| | |
|-------------------------------------|---|
| 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 | 20 MHz ▼ |
| Channel Selection | <input checked="" type="radio"/> Auto <input type="radio"/> Custom |
| Data Rate | <input checked="" type="radio"/> Auto <input type="radio"/> Fixed |
| Output Power | Max ▼ <input type="checkbox"/> Boost |
| Roaming | <input type="checkbox"/> |
| Connect to Any Open Mode AP  | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Beacon Miss Counter | 5 |

| Wi-Fi WAN Settings | |
|--------------------------|---|
| Channel Width | Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz |
| Channel Selection | Determine whether the channel will be automatically selected. If you select custom, the following table will appear: |

| | |
|--|---|
|  | |
| Data Rate | Selecting Auto will enable the router to automatically determine the best data rate, while manually selecting a rate will force devices to connect using the fixed rate. |
| Output Power | If you are setting up a network with many Wi-Fi devices in close proximity, then you can configure the output power here. Click the “boost” button for additional power. However, with that option ticked, output power may 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 | <p>If Error! Reference source not found. is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance.</p> <p>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.</p> |
| 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 | ? | DNS Lookup |
| Health Check DNS Servers | ? | Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers |

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

Health Check DNS Servers

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

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

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

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

Health Check Method: HTTP

| | | |
|---------------------|---|---|
| Health Check Method | ? | HTTP |
| URL 1 | ? | http:// <input type="text"/> Matching String: <input type="checkbox"/> |
| URL 2 | ? | 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 | |
| Password | |
| Confirm Password | |
| Update All Hosts | <input type="checkbox"/> |
| Hosts / IDs | |

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

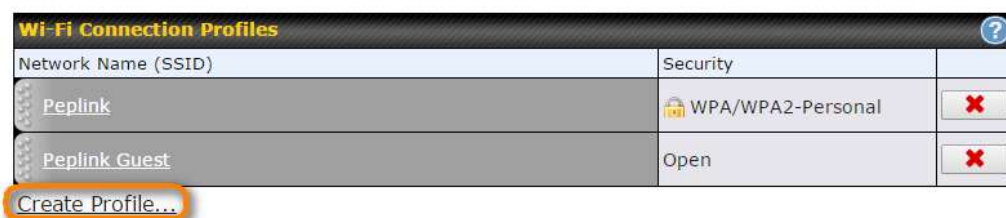
In order to use dynamic DNS services, appropriate hostname registration(s), as well as a valid account with a supported dynamic DNS service provider, are required.

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.

10.3.1 Creating Wi-Fi Connection Profiles

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



This will open a window similar to the one shown below

Create Wi-Fi Connection Profile

Wi-Fi Connection

| | |
|---------------------|---|
| Network Name (SSID) | <input type="text"/> |
| Security | Open |
| IP Address | <input checked="" type="radio"/> Obtain an IP address automatically <input type="radio"/> Static |

OK

Cancel

Wi-Fi Connection Profile Settings

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------------------------|--|----------|------|----------|-----|----------------|--|----------|-------------------|------------|--|----------|---------------------|----------|----------------------|----------|----------------------|------------------|----------------------|------------|------|--------------------|----------|-----------------------------------|---|
| Type | Select whether the network will connect automatically or manually. | | | | | | | | | | | | | | | | | | | | | | | | |
| Network Name (SSID) | Enter a name to represent this Wi-Fi connection. | | | | | | | | | | | | | | | | | | | | | | | | |
| | This option allows you to select which security policy is used for this wireless network. | | | | | | | | | | | | | | | | | | | | | | | | |
| | Available options: | | | | | | | | | | | | | | | | | | | | | | | | |
| | <ul style="list-style-type: none"> Open <table> <tr> <td>Security</td> <td>Open</td> </tr> </table> WEP <table> <tr> <td>Security</td> <td>WEP</td> </tr> <tr> <td>Encryption Key</td> <td> <input type="text"/> <input checked="" type="checkbox"/> Hide Characters </td> </tr> </table> WPA/WPA2 – Personal <table> <tr> <td>Security</td> <td>WPA/WPA2-Personal</td> </tr> <tr> <td>Shared Key</td> <td> <input type="text"/> <input checked="" type="checkbox"/> Hide Characters </td> </tr> </table> WPA/WPA2 – Enterprise <table> <tr> <td>Security</td> <td>WPA/WPA2-Enterprise</td> </tr> <tr> <td>Login ID</td> <td><input type="text"/></td> </tr> <tr> <td>Password</td> <td><input type="text"/></td> </tr> <tr> <td>Confirm Password</td> <td><input type="text"/></td> </tr> <tr> <td>EAP Method</td> <td>PEAP</td> </tr> <tr> <td>EAP Phase 2 Method</td> <td>EAP/CHAP</td> </tr> <tr> <td>EAP outer authentication identity</td> <td> <input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/> </td> </tr> </table> | Security | Open | Security | WEP | Encryption Key | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | Security | WPA/WPA2-Personal | Shared Key | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | Security | WPA/WPA2-Enterprise | Login ID | <input type="text"/> | Password | <input type="text"/> | Confirm Password | <input type="text"/> | EAP Method | PEAP | EAP Phase 2 Method | EAP/CHAP | EAP outer authentication identity | <input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/> |
| Security | Open | | | | | | | | | | | | | | | | | | | | | | | | |
| Security | WEP | | | | | | | | | | | | | | | | | | | | | | | | |
| Encryption Key | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | | | | | | | | | | | |
| Security | WPA/WPA2-Personal | | | | | | | | | | | | | | | | | | | | | | | | |
| Shared Key | <input type="text"/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | | | | | | | | | | | | | |
| Security | WPA/WPA2-Enterprise | | | | | | | | | | | | | | | | | | | | | | | | |
| Login ID | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Password | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Confirm Password | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| EAP Method | PEAP | | | | | | | | | | | | | | | | | | | | | | | | |
| EAP Phase 2 Method | EAP/CHAP | | | | | | | | | | | | | | | | | | | | | | | | |
| EAP outer authentication identity | <input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Security | | | | | | | | | | | | | | | | | | | | | | | | | |

10.4 WAN Health Check

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

| Health Check Settings | |
|---|--|
| Method | This setting specifies the health check method for the WAN connection. This value can be configured as Disabled , PING , DNS Lookup , or HTTP . The default method is DNS Lookup . For mobile Internet connections, the value of Method can be configured as Disabled or SmartCheck . |
| Health Check Disabled | |
| Health Check Method | <div>Disabled</div> <div>Health Check disabled. Network problem cannot be detected.</div> |
| 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 | <div>PING</div> |
| PING Hosts | <div>Host 1: <input type="text"/></div> <div>Host 2: <input type="text"/></div> <div><input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts</div> |
| 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 | <div>DNS Lookup</div> |
| Health Check DNS Servers | <div>Host 1: <input type="text"/></div> <div>Host 2: <input type="text"/></div> <div><input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers</div> <div><input type="checkbox"/> Include public DNS servers</div> |
| 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

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

Other Health Check Settings

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

Automatic Public DNS Server Check on DNS Test Failure

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

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

10.5 Dynamic DNS Settings

Pepwave routers are capable of registering the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address from the external, even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

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

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

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

| Dynamic DNS Settings | |
|-------------------------------------|---|
| Dynamic DNS | <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 • Others... <p>Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.</p> <p>Select Disabled to disable this feature.</p> |
| 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 |
|--|
| <p>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.</p> |

11 Advanced Wi-Fi Settings

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

| AP Settings | |
|---------------------|---|
| SSID | 2.4 GHz 5 GHz Integrated AP supports 2.4 GHz only. <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> 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 | Untagged LAN (No VLAN) ▼ |
| Operating Schedule | Always on ▼ |
| Beacon Rate | 1 Mbps ▼ 6 Mbps will be used for 5 GHz radio |
| Beacon Interval | 100 ms ▼ |
| DTIM | 1 <input type="button" value="Default"/> |
| RTS Threshold | 0 <input type="button" value="Default"/> |
| Fragmentation Threshold | 0 (0: Disable) <input type="button" value="Default"/> |
| Distance / Time Converter | 4050 m <small>Note: Input distance for recommended values</small> |
| Slot Time | <input type="radio"/> Auto <input checked="" type="radio"/> Custom 9 <input type="text"/> μs <input type="button" value="Default"/> |
| ACK Timeout | 48 <input type="text"/> μs <input type="button" value="Default"/> |
| Frame Aggregation | <input type="checkbox"/> |

| Advanced AP Settings | |
|---|---|
| Management VLAN ID | <p>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.</p> <p>NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller.</p> |
| Operating Schedule | Choose from the schedules that you have defined in System>Schedule. Select the schedule for the integrated AP to follow from the drop-down menu. |
| Beacon Rate ^A | This option is for setting the transmit bit rate for sending a beacon. By default, 1Mbps is selected. |
| Beacon Interval ^A | This option is for setting the time interval between each beacon. By default, 100ms is selected. |
| DTIM ^A | This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to 1 ms . |
| RTS Threshold ^A | The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500. |
| Fragmentation Threshold ^A | This setting determines the maximum size of a packet before it gets fragmented into multiple pieces. |
| Distance / Time Convertor | Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout. |

| | |
|---------------------------------------|--|
| Slot Time ^A | This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to 9 μs . |
| ACK Timeout ^A | This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 μs . |
| Frame Aggregation ^A | This option allows you to enable frame aggregation to increase transmission throughput. |

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

| Web Administration Settings (on External AP) | |
|--|---|
| Enable | <input checked="" type="checkbox"/> |
| Web Access Protocol | <input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS |
| Management Port | 443 |
| HTTP to HTTPS Redirection | <input checked="" type="checkbox"/> |
| Admin Username | admin |
| Admin Password | 601202b1afc6 <input type="button" value="Generate"/> |

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

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

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

| Wi-Fi WAN Settings | |
|----------------------|--|
| Channel Width | Available options are 20/40 MHz and 20 MHz . Default is 20/40 MHz , which allows both widths to be used simultaneously. |
| Bit Rate | This option allows you to select a specific bit rate for data transfer over the device's Wi-Fi network. By default, Auto is selected. |
| Output Power | This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – Max , High , Mid , and Low . The actual output power will be bound by the regulatory limits of the selected country. Note that selecting the Boost option may cause the MAX's radio output to exceed local regulatory limits. |

12 MediaFast Configuration

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

12.1 Setting Up MediaFast Content Caching

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

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

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


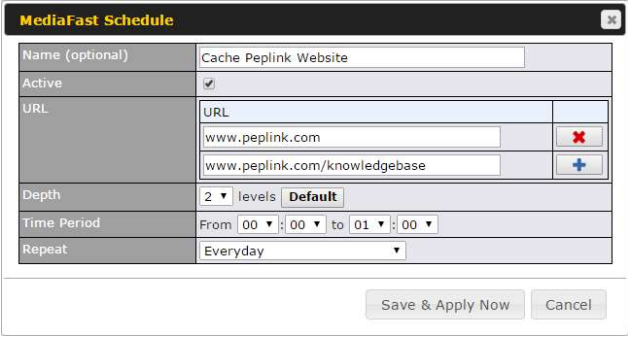
12.2 Scheduling Content Prefetching

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

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

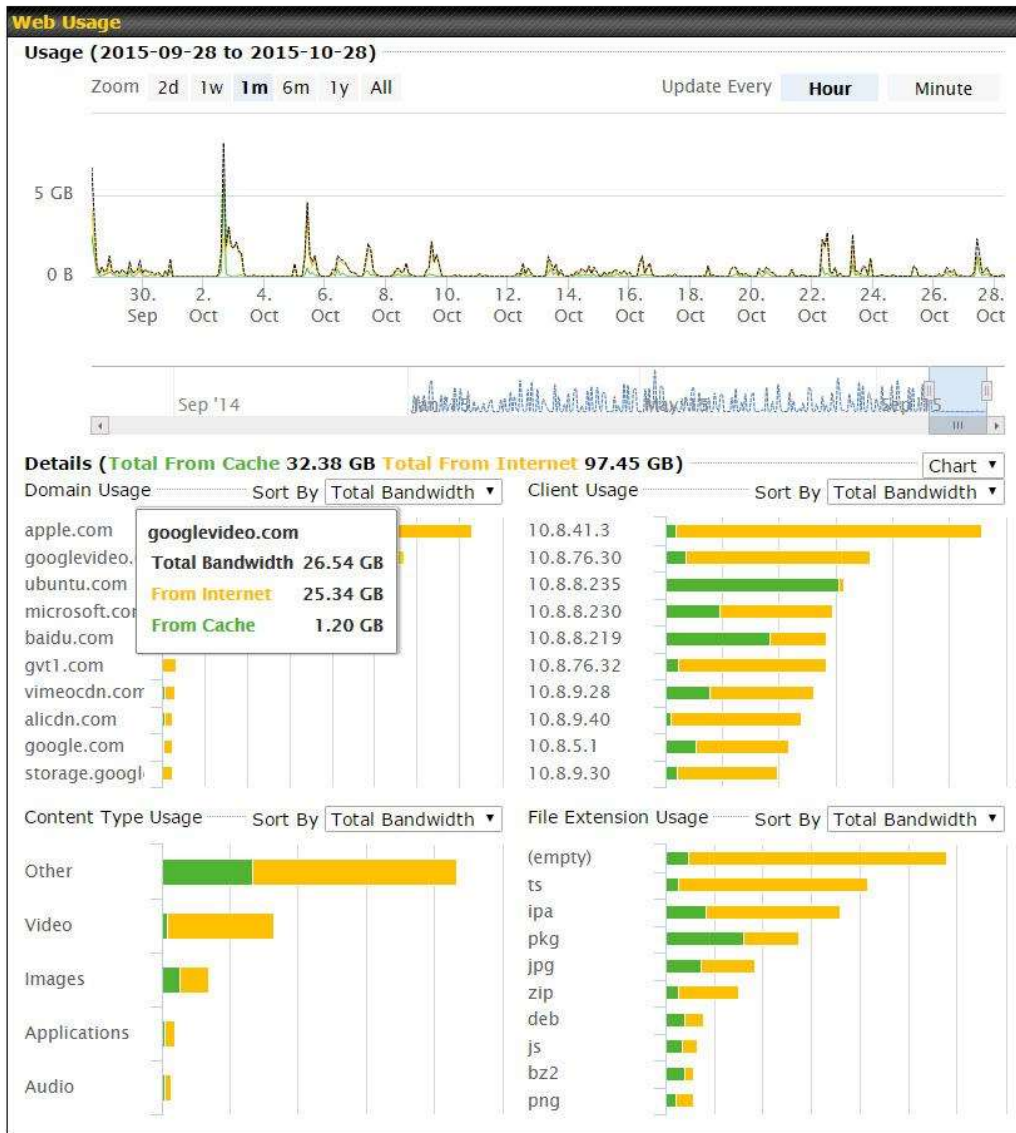
| Tools | |
|---------------------------------|----------------------------------|
| Clear Web Cache | Clear Statistics |

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

| | |
|-------------------------|---|
| | To delete a scheduled download, click  . |
| | Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear: |
| New Schedule |  <p>The screenshot shows a 'MediaFast Schedule' dialog box with the following fields: 'Name (optional)' set to 'Cache Peplink Website', 'Active' checked, 'URL' containing 'www.peplink.com' and 'www.peplink.com/knowledgebase' (with a red X icon next to the first entry and a blue plus icon next to the second), 'Depth' set to '2 levels' and 'Default', 'Time Period' set to 'From 00:00 to 01:00', and 'Repeat' set to 'Everyday'. At the bottom are 'Save & Apply Now' and 'Cancel' buttons.</p> |
| | Simply provide the requested information to create your schedule. |
| Clear Web Cache | To clear all cached content, click this button. Note that this action cannot be undone. |
| Clear Statistics | To clear all prefetch and status page statistics, click this button. |

12.3 Viewing MediaFast Statistics

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



13 Bandwidth Bonding SpeedFusion™ / PepVPN



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

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

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


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


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




13.1 PepVPN

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


PepVPN with SpeedFusion™





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

| Profile | Remote ID | Remote Address(es) | |
|---|----------------|--------------------|---|
|  FL Office | 8345-5F7A-DE97 | |   |
| <div>New Profile</div> | | | |


Send All Traffic To

No PepVPN profile selected 

PepVPN

Local ID  MAX_HD2_DEF1 

Link Failure Detection

Link Failure Detection Time 

☒ Recommended (Approx. 15 secs)

☐ Fast (Approx. 6 secs)

☐ Faster (Approx. 2 secs)

☐ Extreme (Under 1 sec)

Shorter detection time incurs more health checks and higher bandwidth overhead

Save

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


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

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

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

| PepVPN Profile | | | | | |
|---|--|-----------|----------------|----------------------|----------------------|
| Name | <input type="text"/> | | | | |
| Active | <input checked="" type="checkbox"/> | | | | |
| Encryption | <input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF | | | | |
| Authentication | <input checked="" type="radio"/> Remote ID / Pre-shared Key <input type="radio"/> X.509 | | | | |
| Remote ID / Pre-shared Key | <table border="1"> <tr> <td>Remote ID</td> <td>Pre-shared Key</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </table> | Remote ID | Pre-shared Key | <input type="text"/> | <input type="text"/> |
| Remote ID | Pre-shared Key | | | | |
| <input type="text"/> | <input type="text"/> | | | | |
| NAT Mode | <input type="checkbox"/> | | | | |
| Remote IP Address / Host Names (Optional) | <input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small> | | | | |
| Cost | <input type="text" value="10"/> | | | | |
| Data Port | <input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/> | | | | |
| Bandwidth Limit | <input type="checkbox"/> | | | | |
| WAN Smoothing | <input type="text" value="Off"/> | | | | |
| Use IP ToS | <input type="checkbox"/> | | | | |
| Latency Difference Cutoff | <input type="text" value="500"/> ms | | | | |

| PepVPN Profile Settings | |
|-------------------------|---|
| Name | This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces (). |


| | |
|--|---|
| Active | When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled. |
| Encryption | By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied. |
| Authentication | Select from By Remote ID Only , Preshared Key , or X.509 to specify the method the Peplink Balance will use to authenticate peers. When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field. |
| Remote ID / Pre-shared Key | <p>This optional field becomes available when Remote ID / Pre-shared Key is selected as the Peplink Balance's VPN Authentication method, as explained above. Pre-shared Key defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.</p> <p>Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the  icon next to the "Remote ID / Preshared Key" setting.</p> |
| Remote ID/Remote Certificate | These optional fields become available when X.509 is selected as the Peplink Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the Show Details link below the field. |
| Allow Shared Remote ID | When this option is enabled, the router will allow multiple peers to run using the same remote ID. |
| NAT Mode | Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation. |
| Remote IP Address / Host Names (Optional) | <p>If NAT Mode is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.</p> <p>This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.</p> |
| Cost | <p>Define path cost for this profile.</p> <p>OSPF will determine the best route through the network using the assigned cost. Default: 10</p> |
| Data Port | This field is used to specify a UDP port number for transporting outgoing VPN |

| | |
|----------------------------------|---|
| | data. If Default is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If Custom is selected, enter an outgoing port number from 1 to 65535. |
| Bandwidth Limit | Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above. |
| Cost | Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10 |
| WAN Smoothing^A | Select the degree to which WAN Smoothing will be implemented across your WAN links. |
| Use IP ToS | Checking this button enables the use of IP ToS header field. |
| Latency Difference Cutoff | Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used) |

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

To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>Basic Settings>*LAN Profile Name*** and refer to instructions in section 9.1

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


| WAN Connection Priority | |
|--------------------------------|--|
| WAN Connection Priority | <p>If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to OFF will never be used. Only available WAN connections with the highest priority will be used.</p> <p>To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the  button.</p> |

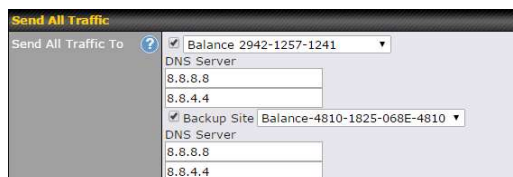


Send All Traffic To


No PepVPN profile selected

Send All Traffic To

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



Send All Traffic

Send All Traffic To  ☒ Balance 2942-1257-1241 ▼

DNS Server
8.8.8.8
8.8.4.4

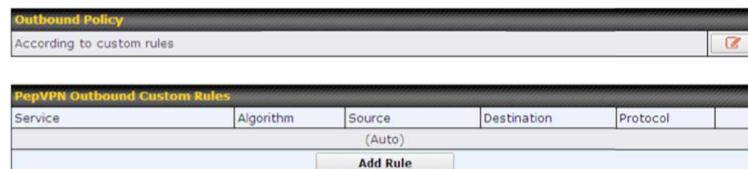
☒ Backup Site Balance-4810-1825-068E-4810 ▼

DNS Server
8.8.8.8
8.8.4.4

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

Outbound Policy/PepVPN Outbound Custom Rules

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



Outbound Policy

According to custom rules 

PepVPN Outbound Custom Rules


| Service | Algorithm | Source | Destination | Protocol |
|-----------------|-----------|--------|-------------|----------|
| (Auto) | | | | |
| Add Rule | | | | |



PepVPN Local ID

Local ID  MAX_HD2_8D1C 

PepVPN Local ID

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

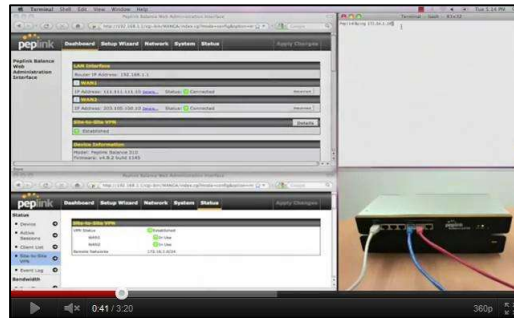
| PepVPN Settings | |
|-----------------------------|--|
| Handshake Port | <input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/> |
| Backward Compatibility | <input checked="" type="radio"/> High (firmware 5.3+) <input type="radio"/> Latest (firmware 6.2+) |
| Link Failure Detection Time | <input type="radio"/> Recommended (Approx. 15 secs) <input type="radio"/> Fast (Approx. 6 secs) <input type="radio"/> Faster (Approx. 2 secs) <input checked="" type="radio"/> Extreme (Under 1 sec) <small>Shorter detection time incurs more health checks and higher bandwidth overhead</small> |

| PepVPN Settings | |
|------------------------------------|---|
| Handshake Port^A | To designate a custom handshake port (TCP), click the custom radio button and enter the port number you wish to designate. |
| Backward Compatibility | Determine the level of backward compatibility needed for PepVPN tunnels. The use of the Latest setting is recommended as it will improve the performance and resilience of SpeedFusion connections. |
| Link Failure Detection Time | <p>The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed.</p> <p>When Recommended (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds.</p> <p>When Fast is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds.</p> <p>When Faster is selected, a health check packet is sent every second, and the expected detection time is two seconds.</p> <p>When Extreme is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.</p> |

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

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

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



<http://youtu.be/TLQgdpPSY88>

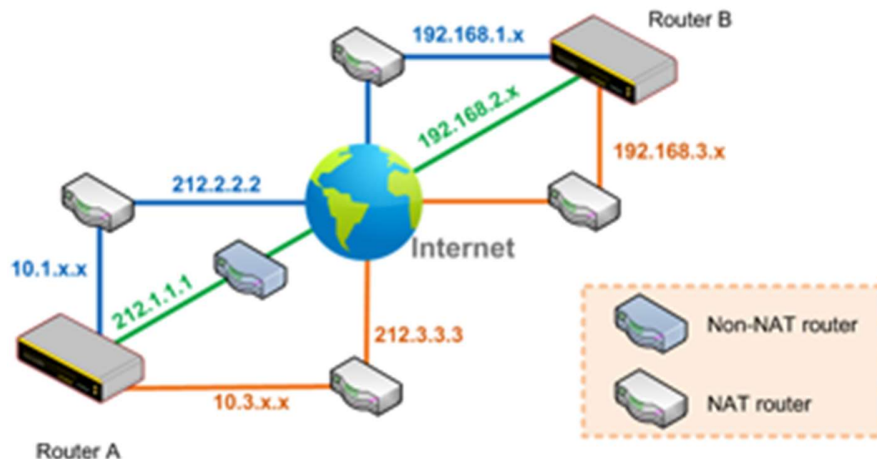
13.2 The Pepwave Router Behind a NAT Router

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

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

If one or more WAN connections on Unit A can accept VPN connections (by means of port forwarding or not), while none of the WAN connections on the peer Unit B can do so, you should enter all of Unit A's public IP addresses or hostnames into Unit B's **Remote IP Addresses / Host Names** field. Leave the field in Unit A blank. With this setting, a SpeedFusion™ connection can be set up and all WAN connections on both sides will be utilized.

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



One of the WANs connected to Router A is non-NAT'd (212.1.1.1). The rest of the WANs connected to Router A and all WANs connected to Router B are NAT'd. In this case, the **Peer IP Addresses / Host Names** field for Router B should be filled with all of Router A's hostnames or

public IP addresses (i.e., 212.1.1.1, 212.2.2.2, and 212.3.3.3), and the field in Router A can be left blank. The two NAT routers on WAN1 and WAN3 connected to Router A should inbound port-forward TCP port 32015 to Router A so that all WANs will be utilized in establishing the VPN.

13.3 SpeedFusion™ Status

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

| SpeedFusion™ | | Status |
|--------------|-------------|--------|
| FL Office | Established | |
| NY Office | Established | |

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

IP Subnets Must Be Unique Among VPN Peers

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

14 IPsec VPN

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

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

14.1 IPsec VPN Settings

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

To configure IPsec VPN on Pepwave devices that support it, navigate to **Advanced>IPsec VPN**.

| | | |
|----------------------|---------|---|
| NAT-Traversal | Enabled |  |
|----------------------|---------|---|

| IPsec VPN Profiles | Remote Networks |
|-------------------------------|------------------------|
| No IPsec VPN Profile Defined. | |
| <div>New Profile</div> | |

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

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

| | |
|--------------------------|---|
| IPsec VPN Profile |  |
|--------------------------|---|

| Name | Profile 1 | | | | | | | | | | | | |
|--|--|----------------------------------|-------------|---|---|---|--|--|---|--|---|--|--------------------------------------|
| Active | <input checked="" type="checkbox"/> | | | | | | | | | | | | |
| Connect Upon Disconnection of | <input checked="" type="checkbox"/> WAN 2 | | | | | | | | | | | | |
| Remote Gateway IP Address / Host Name | 12.12.12.12 | | | | | | | | | | | | |
| Local Networks | <p>Propose the following networks to remote gateway:</p> <p><input type="checkbox"/> 172.16.1.1/24</p> <p><input type="checkbox"/> 172.16.2.1/24</p> <p><input type="checkbox"/> 172.16.3.1/24</p> <p><input checked="" type="checkbox"/> 10.10.0.1/32</p> <p><input checked="" type="checkbox"/> 192.168.10.0/24</p> <p><input checked="" type="checkbox"/> 192.168.11.0/24</p> <p><input type="checkbox"/> <input type="text"/></p> <p>Apply the following NAT policies:</p> <table border="0"> <tr> <td><input checked="" type="checkbox"/> 172.16.1.0/24</td><td><input checked="" type="checkbox"/> 192.168.10.0/24</td></tr> <tr> <td><input checked="" type="checkbox"/> 172.16.2.0/24</td><td><input checked="" type="checkbox"/> 10.10.0.1/32</td></tr> <tr> <td><input checked="" type="checkbox"/> 172.16.3.11/32</td><td><input checked="" type="checkbox"/> 192.168.11.101/32</td></tr> <tr> <td><input checked="" type="checkbox"/> 172.16.3.21/32</td><td><input checked="" type="checkbox"/> 192.168.11.201/32</td></tr> <tr> <td><input type="checkbox"/> Local Network</td><td><input type="checkbox"/> NAT Network</td></tr> </table> | | | <input checked="" type="checkbox"/> 172.16.1.0/24 | <input checked="" type="checkbox"/> 192.168.10.0/24 | <input checked="" type="checkbox"/> 172.16.2.0/24 | <input checked="" type="checkbox"/> 10.10.0.1/32 | <input checked="" type="checkbox"/> 172.16.3.11/32 | <input checked="" type="checkbox"/> 192.168.11.101/32 | <input checked="" type="checkbox"/> 172.16.3.21/32 | <input checked="" type="checkbox"/> 192.168.11.201/32 | <input type="checkbox"/> Local Network | <input type="checkbox"/> NAT Network |
| <input checked="" type="checkbox"/> 172.16.1.0/24 | <input checked="" type="checkbox"/> 192.168.10.0/24 | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> 172.16.2.0/24 | <input checked="" type="checkbox"/> 10.10.0.1/32 | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> 172.16.3.11/32 | <input checked="" type="checkbox"/> 192.168.11.101/32 | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> 172.16.3.21/32 | <input checked="" type="checkbox"/> 192.168.11.201/32 | | | | | | | | | | | | |
| <input type="checkbox"/> Local Network | <input type="checkbox"/> NAT Network | | | | | | | | | | | | |
| Remote Networks | <table border="1"> <thead> <tr> <th>Network</th><th>Subnet Mask</th><th></th></tr> </thead> <tbody> <tr> <td>192.167.11.193</td><td>255.255.255.0 (/24)</td><td><input type="button" value="+"/></td></tr> </tbody> </table> | Network | Subnet Mask | | 192.167.11.193 | 255.255.255.0 (/24) | <input type="button" value="+"/> | | | | | | |
| Network | Subnet Mask | | | | | | | | | | | | |
| 192.167.11.193 | 255.255.255.0 (/24) | <input type="button" value="+"/> | | | | | | | | | | | |
| Authentication | <input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate | | | | | | | | | | | | |
| Mode | <input checked="" type="radio"/> Main Mode (All WANs need to have Static IP) <input type="radio"/> Aggressive Mode | | | | | | | | | | | | |
| Force UDP Encapsulation | <input type="checkbox"/> | | | | | | | | | | | | |
| Preshared Key | <input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters | | | | | | | | | | | | |
| Local ID | <input type="text"/> | | | | | | | | | | | | |
| Remote ID | <input type="text"/> | | | | | | | | | | | | |
| Phase 1 (IKE) Proposal | 1 <input type="text" value="AES-256 & SHA1"/> 2 <input type="text" value="-----"/> | | | | | | | | | | | | |
| Phase 1 DH Group | <input checked="" type="checkbox"/> Group 2: MODP 1024 <input type="checkbox"/> Group 5: MODP 1536 | | | | | | | | | | | | |
| Phase 1 SA Lifetime | <input type="text" value="3600"/> seconds <input type="button" value="Default"/> | | | | | | | | | | | | |
| Phase 2 (ESP) Proposal | 1 <input type="text" value="AES-256 & SHA1"/> 2 <input type="text" value="-----"/> | | | | | | | | | | | | |
| Phase 2 PFS Group | <input checked="" type="radio"/> None <input type="radio"/> Group 2: MODP 1024 <input type="radio"/> Group 5: MODP 1536 | | | | | | | | | | | | |
| Phase 2 SA Lifetime | <input type="text" value="28800"/> seconds <input type="button" value="Default"/> | | | | | | | | | | | | |

| IPsec VPN Settings | |
|--|--|
| Name | This field is for specifying a local name to represent this connection profile. |
| Active | When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled. |
| Connect Upon Disconnection of | Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected. |
| Remote Gateway IP Address / Host Name | Enter the remote peer's public IP address. For Aggressive Mode , this is optional. |
| Local Networks | <p>Enter the local LAN subnets here. If you have defined static routes, they will be shown here.</p> <p>Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allow you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site.</p> <p>Two types of NAT policies can be defined:</p> <p>One-to-One NAT policy: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too.</p> <p>Many-to-One NAT policy: if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 > 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.</p> |
| Remote Networks | Enter the LAN and subnets that are located at the remote site here. |
| Authentication | To access your VPN, clients will need to authenticate by your choice of methods. Choose between the Preshared Key and X.509 Certificate methods of authentication. |
| Mode | Choose Main Mode if both IPsec peers use static IP addresses. Choose Aggressive Mode if one of the IPsec peers uses dynamic IP addresses. |

| | |
|---|---|
| Force UDP Encapsulation | For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox. |
| Pre-shared Key | This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match. |
| Remote Certificate (pem encoded) | Available only when X.509 Certificate is chosen as the Authentication method, this field allows you to paste a valid X.509 certificate. |
| Local ID | In Main Mode , this field can be left blank. In Aggressive Mode , if Remote Gateway IP Address is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN. |
| Remote ID | In Main Mode , this field can be left blank. In Aggressive Mode , if Remote Gateway IP Address is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN. |
| Phase 1 (IKE) Proposal | In Main Mode , this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In Aggressive Mode , only one selection is permitted. |
| Phase 1 DH Group | This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. Group 2: 1024-bit is the default value. Group 5: 1536-bit is the alternative option. |
| Phase 1 SA Lifetime | This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at 3600 seconds. |
| Phase 2 (ESP) Proposal | In Main Mode , this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In Aggressive Mode , only one selection is permitted. |
| Phase 2 PFS Group | Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. None - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. Group 2: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. Group 5: 1536-bit is the third option. |
| Phase 2 SA Lifetime | This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at 28800 seconds. |

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

WAN Connection Priority

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

15 Outbound Policy Management

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

Important Note

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

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

| Outbound Policy | | | | | |
|---|--------------------------|--------|-------------|-----------------|--|
| Custom | | | | | |
| Rules (Drag and drop rows to change rule order) | | | | | |
| Service | Algorithm | Source | Destination | Protocol / Port | |
| HTTPS Persistence | Persistence (Src) (Auto) | Any | Any | TCP 443 | |
| Default | (Auto) | | | | |
| Add Rule | | | | | |

15.1 Outbound Policy

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



There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

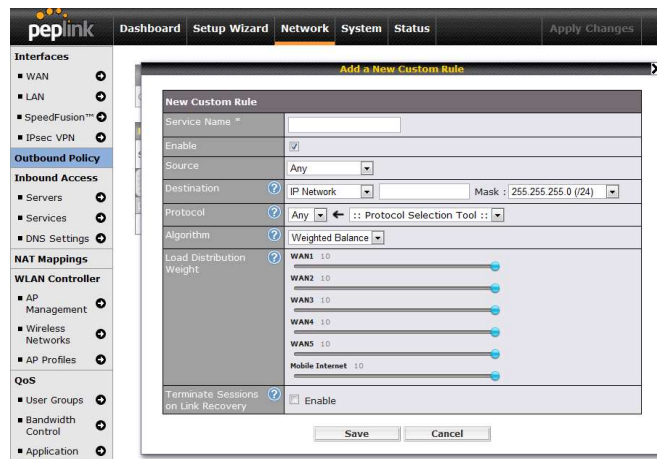
Note that some Pepwave routers provide only the **Send All Traffic To** setting here. See **Section 12.1** for details.

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

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


Tip


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





http://youtu.be/rKH4AS_bQnE


15.2 Custom Rules for Outbound Policy


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


Outbound Policy


Custom


Rules (Drag and drop rows to change rule order)


| Service | Algorithm | Source | Destination | Protocol / Port | |
|-------------------|--------------------------|--------|----------------------------|-----------------|---|
| HTTPS Persistence | Persistence (Src) (Auto) | Any | IP Network 192.168.50.0/24 | TCP 443 |  |
| PepVPN Routes | | | | | |
| Default | (Auto) | | | | |
| Add Rule | | | | | |

Expert Mode


Enabled


15.2.1 Algorithm: Weighted Balance

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

| | |
|----------------------------|---|
| Algorithm ? | Weighted Balance ▼ |
| Load Distribution Weight ? | <div>WAN 1 10</div> <div>WAN 2 10</div> <div>Wi-Fi WAN 10</div> <div>Cellular 1 10</div> <div>Cellular 2 10</div> <div>USB 10</div> |

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

For example, with the following weight settings:

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

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

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

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

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

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

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

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

15.2.2 Algorithm: Persistence

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

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

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

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

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

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

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

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

15.2.3 Algorithm: Enforced

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

| | | |
|---------------------|---|--|
| Algorithm | ? | Enforced |
| Enforced Connection | ? | <div> <div>WAN: WAN 1</div> <div> <div>WAN: WAN 1</div> <div>WAN: WAN 2</div> <div>WAN: Wi-Fi WAN</div> <div>WAN: Cellular 1</div> <div>WAN: Cellular 2</div> <div>WAN: USB</div> <div>VPN: Connection 1</div> </div> </div> |
| | | <div>Save</div> <div>Cancel</div> |

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

15.2.4 Algorithm: Priority

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

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

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

Tip

Configure multiple distribution rules to accommodate different kinds of services.

15.2.5 Algorithm: Overflow

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