Peplink Balance Multi-WAN Bonding Routers

User Manual

For Models:
ONE/20/30/30 LTE/50/210/310/305/380/580/710/1350/2500
MediaFast 200/500/750

Peplink Balance Firmware 6.3

August 2016
# TABLE OF CONTENTS

1  INTRODUCTION AND SCOPE ........................................................................................................ 7  
2  GLOSSARY ................................................................................................................................... 8  
3  PRODUCT COMPARISON CHART ................................................................................................. 9  
4  PRODUCT FEATURES .................................................................................................................... 11  
   4.1 Supported Network Features .................................................................................................. 11  
   4.2 WAN ....................................................................................................................................... 11  
   4.3 LAN ....................................................................................................................................... 11  
   4.4 VPN ....................................................................................................................................... 11  
   4.5 Inbound Traffic Management ............................................................................................... 12  
   4.6 Outbound Policy ..................................................................................................................... 12  
   4.7 AP Controller .......................................................................................................................... 12  
   4.8 QoS ........................................................................................................................................ 12  
   4.9 Firewall .................................................................................................................................. 13  
   4.10 Captive Portal ....................................................................................................................... 13  
   4.11 Other Supported Features .................................................................................................... 14  
5  ADVANCED FEATURE SUMMARY ................................................................................................. 15  
   5.1 Drop-in Mode and LAN Bypass: Transparent Deployment .................................................. 15  
   5.2 QoS: Clearer VoIP .................................................................................................................... 15  
   5.3 Per-User Bandwidth Control ................................................................................................ 16  
   5.4 High Availability via VRRP .................................................................................................... 16  
   5.5 USB Modem and Android Tethering ..................................................................................... 17  
   5.6 Built-In Remote User VPN Support ....................................................................................... 17  
   5.7 LACP NIC Bonding ................................................................................................................ 18  
6  PACKAGE CONTENTS .................................................................................................................... 19  
   6.1 Peplink Balance One ................................................................................................................ 19  
   6.2 Peplink Balance 20/30/30 LTE/50 ....................................................................................... 19  
   6.3 Peplink Balance 210/310 ....................................................................................................... 19  
   6.4 Peplink Balance 305/380/580/710/1350/2500 ................................................................. 19  
   6.5 Peplink MediaFast 200 .......................................................................................................... 19  
   6.6 Peplink MediaFast 500 .......................................................................................................... 19  
7  PEPLINK BALANCE OVERVIEW .................................................................................................. 20  
   7.1 Peplink Balance One ................................................................................................................ 20  
   7.2 Peplink Balance 20 ................................................................................................................ 22  
   7.3 Peplink Balance 30 ................................................................................................................ 24  
   7.4 Peplink Balance 30 LTE ....................................................................................................... 26  
   7.5 Peplink Balance 50 ................................................................................................................ 28  

http://www.peplink.com -2 / 266- Copyright © 2016 Peplink
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>IPSEC VPN</td>
<td>121</td>
</tr>
<tr>
<td></td>
<td>15.1 IPsec VPN Settings</td>
<td>121</td>
</tr>
<tr>
<td></td>
<td>15.2 IPsec Status</td>
<td>125</td>
</tr>
<tr>
<td>16</td>
<td>OUTBOUND POLICY MANAGEMENT</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>16.1 Outbound Policy</td>
<td>127</td>
</tr>
<tr>
<td></td>
<td>16.2 Custom Rules for Outbound Policy</td>
<td>128</td>
</tr>
<tr>
<td>17</td>
<td>INBOUND ACCESS</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>17.1 Definition of Servers on LAN</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>17.2 Definition of Port Forwarding</td>
<td>137</td>
</tr>
<tr>
<td></td>
<td>17.3 Inbound Access Services</td>
<td>139</td>
</tr>
<tr>
<td></td>
<td>17.4 Reverse Lookup Zones</td>
<td>155</td>
</tr>
<tr>
<td></td>
<td>17.5 DNS Record Import Wizard</td>
<td>159</td>
</tr>
<tr>
<td>18</td>
<td>NAT MAPPINGS</td>
<td>163</td>
</tr>
<tr>
<td>19</td>
<td>CAPTIVE PORTAL</td>
<td>165</td>
</tr>
<tr>
<td>20</td>
<td>QOS</td>
<td>168</td>
</tr>
<tr>
<td></td>
<td>20.1 User Groups</td>
<td>168</td>
</tr>
<tr>
<td></td>
<td>20.2 Bandwidth Control</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td>20.3 Application</td>
<td>170</td>
</tr>
<tr>
<td>21</td>
<td>FIREWALL</td>
<td>172</td>
</tr>
<tr>
<td></td>
<td>21.1 Outbound and Inbound Firewall Rules</td>
<td>172</td>
</tr>
<tr>
<td></td>
<td>21.2 Content Blocking</td>
<td>179</td>
</tr>
<tr>
<td>22</td>
<td>OSPF &amp; RIPV2</td>
<td>181</td>
</tr>
<tr>
<td>23</td>
<td>REMOTE USER ACCESS</td>
<td>184</td>
</tr>
<tr>
<td>24</td>
<td>AP</td>
<td>193</td>
</tr>
<tr>
<td></td>
<td>24.1 AP Controller</td>
<td>193</td>
</tr>
<tr>
<td></td>
<td>24.2 Wireless SSID</td>
<td>194</td>
</tr>
<tr>
<td></td>
<td>24.3 Profiles</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>24.4 Info</td>
<td>204</td>
</tr>
<tr>
<td></td>
<td>24.5 Usage</td>
<td>205</td>
</tr>
<tr>
<td></td>
<td>24.6 SSID</td>
<td>208</td>
</tr>
<tr>
<td></td>
<td>24.7 Wireless Client</td>
<td>208</td>
</tr>
</tbody>
</table>
D.6 Inbound Access Restriction ................................................................. 261
D.7 Outbound Access Restriction .............................................................. 262
APPENDIX E. TROUBLESHOOTING ............................................................. 263
APPENDIX F. DECLARATION ........................................................................ 264
1 Introduction and Scope

The Peplink Balance series provides link aggregation and load balancing across up to thirteen WAN connections.

The Peplink Balance series offers cost-effective solutions suitable for SOHO/power users and small businesses. The Balance lineup also features a range of advanced enterprise solutions. Peplink enterprise routers are ideal single-box solutions for medium to large business environments, and they allow service providers to enable highly available multi-network services.

The Peplink MediaFast series downloads and buffers video, audio, iTunes/iTunes U, HTTP, and other content for uninterrupted learning and fun anytime.

This manual applies to the following Peplink Balance products running firmware 6.3:

- Peplink Balance 20/30
- Peplink Balance 30 LTE
- Peplink Balance 50
- Peplink Balance 210/310
- Peplink Balance 380
- Peplink Balance 580
- Peplink Balance 710
- Peplink Balance 1350
- Peplink Balance 2500
- Peplink MediaFast 200/500

The manual covers setting up your Peplink Balance or MediaFast and provides a collection of case studies detailing the advanced features of the Peplink Balance.

Important Note to Users Upgrading from Firmware 4.7 or below

If your current firmware version is 4.7 or below, please upgrade to Firmware 4.8.2 before upgrading to firmware 6.3.

Important Note to Users of the Peplink Balance 30 (Classic Edition)

Firmware 5.0 or above is NOT applicable to the Peplink Balance 30 (Classic Edition). For more information on identifying the generation of your Peplink Balance 30, please visit our knowledgebase at <http://www.peplink.com/index.php?view=faq&id=231&path=16>. 
## Glossary

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>3rd generation standards for wireless communications (e.g., HSDPA)</td>
</tr>
<tr>
<td>4G</td>
<td>4th generation standards for wireless communications (e.g., LTE)</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>EVDO</td>
<td>Evolution-Data Optimized</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>HSDPA</td>
<td>High-Speed Downlink Packet Access</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper-Text Transfer Protocol</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Media Access Control Address</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>MSS</td>
<td>Maximum Segment Size</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>PPPoE</td>
<td>Point to Point Protocol over Ethernet</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WINS</td>
<td>Windows Internet Name Service</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>210+</td>
<td>Refers to Peplink Balance 210/310/380/580/710/1350/2500</td>
</tr>
<tr>
<td>380+</td>
<td>Refers to Peplink Balance 380/580/710/1350/2500</td>
</tr>
</tbody>
</table>
## 3  Product Comparison Chart

Click underlined features to reach the relevant portion of the manual.

<table>
<thead>
<tr>
<th></th>
<th>20/30/50</th>
<th>30LTE</th>
<th>One</th>
<th>210</th>
<th>310</th>
<th>305</th>
<th>380</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN Ports</strong></td>
<td>2/3/5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td><strong>Throughput (Mbps)</strong></td>
<td>150</td>
<td>150</td>
<td>600</td>
<td>200</td>
<td>200</td>
<td>1Gbps</td>
<td>1Gbps</td>
</tr>
<tr>
<td><strong>Embedded 4G LTE Modem</strong></td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>PepVPN</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SpeedFusion Hot Failover</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>^</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td><strong>SF Bandwidth Bonding</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>^</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td><strong>SF WAN Smoothing</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>^</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td><strong>Drop-In Mode</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Simultaneous Dual-Band 802.11a/b/g/n Wi-Fi AP</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>AP Controller</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Remote AP Management</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Web Filtering Blacklist</strong></td>
<td>-</td>
<td>-</td>
<td>Light</td>
<td>Light</td>
<td>Light</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td><strong>MediaFast Content Caching</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

^-Available as an optional feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>580</th>
<th>710</th>
<th>1350</th>
<th>2500</th>
<th>MFA200</th>
<th>MFA500</th>
<th>MFA750</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN Ports</strong></td>
<td>5</td>
<td>7</td>
<td>13</td>
<td>12</td>
<td>2</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td><strong>Throughput (Mbps)</strong></td>
<td>1.5Gbps</td>
<td>2.5Gbps</td>
<td>5Gbps</td>
<td>8Gbps</td>
<td>200</td>
<td>800</td>
<td>1.5Gbps</td>
</tr>
<tr>
<td><strong>Embedded 4G LTE Modem</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>PepVPN</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SpeedFusion Hot Failover</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SF Bandwidth Bonding</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SF WAN Smoothing</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Drop-In Mode</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Simultaneous Dual-Band 802.11a/b/g/n Wi-Fi AP</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>AP Controller</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Remote AP Management</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Web Filtering Blacklist</strong></td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Light</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td><strong>MediaFast Content Caching</strong></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

^Available as an optional feature

Full product comparison available at:
http://www.peplink.com/products/balance/model-comparison/
4  Product Features

Peplink Balance Series products enable all LAN users to share broadband Internet connections and provide advanced features to enhance Internet access. The following is a list of supported features:

4.1 Supported Network Features

4.2 WAN

- Multiple public IP support (DHCP, PPPoE, static IP address)
- Static IP support for PPPoE
- 10/100/1000Mbps Ethernet connection in full/half duplex
- Built-in HSPA and EVDO cellular modems
- USB mobile connection (only one USB modem can be connected at a time)
- Drop-in mode on selectable WAN port with MAC address passthrough network address translation (NAT) / port address translation (PAT)
- Inbound and outbound NAT mapping
- Multiple static IP addresses per WAN connection
- MAC address clone
- 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

4.3 LAN

- DHCP server on LAN
- Extended DHCP option support
- Static routing rules
- Local DNS proxy server
- VLAN on LAN support

4.4 VPN

- Secure SpeedFusion™
- SpeedFusion performance analyzer
- X.509 certificate support (feature activation required on some Balance models)
- Bandwidth bonding and failover among selected WAN connections
- Ability to route traffic to a remote VPN peer
- Optional pre-shared key setting
- Layer 2 bridging
- Layer 2 Peer Isolation
- SpeedFusion™ throughput, ping, and traceroute tests
- Built-in L2TP / PPTP VPN server
- Authenticate L2TP / PPTP clients using RADIUS and LDAP servers
- Multi-Site PepVPN Profile
- IPsec VPN for network-to-network connections (works with Cisco and Juniper only)
- L2TP / PPTP and IPsec passthrough

4.5 Inbound Traffic Management
- TCP/UDP traffic redirection to dedicated LAN server(s)
- Inbound link load balancing by means of DNS

4.6 Outbound Policy
- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms
- Time-based scheduling

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

4.8 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 optimization
4.9 **Firewall**
- Outbound (LAN to WAN) firewall rules
- Inbound (WAN to LAN) firewall rules per WAN connection
- Intrusion detection and prevention
- Specification of NAT mappings
- Web blocking
- Application blocking
- Time-based scheduling
- Outbound firewall rules can be defined by destination domain name

4.10 **Captive Portal**
- Social Wi-Fi Hotspot Support
- Splash screen of open networks, login page for secure networks
- Customizable built-in captive portal
- Supports linking to outside page for captive portal
4.11 Other Supported Features

- Easy-to-use web administration interface
- HTTP and HTTPS support for web administration interface
- Configurable web administration port and administrator password
- Read-only user for web admin
- Shared-IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Firmware upgrades, configuration backups, ping, and traceroute via web administration interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Remote reporting to Peplink Balance reporting server
- Hardware high availability via VRRP, with automatic configuration synchronization
- Real-time, hourly, daily and monthly bandwidth usage reports and charts
- Hardware backup via LAN bypass
- Built-in WINS server
- Time server synchronization
- SNMP
- Email notification
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Active sessions
- Active client list
- WINS client list
- UPnP / NAT-PMP
- Improved active sessions page
- Event log is persistent across reboots
- IPv6 support
- Support for USB tethering on Android 2.2+ phones
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.

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.
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.

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 LACP NIC Bonding

Use 802.3ad to combine multiple LAN connections into a virtual LAN connection. This virtual connection has higher throughput and redundancy in case any single link fails.
6 Package Contents

The contents of Peplink Balance product packages are as follows:

6.1 Peplink Balance One

- Peplink Balance One
- Power adapter
- Information slip

6.2 Peplink Balance 20/30/30 LTE/50

- Peplink Balance 20/30/30 LTE/50
- Power adapter
- Information slip

6.3 Peplink Balance 210/310

- Peplink Balance 210/310
- Power adapter
- Information slip
- Rackmount kit

6.4 Peplink Balance 305/380/580/710/1350/2500

- Peplink Balance 305/380/580/710/1350/2500
- Power cord
- Information slip
- Rackmount kit

6.5 Peplink MediaFast 200

- Peplink MediaFast 200
- Power adapter
- Information slip

6.6 Peplink MediaFast 500

- Peplink MediaFast 500
- Power cord
- Information slip
- Rackmount kit
7 Peplink Balance Overview

7.1 Peplink Balance One

7.1.1 Front Panel Appearance

7.1.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Power and Status Indicators</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wi-Fi</strong></td>
<td>OFF – Wi-Fi is off</td>
</tr>
<tr>
<td></td>
<td>Green – Ready</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>OFF – Upgrading firmware</td>
</tr>
<tr>
<td></td>
<td>Red – Booting up or busy</td>
</tr>
<tr>
<td></td>
<td>Blinking red – Boot up error</td>
</tr>
<tr>
<td></td>
<td>Green – Ready</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN and WAN Ports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Green LED</strong></td>
<td>ON – 10 / 100 / 1000 Mbps</td>
</tr>
<tr>
<td><strong>Orange LED</strong></td>
<td>Blinking – Data is transferring</td>
</tr>
<tr>
<td></td>
<td>OFF – No data is being transferred or port is not connected</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

**USB Port**
USB Ports

For future functionality

7.1.3 Rear Panel Appearance

7.1.4 Product Label

Peplink Balance One
Product Code: BPL-ONE
Serial No.: 2830-CAEB-5803
LAN MAC: 00-1A-DD-C2-20-80

Default Access
Username: admin
http://192.168.1.1 Password: admin

Input: 12V-24V DC
Made in Taiwan
FCC ID: U8G-P1805
### 7.2 Peplink Balance 20

#### 7.2.1 Front Panel Appearance

![Front Panel Diagram](image)

#### 7.2.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Power</th>
<th>Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF - Power off</td>
<td>Green - Power on</td>
<td></td>
</tr>
<tr>
<td>OFF - Upgrading firmware</td>
<td>Red - Booting up or busy</td>
<td></td>
</tr>
<tr>
<td>Blinking red - Boot up error</td>
<td>Green - Ready</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN and WAN Ports</th>
<th>Power LED</th>
<th>Reset Button</th>
<th>Status LED</th>
<th>LAN Ports</th>
<th>WAN Ports</th>
<th>USB Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green LED</td>
<td>ON - 10 / 100 / 1000 Mbps</td>
<td>Blinking - Data is transferring</td>
<td>OFF - No data is being transferred or port is not connected</td>
<td>Auto MDI/MDI-X ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orange LED</td>
<td>Auto MDI/MDI-X ports</td>
<td>For connecting a 4G/3G USB modem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**USB Port**

For connecting a 4G/3G USB modem
7.2.3 Rear Panel Appearance

- Power Connector

7.2.4 Unit Base Appearance

- Serial Number and LAN MAC Address
- Kensington Security Slot
7.3 Peplink Balance 30

7.3.1 Front Panel Appearance

![Front Panel Appearance Diagram]

7.3.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Power and Status Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
</tr>
<tr>
<td>OFF – Power off</td>
</tr>
<tr>
<td>Green – Power on</td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>OFF – Upgrading firmware</td>
</tr>
<tr>
<td>Red – Booting up or busy</td>
</tr>
<tr>
<td>Blinking red – Boot up error</td>
</tr>
<tr>
<td>Green – Ready</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN and WAN Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Green LED</strong></td>
</tr>
<tr>
<td>ON – 10 / 100 /1000 Mbps</td>
</tr>
<tr>
<td>Blinking – Data is transferring</td>
</tr>
<tr>
<td>OFF – No data is being transferred or port is not connected</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
</tr>
<tr>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USB Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>USB Ports</strong></td>
</tr>
<tr>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.3.3 Rear Panel Appearance

- Power Connector
- Kensington Security Slot

7.3.4 Unit Base Appearance

- Serial Number and LAN MAC Address
7.4 Peplink Balance 30 LTE

7.4.1 Front Panel Appearance

![Front Panel Diagram]

7.4.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Power and Status Indicators</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td></td>
</tr>
<tr>
<td>OFF – Power off</td>
<td></td>
</tr>
<tr>
<td><strong>Green</strong> – Power on</td>
<td></td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td></td>
</tr>
<tr>
<td>OFF – Upgrading firmware</td>
<td></td>
</tr>
<tr>
<td><strong>Red</strong> – Booting up or busy</td>
<td></td>
</tr>
<tr>
<td><strong>Blinking red</strong> – Boot up error</td>
<td></td>
</tr>
<tr>
<td><strong>Green</strong> – Ready</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN and WAN Ports</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Green LED</strong></td>
<td></td>
</tr>
<tr>
<td>ON – 10 / 100 /1000 Mbps</td>
<td></td>
</tr>
<tr>
<td><strong>Orange LED</strong></td>
<td></td>
</tr>
<tr>
<td>Blinking – Data is transferring</td>
<td></td>
</tr>
<tr>
<td>OFF – No data is being transferred or port is not connected</td>
<td></td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
<td></td>
</tr>
<tr>
<td>Auto MDI/MDI-X ports</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USB Port</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>USB Ports</strong></td>
<td></td>
</tr>
<tr>
<td>For connecting a 4G/3G USB modem</td>
<td></td>
</tr>
</tbody>
</table>
7.4.3 Rear Panel Appearance

- Power Connector
- Cellular SIM Slot

7.4.4 Unit Base Appearance

- Serial Number and LAN MAC Address
7.5 Peplink Balance 50

7.5.1 Front Panel Appearance

7.5.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Power and Status Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
</tr>
<tr>
<td>OFF – Power off</td>
</tr>
<tr>
<td>Green – Power on</td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>OFF – Upgrading firmware</td>
</tr>
<tr>
<td>Red – Booting up or busy</td>
</tr>
<tr>
<td>Blinking red – Boot up error</td>
</tr>
<tr>
<td>Green – Ready</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN and WAN Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Green LED</strong></td>
</tr>
<tr>
<td>ON – 10 / 100 /1000 Mbps</td>
</tr>
<tr>
<td><strong>Orange LED</strong></td>
</tr>
<tr>
<td>Blinking – Data is transferring</td>
</tr>
<tr>
<td>OFF – No data is being transferred or port is not connected</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
</tr>
<tr>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USB Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>USB Ports</strong></td>
</tr>
<tr>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.5.3  Rear Panel Appearance

- Power Connector
- Kensington Security Slot
7.6 Peplink Balance 210

7.6.1 Front Panel Appearance

![Front Panel Appearance](image)

7.6.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Power and Status Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Upgrading firmware</td>
</tr>
<tr>
<td>Red</td>
<td>Booting up or busy</td>
</tr>
<tr>
<td>Blinking red</td>
<td>Boot up error</td>
</tr>
<tr>
<td>Green</td>
<td>Ready</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>LAN and WAN Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green LED</td>
<td>ON – 10 / 100 / 1000 Mbps</td>
</tr>
<tr>
<td>Orange LED</td>
<td>Blinking – Data is transferring</td>
</tr>
<tr>
<td></td>
<td>OFF – No data is being transferred or port is not connected</td>
</tr>
<tr>
<td>Port Type</td>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>USB Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Ports</td>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.6.3 Rear Panel Appearance

- Power Connector

7.6.4 Unit Base Appearance

- Serial Number and LAN MAC Address
7.7 Peplink Balance 310

7.7.1 Front Panel Appearance

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Power and Status Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>Upgrading firmware</td>
</tr>
<tr>
<td>Red</td>
<td>Booting up or busy</td>
</tr>
<tr>
<td>Blinking red</td>
<td>Boot up error</td>
</tr>
<tr>
<td>Green</td>
<td>Ready</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Green LED</th>
<th>LAN and WAN Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>10 / 100 / 1000 Mbps</td>
</tr>
<tr>
<td>Blinking</td>
<td>Data is transferring</td>
</tr>
<tr>
<td>OFF</td>
<td>No data is being transferred or port is not connected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Type</th>
<th>USB Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto MDI/MDI-X ports</td>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.7.3 Rear Panel Appearance

- Power Connector

7.7.4 Unit Base Appearance

- Serial Number and LAN MAC Address
7.8 Peplink Balance 305

7.8.1 Front Panel Appearance

![Front Panel Diagram]

7.8.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Power and Status Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
</tr>
<tr>
<td>OFF – Power off</td>
</tr>
<tr>
<td>GREEN – Power on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Port, WAN 1 – 3 Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right LED</td>
</tr>
<tr>
<td>ORANGE – 1000 Mbps</td>
</tr>
<tr>
<td>GREEN – 100 Mbps</td>
</tr>
<tr>
<td>OFF – 10 Mbps</td>
</tr>
</tbody>
</table>

| Left LED                   |
| Solid – Port is connected without traffic |
| Blinking – Data is transferring |
| OFF – Port is not connected |

| Port Type                  |
| Auto MDI/MDI-X ports       |

<table>
<thead>
<tr>
<th>Console and USB Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Port</td>
</tr>
<tr>
<td>Reserved for engineering use</td>
</tr>
</tbody>
</table>

| USB Ports                  |
| For connecting a 4G/3G USB modem |
7.8.3 LCD Display Menu

- HA State: Master/Slave
- LAN IP
- VIP
- System Status
  - System:
    - Firmware ver. (shows firmware version)
    - Serial number (shows serial number)
    - System time (shows current time)
    - System up time (shows system uptime since last reboot)
    - CPU load (shows current CPU loading, 0-100%)
    - LAN:
      - Status (shows LAN port physical status)
      - IP address (shows LAN IP address)
      - Subnet mask (shows LAN subnet mask)
      - LAN Status (shows Connected/Disconnected, IP address list)
- Link status
  - WAN1
  - WAN2
  - WAN3
- VPN status
  - VPN Profile 1
  - VPN Profile 2
  - ...
  - VPN Profile n (shows Connected/Disconnected)
- Link usage
  - Throughput in
    - WAN1
    - WAN2
    - WAN3
  - Throughput out
    - WAN1
    - WAN2
    - WAN3
- Data Transfer'd
  - WAN1
  - WAN2
  - WAN3
- Maintenance
  - Reboot
    - Reboot? (Yes/No) (to reboot the unit)
  - Factory default
    - Factory default? (Yes/No) (to restore factory defaults)
- LAN config
  - Port speed
    - LAN
    - WAN1
    - WAN2
    - WAN3

(shows transfer rate in Kbps)
(shows volume transferred since last reboot in MB)
(shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
7.8.4 Rear Panel Appearance

![Power Switch and Power Connector]

**Connector Ports**

<table>
<thead>
<tr>
<th><strong>Power Connector</strong></th>
<th>AC input 110/220V</th>
</tr>
</thead>
</table>

**Switch**

<table>
<thead>
<tr>
<th><strong>Power Switch</strong></th>
<th>Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit.</th>
</tr>
</thead>
</table>

7.8.5 Unit Label Appearance

![Image of unit label]

**Peplink Balance 305**

- **Product Code:** BPL-305
- **Serial:** 1824-A94A-3A4D
- **LAN MAC:** 10-56-CA-07-3F-78

**Default Access**

- **Username:** admin
- **Password:** admin

**Input:** 100V-240V AC
**Made in Taiwan**

http://www.peplink.com
7.9 Peplink Balance 380

7.9.1 Front Panel Appearance

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

<table>
<thead>
<tr>
<th>Power and Status Indicators</th>
<th>Power LED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OFF – Power off</td>
</tr>
<tr>
<td></td>
<td>GREEN – Power on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Port, WAN 1 – 3 Ports</th>
<th>Right LED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ORANGE – 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>GREEN – 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>OFF – 10 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Left LED</th>
<th>Port Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid – Port is connected without traffic</td>
<td>Auto MDI/MDI-X ports</td>
</tr>
<tr>
<td>Blinking – Data is transferring</td>
<td></td>
</tr>
<tr>
<td>OFF – Port is not connected</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Console and USB Ports</th>
<th>Console Port</th>
<th>USB Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reserved for engineering use</td>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.9.3 LCD Display Menu

> HA State: Master/Slave
> LAN IP
> VIP
> System Status
> System
  > Firmware ver. (shows firmware version)
  > Serial number (shows serial number)
  > System time (shows current time)
  > System up time (shows system uptime since last reboot)
  > CPU load (shows current CPU loading, 0-100%)
  > LAN
    > Status (shows LAN port physical status)
    > IP address (shows LAN IP address)
    > Subnet mask (shows LAN subnet mask)
> Link status
  > WAN1
  > WAN2
  > WAN3
> VPN status
  > VPN Profile 1
  > VPN Profile 2
  > ...
  > VPN Profile n
> Link usage
  > Throughput in (shows transfer rate in Kbps)
    > WAN1
    > WAN2
    > WAN3
  > Throughput out (shows transfer rate in Kbps)
    > WAN1
    > WAN2
    > WAN3
> Data Transfer’d (shows volume transferred since last reboot in MB)
  > WAN1
  > WAN2
  > WAN3
> Maintenance
  > Reboot > Reboot? (Yes/No) (to reboot the unit)
  > Factory default > Factory default? (Yes/No) (to restore factory defaults)
> LAN config
  > Port speed (shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseT-FD, 100baseT-HD, 1000baseT-FD).
    > LAN
    > WAN1
    > WAN2
    > WAN3
7.9.4 Rear Panel Appearance

![Power Switch]

**Power Switch**
- Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit.

### Connector Ports

| Power Connector | AC input 110/220V |

### Switch

<table>
<thead>
<tr>
<th>Power Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit.</td>
</tr>
</tbody>
</table>

7.9.5 Unit Label Appearance

![Peplink Balance 380]

- **Product Code:** BPL-380
- **Serial:** 1824-6144-F2A7
- **LAN MAC:** 10-56-CA-03-DF-30
- **Default Access**
  - Username: admin
  - Password: admin

- **Made in Taiwan**
- **http://www.peplink.com**

- **Serial Number and LAN MAC Address**
7.10 Peplink Balance 580

7.10.1 Front Panel Appearance

7.10.2 LED Indicators

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

<table>
<thead>
<tr>
<th>Power and Status Indicators</th>
<th>Power LED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OFF – Power off</td>
</tr>
<tr>
<td></td>
<td>GREEN – Power on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Port, WAN 1 – 5 Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Right LED</strong></td>
</tr>
<tr>
<td>ORANGE – 1000 Mbps</td>
</tr>
<tr>
<td>GREEN – 100 Mbps</td>
</tr>
<tr>
<td>OFF – 10 Mbps</td>
</tr>
<tr>
<td><strong>Left LED</strong></td>
</tr>
<tr>
<td>Solid – Port is connected without traffic</td>
</tr>
<tr>
<td>Blinking – Data is transferring</td>
</tr>
<tr>
<td>OFF – Port is not connected</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
</tr>
<tr>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Console and USB Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Console Port</strong></td>
</tr>
<tr>
<td>Reserved for engineering use</td>
</tr>
<tr>
<td><strong>USB Ports</strong></td>
</tr>
<tr>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>

7.10.3 LCD Display Menu
> HA State: Master/Slave

> System Status

> System
> Firmware ver. (shows firmware version)
> Serial number (shows serial number)
> System time (shows current time)
> System up time (shows system uptime since last reboot)
> CPU load (shows current CPU loading, 0-100%)
> LAN
> Status (shows LAN port physical status)
> IP address (shows LAN IP address)
> Subnet mask (shows LAN subnet mask)
> Link status
> WAN1
> WAN2
> ...
> WAN5

> VPN status
> VPN Profile 1
> VPN Profile 2
> ...
> VPN Profile n

> Link usage
> Throughput in
> WAN1
> WAN2
> ...
> WAN5
> Throughput out
> WAN1
> WAN2
> ...
> WAN5

> Data Transfer’d
> WAN1
> WAN2
> ...
> WAN5

> Maintenance
> Reboot > Reboot? (Yes/No) (to reboot the unit)
> Factory default > Factory default? (Yes/No) (to restore factory defaults)

> LAN config
> Port speed
> LAN
> WAN1
> WAN2
> ...
> WAN5

> Port speed (shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
Rear Panel Appearance

Connector Ports

| Power Connector | AC input 110/220V |

Switch

| Power Switch | Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit. |

7.10.4 Unit Label Appearance

Peplink Balance 580
Product Code: BPL-580
Serial: 1824-61DE-6B04
LAN MAC: 10-56-CA-03-E6-68

Default Access
http://192.168.1.1
Username: admin
Password: admin

Serial Number and LAN MAC Address

Made in Taiwan

http://www.peplink.com
7.11 Peplink Balance 710

7.11.1 Front Panel Appearance

Status indicated in the front panel is as follows:

<table>
<thead>
<tr>
<th>LED Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power LED</strong></td>
<td>OFF – Power off</td>
</tr>
<tr>
<td></td>
<td>GREEN – Power on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Port, WAN 1 – 7 Ports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Green LED</strong></td>
<td>ON – 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>OFF – 100/10 Mbps</td>
</tr>
<tr>
<td></td>
<td>Solid – Port is connected without traffic</td>
</tr>
<tr>
<td><strong>Orange LED</strong></td>
<td>Blinking – Data is transferring</td>
</tr>
<tr>
<td></td>
<td>OFF – Port is not connected</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Console &amp; USB Ports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Console Port</strong></td>
<td>Reserved for engineering use</td>
</tr>
<tr>
<td><strong>USB Ports</strong></td>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.11.2 LCD Display Menu

- HA State: Master/Slave
- LAN IP
- VIP
- System Status
  - System
    - Firmware ver. (shows firmware version)
    - Serial number (shows serial number)
    - System time (shows current time)
    - System up time (shows system uptime since last reboot)
    - CPU load (shows current CPU loading, 0-100%)
  - LAN
    - Status (shows LAN port physical status)
    - IP address (shows LAN IP address)
    - Subnet mask (shows LAN subnet mask)
- Link status
  - WAN1
  - WAN2
  - ...
  - WAN7
- VPN status
  - VPN Profile 1
  - VPN Profile 2
  - ...
  - VPN Profile n
- Link usage
  - Throughput in
    - WAN1
    - WAN2
    - ...
    - WAN7
  - Throughput out
    - WAN1
    - WAN2
    - ...
    - WAN7
- Data Transfer’d
  - WAN1
  - WAN2
  - ...
  - WAN7
- Maintenance
  - Reboot
  - Reboot? (Yes/No) (to reboot the unit)
  - Factory default
  - Factory default? (Yes/No) (to restore factory defaults)
- LAN config
  - Port speed
    - LAN
    - WAN1
    - WAN2
    - ...
    - WAN7

http://www.peplink.com -44 / 266 - Copyright © 2016 Peplink
7.11.3 Rear Panel Appearance

![Rear Panel Appearance Diagram]

<table>
<thead>
<tr>
<th>Connector Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RS-232 Port</strong></td>
</tr>
<tr>
<td><strong>Power Connector</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Switch</strong></td>
</tr>
<tr>
<td><strong>Reset Switch</strong></td>
</tr>
</tbody>
</table>

7.11.4 Unit Label Appearance

![Unit Label Appearance]

- Default Access: http://192.168.1.1
  - Username: admin
  - Password: admin

Made in Taiwan

http://www.peplink.com
7.12 Peplink Balance 1350

7.12.1 Front Panel Appearance

Status indicated in the front panel is as follows:

<table>
<thead>
<tr>
<th>LED Indicator</th>
<th>Power LED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OFF – Power off</td>
</tr>
<tr>
<td></td>
<td>GREEN – Power on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>LAN Port, WAN 1 – 13 Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Right LED</strong></td>
<td><strong>ORANGE</strong> – 1000 Mbps</td>
</tr>
<tr>
<td><strong>GREEN</strong> – 100 Mbps</td>
<td></td>
</tr>
<tr>
<td><strong>OFF</strong> – 10 Mbps</td>
<td></td>
</tr>
<tr>
<td><strong>Left LED</strong></td>
<td>Solid – Port is connected without traffic</td>
</tr>
<tr>
<td>Blinking – Data is transferring</td>
<td></td>
</tr>
<tr>
<td><strong>OFF</strong> – Port is not connected</td>
<td></td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Console &amp; USB Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Console Port</strong></td>
<td>Reserved for engineering use</td>
</tr>
<tr>
<td><strong>USB Ports</strong></td>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.12.2 LCD Display Menu

> HA State: Master/Slave
> LAN IP
> VIP
> System Status
> System
  > Firmware ver. (shows firmware version)
  > Serial number (shows serial number)
  > System time (shows current time)
  > System up time (shows system uptime since last reboot)
  > CPU load (shows current CPU loading, 0-100%)
  > LAN
    > Status (shows LAN port physical status)
    > IP address (shows LAN IP address)
    > Subnet mask (shows LAN subnet mask)
> Link status
  > WAN1
  > WAN2
  > ...
  > WAN13
> VPN status
  > VPN Profile 1 (shows Connected/Disconnected)
  > VPN Profile 2
  > ...
  > VPN Profile n
> Link usage
  > Throughput in
    > WAN1
    > WAN2
    > ...
    > WAN13
  > Throughput out
    > WAN1
    > WAN2
    > ...
    > WAN13
> Data Transfer’d
  > WAN1
  > WAN2
  > ...
  > WAN13
> Maintenance
  > Reboot > Reboot? (Yes/No) (to reboot the unit)
  > Factory default > Factory default? (Yes/No) (to restore factory defaults)
> LAN config
  > Port speed
    > LAN
    > WAN1
    > WAN2
    > ...
    > WAN13
7.12.3 Rear Panel Appearance

Power Switch
Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit.

7.12.4 Unit Label Appearance

Serial Number and LAN MAC Address
7.13 Peplink Balance 2500

7.13.1 Front Panel Appearance

BPL-2500

BPL-2500-SFP
Status indicated in the front panel is as follows:

<table>
<thead>
<tr>
<th>LED Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power LED</strong></td>
</tr>
<tr>
<td>OFF – Power off</td>
</tr>
<tr>
<td>GREEN – Power on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN and WAN Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Right LED</strong></td>
</tr>
<tr>
<td>ORANGE – 1000 Mbps</td>
</tr>
<tr>
<td>GREEN – 100 Mbps</td>
</tr>
<tr>
<td>OFF – 10 Mbps</td>
</tr>
<tr>
<td><strong>Left LED</strong></td>
</tr>
<tr>
<td>Solid – Port is connected without traffic</td>
</tr>
<tr>
<td>Blinking – Data is transferring</td>
</tr>
<tr>
<td>OFF – Port is not connected</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
</tr>
<tr>
<td>Auto MDI/MDI-X ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Console &amp; USB Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Console Port</strong></td>
</tr>
<tr>
<td>Reserved for engineering use</td>
</tr>
<tr>
<td><strong>USB Ports</strong></td>
</tr>
<tr>
<td>For connecting a 4G/3G USB modem</td>
</tr>
</tbody>
</table>
7.13.2 LCD Display Menu

> HA State: Master/Slave
> LAN IP
> VIP
> System Status
  > System
    > Firmware ver. (shows firmware version)
    > Serial number (shows serial number)
    > System time (shows current time)
    > System up time (shows system uptime since last reboot)
    > CPU load (shows current CPU loading, 0-100%)
  > LAN
    > Status (shows LAN port physical status)
    > IP address (shows LAN IP address)
    > Subnet mask (shows LAN subnet mask)
> Link status
  > WAN1
  > WAN2
  > ...
  > WAN13
> VPN status
  > VPN Profile 1
  > VPN Profile 2
  > ...
  > VPN Profile n
> Link usage
  > Throughput in
    > WAN1
    > WAN2
    > ...
    > WAN13
  > Throughput out
    > WAN1
    > WAN2
    > ...
    > WAN13
> Data Transfer'd
  > WAN1
  > WAN2
  > ...
  > WAN13
> Maintenance
  > Reboot > Reboot? (Yes/No) (to reboot the unit)
  > Factory default > Factory default? (Yes/No) (to restore factory defaults)
> LAN config
  > Port speed
    > LAN
    > WAN1
    > WAN2
    > ...
    > WAN13
7.13.3 Rear Panel Appearance

- **Power Switch**: Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit.

## Connector Ports

<table>
<thead>
<tr>
<th>Power Connector</th>
<th>AC input 100-240V</th>
</tr>
</thead>
</table>

## Switches

- **Power Switch**
  - Pressing and holding the key for four seconds will power down the unit.
  - When the unit is powered off, pressing this switch will power on the unit.

7.13.4 Unit Label Appearance

**BPL-2500**

![Label Image]

**BPL-2500-SFP**

![Label Image]
7.14 Peplink MediaFast 500

7.14.1 Front Panel Appearance

Status indicated in the front panel is as follows:

<table>
<thead>
<tr>
<th>LED Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power LED</strong></td>
<td>OFF – Power off&lt;br&gt;GREEN – Power on</td>
</tr>
<tr>
<td><strong>LAN 1-3 Ports, WAN 1-5 Ports</strong></td>
<td></td>
</tr>
<tr>
<td>Right LED</td>
<td>ORANGE – 1000 Mbps&lt;br&gt;GREEN – 100 Mbps&lt;br&gt;OFF – 10 Mbps</td>
</tr>
<tr>
<td>Left LED</td>
<td>Solid – Port is connected without traffic&lt;br&gt;Blinking – Data is transferring&lt;br&gt;OFF – Port is not connected</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
<td>Auto MDI/MDI-X ports</td>
</tr>
<tr>
<td><strong>Console &amp; USB Ports</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Console Port</strong></td>
<td>Reserved for engineering use</td>
</tr>
<tr>
<td><strong>USB Ports</strong></td>
<td>For connecting 4G/3G USB modems</td>
</tr>
</tbody>
</table>
7.14.2 LCD Display Menu

> HA State: Master/Slave
> LAN IP
> VIP
> System Status
  > System
    > Firmware ver. (shows firmware version)
    > Serial number (shows serial number)
    > System time (shows current time)
    > System up time (shows system uptime since last reboot)
    > CPU load (shows current CPU loading, 0-100%)
    > LAN
      > Status (shows LAN port physical status)
      > IP address (shows LAN IP address)
      > Subnet mask (shows LAN subnet mask)
    > Link status
      > WAN1
      > WAN2
      > ...
      > WAN5
> VPN status
  > VPN Profile 1
  > VPN Profile 2
  > ...
  > VPN Profile n
> Link usage
  > Throughput in
    > WAN1
    > WAN2
    > ...
    > WAN5
  > Throughput out
    > WAN1
    > WAN2
    > ...
    > WAN5
> Data Transfer’d
  > WAN1
  > WAN2
  > ...
  > WAN5
> Maintenance
  > Reboot
    > Reboot? (Yes/No) (to reboot the unit)
  > Factory default
    > Factory default? (Yes/No) (to restore factory defaults)
> LAN config
  > Port speed
    > LAN
    > WAN1
    > WAN2
    > ...
    > WAN5

http://www.peplink.com -54 / 266 - Copyright © 2016 Peplink
7.14.3 Rear Panel Appearance

<table>
<thead>
<tr>
<th>Connector Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Connector</strong></td>
</tr>
<tr>
<td>AC input 100-240V</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Switch</strong></td>
</tr>
<tr>
<td>Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit.</td>
</tr>
</tbody>
</table>
8 Installation

The following section details connecting the Peplink Balance to your network:

8.1 Preparation

Before installing your Peplink Balance, please prepare the following:

- At least one Internet/WAN access account
- For each network connection, one 10/100BaseT UTP cable with RJ45 connector, one 1000BaseT Cat5E UTP cable for the Gigabit port, or one USB modem for the USB WAN port
- A computer with the TCP/IP network protocol and a web browser installed—supported browsers include Microsoft Internet Explorer 8.0 and above, Mozilla Firefox 10.0 and above, Apple Safari 5.1 and above, and Google Chrome 18 and above

8.2 Constructing the Network

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

1. With an Ethernet cable, connect a computer to one of the LAN ports on the Peplink Balance. For Peplink Balance models that support multiple connections, repeat with different cables for up to four computers to be connected.
2. With another Ethernet cable, connect the WAN/broadband modem to one of the WAN ports on the Peplink Balance. Repeat using different cables to connect from two to 13 WAN/broadband connections or connect a USB modem to the USB WAN port.
3. Connect the provided power adapter or cord to the power connector on the Peplink Balance, and then plug the power adapter into a power outlet.
The following figure schematically illustrates the resulting configuration:
8.3 Configuring the Network Environment

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

- LAN configuration
  For basic configuration, refer to Section 9, Basic Configuration.
  For advanced configuration, refer to Section 0, Configuring the LAN Interface(s).

- WAN configuration
  For basic configuration, refer to Section 9, Basic Configuration.
  For advanced configuration, refer to Section 13, Configuring the WAN Interface(s).

- MediaFast configuration
  For MediaFast configuration, refer to Section 10, MediaFast Configuration.
9 Basic Configuration

9.1 Connecting to the Web Admin Interface

1. Start a web browser on a computer that is connected with the Peplink Balance through the LAN.

2. To connect to the web admin of the Peplink Balance, enter the following LAN IP address in the address field of the web browser:

   http://192.168.1.1

   (This is the default LAN IP address of the Peplink Balance.)

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

   **Username**: admin  
   **Password**: admin

   (This is the default admin user login of the Peplink Balance. The admin and read-only user password can be changed at System>Admin Security.)

4. After successful login, the **Dashboard** of the web admin interface will be displayed. It looks similar to the following:

   ![Dashboard of the web admin interface](image-url)
Important Note

The **Save** button causes the changes to be saved. Configuration changes (e.g., WAN, LAN, admin settings, etc.) take effect after clicking the **Apply Changes** button on each page’s top-right corner.

9.2 **Configuration with the Setup Wizard**

The Setup Wizard simplifies the task of configuring WAN connection(s) by guiding the configuration process step-by-step.

To begin, click **Setup Wizard** after connecting to the web admin interface.

Click **Next >>** to begin.

Select **Yes** if you want to set up drop-in mode using the Setup Wizard.
Click on the appropriate checkbox(es) to select the WAN connection(s) to be configured. If you have chosen to configure drop-in mode using the Setup Wizard, the WAN port to be configured in drop-in mode will be checked by default.

If drop-in mode is going to be configured, the setup wizard will move on to **Drop-in Settings**.
If you are not using drop-in mode, select the connection method for the WAN connection(s) from the following screen:

Depending on the selection of connection type, further configuration may be needed. For example, PPPoE and static IP require additional settings for the selected WAN port. Please refer to Section 13, Configuring the WAN Interface(s) for details on setting up DHCP, static IP, and PPPoE.

If Mobile Internet Connection is checked, the setup wizard will move on to Operator Settings.

If Custom Mobile Operator Settings is selected, APN parameters are required. Some service providers may charge a fee for connecting to a different APN. Please consult your service provider for the correct settings.
Click on the appropriate check box(es) to select the preferred WAN connection(s). Connection(s) not selected in this step will be used as backup only. Click Next >> to continue.

Choose the time zone of your country/region. Check the box Show all to display all time zone options.

Check in the following screen to make sure all settings have been configured correctly, and then click Save Settings to confirm.

After finishing the last step in the setup wizard, click Apply Changes on the page header to allow the configuration changes to take effect.
9.3 Advanced Setup

Advanced settings can be configured from the **Network** menu. WAN connections can be configured by entering the corresponding WAN connection information at **Network>Interfaces>WAN**.

**Tip**

Please refer to Section 13, Configuring the WAN Interface(s), for details on setting up DHCP, static IP, PPPoE, L2TP, and mobile Internet connections.
9.4 Cellular WAN

To access cellular WAN settings, click Network>WAN>Details next to the appropriate cellular connection listing.

**Cellular Status**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IMSI</strong></td>
<td>This is the International Mobile Subscriber Identity, which uniquely identifies the SIM card. This is applicable to 3G modems only.</td>
</tr>
<tr>
<td><strong>MEID</strong></td>
<td>Some Balance models 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.</td>
</tr>
<tr>
<td><strong>ESN</strong></td>
<td>This serves the same purpose as MEID HEX but uses an older format.</td>
</tr>
<tr>
<td><strong>IMEI</strong></td>
<td>This is the unique ID for identifying the modem in GSM/HSPA mode.</td>
</tr>
<tr>
<td><strong>Network Mode</strong></td>
<td>This field displays the network mode, such as HSPA, for the listed cellular connection.</td>
</tr>
<tr>
<td><strong>WAN Connection Name</strong></td>
<td>Enter a name to represent this WAN connection.</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td><strong>Network Mode</strong></td>
<td>Choose the appropriate network mode for the cellular connection.</td>
</tr>
<tr>
<td><strong>Routing Mode</strong></td>
<td>Select the routing method to be used in routing IP frames via the WAN connection. The mode can be either <strong>NAT</strong> (network address translation) or <strong>IP Forwarding</strong>. Click the button to enable IP forwarding.</td>
</tr>
<tr>
<td><strong>DNS Servers</strong></td>
<td>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 <strong>Obtain DNS server address automatically</strong> results in the DNS servers assigned by the PPPoE server being used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.) When <strong>Use the following DNS server address(es)</strong> is selected, you can put custom DNS server addresses for this WAN connection into the <strong>DNS Server 1</strong> and <strong>DNS Server 2</strong> fields.</td>
</tr>
</tbody>
</table>
### Cellular Settings

#### 3G/2G
Select **Auto**, **3G Only**, or **2G Only**. Click 📦 to display advanced band selection options.

#### Authentication
Choose from **Auto**, **PAP Only**, or **CHAP Only** to authenticate cellular connections.

#### Band Selection
Select one or more bands to restrict cellular traffic to those bands.

#### 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 afterwards. If there is any difficulty in making a connection, you may select **Custom** to enter your carrier’s APN, **Username**, and **Password** settings manually. The correct values can be obtained from your carrier. The default and recommended value for **Operator Settings** is **Auto**.
APN / Username / 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. Click [link](http://www.peplink.com) to display a link to manage your SIM pin.

Bandwidth Allowance Monitor

Check **Enable** to turn on 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

**IP Passthrough**

When **IP Passthrough** is checked, after the cellular WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT.

Regardless the WAN connection's state, the router always binds to the LAN IP address (default: 192.168.50.1). When the cellular WAN is connected, the LAN client could access the router's web admin by manually configuring its IP address to the same subnet as the router's LAN IP address (e.g., 192.168.50.10).

**Note:** when this option is first enabled, the LAN client may not be able to refresh its IP address to the cellular WAN IP address in a timely fashion. The LAN client may have to manually renew its IP address from DHCP server. After this option is enabled, the DHCP lease time will be two minutes (i.e., the LAN client could refresh its IP address and access the network at most one minute after the cellular WAN connection goes up).

Also note that if an Ethernet WAN link fails during IP passthrough, the router can failover to a cellular WAN link that is also using IP passthrough.
### Standby State

This option allows you to choose whether to remain connected or disconnect when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, setting this WAN connection as active will make 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 reactivated.

#### Health Check Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Check Method</td>
<td>SmartCheck</td>
</tr>
<tr>
<td>Timeout</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Health Check Interval</td>
<td>10 seconds</td>
</tr>
<tr>
<td>Health Check Retries</td>
<td>3</td>
</tr>
<tr>
<td>Recovery Retries</td>
<td>3</td>
</tr>
</tbody>
</table>

### Health Check Settings

- **Health Check Method**: This setting allows you to specify the health check method for the cellular connection. The available options are **Disabled**, **Ping**, **DNS Lookup**, **HTTP**, and **SmartCheck**. The default method is **DNS Lookup**. See Section 13.3 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

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

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

Select Disabled to disable this feature. See Section 13.6 for configuration details.

MTU

MTU determines the maximum allowable size per packet, in bytes.
10 MediaFast Configuration

MediaFast settings can be configured from the Network menu.

10.1 Setting Up MediaFast Content Caching

To access MediaFast content caching settings, select Network>MediaFast.

<table>
<thead>
<tr>
<th>Enable</th>
<th>Click the checkbox to enable MediaFast content caching.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains / IP Addresses</td>
<td>Choose to Cache on all domains, or enter domain names and then choose either Whitelist (cache the specified domains only) or Blacklist (do not cache the specified domains).</td>
</tr>
</tbody>
</table>

The Secure Content Caching menu operates identically to the MediaFast menu, except it is for secure contenting accessible through https://.
### Cache Control

**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.

### 10.2 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 **Network>MediaFast>Prefetch Schedule.**
Prefetch Schedule Settings

Name
This field displays the name given to the scheduled download.

Status
Check the status of your scheduled download here.

Next Run Time/Last Run Time
These fields display the date and time of the next and most recent occurrences of the scheduled download.

Last Duration
Check this field to ensure that the most recent download took as long as expected to complete. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time.

Result
This field indicates whether downloads are in progress (✓) or complete (✓).

Last Download
Check this field to ensure that the most recent download file size is within the expected range. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time. This field is also useful for quickly seeing which downloads are consuming the most storage space.

Actions
To begin a scheduled download immediately, click ✉️.
To cancel a scheduled download, click ☑️.
To edit a scheduled download, click ✏️.
To delete a scheduled download, click ✖️.

New Schedule
Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:
Simply provide the requested information to create your schedule.

**Clear Web Cache**
Click to clear all cached content. Note that this action cannot be undone.

**Clear Statistics**
Click to clear all prefetch and status page statistics.

### 10.3 MDM Settings

In addition to performing content caching, MediaFast-enabled routers can also serve as an MDM, administrating to client devices.

<table>
<thead>
<tr>
<th>MDM Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
</tr>
<tr>
<td><strong>Account Settings</strong></td>
</tr>
<tr>
<td><strong>Username</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
</tr>
</tbody>
</table>

**Enable**
Click this checkbox to enable MDM on your router.

**Account Settings**
Click Follow Web Admin Account to allow client devices to use the built-in administrator account when performing MDM. Set Custom to specify a username and password your router will use to log into your client devices.
10.4 **Viewing MediaFast Statistics**

To get details on storage and bandwidth usage, select **Status>MediaFast**.
11 Configuring the LAN Interface(s)

LAN Interface settings are located at **Network>LAN>Network Settings**. Begin setting up your physical LAN by entering IP settings (VLAN configuration will be covered following physical LAN setup).

Navigating to that page will result in the following dashboard:

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 Address & Subnet Mask**
  - Enter the Peplink Balance's IP address and subnet mask values to be used on the LAN. To enable multiple VLANs, press the button on the top right-hand corner.

If drop-in mode will be used, you can configure it in the next section.
### Drop-in Mode Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
<td>Enable the drop-in mode feature. Drop-in mode eases the installation of the Peplink Balance 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. Please refer to Section 12, Drop-in Mode for details.</td>
</tr>
<tr>
<td><strong>WAN for Drop-in Mode</strong></td>
<td>Select the WAN port to be used for drop-in mode. If <strong>WAN 1 with LAN Bypass</strong> is selected, the high availability feature will be disabled automatically.</td>
</tr>
<tr>
<td><strong>Shared Drop-In IP</strong></td>
<td>When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Balance will listen for this IP address when WAN hosts access services provided by the Balance (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 Balance will listen for this IP address when LAN hosts access services provided by the Balance (web admin access from the WAN, DNS proxy, etc.).</td>
</tr>
<tr>
<td><strong>Shared IP Address</strong></td>
<td>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 (e.g., 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 (e.g., web admin accesses from WAN, DNS server, etc.).</td>
</tr>
<tr>
<td><strong>WAN Default Gateway</strong></td>
<td>Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the button next to &quot;WAN Default Gateway&quot; and check the <strong>I have other host(s) on WAN segment</strong> box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.</td>
</tr>
<tr>
<td><strong>WAN DNS</strong></td>
<td>Enter the selected WAN's corresponding DNS server IP addresses.</td>
</tr>
</tbody>
</table>

**NOTE:** The DHCP Server Settings will be overwritten.

The following WAN 1 with LAN bypass settings will be overwritten: Enable, Connection Method, Routing Mode, Connection Type, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.

The PPTP Server will be disabled.

High Availability will be disabled.

Tip: please review the DNS Forwarding setting under the Service Forwarding section.
Servers

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

Layer 2 PepVPN Bridging Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PepVPN Profiles to Bridge</td>
<td>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.</td>
</tr>
<tr>
<td>Remote Network Isolation</td>
<td>Enable this option if you want to block network traffic between the remote networks. This will not affect the connectivity between them and this local LAN.</td>
</tr>
<tr>
<td>Spanning Tree Protocol</td>
<td>Click this checkbox to enable spanning tree protocol in your L2 PepVPN.</td>
</tr>
<tr>
<td>Override IP Address when bridge connected</td>
<td>Select Do not override if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up. If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.</td>
</tr>
</tbody>
</table>

Note: drop-in mode and VLAN functionality are mutually exclusive. To change DHCP settings, continue to the next section.
### DHCP Server Settings

**DHCP Server**
When this setting is enabled, the Peplink Balance'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 Peplink Balance's DHCP server can prevent IP address collisions on the LAN.

**DHCP Server Logging**
Check this box to log DHCP server activity.

**IP Range & Subnet Mask**
These settings allocate a range of IP addresses that will be assigned to LAN computers by the Peplink Balance'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 Peplink Balance’s built-in DNS server address (i.e., LAN IP address) will be offered.

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

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

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

**Extended DHCP Option**
In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.
To define an extended DHCP option, click the **Add** button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.

### DHCP Reservation

This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses.

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

**Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in **00:AA:BB:CC:DD:EE** format. 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 27.3**.

Next, choose port settings.

**LAN Physical Settings**

**Speed**

The default speed setting is **Auto**, which allows the Balance to detect and apply an appropriate speed setting. You can also set the speed manually, as well as specify whether the speed will be advertised on the network. Generally, advertising port speed is necessary only when the port experiences difficulty negotiating speeds with peer devices.

**IEEE 802.3ad Link Aggregation**

Choose the interfaces that you wish to aggregate here if needed.

If required, enter static route and/or WINS server settings.

**DHCP relay settings** is an advanced feature. To enable it, click the **Enable** button next to **DHCP Server**.
DHCP Relay Settings

DHCP Relay
Enter the address of the DHCP server here. DHCP requests will be relayed to it.

DHCP Server IP Address
DHCP requests from the LAN are relayed to the entered DHCP server. For active-passive DHCP server configurations, enter active and passive DHCP server IPs into the DHCP Server 1 and DHCP Server 2 fields.

DHCP Option 82
This feature includes device information as relay agent for the attached client when forwarding DHCP requests from a DHCP client to a DHCP server. Device MAC address and network name are embedded to circuit ID and Remote ID in option 82.

DHCP Relay Logging
Check this box to log DHCP relay activity.

Static Route Settings

<table>
<thead>
<tr>
<th>Static Route</th>
<th>Destination Network</th>
<th>Subnet Mask</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>255.255.255.0 (24)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Static routes will be advertised to remote Peplink peers.

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. Click to create a new route. Click to remove a route.

WINS Server Settings

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

Enter any needed DNS proxy settings. Once all settings have been entered, click Save to store your changes.
### 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 improve DNS response time by storing all received DNS results for faster DNS lookup. However, it cannot return the most updated result for 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 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 Peplink Balance, the corresponding IP address will be returned. To display the option to set TTL manually, click 💡. Click ✨ to create a new record. Click ✗ to remove a record.

**Domain Lookup Policy**

DNS proxy will look up the domain names defined here using only the specified connections.

**DNS Resolvers**

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 your Bonjour forwarding settings. Once all settings have been entered, click Save to store your changes.

<table>
<thead>
<tr>
<th>Bonjour Forwarding Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
</tr>
<tr>
<td>Check this box to turn on Bonjour forwarding.</td>
</tr>
<tr>
<td><strong>Bonjour Service</strong></td>
</tr>
<tr>
<td>Choose <strong>Service</strong> and <strong>Client</strong> networks from the drop-down menus, and then click to add the networks. To delete an existing Bonjour listing, click .</td>
</tr>
</tbody>
</table>
11.1 LAN Configuration with VLAN

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:

- **IP Address**: Enter the Peplink Balance’s IP address and subnet mask values to be used on the LAN.
- **Name**: Enter a name for the LAN.
- **VLAN ID**: Enter a VLAN ID for your LAN.
- **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**
Drop-in mode eases the installation of the Peplink Balance 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.

Please refer to Section 12, Drop-in Mode for details.

**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.

**Shared Drop-In IP**
When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Balance will listen for this IP address when WAN hosts access services provided by the Balance (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 Balance will listen for this IP address when LAN hosts access services provided by the Balance (web admin access from the WAN, DNS proxy, etc.).

**Shared IP Address**
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 (e.g., 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 (e.g., web admin accesses from 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, click the button next to **WAN Default Gateway** and check the box to have other host(s) on WAN segment 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**
The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN. They will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.

**Remote Network Isolation**
Enable this option if you want to block network traffic between remote networks. This will not affect the connectivity between them and this local LAN.

**Spanning Tree Protocol**
When Layer 2 bridging is enabled, this field specifies the port to be bridged to the remote site. If you choose WAN, the selected WAN will be dedicated to bridging with the remote site and will be disabled for WAN purposes. The LAN port will remain unchanged.

**Override IP Address when bridge is connected**
Select “Do not override” if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.
If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.

A - Advanced feature, please click the button on the top right-hand corner of the Network Settings menu to activate.
### DHCP Server Settings

| DHCP Server | When this setting is enabled, the Peplink Balance'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 Peplink Balance's DHCP server can prevent IP address collisions on the LAN. |
| DHCP Server Logging | Check this box to log DHCP server activity. |
| IP Range & Subnet Mask | These settings allocate a range of IP address that will be assigned to LAN computers by the Peplink Balance'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 Peplink Balance's built-in DNS server address (i.e., LAN IP address) will be offered. |
| WINS Servers | This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP WINS Servers setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at Status>WINS Clients. |
| BOOTP | Check this box to enable BOOTP on older networks that still require it. |
| Extended DHCP Option | In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only. |
DHCP Reservation

This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.

Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in 00:AA:BB:CC:DD:EE format. Click + to create a new record. Click - 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 27.3.

Once configuration is complete, click Save to store the changes.

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

<table>
<thead>
<tr>
<th>DHCP Relay Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
</tr>
<tr>
<td>Check this box to turn on DHCP relay.</td>
</tr>
<tr>
<td><strong>DHCP Server IP Address</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>DHCP Option 82</strong></td>
</tr>
<tr>
<td>DCHP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device's MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.</td>
</tr>
<tr>
<td><strong>DHCP Relay Logging</strong></td>
</tr>
<tr>
<td>Check this box to log DHCP relay activity.</td>
</tr>
</tbody>
</table>

Once DHCP is set up, click Save and configure LAN Physical Settings, Static Route Settings, WINS Server Settings, DNS Proxy Settings, and Bonjour Forwarding as noted above.
12 Drop-in Mode

Drop-in mode (or transparent bridging mode) eases the installation of the Peplink Balance on a live network between the firewall and router, such that changes to the settings of existing equipment are not required.

The following diagram illustrates drop-in mode setup:

Enable drop-in mode using the Setup Wizard. After enabling this feature and selecting the WAN for drop-in mode, various settings, including the WAN's connection method and IP address, will be automatically updated.

When drop-in mode is enabled, the LAN and the WAN for drop-in mode ports will be bridged. Traffic between the LAN hosts and WAN router will be forwarded between the devices. In this case, the hosts on both sides will not notice any IP or MAC address changes.

After successfully setting up the Peplink Balance as part of the network using drop-in mode, it will, depending on model, support one or more WAN connections. Some MediaFast units also support multiple WAN connections after activating drop-in mode, though a SpeedFusion license may be required to activate more than one WAN port.

**IMPORTANT NOTE for customers using drop-in mode and planning to upgrade from Firmware 4.8.2 or below to 5.0+**

MAC address passthrough for drop-in mode is implemented in Firmware 5.0 and above. If drop-in mode is enabled when upgrading from a previous firmware version, the ARP tables on hosts on LAN and WAN segments must be flushed once. Alternately, the hosts may be rebooted. Otherwise, hosts on one side may not be able to reach hosts on the other side of the Peplink Balance until old ARP records expire. Units not using drop-in mode are not affected.

**NOTE**

The PPTP server will be disabled in drop-in mode.
To enable drop-in mode, perform the following steps:

1. Check the Enable box under **Drop-in Mode**, located at **Network>LAN>Network Settings**. (After checking the Enable box, most network settings for WAN1 will be hidden in the web admin interface.)

2. Enter the IP address of the WAN1 router in the **WAN Default Gateway** field. Ensure that the Peplink Balance’s IP subnet is the same as the firewall’s WAN port and the router’s LAN port.

3. If there are hosts other than the router on the WAN segment of the Peplink Balance, check the **I have other host(s) on WAN segment** box, enter the IP address(es) of the host(s), and then click the down-arrow to add the hosts.

4. To avoid consuming an IP address, click to turn on the shared IP address feature. Then check **Share Drop-In IP** and enter a **Shared IP Address**.
The following diagram illustrates:

![Diagram showing network setup with Peplink Balance Series device]

**Important Note**

Starting from Firmware version 5.0, drop-in mode can be configured on any WAN port. Please note that only one WAN port can be configured in drop-in mode. If you have selected the LAN bypass port as the WAN for drop-in mode, the high availability feature will be DISABLED automatically.

**Tip**

Want to know more about drop-in mode? Visit our YouTube Channel for video tutorials!

[YouTube Video Link]

http://youtu.be/lZG2-VPml5w
13 Configuring the WAN Interface(s)

WAN interface settings are located at Network>WAN.

<table>
<thead>
<tr>
<th>Connection Name</th>
<th>Method</th>
<th>Routing Mode</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. WAN 1</td>
<td>Static IP</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>2. WAN 2</td>
<td>Static IP</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>3. WAN 3</td>
<td>Static IP</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>4. WAN 4</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>5. WAN 5</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>6. WAN 6</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>7. WAN 7</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>8. WAN 8</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>9. WAN 9</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>10. WAN 10</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>11. WAN 11</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>12. WAN 12</td>
<td>Not Configured</td>
<td>NAT</td>
<td>Always-on</td>
</tr>
<tr>
<td>13. Mobile Internet</td>
<td>PPP</td>
<td>NAT</td>
<td>Backup Group 1</td>
</tr>
</tbody>
</table>

By clicking a Connection Name, connection settings of that WAN can be modified. The connection method and details can be obtained from your ISP.

### Connection Settings

- **WAN Connection Name**: Enter a name to represent this WAN connection.
- **Enable**: Click to enable this WAN connection. If needed, click the drop-down menu to apply a schedule to this connection.
- **Connection Method**: This option allows you to select the connection method for this WAN connection. Available options are:
  1. DHCP
  2. Static IP
  3. PPPoE
  4. L2TP
5. GRE
See Sections 13.2.1, 13.2.2, 13.2.3, 13.2.4 and 13.2.5 for configuration details pertaining to each connection method.

### Routing Mode
This field shows that NAT (network address translation) will be applied to the traffic routing over this WAN connection. IP Forwarding is also available when you click the link in the help text. For further details, please refer to Appendix B, Routing under DHCP, Static IP, and PPPoE.

### Connection Type
This setting specifies the utilization of the WAN connection. **Always-on** results in the WAN connection being used whenever it is available. If **Backup Priority** and a priority group are selected, the WAN connection is treated as a backup connection and is used only in the absence of available always-on WAN connection(s) and higher priority backup connection(s).

<table>
<thead>
<tr>
<th>Connection Type</th>
<th>Always-on</th>
<th>Backup Priority</th>
<th>Group 1 (highest)</th>
<th>Group 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reply to ICMP Ping</td>
<td>Enable</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The default and recommended connection type is **Always-on**.

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

### Upload Bandwidth
This setting specifies the data bandwidth in the outbound direction from the LAN through the WAN interface. This value is provided by your ISP and should reflect the actual speed of the WAN. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. Setting the correct value here can result in effective traffic prioritization and efficient use of upload bandwidth.

### Download Bandwidth
This setting specifies the data bandwidth in the inbound direction from the WAN interface to the LAN. This value is provided by your ISP and should reflect the actual speed of the WAN. This value is referenced as the default weight value when using the **Least Used** or **Persistence (Auto)** algorithms in **Outbound Policy** with **Managed by Custom Rules** chosen.

### IPv6
IPv6 support can be enabled on one of the available Ethernet WAN ports. On this screen, you can choose which WAN will support IPv6.

To enable IPv6 support on a WAN, the WAN router must respond to stateless address auto configuration advertisements and DHCPv6 requests. IPv6 clients on the LAN will acquire their IPv6, gateway, and DNS server addresses from it. The device will also acquire an IPv6 address for performing ping/traceroute checks and accepting web admin accesses.
### 13.1 Physical Interface Settings

<table>
<thead>
<tr>
<th>Physical Interface Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speed</strong></td>
</tr>
<tr>
<td>This setting specifies port speed and duplex configurations of the WAN port. By default, <strong>Auto</strong> is selected, and the appropriate data speed is automatically detected by the Peplink Balance. In the event of negotiation issues, the port speed can be manually specified. You can also choose whether or not to advertise the speed to the peer by selecting <strong>Advertise Speed</strong>.</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
</tr>
<tr>
<td>This setting specifies the maximum transmission unit. By default, MTU is set to <strong>Custom 1440</strong>. You may adjust the MTU value by editing the text field. Click <strong>Default</strong> to restore the default MTU value. Select <strong>Auto</strong>, and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes.</td>
</tr>
<tr>
<td><strong>MSS</strong></td>
</tr>
<tr>
<td>This setting should be configured based on the maximum payload size that the local system can handle. The MSS (maximum segment size) is computed by taking the MTU and subtracting 40 bytes for TCP over IPv4. If MTU is set to <strong>Auto</strong>, MSS will also be set automatically. By default, MSS is set to <strong>Auto</strong>.</td>
</tr>
<tr>
<td><strong>MAC Address Clone</strong></td>
</tr>
<tr>
<td>This setting allows you to configure the MAC address. Some service providers (e.g., cable providers) identify the client’s MAC address and require the client to always use the same MAC address to connect to the network. In such cases, change the WAN interface’s MAC address to the original client PC’s MAC address via this field. The default MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking the <strong>Default</strong> button restores the MAC address to the default value.</td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
</tr>
<tr>
<td>Some service providers require the router to enable VLAN tagging for Internet traffic. If it is required by your service provider, you can enable this field and enter the <strong>VLAN ID</strong> that the provider requires. Note: leave this field disabled if you are not sure.</td>
</tr>
</tbody>
</table>
13.2 Connection Method(s)

There are four possible connection methods:

1. DHCP
2. Static IP
3. PPPoE
4. L2TP
5. Mobile Internet Connection (for USB WAN)

13.2.1 DHCP Connection

The DHCP connection method is suitable if your ISP provides an IP address automatically using DHCP (e.g., cable, metro Ethernet, etc.).

**DHCP Settings**

<table>
<thead>
<tr>
<th>Hostname (Optional)</th>
<th>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 a hostname, you can safely bypass this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Servers</td>
<td>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 <strong>Obtain DNS server address automatically</strong> results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When <strong>Use the following DNS server address(es)</strong> is selected, you may enter custom DNS server addresses for this WAN connection into the <strong>DNS server 1</strong> and <strong>DNS server 2</strong> fields.</td>
</tr>
</tbody>
</table>

Please refer to Sections 13.3, 13.4, 13.5, and 13.6 for details about WAN Health Check, Bandwidth Allowance Monitor, Additional Public IP Settings, and Dynamic DNS Settings.
13.2.2 Static IP Connection

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

### Static IP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>These settings 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 your ISP.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specified in CIDR notation. The typical value is /24 for most connections.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>These settings 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 your ISP.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Each ISP may provide a set of DNS servers for DNS lookups. This field specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. You can input the ISP-provided DNS server addresses into the DNS server 1 and DNS server 2 fields. If no address is entered here, this link will not be used for DNS lookups.</td>
</tr>
</tbody>
</table>

---

http://www.peplink.com  -97 / 266 -  Copyright © 2016 Peplink
13.2.3 PPPoE Connection
This connection method is suitable if your ISP provides a login ID/password to connect via PPPoE.

<table>
<thead>
<tr>
<th>PPPoE Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPPoE User Name</td>
<td>Enter the required information in these fields in order to connect via PPPoE to your ISP. The parameter values are determined by and can be obtained from your ISP.</td>
</tr>
<tr>
<td>PPPoE Password</td>
<td>Verify your password by entering it again in this field.</td>
</tr>
<tr>
<td>Confirm PPPoE Password</td>
<td>Server name is a PPPoE parameter which is provided by your ISP.</td>
</tr>
<tr>
<td>Service Name (Optional)</td>
<td>Note: Leave this field blank unless it is provided by your ISP.</td>
</tr>
<tr>
<td>IP Address (Optional)</td>
<td>PPPoE server address is a parameter which is provided by your ISP.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>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 <strong>Obtain DNS server address automatically</strong> results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.) When <strong>Use the following DNS server address(es)</strong> is selected, you can enter custom DNS server addresses for this WAN connection into the <strong>DNS server 1</strong> and <strong>DNS server 2</strong> fields.</td>
</tr>
</tbody>
</table>

Please refer to Sections 13.3, 13.4, 13.5, and 13.6 for details about **WAN Health Check**, **Bandwidth Allowance Monitor**, **Additional Public IP Settings**, and **Dynamic DNS Settings**.

<table>
<thead>
<tr>
<th>Note</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A PPPoE connection made from a firewall does not work with drop-in mode.</td>
<td></td>
</tr>
</tbody>
</table>
13.2.4 L2TP Connection

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

- **L2TP User Name / Password**: Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.

- **Confirm L2TP Password**: Verify your password by entering it again in this field.

- **Server IP Address / Host**: L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.

- **Address Type**: Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.

- **DNS Servers**: Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.

  - Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)

  - 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.
13.2.5 Mobile Internet Connection

The Mobile Internet Connection method is suitable for USB modem mobile connections, such as 3G, WiMAX, LTE, EVDO, EDGE, and GPRS. Currently, it only applies to connections made via the Balance’s USB mobile WAN port, except in the case of the Balance units that include a built-in 4G LTE modem. For a list of supported modems, please refer to Peplink Modem Support page at http://www.peplink.com/modem.

![Mobile Internet Connection Settings](image)

<table>
<thead>
<tr>
<th><strong>WAN Connection Name</strong></th>
<th>Enter a name for this WAN connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
<td>Click the box to enable the connection.</td>
</tr>
<tr>
<td><strong>Connection Type</strong></td>
<td>This setting specifies the utilization of the WAN connection. <strong>Always-on</strong> results in the WAN connection being used whenever it is available. If <strong>Backup</strong> is selected, the WAN connection is treated as a backup connection and is used only in the absence of an available always-on WAN. The default and recommended connection type is <strong>Always-on</strong>.</td>
</tr>
<tr>
<td><strong>Standby State</strong></td>
<td>This option allows you to choose whether to remain connected or disconnect when this WAN connection is no longer in the highest priority and has entered the standby state. When <strong>Remain connected</strong> is chosen and this WAN connection is made active, the WAN connection will be immediately available for use.</td>
</tr>
<tr>
<td><strong>Idle Disconnect</strong></td>
<td>With this option enabled, an idle connection will be disconnected after a specified period of time. This time value specified is global and will affect all WAN profiles. The mobile connection will re-establish on demand.</td>
</tr>
<tr>
<td><strong>Reply to ICMP Ping</strong></td>
<td>If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.</td>
</tr>
</tbody>
</table>
## Operator Settings
This setting applies to 3G/LTE/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems.

**Operator Settings** allows you to configure the APN settings of your connection. If **Auto** is selected, the Peplink Balance will automatically detect the APN, configure the modem, and make a connection. You may change the APN settings by selecting **Custom Mobile Operator Settings**. The default and recommended **Operator Settings** value is **Auto**. The correct values can be obtained from your mobile Internet service provider.

## SIM PIN (Optional)
This is an optional field which is only needed when there is SIM lock for your SIM card service.

## DNS Servers
Each ISP may provide a set of DNS servers for DNS lookups. This field specifies the DNS servers to be used when a DNS lookup is routed through this connection. You can input the ISP-provided DNS server addresses into the **DNS server 1** and **DNS server 2** fields. If no address is entered here, this link will not be used for DNS lookups.

Please refer to Sections 13.3, 13.4, 13.5, and 13.6 for details about **WAN Health Check**, **Bandwidth Allowance Monitor**, **Additional Public IP Settings**, and **Dynamic DNS Settings**.
13.2.5.1 Modem Specific Custom Settings

The following settings may be available, depending on the modem model. The example below is for a 3G modem.

<table>
<thead>
<tr>
<th>Modem Specific Custom Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem Model</td>
</tr>
<tr>
<td>IMSI</td>
</tr>
<tr>
<td>Network Type</td>
</tr>
<tr>
<td>GSM Frequency Band</td>
</tr>
<tr>
<td>xxx Modem</td>
</tr>
<tr>
<td>123400005678900</td>
</tr>
<tr>
<td>3G preferred</td>
</tr>
<tr>
<td>All Bands</td>
</tr>
</tbody>
</table>

**Modem Specific Custom Settings**

- **Modem Model**: This field displays the manufacturer name of the connected mobile modem.

- **IMSI**: This field shows the IMSI number associated with the SIM inside the mobile modem.

- **Network Type**: This setting allows you to define your preference for using 3G and/or 2G networks. 3G networks include HSPA/UMTS. 2G networks include EDGE/GPRS. If **3G only** or **2G only** is chosen, only the HSPA/UMTS or EDGE/GPRS network will be used, respectively. If the chosen network is not available, no other network will be used, regardless of its availability. The modem connection will remain offline. If **3G preferred** or **2G preferred** is chosen, the chosen network will be used when it is available. If the chosen network is not available, the other network will be used whenever available. The default network type is **3G preferred**.

- **GSM Frequency Band**: This setting allows you to specify which GSM frequency band will be used. GSM1900 is used in the United States, Canada, and many other countries in the Americas. GSM900 / GSM1800 / GSM2100 are used in Europe, the Middle East, Africa, Asia, Oceania, and Brazil. If **All Bands** is chosen, the appropriate frequency band will be used automatically. The default GSM frequency band is **All Bands**.
13.2.5.2 WiMAX Settings

If a WiMAX modem is present in the system, its settings user interface can be accessed at Network>Interfaces>WAN>Mobile Internet. The example shown here relates to Sprint's 250U or 600U WiMAX modems.

<table>
<thead>
<tr>
<th>Modem Specific Custom Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem Model</td>
<td>Sprint Modem</td>
</tr>
<tr>
<td>ESN</td>
<td>C781C781</td>
</tr>
<tr>
<td>Network Type</td>
<td>4G only, 4G only, 3G only</td>
</tr>
</tbody>
</table>

### Modem Specific Custom Settings

<table>
<thead>
<tr>
<th>Modem Model</th>
<th>The brand of the modem is automatically detected and appears here.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESN</td>
<td>The modem's electronic serial number (ESN) is also auto-detected and appears here.</td>
</tr>
<tr>
<td>Network Type</td>
<td>This is to specify the network type (e.g., 3G or 4G) to be used with the modem.</td>
</tr>
</tbody>
</table>
13.3 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Peplink Balance can periodically check the health of each WAN connection. Health Check settings for each WAN connection can be independently configured via Network>Interfaces>WAN>*Connection name*>Health Check Settings.

Enable Health Check by selecting PING, DNS Lookup, or HTTP from the Health Check Method drop-down menu.

<table>
<thead>
<tr>
<th>Health Check Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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

**Health Check Method: PING**

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

**PING Hosts**

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

**Health Check Method: DNS Lookup**

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

**DNS Servers**

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

- If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection’s health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.
- If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

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

### Health Check Method: HTTP

<table>
<thead>
<tr>
<th>Health Check Method</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL 1</td>
<td>http://</td>
</tr>
<tr>
<td>URL 2</td>
<td>http://</td>
</tr>
</tbody>
</table>

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

#### URL 1

WAN Settings > WAN Edit > Health Check Settings > URL 1  
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 > URL 2  
If **URL 2** is also provided, a health check will pass if either one of the tests passed.
Other Health Check Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is 5 seconds.</td>
</tr>
<tr>
<td>Health Check Interval</td>
<td>This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is 5 seconds.</td>
</tr>
<tr>
<td>Health Check Retries</td>
<td>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.</td>
</tr>
<tr>
<td>Recovery Retries</td>
<td>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.</td>
</tr>
</tbody>
</table>

Note

If a WAN connection goes down, all of the WAN connections not set with a Connection Type of Always-on will also be brought up until any one of higher priority WAN connections is up and found to be healthy. This design could increase overall network availability.

For example, if WAN1, WAN2, and WAN3 have connection types of Always-on, Backup Priority Group 1, and Backup Priority Group 2, respectively, when WAN1 goes down, WAN2 and WAN3 will try to connect. If WAN3 is connected first, WAN2 will still be kept connecting. If WAN2 is connected, WAN3 will disconnect or abort making connection.

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to DNS Lookup and checks fail, the Balance will automatically perform DNS lookups on some 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.
13.4 Bandwidth Allowance Monitor

The Bandwidth Allowance Monitor helps track your network usage. Please refer to Section 27.8 to view usage statistics.

<table>
<thead>
<tr>
<th>Bandwidth Allowance Monitor Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
</tr>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Email notification is currently disabled. You can get notified when usage hits 75% or 95% of monthly allowance by enabling <strong>Email Notification</strong>. Disconnect when usage hits 100% of monthly allowance.</td>
</tr>
<tr>
<td><strong>Start Day</strong></td>
</tr>
<tr>
<td>On 1st of each month at 00:00 midnight</td>
</tr>
<tr>
<td><strong>Monthly Allowance</strong></td>
</tr>
<tr>
<td>100 GB</td>
</tr>
</tbody>
</table>

**Bandwidth Allowance Monitor**

**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.

**Monthly Allowance**

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

**Disclaimer**

Due to different network protocol overheads and conversions, the amount of data reported by this Peplink device is not representative of actual billable data usage as metered by your network provider. Peplink disclaims any obligation or responsibility for any events arising from use of the numbers shown here.
13.5 Additional Public IP Settings

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

The Peplink Balance allows registering 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 hostname. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address externally 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 Peplink Balance will connect to the dynamic DNS service provider to update the provider's IP address records.

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via Network>Interfaces>WAN>*Connection name*>Dynamic DNS Settings.

If your desired provider is not listed, you may check with DNS-O-Matic. This service supports updating 30 other dynamic DNS service providers. (Note: Peplink is not affiliated with DNS-O-Matic.)
## Dynamic DNS Settings

This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:

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

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

Select **Disabled** to disable this feature.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Provider</strong></td>
<td>This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:</td>
</tr>
<tr>
<td></td>
<td>• changeip.com</td>
</tr>
<tr>
<td></td>
<td>• dyndns.org</td>
</tr>
<tr>
<td></td>
<td>• no-ip.org</td>
</tr>
<tr>
<td></td>
<td>• tzo.com</td>
</tr>
<tr>
<td></td>
<td>• DNS-O-Matic</td>
</tr>
<tr>
<td></td>
<td>• Others…</td>
</tr>
<tr>
<td><strong>User ID / User / Email</strong></td>
<td>This setting specifies the registered user name for the dynamic DNS service.</td>
</tr>
<tr>
<td><strong>Password / Pass / TZO Key</strong></td>
<td>This setting specifies the password for the dynamic DNS service.</td>
</tr>
<tr>
<td><strong>Update All Hosts</strong></td>
<td>Check this box to automatically update all hosts.</td>
</tr>
<tr>
<td><strong>Hosts / Domain</strong></td>
<td>This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.</td>
</tr>
</tbody>
</table>

## Important Note

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

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

Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been not updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a WAN's IP address did not change.
Peplink Balance SpeedFusion™ Bandwidth Bonding is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion securely connects one or more branch offices to your company's main headquarters or to other branches. The data, voice, and video communications between these locations are kept confidential across the public Internet.

The SpeedFusion™ of the Peplink Balance is specifically designed for multi-WAN environments. With SpeedFusion, in case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic. The Peplink Balance can bond all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, the Peplink Balance can keep the VPN up and running. Bandwidth bonding is enabled by default.

**14.1 SpeedFusion™ Settings**

Some Peplink Balance models support making multiple SpeedFusion™ connections with a remote Peplink Balance, MediaFast, or Pepwave MAX mobile router. 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.

A Peplink Balance that supports multiple VPN connections can act as a central hub which connects branch offices. For example, if Branch Office A and Branch Office B make VPN connections to Headquarters C, both branch office LAN subnets and the subnets behind them (i.e., static routes) will also be advertised to Headquarters C and the other branches. So Branch Office A will be able to access Branch Office B via Headquarters C in this case.

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 with 256-bit AES encryption standard. To configure this, navigate to **Network>Interfaces>SpeedFusion**.

### PepVPN with SpeedFusion

InControl management enabled. Settings can now be configured on InControl.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Remote ID</th>
<th>Remote Address(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IL Office</td>
<td>Balance_2003</td>
<td>x</td>
</tr>
<tr>
<td>NY Office</td>
<td>Balance_FBDS</td>
<td>x</td>
</tr>
</tbody>
</table>

#### Send All Traffic To

No PepVPN profile selected

#### PepVPN Local ID

Local ID: Balance_01AA

#### PepVPN Settings

- **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 button]

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

### PepVPN Profile Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>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 ( ). Click the icon next to the PepVPN Profile title bar to use the IP ToS field of your data packet on PepVPN WAN traffic.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Remote ID / Pre-shared Key</strong></td>
<td>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. 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.</td>
</tr>
<tr>
<td><strong>Remote ID/Remote Certificate</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Allow Shared Remote ID</strong></td>
<td>When this option is enabled, the router will allow multiple peers to run using the same remote ID.</td>
</tr>
<tr>
<td><strong>NAT Mode</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Remote IP Address / Host Names</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

Click the icon to customize the handshake port (TCP)

<table>
<thead>
<tr>
<th>Data Port</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Limit</td>
<td>Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.</td>
</tr>
<tr>
<td>Cost</td>
<td>Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10</td>
</tr>
<tr>
<td>WAN Smoothing</td>
<td>While using PepVPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN's available bandwidth.</td>
</tr>
</tbody>
</table>

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>*LAN Profile Name* and refer to instructions in section 0.
WAN Connection Priority

These settings specify the priority of the WAN connections to be used in making VPN bonding connections. A WAN connection will never be used when OFF is selected. Only available WAN connections with the highest priority will be utilized.

To allow connection mapping to remote WANs, click the question mark icon found at the top right of this section, and then click the displayed link to reveal the Connect to Remote drop-down menu.

Send All Traffic To

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

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

PepVPN Local ID

This feature allows you to change the local ID of a PepVPN connection. Click the button to select your...
connection and the following menu will appear:

![PepVPN Settings](image)

After updating the local ID, click **Save** to store your changes.

---

**Link Failure Detection**

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.

**Link Failure Detection Time**

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

---

**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 Peplink Balance 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**
Watch a video walkthrough of setting up a SpeedFusion™ VPN on our YouTube Channel!

http://youtu.be/xNaq13FWu_g
14.2 The Peplink Balance Behind a NAT Router

The Peplink Balance supports 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 Peplink Balance.

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:

![Diagram of Peplink Balance Behind a NAT Router]

One of the WANs connected to Balance A is non-NAT’d (212.1.1.1). The rest of the WANs connected to Balance A and all WANs connected to Balance B are NAT’d. In this case, the Peer IP Addresses / Host Names field for Balance B should be filled with all of Balance 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 Balance A can be left blank. The two NAT routers on WAN1 and WAN3 connected to Balance A should inbound port-forward TCP port 32015 to Balance A so that all WANs will be utilized in establishing the VPN.
14.3 SpeedFusion™ Status

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

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 27.6 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.
15 IPsec VPN

Peplink Balance 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 the Peplink Balance is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for his 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.

15.1 IPsec VPN Settings

All Peplink products can make multiple IPsec VPN connections with Peplink routers, as well as 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, navigate to Network>Interfaces>IPsec VPN.

A NAT-Traversal option and list of defined IPsec VPN profiles will be shown. NAT-Traversal should be enabled if your system is behind a NAT router.

Click the New Profile button to create new IPsec VPN profiles that make VPN connections to remote Peplink Balance, 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Profile 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>✔</td>
</tr>
</tbody>
</table>

**Connect Upon Disconnection of**
- ✔ WAN 2

**Remote Gateway IP Address / Host Name**
- 12.12.12.12

**Local Networks**
- Propose the following networks to remote gateway:
  - ✔ 172.16.1.1/24
  - ✔ 172.16.2.1/24
  - ✔ 172.16.3.1/24
  - ✔ 10.10.0.1/32
  - ✔ 192.168.10.0/24
  - ✔ 192.168.11.0/24

**Apply the following NAT policies:**
- ✔ 172.16.1.0/24
- ✔ 172.16.2.0/24
- ✔ 172.16.3.0/24
- ✔ 192.168.10.0/24
- ✔ 192.168.11.0/24

**Remote Networks**

<table>
<thead>
<tr>
<th>Network</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.167.11.193</td>
<td>255.255.255.0 (24)</td>
</tr>
</tbody>
</table>

**Authentication**
- ✔ Pre-shared Key
- X.509 Certificate

**Mode**
- ✔ Main Mode (All WANs need to have Static IP)
- Aggressive Mode

**Force UDP Encapsulation**
- ✔

**Pre-shared Key**
- ************
- ✔ Hide Characters

**Local ID**
- 

**Remote ID**
- 

**Phase 1 (IKE) Proposal**
1. AES-256 & SHA1
2. 

**Phase 1 DH Group**
- ✔ Group 2: MODP 1024
- Group 5: MODP 1536

**Phase 1 SA Lifetime**
- 3600 seconds Default

**Phase 2 (ESP) Proposal**
1. AES-256 & SHA1
2. 

**Phase 2 PFS Group**
- ✔ None
- Group 2: MODP 1024
- Group 5: MODP 1536

**Phase 2 SA Lifetime**
- 28800 seconds Default
## IPsec VPN Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>This field is for specifying a local name to represent this connection profile.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.</td>
</tr>
<tr>
<td><strong>Connect Upon Disconnection of</strong></td>
<td>Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected. To activate this function, click the button next to the “Active” option.</td>
</tr>
<tr>
<td><strong>Remote Gateway IP Address / Host Name</strong></td>
<td>Enter the remote peer’s public IP address. For <strong>Aggressive Mode</strong>, this is optional.</td>
</tr>
<tr>
<td><strong>Local Networks</strong></td>
<td>Enter the local LAN subnets here. If you have defined static routes, they will be shown here. 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. Two types of NAT policies can be defined: <strong>One-to-One NAT policy:</strong> if the defined subnet in Local Network and NAT Network has the same size, for example, policy “192.168.50.0/24 &gt; 172.16.1.0/24” will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too. <strong>Many-to-One NAT policy:</strong> if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy “192.168.1.0/24 &gt; 172.168.50.1/32” will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.</td>
</tr>
<tr>
<td><strong>Remote Networks</strong></td>
<td>Enter the LAN and subnets that are located at the remote site here.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>To access your VPN, clients will need to authenticate by your choice of methods. Choose between the <strong>Preshared Key</strong> and <strong>X.509 Certificate</strong> methods of authentication.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Choose <strong>Main Mode</strong> if both IPsec peers use static IP addresses. Choose <strong>Aggressive Mode</strong> if one of the IPsec peers uses dynamic IP addresses.</td>
</tr>
<tr>
<td><strong>Force UDP Encapsulation</strong></td>
<td>For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.</td>
</tr>
<tr>
<td><strong>Pre-shared</strong></td>
<td>This defines the peer authentication pre-shared key used to authenticate this VPN</td>
</tr>
</tbody>
</table>
### Key

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

<table>
<thead>
<tr>
<th>Priority</th>
<th>WAN Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WAN 1</td>
</tr>
<tr>
<td>2</td>
<td>----</td>
</tr>
</tbody>
</table>
15.2 **IPsec Status**

**IPsec Status** shows the current connection status of each connection profile and is displayed at **Status>IPsec VPN**.
Outbound Policy Management

The Peplink Balance 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 **Network>Outbound Policy**.

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

There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

<table>
<thead>
<tr>
<th>Outbound Policy Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Application Compatibility</strong></td>
</tr>
<tr>
<td><strong>Normal Application Compatibility</strong></td>
</tr>
<tr>
<td><strong>Custom</strong></td>
</tr>
</tbody>
</table>

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
16.2 Custom Rules for Outbound Policy

Click [ ] in the Outbound Policy form. Choose Custom and press the Save button. The following screen will then be displayed:

The bottom-most rule is Default. Edit this rule to change the device’s default manner of controlling outbound traffic for all connections that do not match any of the rules above it. Under the Service heading, Default to change these settings. To rearrange the priority of outbound rules, drag and drop them into the desired sequence.

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

To create a custom rule, click Add Rule at the bottom of the table. The following window will be displayed:
New Custom Rule Settings

<table>
<thead>
<tr>
<th>Service Name</th>
<th>This setting specifies the name of the outbound traffic rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>This setting specifies whether the outbound traffic rule takes effect. When Enable is checked, the rule takes effect: traffic is matched and actions are taken by the Peplink Balance based on the other parameters of the rule. When Enable is unchecked, the rule does not take effect: the Peplink Balance disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.</td>
</tr>
<tr>
<td>Source</td>
<td>This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.</td>
</tr>
</tbody>
</table>
Destination

This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.

If **Domain Name** is chosen and a domain name, such as foobar.com, is entered, any outgoing accesses to foobar.com and *.foobar.com will match this criterion. You may enter a wildcard (\*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter foobar.\*, for example, www.foobar.com, www.foobar.co.jp, or foobar.co.uk will also match. Placing wildcards in any other position is not supported.

NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.

Protocol and Port

This setting specifies the IP protocol and port of traffic that matches this rule. You may select common protocols from the **Protocol Selection Tool** drop-down menu.

Algorithm

This setting specifies the behavior of the Peplink Balance for the custom rule. One of the following values can be selected:

- Weighted Balance
- Persistence
- Enforced
- Priority
- Overflow
- Least Used
- Lowest Latency

The upcoming sections detail the listed algorithms.

Terminate Sessions on Link Recovery

This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the **Weighted**, **Persistence**, and **Priority** algorithms.

By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.

16.2.1 Algorithm: Weighted Balance

This setting specifies the ratio of WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Weighted Balance**.
The amount of matching traffic that is distributed to a WAN connection is proportional to the weight of the WAN connection relative to the total weight. Use the sliders to change each WAN’s weight.

For example, with the following weight settings on a Peplink Balance 310:

- WAN1: 10
- WAN2: 10
- WAN3: 5

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

Matching traffic distributed to WAN1 is 40% = (10 / 25) x 100%.

Matching traffic distributed to WAN2 is 40% = (10 / 25) x 100%.

Matching traffic distributed to WAN3 is 20% = (5 / 25) x 100%.

16.2.2 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.

The Peplink Balance 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 Peplink Balance may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Peplink Balance with three WAN connections may communicate on the Internet using three different IP addresses.

With the persistence feature of Peplink Balance, rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate using one IP address, eliminating the issues mentioned above.
There are two persistent modes: **By Source** and **By Destination**.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>By Source</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>By Destination</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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 **Download Bandwidth**, which is specified in the WAN settings page (see Section 13, Configuring the WAN Interface(s)). If you choose **Custom**, you can customize the weight of each WAN manually using the provided sliders.

### 16.2.3 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**.

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.

### 16.2.4 Algorithm: Priority

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

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

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

16.2.5 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.

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

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

16.2.7 Algorithm: Lowest Latency

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

Tip

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

- All WAN connections are symmetric; or
- A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN’s available bandwidth.
16.2.8 Expert Mode

**Expert Mode** is available for advanced users. To enable the feature, click on the help icon beside the **Rules** menu and click **turn on Expert Mode**.

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

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

Inbound access is also known as inbound port address translation. On a NAT WAN connection, all inbound traffic to the server behind the Peplink unit requires inbound access rules.

By the custom definition of servers and services for inbound access, Internet users can access the servers behind Peplink Balance. Advanced configurations allow inbound access to be distributed among multiple servers on the LAN.

<table>
<thead>
<tr>
<th>Important Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound access applies only to WAN connections that operate in NAT mode. For WAN connections that operate in drop-in mode or IP forwarding, inbound traffic is forwarded to the LAN by default.</td>
</tr>
</tbody>
</table>

17.1 Definition of Servers on LAN

The settings to configure servers on the LAN are located at Network> Inbound Access> Servers.

Inbound connections from the Internet will be forwarded to the specified Inbound IP address(es) based on the protocol and port number. When more than one server is defined, requests will be distributed to the servers in the weight ratio specified for each server.

To define a new server, click Add Server, which displays the following screen:

Enter a valid server name and its corresponding LAN IP address. Upon clicking Save after entering required information, the following screen appears.

To define additional servers, click Add Server and repeat the above steps.
17.2 Definition of Port Forwarding

Inbound port forwarding rules are defined at Network>Inbound Access>Port Forwarding.

To define a new service, click the Add Service button after adding a server under Network>Inbound Access>Service. The following screen is displayed:

![Port Forwarding Settings](image)

**Enable**
This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Peplink Balance based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Peplink Balance disregards the other parameters of the rule.

**Service Name**
This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore "_" characters.

**IP Protocol**
The IP Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Peplink Balance via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the Servers setting. Please see below for details on the Port and Servers settings. Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.) After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remain manually modifiable.
The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:

**Any Port, Single Port, Port Range, Port Map, and Range Mapping**

<table>
<thead>
<tr>
<th>Port</th>
<th>Any Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Any Port</strong></td>
<td>all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the <strong>Servers</strong> setting. For example, with <strong>IP Protocol</strong> set to TCP, and <strong>Port</strong> set to <strong>Any Port</strong>, all TCP traffic is forwarded to the configured servers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Single Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single Port</strong></td>
<td>traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the <strong>Servers</strong> setting. For example, with <strong>IP Protocol</strong> set to TCP, and <strong>Port</strong> set to <strong>Single Port</strong> and <strong>Service Port</strong> 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Range</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port Range</strong></td>
<td>traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the <strong>Servers</strong> setting. For example, with <strong>IP Protocol</strong> set to TCP, and <strong>Port</strong> set to <strong>Port Range</strong> and <strong>Service Ports</strong> 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port Mapping</strong></td>
<td>traffic that is received by Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the <strong>Servers</strong> setting. For example, with IP Protocol set to TCP, and Port set to <strong>Port Mapping</strong>, <strong>Service Port</strong> 80, and <strong>Map to Port</strong> 88, TCP traffic on Port 80 is forwarded to the configured servers via Port 88. (Please see below for details on the <strong>Servers</strong> setting.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Range Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Range Mapping</strong></td>
<td>traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the <strong>Servers</strong> setting.</td>
</tr>
</tbody>
</table>

**Inbound IP Address(es)**  This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.

**Server IP Address**  This setting specifies the LAN IP address of the server that handles the requests for the service.
17.3 Inbound Access Services

17.3.1 Definition of Services

Services are defined at Network>Inbound Access>Services.

Tip

At least one server must be defined before services can be added.

To define a new service, click the Add Service button, upon which the following menu appears:

- **Enable**
  - This setting specifies whether the inbound service rule takes effect.
  - When Yes is selected, the inbound service rule takes effect. If the inbound traffic matches the specified IP protocol and port, action will be taken by the Peplink Balance based on the other parameters of the rule.
  - When No is selected, the inbound service rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.

- **Service Name**
  - This setting identifies the service to the system administrator. Only alphanumeric and the underscore "_" characters are valid.

- **IP Protocol**
  - The IP Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Inbound traffic that matches the specified IP Protocol and Port(s) will be forwarded to the LAN hosts specified by the Servers setting.
  - Upon choosing a protocol, the Protocol Selection Tool drop-down menu can be used to automatically the port information of common Internet services (e.g. HTTP, HTTPS, etc.).
  - After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and the port number will remain manually modifiable.
The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:

**Any Port, Single Port, Port Range, Port Map, and Range Mapping**

**Any Port**: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, if **IP Protocol** is set to TCP and **Port** is set to **Any Port**, then all TCP traffic will be forwarded to the configured servers.

![Any Port](image)

**Single Port**: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, if **IP Protocol** is set to TCP, **Port** is set to **Single Port**, and **Service Port** is set to 80, then TCP traffic received on Port 80 will be forwarded to the configured servers via port 80.

![Single Port](image)

**Port Range**: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, if **IP Protocol** is set to TCP, **Port** is set to **Port Range**, and **Service Port** is set to 80-88, then TCP traffic received on ports 80 through 88 will be forwarded to the configured servers via the respective ports.

![Port Range](image)

**Port Mapping**: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. For example, if **IP Protocol** is set to TCP, **Port** is set to **Port Mapping**, **Service Port** is set to 80, and **Map to Port** is set to 88, then TCP traffic on port 80 is forwarded to the configured servers via port 88.

![Port Mapping](image)

(Please see below for details on the **Servers** setting.)

**Range Mapping**: traffic that is received by Peplink Balance via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.

![Range Mapping](image)

**Inbound IP Address(es)**: This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.

**Included Server(s)**: This setting specifies the LAN servers that handle requests for the service, and the relative weight values. The amount of traffic that is distributed to a server is proportional to the weight value assigned to the server relative to the total weight. Example:

With the following weight settings on a Peplink Balance:

- demo_server_1: 10
- demo_server_2: 5

The total weight is 15 = (10 + 5)

Matching traffic distributed to demo_server_1: 67% = (10 / 15) x 100%

Matching traffic distributed to demo_server_2: 33% = (5 / 15) x 100%
17.3.2 UPnP / NAT-PMP Settings

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

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

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

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

17.3.3 Definition of DNS Records

The built-in DNS server functionality of the Peplink Balance facilitates inbound load balancing. With this functionality, NS/SOA DNS records for a domain name can be delegated to the Internet IP address(es) of the Peplink Balance. Upon receiving a DNS query, the Peplink Balance can return (as an “A” record) the IP address for the domain name on the most appropriate healthy WAN connection. It can also act as a generic DNS server for hosting “A”, “CNAME”, “MX”, “TXT” and “NS” records.

For example:

(This example is for illustration only; the actual resolution that takes place in implementation will likely be different.)

The DNS resolution of the domain name www.mycompany.com is delegated to the WAN2 Internet IP addresses of the Peplink Balance.

Upon receiving the DNS query, the Peplink Balance returns (as an “A” record) the IP address for www.mycompany.com on WAN1 because WAN1 is the most appropriate healthy link.

The settings for defining the DNS records to be hosted by the Peplink Balance are located at Network>Inbound Access>DNS Settings.
DNS Settings

This setting specifies the WAN IP addresses on which the DNS server of the Peplink Balance should listen.

If no addresses are selected, the inbound link load balancing feature will be disabled and the Peplink Balance will not respond to DNS requests.

To specify and/or modify the IP addresses on which the DNS server should listen, click the button that corresponds to DNS Server, and the following screen is displayed:

DNS Servers

To specify the Internet IP addresses on which the DNS server should listen, select the desired WAN connection then select the desired associated IP addresses. (Multiple items in the list can be selected by holding CTRL and clicking on the items.)

Click Save to save the settings when configuration is complete.
### Zone Transfer

This setting specifies the IP address(es) of the secondary DNS server(s) authorized to retrieve zone records from the DNS server of the Peplink Balance. The zone transfer server of the Peplink Balance listens on TCP port 53.

<table>
<thead>
<tr>
<th>Zone Transfer Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Clients</td>
</tr>
<tr>
<td>11.12.13.123</td>
</tr>
</tbody>
</table>

The Peplink Balance serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing its LAN interface.

### Routing Control by Subnet Database

When this function is enabled, the system will check to see if an incoming DNS client is within any WAN's ISP subnet. Only the matched WAN(s)'s IP addresses will be returned. Note that this feature is available only when a subnet database has been defined.

### Default SOA / NS

Click the button to define a default SOA / NS record for all domain names. For configuration details please refer to Section 17.3.5.

<table>
<thead>
<tr>
<th>Default SOA Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Server</td>
</tr>
<tr>
<td>Name Server IP Address</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>Refresh (sec)</td>
</tr>
<tr>
<td>Retry (sec)</td>
</tr>
<tr>
<td>Expire (sec)</td>
</tr>
<tr>
<td>Min Time (sec)</td>
</tr>
<tr>
<td>TTL (sec)</td>
</tr>
</tbody>
</table>

When defining a default SOA record, **Name Server IP Address** is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain. For defining default NS records, the host [domain] indicates that this record is for the domain name itself without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the **Host** field left empty. When the entered name server is a fully qualified domain name (FQDN), the **IP Address** field will be disabled.

### Default Connection Priority

**Default Connection Priority** defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the **Connection Priority** set to **Default**. Please refer to Section 17.3.9 for details.

The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable.

To specify the primary and backup connections, click the button that corresponds to **Default Connection Priority**. The following screen will appear:
Each WAN connection is associated with a priority number. Click **Save** to save the settings when configuration is complete.

<table>
<thead>
<tr>
<th>Domain name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its “NS”, “MX” and “TXT” records, and its sub-domains’ “A” and “CNAME” records. Add a new record by clicking the <strong>New Domain Name</strong> button. Click on a domain name to edit. Press <strong>X</strong> to remove a domain name.</td>
</tr>
</tbody>
</table>
17.3.4 Creating DNS Records

To create new DNS records for a domain, perform the following steps:

From **Network > Inbound Access > DNS Settings**, click **New Domain Name** in the **Domain Name** field. Then click on the newly created domain name and the following screen will be displayed:

This page is for defining the domain’s SOA, NS, MX, CNAME, A, TXT, and SRV records. Seven tables are presented in this page for defining the five types of records.
17.3.5 SOA Records

Click on the icon to choose whether to use the pre-defined default SOA record and NS records. If the option **Use Default SOA and NS Records** is selected, any changes made in the default SOA/NS records will be applied to this domain automatically. Otherwise, select the option **Customize SOA Record** for this domain to customize this domain's SOA and NS records.

This table displays the current SOA record. When the option **Customize SOA Record for this domain** is selected, you can click the link **Click here to define SOA record** to create or click on the **Name Server** field to edit the SOA record.

In the SOA record, you have to fill out the fields **Name Server**, **Name Server IP Address**, **Email**, **Refresh**, **Retry**, **Expire**, **Min Time**, and **TTL**.

Default values are set for SOA and NS records,

- **Name Server IP Address**: This is the IP address of the authoritative name server. An entry in this field is optional. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically. If it is left blank, the A record for the name server must be created manually.
• **E-mail**: Defines the e-mail address of the person responsible for this zone. Note: format should be `mailbox-name.domain.com`, e.g., `hostmaster.example.com`.

• **Refresh**: Indicates the length of time (in seconds) when the slave will try to refresh the zone from the master.

• **Retry**: Defines the duration (in seconds) between retries if the slave (secondary) fails to contact the master and the refresh (above) has expired.

• **Expire**: Indicates the time (in seconds) when the zone data is no longer authoritative. This option applies to slave DNS servers only.

• **Min Time**: Is the negative caching time which defines the time (in seconds) after an error record is cached.

• **TTL (Time-to-Live)**: Defines the duration (in seconds) that the record may be cached.

### 17.3.6 NS Records

The **NS Records** table shows the NS servers and TTL that correspond to the domain. The NS record of the name server defined in the SOA record is automatically added here.

To add a new NS record, click the **New NS Records** button in the **NS Records** box. Then the table will expand to look like the following:

![NS Records Table](image)

When creating an NS record for the domain itself (not a sub-domain), the **Host** field should be left blank.

Enter a name server host name and its IP address into the corresponding boxes. The host name can be a non-FQDN (fully qualified domain name). Please be sure that a corresponding A record is created. Click the **+** button on the right to finish and to add other name servers. Click the **Save** button to save your changes.
17.3.7 MX Records

The **MX Record** table shows the domain's MX records. To add a new MX record, click the **New MX Records** button in the **MX Records** box. Then the table will expand to look like the following:

![MX Records](image)

When creating an MX record for the domain itself (not a sub-domain), the **Host** field should be left blank.

For each record, **Priority** and **Mail Server name** must be entered. **Priority** typically ranges from 10 to 100. Smaller numbers have a higher a priority. After finishing adding MX records, click the **Save** button.

17.3.8 CNAME Record

The **CNAME Record** table shows the domain's CNAME records. To add a new CNAME record, click the **New CNAME Records** button in the **CNAME Record** box. Then the table will expand to look like the following:

![CNAME Record](image)

When creating a CNAME record for the domain itself (not a sub-domain), the **Host** field should be left blank.

The wildcard character "*" is supported in the **Host** field. The reference of ".domain.name" will be returned for every name ending with ".domain.name" except names that have their own records.

The **TTL** field tells the time to live of the record in external DNS caches.
17.3.9 A Record

This table shows the A records of the domain name. To add an A record, click the New A Record button. The following screen will appear:

![A Record](image)

A record may be automatically added for the SOA records with a name server IP address provided.

<table>
<thead>
<tr>
<th>A Record</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Name</strong></td>
<td>This field specifies the A record of this sub-domain to be served by the Peplink Balance. The wildcard character &quot;<em>&quot; is supported. The IP addresses of &quot;</em>.domain.name&quot; will be returned for every name ending with &quot;.domain.name&quot; except names that have their own records.</td>
</tr>
<tr>
<td><strong>TTL</strong></td>
<td>This setting specifies the time to live of this record in external DNS caches. In order to reflect any dynamic changes on the IP addresses in case of link failure and...</td>
</tr>
</tbody>
</table>
Priority

This option specifies the priority of different connections. Select the Default option to apply the Default Connection Priority (refer to the table shown on the main DNS settings page) to an A record. To customize priorities, choose the Custom option and a priority selection table will be shown at the bottom.

Included IP Address(es)

This setting specifies lists of WAN-specific Internet IP addresses that are candidates to be returned when the Peplink Balance responds to DNS queries for the domain name specified by Host Name.

The IP addresses listed in each box as default are the Internet IP addresses associated with each of the WAN connections. Static IP addresses that are not associated with any WAN can be entered into the Custom IP list. A PTR record is also created for each custom IP.

For WAN connections that operate under drop-in mode, there may be other routable IP addresses in addition to the default IP address. Therefore, the Peplink Balance allows custom Internet IP addresses to be added manually via filling the text box on the right-hand side and clicking the button.

Only the checked IP addresses in the lists are candidates to be returned when responding to a DNS query.

If a WAN connection is down, the corresponding set of IP addresses will not be returned. However, the IP addresses in the Custom IP Address field will always be returned.

If the Connection Priority field is set to Custom, you can also specify the usage priority of each WAN connection. Only selected IP address(es) of available connection(s) with the highest priority, and custom IP addresses will be returned. By default, Connection Priority is set to Default.

17.3.10 PTR Records

PTR records are created along with A records pointing to custom IPs. Please refer to Section 17.3.9 for details. For example, if you created an A record www.mydomain.com pointing to 11.22.33.44, then a PTR record 44.33.22.11.in-addr.arpa pointing to www.mydomain.com will also be created. When there are multiple host names pointing to the same IP address, only one PTR record for the IP address will be created. In order for PTR records to function, you also need to create NS records. For example, if the IP address range 11.22.33.0 to 11.22.33.255 is delegated to the DNS server on the Peplink Balance, you will also have to create a domain 33.22.11.in-addr.arpa and have its NS records pointing to your DNS server's (the Peplink Balance's) public IP addresses. With the above records created, the PTR record creation is complete.

17.3.11 TXT Records

This table shows the TXT record of the domain name.
To add a new TXT record, click the **New TXT Record** button in the **TXT Records** box. Click the **Edit** button to edit the record. The time-to-live value and the TXT record’s value can be entered. Click the **Save** button to finish.

When creating a TXT record for the domain itself (not a sub-domain), the **Host** field should be left blank.

The maximum size of the TXT Value is 255 bytes.

After editing the five types of records, you can leave the page by simply going to another section of the web admin interface.

### 17.3.12 SRV Records

To add a new SRV record, click the **New SRV Record** button in the **SRV Records** box.

- **Service**: The symbolic name of the desired service.
- **Priority**: Indicates the priority of the target; the smaller the value, the higher the priority.
- **Weight**: A relative weight for records with the same priority.
- **Target**: The canonical hostname of the machine providing the service.
- **Port**: Enter the TCP or UDP port number on which the service is to be found.
Domain Delegation

These are the steps to follow when you host your domain at an ISP or domain registrar and want to delegate a sub-domain to be resolved and managed by the Peplink Balance.

- Click the **New Domain Name** button to add a domain name (e.g., www.mycompany.com). Click the corresponding domain name to view and edit record details.

- Create SOA/NS records named *ns1*, *ns2*, etc. The IP addresses are the Balance’s DNS server addresses.

- Then create an A record with an empty host name.
If ISC BIND 8 or 9 is being utilized in the zone file mycompany.com, add the following lines:

```
www IN NS balancewan1
www IN NS balancewan2
balancewan1 IN A 202.153.122.108
balancewan2 IN A 67.38.212.18
```

202.153.122.108 and 67.38.212.18 represent the WAN1 and WAN2 Internet IP addresses of the Peplink Balance, respectively. The values of the IP addresses are fictitious and for illustration only.

**Hosting the complete domain at Peplink Balance**

To host your own DNS server, contact the DNS registrar to have the NS records of the domain (e.g., mycompany.com) point to your Balance's WAN IP addresses. Then follow these instructions:

1. Under **Network>Inbound Access>DNS Settings**, create a new domain (e.g., mycompany.com).
2. Create NS records named *ns1*, *ns2*, etc. The IP addresses are the Balance’s DNS server addresses (same...
3. Create the corresponding A, CNAME, MX, and TXT records as you wish. The A record resembles the one below:

![A Records](image)

### Testing the DNS Configuration

The following steps can be used to test the DNS configuration:

From a host on the Internet, use an IP address of the Peplink Balance and nslookup to lookup the corresponding host name. Check the information that is returned for the expected results.

An nslookup in Windows will appear as follows:

```
C:\Documents and Settings\User Name>nslookup
Default Server: ns1.myisp.com
Address: 147.22.11.2
>server 202.153.122.108 (This is Peplink Balance’s WAN IP address.)
Default Server: balance.mycompany.com
Address: 202.153.122.108
>www.mycompany.com (This is the hostname to be looked up.)
Default Server: balance.mycompany.com
Address: 202.153.122.108
Name: www.mycompany.com
Address: 202.153.122.109, 67.38.212.19
```

Please note that the values of the IP addresses are fictitious and for illustration only.
17.4 Reverse Lookup Zones

Reverse lookup zones can be configured in Network>Inbound Access>DNS Settings.

Reverse lookup refers to performing a DNS query to find one or more DNS names associated with a given IP address. The DNS stores IP addresses in the form of specially formatted names as pointer (PTR) records using special domains/zones. The zone is `in-addr.arpa`.

To enable DNS clients to perform a reverse lookup for a host, perform two steps:

- Create a reverse lookup zone that corresponds to the subnet network address of the host. In the reverse lookup zone, add a pointer (PTR) resource record that maps the host IP address to the host name.
- Click the New Reverse Lookup Zone button and enter a reverse lookup zone name. If you are delegated the subnet 11.22.33.0/24, the Zone Name should be 33.22.11.in-addr.arpa. PTR records for 11.22.33.1, 11.22.33.2, ... 11.22.33.254 should be defined in this zone where the host IP numbers are 1, 2, ... 254, respectively.
17.4.1 SOA Record

You can click the link **Click here to define SOA record** to create or click on the **Name Server** field to edit the SOA record.

**Name Server**: Enter the NS record's FQDN server name here.

For example:

"ns1.mydomain.com" (equivalent to "www.1stdomain.com.")

"ns2.mydomain.com."

**Email, Refresh, Retry, Expire, Min Time, and TTL** are entered in the same way as in
the forward zone. Please refer to Section 17.3.5 for details.

17.4.2 NS Records

The NS record of the name server defined in the SOA record is automatically added here. To create a new NS record, click the New NS Records button.

When creating an NS record for the reverse lookup zone itself (not a sub-domain or dedicated zone), the Host field should be left blank. Name Server must be a FQDN.

17.4.3 CNAME Records

To create a new CNAME record, click the New CNAME Record button.

CNAME records are typically used for defining classless reverse lookup zones. Subnetted reverse lookup zones are further described in RFC 2317, "Classless IN-ADDR.ARPA delegation."
17.4.4 PTR Records

To create a new PTR record, click the **New PTR Record** button.

For **Host IP Number** field, enter the last integer in the IP address of a PTR record. For example, for the IP address **11.22.33.44**, where the reverse lookup zone is **33.22.11.in-arpa.addr**, the **Host IP Number** should be **44**.

The **Points To** field defines the host name which the PTR record should be pointed to. It must be a FQDN.
17.5 DNS Record Import Wizard

At the bottom of the DNS settings page, the link **Import records via zone transfer...** is used to import DNS record using an import wizard.

- Select **Next >>** to continue.

- In the **Target DNS Server IP Address** field, enter the IP address of the DNS server.
- In the **Transfer via...** field, choose the connection which you would like to transfer through.
- Select **Next >>** to continue.
• In the blank space, enter the **Domain Names (Zones)** which you would like to assign the IP address entered in the previous step. Enter one domain name per line.

• Select **Next >>** to continue.

**Important Note**

If you have entered domain(s) which already exist in your settings, a warning message will appear. Select **Next >>** to overwrite the existing record or **<< Back** to go back to the previous step.
DNS Record Import Wizard

Fetching zone records...

Abort

DNS Record Import Wizard

Step 3 of 3
Fetch Results

<table>
<thead>
<tr>
<th>Domain</th>
<th>Result</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>peplink.com</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>mycompany.com</td>
<td>Ok</td>
<td></td>
</tr>
</tbody>
</table>

Cancel
After the zone records process have been fetched, the fetch results would be shown as above. You can view import details by clicking the corresponding hyperlink on the right-hand side.

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOA</td>
<td>mytest.com</td>
<td>ns1.mytest.com.</td>
</tr>
<tr>
<td>NS</td>
<td>mytest.com</td>
<td>ns1.mytest.com.</td>
</tr>
<tr>
<td>NS</td>
<td>mytest.com</td>
<td>ns2.mytest.com.</td>
</tr>
<tr>
<td>MX</td>
<td>mytest.com</td>
<td>mail01.mytest.com.</td>
</tr>
<tr>
<td>MX</td>
<td>mytest.com</td>
<td>1.us.testinglabs.com</td>
</tr>
<tr>
<td>MX</td>
<td>mytest.com</td>
<td>2.us.testinglabs.com</td>
</tr>
<tr>
<td>A</td>
<td>backup.mytest.com</td>
<td>210.120.111.12</td>
</tr>
<tr>
<td>A</td>
<td>download.mytest.com</td>
<td>33.11.22.33</td>
</tr>
<tr>
<td>A</td>
<td>guest.mytest.com</td>
<td>126.132.111.0</td>
</tr>
</tbody>
</table>
18  NAT Mappings

The Peplink Balance allows the IP address mapping of all inbound and outbound NAT’ed traffic to and from an internal client IP address.

NAT mappings can be configured at **Network>NAT Mappings**.

To add a rule for NAT mappings, click **Add NAT Rule** and the following screen will be displayed:
### NAT Mapping Settings

<table>
<thead>
<tr>
<th>LAN Client(s)</th>
<th>NAT Mapping rules can be defined for a single LAN <strong>IP Address</strong>, an <strong>IP Range</strong>, or an <strong>IP Network</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>This refers to the LAN host’s private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when <strong>IP Address</strong> is selected.</td>
</tr>
<tr>
<td>Range</td>
<td>The IP range is a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when <strong>IP Range</strong> is selected.</td>
</tr>
<tr>
<td>Network</td>
<td>The IP network refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when <strong>IP Network</strong> is selected.</td>
</tr>
</tbody>
</table>
| Inbound Mappings | This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when **IP Address** is selected in the **LAN Client(s)** field.  

  **Note 1:** Inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode.  

  **Note 2:** Each WAN IP address can be associated to one NAT mapping only. |
| Outbound Mappings | This setting specifies the WAN IP addresses should be used when an IP connection is made from a LAN host to the Internet.  

  Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN’s IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility).  

  **Note 1:** If you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the **Outbound Policy** section.  

  **Note 2:** WAN connections in drop-in mode or IP forwarding mode are not shown here. |

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

<table>
<thead>
<tr>
<th>Important Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound firewall rules override inbound mapping settings.</td>
</tr>
</tbody>
</table>
19 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>Captive Portal**.

### Captive Portal Settings

<table>
<thead>
<tr>
<th><strong>Enable</strong></th>
<th>Check <strong>Enable</strong> and then, optionally, select the LANs/VLANs that will use the captive portal.</th>
</tr>
</thead>
</table>

**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**

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>LDAP Server</td>
</tr>
<tr>
<td>LDAP Server</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Base DN</td>
<td></td>
</tr>
<tr>
<td>Base Filter</td>
<td></td>
</tr>
</tbody>
</table>

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 `X` button next to the listing.

### Allowed Clients

To whitelist a client, enter the MAC address / IP address here and click `+`. To delete an existing client from the list of allowed clients, click the `X` button next to the listing.

### Splash Page

Here, you can choose between using the Balance’s built-in captive portal and redirecting clients to a URL you define.
The **Portal Customization** menu has two options: [Preview] and [Logo]. Clicking [Preview] will result in a pop-up previewing the captive portal that your clients will see. Clicking [Logo] will result in the appearance of following menu:

### Portal Customization

<table>
<thead>
<tr>
<th><strong>Logo Image</strong></th>
<th><strong>Message</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>[No image] Use default Logo Image</td>
<td>[No image] Use default Terms &amp; Conditions</td>
</tr>
<tr>
<td>[Choose File] No file chosen</td>
<td>[Choose File] No terms and conditions chosen</td>
</tr>
</tbody>
</table>

**NOTE:** Size max 256KB. Supported image types: JPEG, PNG and GIF.

<table>
<thead>
<tr>
<th><strong>Terms &amp; Conditions</strong></th>
<th><strong>Custom Landing Page</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>[Use default Terms &amp; Conditions]</td>
<td>[Use default Custom Landing Page]</td>
</tr>
</tbody>
</table>

**Custom Landing Page**

- Fill in this field to redirect clients to an external URL.

- 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.

- If you have any additional messages for your users, enter them in this field.

- Click the **Choose File** button to select an logo to use for the built-in portal.
20 QoS

20.1 User Groups

LAN and PPTP clients can be categorized into three user groups - Manager, Staff, and Guest. This menu allows you to define rules and assign client IP addresses or subnets to a user group. You can apply different bandwidth and traffic prioritization policies on each user group in the Bandwidth Control and Application sections.

The table is automatically sorted, and the table order signifies the rules' precedence. The smaller and more specific subnets are put towards the top of the table and have higher precedence; larger and less specific subnets are placed towards the bottom.

Click the Add button to define clients and their user group. Click the button to remove the defined rule.

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

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

This section is to define how much minimum bandwidth will be reserved to each user group when a WAN connection is in full load. When this feature is enabled, a slider with two indicators will be shown. You can move the indicators to adjust each group’s weighting. The lower part of the table shows the corresponding reserved download and uploads bandwidth value of each connection.

By default, 50% of bandwidth has been reserved for Manager, 30% for Staff, and 20% for Guest.

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

20.3.1 Application Prioritization

You can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.

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

20.3.2 Prioritization for Custom Application

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

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

Category and Application availability will be different across different Peplink Balance models.
20.3.3 DSL/Cable Optimization

DSL/cable-based WAN connections have lower upload bandwidth and higher download bandwidth.

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

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

The firewall functionality of Peplink Balance supports the selective filtering of data traffic in both directions:

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

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

21.1 Outbound and Inbound Firewall Rules

21.1.1 Access Rules

The outbound firewall settings are located at Network>Firewall>Access Rules.
Click **Add Rule** to display the following screen:

![Add a New Outbound Firewall Rule](image1)

The inbound firewall settings are located at **Network>Firewall>Access Rules**.

![Inbound Firewall Rules](image2)
Click **Add Rule** to display the following window:

![Add a New Inbound Firewall Rule](image)

### Inbound / Outbound Firewall Settings

<table>
<thead>
<tr>
<th><strong>Rule Name</strong></th>
<th>This setting specifies a name for the firewall rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
<td>This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule. Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</td>
</tr>
<tr>
<td><strong>WAN Connection (Inbound)</strong></td>
<td>Select the WAN connection that this firewall rule should apply to.</td>
</tr>
</tbody>
</table>
### Protocol

This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:

- TCP
- UDP
- ICMP
- IP

Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.

### Source IP & Port

This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Source IP & Port** setting, as indicated with the following screenshots:

In addition, a single port, or a range of ports, can be specified for the **Source IP & Port** settings.

### Destination IP & Port

This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Destination IP & Port** setting, as indicated with the following screenshots:

In addition, a single port, or a range of ports, can be specified for the **Destination IP & Port** settings.

### Action

This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:

- Source IP & port
- Destination IP & port

With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded).

### Event Logging

This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows:

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

- **CONN**: The connection where the log entry refers to
- **SRC**: Source IP address
- **DST**: Destination IP address
- **LEN**: Packet length
Click **Save** to store your changes. To create an additional firewall rule, click **Add Rule** and repeat the above steps.
To change a rule's priority, simply drag and drop the rule:

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

To remove a rule, click the button.

Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the Default rule will be applied.

The Default rule is Allow for both outbound and inbound access.

Tip

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

The Balance can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click , check the Enable check box for the Intrusion Detection and DoS Prevention, and press the Save button.

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

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

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

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

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

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

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

21.2.1.3 Customized Domains

Enter an appropriate website address, and the Peplink Balance will block and disallow LAN/PPTP/SpeedFusion™ peer clients to access these websites. Exceptions can be added using the instructions in Sections 21.2.1.4 and 21.2.1.5.

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

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

21.2.1.4 Exempted User Groups

Check and select pre-defined user group(s) who can be exempted from the access blocking rules. User groups can be defined at QoS>User Groups section. Please refer to Section 20.1 for details.

21.2.1.5 Exempted Subnets

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

21.2.1.6 URL Logging

Click enable, and the enter the ip address and port (if applicable) where your remote syslog server is located.
The Peplink Balance supports OSPF and RIPv2 dynamic routing protocols. Click the Network tab from the top bar, and then click the OSPF & RIPv2 item on the sidebar to reach the following menu:

**22 OSPF & RIPv2**

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

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

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Determine the name of your <strong>Area ID</strong> to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Type</td>
<td>Choose the network type that this area will use.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Choose an authentication method, if one is used, from this drop-down menu. Available options are <strong>MD5</strong> and <strong>Text</strong>. Enter the authentication key next to the drop-down menu.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Determine which interfaces this area will use to listen to and deliver OSPF packets</td>
</tr>
</tbody>
</table>

**OSPF Settings**

- **Area ID**: Enter the name of your area ID to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.
- **Link Type**: Choose the network type that this area will use.
- **Authentication**: Choose an authentication method, if one is used, from this drop-down menu. Available options are **MD5** and **Text**. Enter the authentication key next to the drop-down menu.
- **Interfaces**: Select the interfaces this area will use to listen to and deliver OSPF packets.
To access RIPv2 settings, click ![RIPv2 Settings](image).

### RIPv2 Settings

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose an authentication method, if one is used, from this drop-down menu. Available options are MD5 and Text. Enter the authentication key next to the drop-down menu.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Determine which interfaces this group will use to listen to and deliver RIPv2 packets.</strong></td>
<td></td>
</tr>
</tbody>
</table>
23 Remote User Access

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

### Remote User Access Settings

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

Click the button to switch to enters user accounts by pasting the information in CSV format.
Miscellaneous Settings

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

23.1 High Availability

The Peplink Balance supports high availability (HA) configurations via an open standard virtual router redundancy protocol (VRRP, RFC 3768).

In an HA configuration, two same-model Peplink Balance units provide redundancy and failover in a master-slave arrangement. In the event that the master unit is down, the slave unit becomes active.

High availability will be disabled automatically where there is a drop-in connection configured on a LAN bypass port.

The following diagram illustrates an HA configuration with two Peplink Balance units and two Internet connections:

In the diagram, the WAN ports of each Peplink Balance unit connect to the router and to the modem. Both Peplink Balance units connect to the same LAN switch via a LAN port.

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

- In an HA configuration, the two Peplink Balance units communicate with each other using VRRP over the LAN.
- The two Peplink Balance units broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the master Peplink Balance unit is received in 3 seconds (or longer) since the last heartbeat signal, the slave Peplink Balance unit becomes active.
- The slave Peplink Balance unit initiates the WAN connections and binds to a previously configured LAN IP address.
- At a subsequent point when the master Peplink Balance unit recovers, it will
once again become active.
You can configure high availability at **Network>Misc. Settings>High Availability**.

### Interface for Master Router

<table>
<thead>
<tr>
<th>High Availability</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>y</td>
</tr>
<tr>
<td>Group Number</td>
<td>5</td>
</tr>
<tr>
<td>Preferred Role</td>
<td>Master</td>
</tr>
<tr>
<td>Resume Master Role</td>
<td>y</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>LAN Administration IP</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

### Interface for Slave Router

<table>
<thead>
<tr>
<th>High Availability</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>y</td>
</tr>
<tr>
<td>Group Number</td>
<td>5</td>
</tr>
<tr>
<td>Preferred Role</td>
<td>Slave</td>
</tr>
<tr>
<td>Configuration Sync.</td>
<td></td>
</tr>
<tr>
<td>Virtual IP</td>
<td></td>
</tr>
<tr>
<td>LAN Administration IP</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
</tbody>
</table>

### High Availability

- **Enable**
  Checking this box specifies that the Peplink Balance unit is part of a high availability configuration.

- **Group Number**
  This number identifies a pair of Peplink Balance units operating in a high availability configuration. The two Peplink Balance units in the pair must have the same **Group Number** value.

- **Preferred Role**
  This setting specifies whether the Peplink Balance unit operates in master or slave mode. Click the corresponding radio button to set the role of the unit. One of the units in the pair must be configured as the master, and the other unit must be configured as the slave.

- **Resume Master Role Upon Recovery**
  This option is displayed when **Master** mode is selected in **Preferred Role**. If this option is enabled, once the device has recovered from an outage, it will take over and resume its **Master** role from the slave unit.

- **Configuration Sync.**
  This option is displayed when **Slave** mode is selected in **Preferred Role**. If this option is enabled and the **Master Serial Number** entered matches with the actual master unit’s, the master unit will automatically transfer the configuration to this unit. Please make sure the **LAN IP Address** and the **Subnet Mask** fields are set correctly in the LAN settings page. You can refer to the **Event Log** for the configuration synchronization status.

- **Master Serial Number**
  If **Configuration Sync.** is checked, the serial number of the master unit is required here for the feature to work properly.

- **Virtual IP**
  The HA pair must share the same **Virtual IP**. The **Virtual IP** and the **LAN Administration IP** must be under the same network.

- **LAN Administration IP**
  This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN.

- **Subnet Mask**
  This setting specifies the subnet mask of the LAN.
Important Note

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

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

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

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

23.3 Service Forwarding

Service forwarding settings are located at Network>Misc. Settings>Service Forwarding.

<table>
<thead>
<tr>
<th>Service Forwarding</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Forwarding</td>
<td>When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting Enable.</td>
</tr>
<tr>
<td>Web Proxy Forwarding</td>
<td>When this option is enabled, all outgoing connections destined for the proxy server specified in Web Proxy Interception Settings will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting Enable.</td>
</tr>
<tr>
<td>DNS Forwarding</td>
<td>When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down.</td>
</tr>
<tr>
<td>Custom Service Forwarding</td>
<td>When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number.</td>
</tr>
</tbody>
</table>
23.3.1 SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP’s SMTP server. All outgoing SMTP connections are blocked except those connecting to the ISP’s. The Peplink Balance supports the interception and redirection of all outgoing SMTP connections (destined for TCP port 25) via a WAN connection to the WAN’s corresponding SMTP server.

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

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

<table>
<thead>
<tr>
<th>Connection</th>
<th>Enable Forwarding?</th>
<th>SMTP Server</th>
<th>SMTP Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN 2</td>
<td>✓</td>
<td>22.2.2.2</td>
<td>25</td>
</tr>
<tr>
<td>WAN 3</td>
<td></td>
<td>33.3.3.2</td>
<td>25</td>
</tr>
<tr>
<td>WAN 4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see Section 16.1).

23.3.2 Web Proxy Forwarding

When this feature is enabled, the Peplink Balance will intercept all outgoing connections destined for the proxy server specified in Web Proxy Server Interception Settings. Then it will choose a WAN connection according to the outbound policy and forward the connection to the specified web proxy server and port number. Redirected server settings for each WAN can be set here. If forwarding is disabled for a WAN, then web proxy connections for that WAN will simply be forwarded to the connection’s original...
destination.

23.3.3 DNS Forwarding

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

23.3.4 Custom Service Forwarding

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

23.4 Service Passthrough

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

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

<table>
<thead>
<tr>
<th>Service Passthrough Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP</strong></td>
</tr>
<tr>
<td>Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Peplink Balance can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets</td>
</tr>
</tbody>
</table>
correctly in NAT mode. Such passthrough support is always enabled and there are two modes for selection: **Standard Mode** and **Compatibility Mode**.

If your SIP server’s signal port number is non-standard, you can check the box **Define custom signal ports** and input the port numbers to the text boxes.

<table>
<thead>
<tr>
<th>H.323</th>
<th>With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and passthrough the Balance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>FTP sessions consist of two TCP connections; one for control and one for data. In a multi-WAN situation, they must be routed to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Peplink Balance monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, you can check <strong>Define custom control ports</strong> and enter the port numbers in the text boxes.</td>
</tr>
<tr>
<td>TFTP</td>
<td>The Peplink Balance monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select <strong>Enable</strong> if you want to enable TFTP passthrough support.</td>
</tr>
<tr>
<td>IPsec NAT-T</td>
<td>This field is for enabling the support of IPsec NAT-T passthrough. UDP ports 500, 4500, and 10000 are monitored by default. You may add more custom data ports that your IPsec system uses by checking <strong>Define custom ports</strong>. If the VPN contains IPsec site-to-site VPN traffic, check <strong>Route IPsec Site-to-Site VPN</strong> and choose the WAN connection to route the traffic to.</td>
</tr>
</tbody>
</table>
24 AP

The AP controller acts as a centralized controller of Pepwave AP devices. With this feature, users will be able to customize and manage multiple APs from a single Peplink Balance interface.

<table>
<thead>
<tr>
<th>Special Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>With the installation of Firmware 6.2.1 and upwards, full AP support is included free.</td>
</tr>
</tbody>
</table>

24.1 AP Controller

Clicking on the AP tab will default to this menu, where you can view basic AP management options:

<table>
<thead>
<tr>
<th>AP Management</th>
<th>Support Remote AP</th>
<th>Permitted AP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

The AP controller supports remote management of Pepwave APs. When this option is enabled, the AP controller will wait for management connections originating from remote APs over the WAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443.

The DHCP server and/or local DNS server of the remote AP’s network should be configured in the DNS Proxy Settings menu under Network>LAN. The procedure is as follows:

1. Define an extended DHCP option, CAPWAP Access Controller addresses (field 138), in the DHCP server, where the values are the AP controller’s public IP addresses; and/or
2. Create a local DNS record for the AP controller with a value corresponding to the AP controller’s public IP address.
24.2 Wireless SSID

Wireless network settings, including the name of the network (SSID) and security policy, can be defined and managed in this section. After defining a wireless network, users can choose the network in AP Profiles.

Click the button New SSID to create a new network profile, or click the existing network profile to modify its settings.

<table>
<thead>
<tr>
<th>SSID</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEPLINK_E7JD</td>
<td>WPA/WPA2 - Personal</td>
</tr>
</tbody>
</table>

**SSID**

- **SSID**: This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
- **VLAN ID**: This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is 0, which means VLAN tagging is disabled (instead of tagged with zero).
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast SSID</td>
<td>This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. <em>Broadcast SSID</em> is enabled by default.</td>
</tr>
<tr>
<td>Data Rate</td>
<td>Select <em>Auto</em> to allow the Peplink Balance to set the data rate automatically, or select <em>Fixed</em> and choose a rate from the displayed drop-down menu.</td>
</tr>
<tr>
<td>Multicast Filter</td>
<td>This setting enables the filtering of multicast network traffic to the wireless SSID.</td>
</tr>
<tr>
<td>Multicast Rate</td>
<td>This setting specifies the transmit rate to be used for sending multicast network traffic. The selected <em>Protocol</em> and <em>Channel Bonding</em> settings will affect the rate options and values available here.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>To allow the Peplink Balance to listen to internet group management protocol (IGMP) network traffic, select this option.</td>
</tr>
<tr>
<td>DHCP Option 82</td>
<td>If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.</td>
</tr>
<tr>
<td>Network Priority (QoS)</td>
<td>Select from <em>Gold</em>, <em>Silver</em>, and <em>Bronze</em> to control the QoS priority of this wireless network’s traffic.</td>
</tr>
<tr>
<td>Layer 2 Isolation</td>
<td><em>Layer 2</em> refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.</td>
</tr>
<tr>
<td>Band Steering</td>
<td>Band steering allows the Peplink Balance to steer AP clients from the 2.4 GHz band to the 5GHz band for better usage of bandwidth. To make steering mandatory, select <em>Enforce</em>. To cause the Peplink Balance to preferentially choose steering, select <em>Prefer</em>. The default for this setting is <em>Disable</em>.</td>
</tr>
</tbody>
</table>

* - Advanced feature. Click the button on the top right-hand corner to activate.

Security Settings

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

The settings allow administrator to control access using Mac address filtering. Available options are **None**, **Deny all except listed**, **Accept all except listed**, and **RADIUS MAC Authentication**.

When **WPA/WPA2 - Enterprise** is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the **Shared Key** option should be disabled. When using this method, select the appropriate version using the **V1/V2** controls. The security level of this method is known to be very high.

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

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

### MAC Address List

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

---

<table>
<thead>
<tr>
<th>RADIUS Server Settings</th>
<th>Primary Server</th>
<th>Secondary Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Secret</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication Port</strong></td>
<td>1812</td>
<td>1812</td>
</tr>
<tr>
<td><strong>Accounting Port</strong></td>
<td>1813</td>
<td>1813</td>
</tr>
</tbody>
</table>
**Guest Protect**

- **Block All Private IP**: Check this box to deny all connection attempts by private IP addresses.

- **Custom Subnet**: To create a custom subnet for guest access, enter the IP address and choose a subnet mask from the drop-down menu. To add the new subnet, click +. To delete a custom subnet, click -.

- **Block Exception**: To block access from a particular subnet, enter the IP address and choose a subnet mask from the drop-down menu. To add the new subnet, click +. To delete a blocked subnet, click -.

- **Block PepVPN**: To block PepVPN access, check this box.

**Bandwidth Management**

- **Upstream Limit**: Enter a value in kbps to limit the wireless network’s upstream bandwidth. Enter 0 to allow unlimited upstream bandwidth.

- **Downstream Limit**: Enter a value in kbps to limit the wireless network’s downstream bandwidth. Enter 0 to allow unlimited downstream bandwidth.

- **Client Upstream Limit**: Enter a value in kbps to limit connected clients’ upstream bandwidth. Enter 0 to allow unlimited upstream bandwidth.

- **Client Downstream Limit**: Enter a value in kbps to limit connected clients’ downstream bandwidth. Enter 0 to allow unlimited downstream bandwidth.
**Downstream Limit**  
unlimited downstream bandwidth.

**Max Number of Clients**  
Enter the maximum number of clients that can simultaneously connect to the wireless network or enter 0 to allow an unlimited number of connections.

### Firewall Settings

**Firewall Mode**  
Choose Flexible – Allow all except… or Lockdown – Block all except… to turn on the firewall. Once you save changes, the [New Rule] button will appear for you to create rules for the firewall exceptions. See the discussion below for details on creating a firewall rule. To delete a rule, click the associated [x] button. To turn off the firewall, select Disable.

### Firewall Rule

**Name**  
Enter a descriptive name for the firewall rule in this field.

**Type**  
Choose Port, Domain, IP Address, or MAC Address to allow or deny traffic from any of those identifiers. Depending on the option chosen, the following fields will vary.

**Protocol / Port**  
Choose TCP or UDP from the Protocol drop-down menu to allow or deny traffic using either of those protocols. From the Port drop-down menu, choose Any Port to allow or deny TCP or UDP traffic on any port. Choose Single Port and then enter a port number in the provided field to allow or block TCP or UDP traffic from that port only. You can also choose Port Range and enter a range of ports in the provided fields to allow or deny TCP or UDP traffic from the specified port range.

**IP Address / Subnet Mask**  
If you have chosen IP Address as your firewall rule type, enter the IP address and subnet mask identifying the subnet to allow or deny.

**MAC Address**  
If you have chosen MAC Address as your firewall rule type, enter the MAC address identifying the machine to allow or deny.
24.3 Profiles

AP profiles assigned to each Pepwave AP device can be configured at AP>Profiles.

Each AP is associated with one AP profile. By default, all devices are associated with the first (default) profile. The default profile cannot be removed.

You can define an AP profile by clicking the New AP Profile button. Click the Clone button of an existing profile to create a new profile based on it. To change the settings of an existing profile, click the profile name, and the following screen will be shown:
## AP Settings

<table>
<thead>
<tr>
<th><strong>AP Profile Name</strong></th>
<th>This field specifies the name of this AP profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSID</strong></td>
<td>These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Peplink Balance does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.</td>
</tr>
</tbody>
</table>
| **Operating Country** | This drop-down menu specifies the national / regional regulations which the AP should follow.  
- If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).  
- If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).  
NOTE: Users are required to choose an option suitable to local laws and regulations.  
Per FCC regulation, the country selection is not available on all models marketed in US.  
All US models are fixed to US channels only. |
| **Preferred Frequency** | These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies. |
| **5 GHz Protocol** | This section displays the 5 GHz protocols your APs are using. |
| **5GHz Channel Bonding** | There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection. |
| **5 GHz Channel** | This drop-down menu selects the 5 GHz 802.11 channel to be utilized. If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically. |
| **2.4 GHz Protocol** | This section displays the 2.4 GHz protocols your APs are using. |
| **2.4 GHz Channel Bonding** | There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection. |
| **2.4 GHz Channel** | This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically. |
| **Management** | This field specifies the VLAN ID to tag to management traffic, such as AP to AP |
| **VLAN ID** | controller communication traffic. The value is 0 by default, meaning that no VLAN tagging will be applied. NOTE: change this value with caution as alterations may result in loss of connection to the AP controller. |
| **Power Boost** | With this option enabled, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to increased interference. |
| **Output Power** | This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When Dynamic settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance. The Dynamic: Auto setting will set the AP to do this automatically. Otherwise, the Dynamic: Manual setting will set the AP to dynamically adjust only if instructed to do so. If you have set Dynamic:Manual, you can go to AP>Toolbox>Auto Power Adj. to give your AP further instructions. |
| **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. |
| **Max number of Clients** | This field determines the maximum clients that can be connected to APs under this profile. |
| **Client Signal Strength Threshold** | This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts. |
| **Beacon Rate** | This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, and 11Mbps. |
| **Beacon Interval** | This drop-down menu provides the option to set the time between each beacon send. Available options are 100ms, 250ms, and 500ms. |
| **DTIM** | This field provides the option to set the frequency for beacon to include delivery traffic indication messages (DTIM). The interval unit is measured in milliseconds. |
| **RTS Threshold** | This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature. |
| **Fragmentation Threshold** | Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation. |
| **Distance/Time Converter** | Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended. |
| **Slot Time** | This field provides the option to modify the unit wait time before it transmits. The default value is 9μs. |
| **ACK Timeout** | This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is 48μs. |
| **Frame Aggregation** | With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission. |
Frame Length

This field is only available when Frame Aggregation is enabled. It specifies the frame length for frame aggregation. By default, it is set to 50000.

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

Web Administration Settings

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

AP Time Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>Check the box to allow the Peplink Balance to manage the web admin access information of the AP.</td>
</tr>
<tr>
<td>Time Server</td>
<td>These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are HTTP and HTTPS.</td>
</tr>
</tbody>
</table>
AP Controller Settings

<table>
<thead>
<tr>
<th>Client Load Balancing</th>
<th>Coverage Redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the box to turn on client load balancing.</td>
<td>Select the degree of coverage redundancy to use. Available values are Low, Medium, and High.</td>
</tr>
</tbody>
</table>

24.4 Info

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

AP Controller

<table>
<thead>
<tr>
<th>License Limit</th>
<th>20</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Subtotal</th>
<th>Default</th>
<th>Main_Office</th>
<th>Main_Office</th>
<th>Marketing</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>No. of APs</th>
<th>Online</th>
<th>Offline</th>
<th>Total AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>2</td>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>

Data Usage

<table>
<thead>
<tr>
<th>Zoom</th>
<th>1h</th>
<th>3h</th>
<th>6h</th>
<th>ALL</th>
</tr>
</thead>
</table>

This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage.

Underneath, there are two check boxes labeled 2.4 Ghz and 5 Ghz. Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.

The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show
### Events

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

### 24.5 Usage

A detailed breakdown of data usage for each AP is available at AP> Access Point. The information is organized by device groups as defined in Section 22.3.
Usage

**AP Name/Serial Number**
This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.

**Online Status**
This button toggles whether your search will include offline devices.

This table shows the detailed information on each AP, including channel, number of clients, upload traffic, and download traffic. Click the blue arrows at the left of the table to expand and collapse information on each device group. You could also expand and collapse all groups by using the [Expand] and [Collapse] buttons.

On the right of the table, you will see the following icons: 🔄 ⏩ 👀. Click the 🔄 icon to see a usage table for each client:

### Client List

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Signal</th>
<th>SSID</th>
<th>Upload</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.2.1</td>
<td>Excellent (42)</td>
<td>Balance</td>
<td>10.0.0.2</td>
<td>6.63 MB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.3.1</td>
<td>Excellent (25)</td>
<td>Balance</td>
<td>10.0.0.3</td>
<td>5.24 MB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.4.1</td>
<td>Excellent (36)</td>
<td>Balance</td>
<td>10.0.0.4</td>
<td>640.25 KB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.5.1</td>
<td>Excellent (39)</td>
<td>Balance</td>
<td>10.0.0.5</td>
<td>2.24 KB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.6.1</td>
<td>Excellent (29)</td>
<td>Balance</td>
<td>10.0.0.6</td>
<td>9.06 MB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.7.1</td>
<td>Wireless</td>
<td>Balance</td>
<td>10.0.0.7</td>
<td>9.06 MB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.8.1</td>
<td>Wireless</td>
<td>Balance</td>
<td>10.0.0.8</td>
<td>118.03 MB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.9.1</td>
<td>Wireless</td>
<td>Balance</td>
<td>10.0.0.9</td>
<td>74.76 MB</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>10.0.0.10.1</td>
<td>Wireless</td>
<td>Balance</td>
<td>10.0.0.10</td>
<td>64.84 KB</td>
</tr>
</tbody>
</table>

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

### Managed Wireless Devices

**AP Details**

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>MAC Address</th>
<th>Product Name</th>
<th>Name</th>
<th>Location</th>
<th>Firmware Version</th>
<th>Firmware Pack</th>
<th>AP Client Limit</th>
<th>2.4 GHz SSID List</th>
<th>5 GHz SSID List</th>
<th>Last config applied by controller</th>
<th>Uptime</th>
<th>Current Channel</th>
<th>Channel</th>
<th>Output Power</th>
</tr>
</thead>
</table>

Click the 👀 icon to view the device details.
Click the icon to see a graph displaying usage:

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

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

In-depth SSID reports are available under AP > SSID.

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

24.7 Wireless Client

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

Here, you will be able to see your network’s heaviest users as well as search for specific users. Click the ⭐ icon to bookmark specific users, and click the 📈 icon for additional details about each user:
24.8 Rogue AP

A listing of suspected rogue devices can be accessed by navigating to **AP>Rogue AP**.
Hovering over the device MAC address will result in a popup with information on how this device was detected. Click the 🔄 🌋 icons and the device will be moved to the bottom table of identified devices.

24.9 Toolbox

Additional tools for managing firmware packs, power adjustment, and channel assignment can be found at AP>Toolbox.

<table>
<thead>
<tr>
<th>Firmware Packs</th>
<th>Auto Power Adj.</th>
<th>Dynamic Channel Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pack ID</td>
<td>Release Date</td>
<td>Details</td>
</tr>
<tr>
<td>1126</td>
<td>2013-08-26</td>
<td><img src="image" alt="Green Check" /></td>
</tr>
<tr>
<td><img src="image" alt="Check for Updates" /></td>
<td><img src="image" alt="Manual Upload" /></td>
<td><img src="image" alt="Default..." /></td>
</tr>
</tbody>
</table>

Firmware Packs

This is the first menu that will appear. Here, you can manage the firmware of your AP. Clicking on ![Check for Updates](image) will display information regarding each firmware pack. To receive new firmware packs, you can either press ![Check for Updates](image) to download new packs or you can press ![Manual Upload](image) to manually upload a firmware pack. Press ![Default...](image) to define which firmware pack is default.
25 System Settings

25.1 Admin Security

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

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

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

**Default**: 4 hours 0 minutes.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Router Name</strong></td>
<td>This field allows you to define a name for this Peplink Balance unit. By default, <strong>Router Name</strong> is set as <strong>Balance_XXXX</strong>, where <strong>XXXX</strong> refers to the last 4 digits of the serial number of that balance unit.</td>
</tr>
<tr>
<td><strong>Admin User Name</strong></td>
<td><strong>Admin User Name</strong> is set as <strong>admin</strong> by default, but can be changed, if desired.</td>
</tr>
<tr>
<td><strong>Admin Password</strong></td>
<td>This field allows you to specify a new administrator password.</td>
</tr>
<tr>
<td><strong>Confirm Admin Password</strong></td>
<td>This field allows you to verify and confirm the new administrator password.</td>
</tr>
<tr>
<td><strong>Read-only User Name</strong></td>
<td><strong>Read-only User Name</strong> is set as <strong>user</strong> by default, but can be changed, if desired.</td>
</tr>
<tr>
<td><strong>User Password</strong></td>
<td>This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.</td>
</tr>
<tr>
<td><strong>Confirm User</strong></td>
<td>This field allows you to verify and confirm the new user password.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Front Panel Passcode</strong></td>
<td>To require a 4-digit passcode to access front panel controls, check this box and then select the code from the drop-down menus.</td>
</tr>
<tr>
<td><strong>Web Session Timeout</strong></td>
<td>This field specifies the number of hours and minutes that a web session can remain idle before the Balance terminates its access to the web admin interface. By default, it is set to <strong>4 hours</strong>.</td>
</tr>
<tr>
<td><strong>Authentication by RADIUS</strong></td>
<td>With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either “admin” with full read-write permission or “user” with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.</td>
</tr>
<tr>
<td><strong>Auth Protocol</strong></td>
<td>This specifies the authentication protocol used. Available options are <strong>MS-CHAP v2</strong> and <strong>PAP</strong>.</td>
</tr>
<tr>
<td><strong>Auth Server</strong></td>
<td>This specifies the access address and port of the external RADIUS server.</td>
</tr>
<tr>
<td><strong>Auth Server Secret</strong></td>
<td>This field is for entering the secret key for accessing the RADIUS server.</td>
</tr>
<tr>
<td><strong>Auth Timeout</strong></td>
<td>This option specifies the time value for authentication timeout.</td>
</tr>
<tr>
<td><strong>Accounting Server</strong></td>
<td>This specifies the access address and port of the external accounting server.</td>
</tr>
<tr>
<td><strong>Accounting Server Secret</strong></td>
<td>This field is for entering the secret key for accessing the accounting server.</td>
</tr>
<tr>
<td><strong>Network Connection</strong></td>
<td>This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.</td>
</tr>
<tr>
<td><strong>Restricted Admin Access</strong></td>
<td>Check this box to restrict management to administrators connected to the management port.</td>
</tr>
<tr>
<td><strong>CLI SSH &amp; Console</strong></td>
<td>The CLI (command line interface) can be accessed via SSH. It can also be accessed from the serial console port on some Peplink Balance models. This field enables CLI support. For additional information regarding CLI, please refer to <strong>Section 22.5</strong>.</td>
</tr>
<tr>
<td><strong>CLI SSH Port</strong></td>
<td>This field determines the port on which clients can access CLI SSH.</td>
</tr>
<tr>
<td><strong>CLI SSH Access</strong></td>
<td>This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>This option is for specifying the protocol(s) through which the web admin interface can be accessed:</td>
</tr>
<tr>
<td></td>
<td>- HTTP</td>
</tr>
<tr>
<td></td>
<td>- HTTPS</td>
</tr>
</tbody>
</table>
- **HTTP/HTTPS**

**Web Admin Port**
This field is for specifying the port number on which the web admin interface can be accessed.

**Web Admin Access**
This option is for specifying the network interfaces through which the web admin interface can be accessed:
- LAN only
- LAN/WAN

If LAN/WAN is chosen, the **WAN Connection Access Settings** form will be displayed.

### WAN Connection Access Settings

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

- **Any** - Allow web admin accesses from anywhere, without IP address restrictions.
- **Allow access from the following IP subnets only** – Restricts the ability to access web admin to only defined IP subnets. When this option is chosen, a text input area will appear:

Enter your allowed IP subnet addresses into this text area. Each IP subnet must be in the form of `w.x.y.z/m`. `w.x.y.z` represents an IP address (e.g., `192.168.0.0`), and `m` represents the subnet mask in CIDR format, which is between 0 and 32 inclusively. For example: `192.168.0.0/24`.

To define multiple subnets, separate each IP subnet, one per line. For example:
- `192.168.0.0/24`
- `10.8.0.0/16`

**Allowed Source IP Subnets**

**Allowed WAN IP Address(es)**
This is to choose which WAN IP address(es) the web server should listen on.
25.2 Firmware

The firmware of Peplink Balance is upgradeable through the web admin interface. Firmware upgrade functionality is located at System>Firmware.

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

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

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

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

Firmware Upgrade Status

Status LED Information during firmware upgrade:

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

The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. Do not disconnect the power during firmware upgrade process. Do not attempt to upload a non-firmware file or a firmware file that is not supported by Peplink. Upgrading the Peplink Balance with an invalid firmware file will damage the unit and may void the warranty.

25.3 Schedule

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

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

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

25.4 **Time**

The time server functionality enables the system clock of the Peplink Balance to be synchronized with a specified time server. The settings for time server configuration are located at **System>Time**.

**Time Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>This specifies the time zone (along with the corresponding Daylight Savings Time scheme) in which Peplink Balance operates. The <strong>Time Zone</strong> value affects the time stamps in the event log of the Peplink Balance and e-mail notifications. Check <strong>Show all</strong> to show all time zone options.</td>
</tr>
<tr>
<td>Time Server</td>
<td>This setting specifies the NTP network time server to be utilized by the Peplink Balance.</td>
</tr>
</tbody>
</table>
### 25.5 Email Notification

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

**Email Notification Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Notification</td>
<td>This setting specifies whether or not to enable email notification. If <strong>Enable</strong> is checked, the Peplink Balance will send email messages to system administrators when the WAN status changes or when new firmware is available. If <strong>Enable</strong> is not checked, email notification is disabled and the Peplink Balance will not send email messages.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check <strong>Require authentication.</strong></td>
</tr>
<tr>
<td>SSL Encryption</td>
<td>Check the box to enable SMTPS. When the box is checked, <strong>SMTP Port</strong> will be changed to <strong>465</strong> automatically.</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>This field is for specifying the SMTP port number. By default, this is set to <strong>25;</strong> when <strong>SSL Encryption</strong> is checked, the default port number will be set to <strong>465.</strong> You may customize the port number by editing this field. Click <strong>Default</strong> to restore the number to its default setting.</td>
</tr>
<tr>
<td>SMTP User Name / Password</td>
<td>This setting specifies the SMTP username and password while sending email. These options are shown only if <strong>Require authentication</strong> is checked in the <strong>SMTP Server</strong> setting.</td>
</tr>
<tr>
<td>Confirm SMTP Password</td>
<td>This field allows you to verify and confirm the new administrator password.</td>
</tr>
<tr>
<td>Sender’s Email Address</td>
<td>This setting specifies the email address which the Peplink Balance will use to send its reports.</td>
</tr>
</tbody>
</table>
Recipient's Email Address

This setting specifies the email address(es) to which the Peplink Balance will send email notifications. For multiple recipients, separate each email using the enter key.

After you have finished setting up email notifications, you can click the Test Email Notification button to test the settings before saving. After Test Email Notification is clicked, you will see this screen to confirm the settings:

<table>
<thead>
<tr>
<th>Test Email Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
</tr>
<tr>
<td>SMTP Port</td>
</tr>
<tr>
<td>SMTP UserName</td>
</tr>
<tr>
<td>Sender's Email Address</td>
</tr>
<tr>
<td>Recipient's Email Address</td>
</tr>
</tbody>
</table>

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

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

### Remote Syslog Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Syslog</td>
<td>This setting specifies whether or not to log events at the specified remote syslog server.</td>
</tr>
<tr>
<td>Remote Syslog Host</td>
<td>This setting specifies the IP address or hostname of the remote syslog server.</td>
</tr>
</tbody>
</table>

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

### Push Events

For more information on the Router Utility, go to: www.peplink.com/products/router-utility
25.7 SNMP

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

### SNMP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Device Name</td>
<td>This field shows the router name defined at System&gt;Admin Security.</td>
</tr>
<tr>
<td>SNMP Port</td>
<td>This option specifies the port which SNMP will use. The default port is 161.</td>
</tr>
<tr>
<td>SNMPv1</td>
<td>This option allows you to enable SNMP version 1.</td>
</tr>
<tr>
<td>SNMPv2</td>
<td>This option allows you to enable SNMP version 2.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>This option allows you to enable SNMP version 3.</td>
</tr>
</tbody>
</table>

**Note:** SNPV3 is not supported in the Peplink Balance unit.
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:

**SNMP Community Settings**

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

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

**SNMPv3 User Settings**

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

- **Privacy Protocol**: This setting specifies via a drop-down menu one of the following valid privacy protocols:
  - NONE
  - DES
  When DES is selected, an entry field will appear for the password.
25.8 InControl

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

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

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

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

Back up Peplink Balance settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Peplink Balance settings is found at System>Configuration.

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

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

![Feature Activation](image)

25.11 Reboot

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

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

![Reboot System](image)
26  Tools

26.1  Ping

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

![Ping utility interface](image)

**Tip**

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

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

![Traceroute Example]

**Tip**

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

26.3 Wake-on-LAN

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

![Wake-on-LAN Example]

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

26.4 CLI (Command Line Interface) Support

The serial console connector on some Peplink Balance units is RJ-45. To access the serial console port, prepare a RJ-45 to DB-9 console cable. Connect the RJ-45 end to the unit's console port and the DB-9 end to a terminal's serial port. The port setting will be 115200,8N1.
The serial console connector on other Peplink Balance units is a DB-9 male connector. To access the serial console port, connect a null modem cable with a DB-9 connector on both ends to a terminal with the port setting of 115200,8N1.
27 Status

27.1 Device

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Router Name</strong></td>
<td>This is the name specified in the Router Name field located at <strong>System&gt;Admin Security</strong>.</td>
</tr>
<tr>
<td><strong>Model</strong></td>
<td>This shows the model name and number of this device.</td>
</tr>
<tr>
<td><strong>Hardware Revision</strong></td>
<td>This shows the hardware version of this device.</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>This shows the serial number of this device.</td>
</tr>
<tr>
<td><strong>Firmware</strong></td>
<td>This shows the firmware version this device is currently running.</td>
</tr>
<tr>
<td><strong>Uptime</strong></td>
<td>This shows the length of time since the device has been rebooted.</td>
</tr>
<tr>
<td><strong>System Time</strong></td>
<td>This shows the current system time.</td>
</tr>
<tr>
<td><strong>Diagnostic Report</strong></td>
<td>The <strong>Download</strong> link is for exporting a diagnostic report file required for system investigation.</td>
</tr>
<tr>
<td><strong>Remote Assistance</strong></td>
<td>Click <strong>Turn on</strong> to enable remote assistance.</td>
</tr>
</tbody>
</table>

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

### Important Note

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

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

This screen displays the number of sessions initiated by each application. Click on each service listing for additional information. This screen also indicates the number of sessions initiated by each WAN port. Finally, you can see which clients are initiating the most sessions.
In addition, you can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to **Status>Active Sessions>Search**.

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

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

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

If the PPTP server (see Section Error! Reference source not found.), SpeedFusion™ see Section 12.1), or AP controller (see Section 19) is enabled, you may see the corresponding connection name listed in the Name field.

27.4 WINS Client

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

The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server (see Section 10). The names of clients retrieved will be automatically matched into the Client List (see previous section). Click Flush All to flush all WINS client records.

27.5 OSPF & RIPv2

Information on OSPF and RIPv2 routing setup can be found at Status>OSPF & RIPv2.
27.6 **SpeedFusion™ Status**

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

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

Click the **button for a chart displaying real-time throughput, latency, and drop-rate information for each WAN connection.**
When pressing the button, the following menu will appear:

![PepVPN performance analysis - 9B0A-A29B-2931](image)

PepVPN Test:
Check the general TCP/UDP throughput.

After clicking the icon, the following menu appears:

![Configuration](image)

![WAN Statistics](image)

Select the L2 protocol (TCP/UDP), direction, and duration and click the Start button to begin the general throughput test.
The bandwidth bonding feature of PepVPN occurs when multiple WAN lines from one end merge with multiple WAN lines from the other end. For this to happen, each WAN line needs to form a connection with all the WAN lines on the opposite end. The function of the PepVPN analyzer is to report the throughput, packet loss, and latency of all possible combinations of connections. **Please note that the PepVPN Analyzer will temporarily interrupt VPN connectivity and will restore after test.**

After clicking the icon, the analyzer will require several minutes to perform its analysis depending on the number of WAN links in the SpeedFusion™ Tunnel. Once the test is complete, the report will appear:
"O" indicates that specific WAN / Tunnel is active for that particular test.
"Tx Avg." is the averaged throughput across the full 10 seconds time, while "Tx Max." is the averaged throughput of the fastest 30% of time.

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

27.7.1 Device Event Log

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

27.7.2 IPsec Event Log

This section displays a list of events that has taken place within an IPsec VPN connection. Check the box next to Auto Refresh and the log will be refreshed automatically. For an AP event log, navigate to AP>Info.
27.8 Bandwidth

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

27.8.1 Real-Time

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

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Download</th>
<th>Upload</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:00</td>
<td>5.647 MB</td>
<td>209 MB</td>
<td>5.842 MB</td>
</tr>
<tr>
<td>14:00</td>
<td>5.117 MB</td>
<td>439 MB</td>
<td>5.556 MB</td>
</tr>
<tr>
<td>15:00</td>
<td>2.414 MB</td>
<td>524 MB</td>
<td>2.940 MB</td>
</tr>
<tr>
<td>16:00</td>
<td>2.470 MB</td>
<td>812 MB</td>
<td>3.282 MB</td>
</tr>
<tr>
<td>17:00</td>
<td>725 MB</td>
<td>488 MB</td>
<td>1.213 MB</td>
</tr>
<tr>
<td>18:00</td>
<td>64 MB</td>
<td>211 MB</td>
<td>275 MB</td>
</tr>
</tbody>
</table>
27.8.3 Daily

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

Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature as shown in Section 13.4, the **Current Billing Cycle** table for that WAN connection will be displayed.

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (MB) or gigabytes (GB).

<table>
<thead>
<tr>
<th>Date</th>
<th>Download</th>
<th>Upload</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-01-01</td>
<td>17550 MB</td>
<td>3508 MB</td>
<td>21058 MB</td>
</tr>
<tr>
<td>2014-01-02</td>
<td>15991 MB</td>
<td>5362 MB</td>
<td>21353 MB</td>
</tr>
<tr>
<td>2013-12-31</td>
<td>31028 MB</td>
<td>3435 MB</td>
<td>34463 MB</td>
</tr>
<tr>
<td>2013-12-30</td>
<td>27372 MB</td>
<td>2287 MB</td>
<td>30659 MB</td>
</tr>
<tr>
<td>2013-12-29</td>
<td>910 MB</td>
<td>2576 MB</td>
<td>3486 MB</td>
</tr>
<tr>
<td>2013-12-28</td>
<td>40337 MB</td>
<td>3739 MB</td>
<td>44076 MB</td>
</tr>
<tr>
<td>2013-12-27</td>
<td>27362 MB</td>
<td>1026 MB</td>
<td>28388 MB</td>
</tr>
<tr>
<td>2013-12-26</td>
<td>90753 MB</td>
<td>2295 MB</td>
<td>93048 MB</td>
</tr>
<tr>
<td>2013-12-25</td>
<td>48085 MB</td>
<td>1576 MB</td>
<td>49661 MB</td>
</tr>
<tr>
<td>2013-12-24</td>
<td>10022 MB</td>
<td>3011 MB</td>
<td>22033 MB</td>
</tr>
<tr>
<td>2013-12-23</td>
<td>24024 MB</td>
<td>1070 MB</td>
<td>25094 MB</td>
</tr>
<tr>
<td>2013-12-22</td>
<td>33788 MB</td>
<td>1195 MB</td>
<td>33983 MB</td>
</tr>
<tr>
<td>2013-12-21</td>
<td>95386 MB</td>
<td>2999 MB</td>
<td>98385 MB</td>
</tr>
<tr>
<td>2013-12-20</td>
<td>89321 MB</td>
<td>4166 MB</td>
<td>93487 MB</td>
</tr>
</tbody>
</table>

**Current Month**

<table>
<thead>
<tr>
<th></th>
<th>Down</th>
<th>Up</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down</td>
<td>33541 MB</td>
<td>8870 MB</td>
<td>42411 MB</td>
</tr>
<tr>
<td>Up</td>
<td>8870 MB</td>
<td>33541 MB</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>42411 MB</td>
</tr>
</tbody>
</table>

**Status**
Click on a specific date to receive a breakdown of all client usage for that date.
27.8.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection. If you have enabled Bandwidth Monitoring feature as shown in Section 13.4, you can check the usage of each particular connection and view the information by Billing Cycle or by Calendar Month.

Click the first two rows to view the client bandwidth usage in the last two months. This feature is not available if you have chosen to view the bandwidth of an individual WAN connection. The scale of the graph can be set to display megabytes (MB) or gigabytes (GB).

Click on a specific month to receive a breakdown of all client usage for that month.
## Appendix A. Restoration of Factory Defaults

To restore the factory default settings on a Peplink Balance unit, perform the following:

**For Balance models with a reset button:**
1. Locate the reset button on the Peplink Balance unit.
2. With a paper clip, press and keep the reset button pressed for at least 10 seconds, until the unit reboots itself.

**For Balance/MediaFast models with an LCD menu:**
- Use the buttons on front panel to control the LCD menu to go to Maintenance>Factory Defaults, and then choose Yes to confirm.

Afterwards, the factory default settings will be restored.

### Important Note

<table>
<thead>
<tr>
<th>Important Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>All user settings will be lost after restoring the factory default settings. Regular backup of configuration parameters is strongly recommended.</td>
</tr>
</tbody>
</table>
Appendix C. Routing under DHCP, Static IP, and PPPoE

The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

C.1 Routing Via Network Address Translation (NAT)

When the Peplink Balance is operating under NAT mode, the source IP addresses of outgoing IP packets are translated to the WAN IP address of the Peplink Balance. With NAT, all LAN devices share the same WAN IP address to access the Internet (i.e., the WAN IP address of the Peplink Balance).

Operating the Peplink Balance in NAT mode requires only one WAN (Internet) IP address. In addition, operating in NAT mode also has security advantages because LAN devices are hidden behind the Peplink Balance. They are not directly accessible from the Internet and hence less vulnerable to attacks.

The following figure shows the packet flow in NAT mode:
C.2 Routing Via IP Forwarding

When the Peplink Balance is operating under IP forwarding mode, the IP addresses of IP packets are unchanged; the Peplink Balance forwards both inbound and outbound IP packets without changing their IP addresses.

The following figure shows the packet flow in IP forwarding mode:
Appendix D. Case Studies

D.1 MPLS Alternative

Our SpeedFusion enabled routers can be used to bond multiple low-cost/commodity Internet connections to replace an expensive managed business Internet connection, private leased line, MPLS, and frame relay without sacrificing reliability and availability.

Belowes are typical deployment for using our Balance routers to replace expensive MPLS connection with commodity connections, such as ADSL, 3G, and 4G LTE links.

Special features of Balance 580: have high availability capability
Special features of Balance 2500: have high availability capability and capable of connecting to optical fiber based LAN through SFP+ connector

Our WAN-bonding routers which comprise our Balance series and MediaFast series are capable of connecting multiple devices, and end users’ networks to the Internet through multiple Internet connections.

Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement

Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your network.
Option 2: MPLS Alternative

1. Head office combines bandwidth from fiber-optic Internet (ROO) service to provide high throughput and reliability.

2. Choose a topology that suits your needs:
   - Hub-and-Spoke: Complete control
   - Mesh: Maximum bandwidth efficiency

3. Branch offices are able to combine the bandwidth of ADSL, cellular, and VSAT lines to achieve MPLS reliability at a fraction of the cost.

Achieve faster speeds and greater reliability while paying only 20% of MPLS costs by connecting multiple ADSL, 3G, and 4G LTE links. Choose a topology that suits your requirements: a hub-and-spoke topology maximizes control over your network, while a meshed topology can reduce your bandwidth overhead by enabling your devices to form Unbreakable VPN connections directly with each other.
Here is an example of supplementing an existing Multi-Office MPLS network with DSL bonding through SpeedFusion using a Balance 580 at the headquarters and Balance 210/310 at branch offices.

**Environment:**
- This organization has one head office with two branch offices, with most of the crucial information stored in a server room at the head office.
- They are connecting the offices together using a managed MPLS Solution. However, the MPLS Network is operating at capacity and upgrading the links is cost prohibitive.
- As the organization grows, it needs a cost-efficient way to add more bandwidth to its wide area network.
- Internet access at the remote sites is sent via a web proxy at head office for corporate web filtering compliance.

**Requirement:**
- User sessions need to remain uninterrupted
- More bandwidth is required at the head office location for direct internet access.

**Recommended Solution:**
- Form a SpeedFusion tunnel between the branch offices and head office to bond the MPLS and additional DSL lines.
- SpeedFusion allows for hot failover, maintaining a persistent session while switching connections.
- The DSLs at head office can be used for direct internet access providing lots of cheap internet bandwidth.
- Head office can use outbound policies to send internet traffic out over the DSLs and only use the MPLS connection for speedfusion, freeing up bandwidth.

**Devices Deployed:** Balance 210, Balance 310, Balance 580
Harrington Industrial Plastics

Overview

Harrington Plastics, the US’s largest industrial plastics distributor, was looking to upgrade its network equipment. Harrington’s team came across Peplink and started thinking about MPLS alternatives. By choosing Peplink, they saved a fortune on upgrades and ended up with yearly savings of up to $100,000.

Requirements
- Zero network outages
- Flexible resilience options
- Cost-effective solution

Solution
- Peplink Balance 1350
- Peplink Balance 380
- Unbreakable VPN

Benefits
- Extreme savings of $100,000 per year
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems
Time For An Upgrade

Harrington Industrial Plastics decided it was time to upgrade its network equipment. Its existing solution used redundant MPLS for site-to-site traffic and broadband connections for Internet access. Harrington is the US’s largest distributor of industrial plastics piping, serving all industries with corrosive and high-purity applications. It requires peak performance at all times in order to serve its large customer base and 43 busy branches.

Quick Deployment and Unbreakable Connectivity

In evaluating an upgrade to its network infrastructure, it was only natural that Harrington settled on the best in the industry — Peplink. Peplink partner Frontier Computer Corporation was chosen to help design and deploy the solution. Since Peplink gear is so easy to configure and install, Harrington was able to design, prototype and roll out the entire solution to the corporate headquarters and all 43 branches within just one year.
The corporate office houses a pair of redundant Balance 1350s for hardware resilience. Served by 4 separate links from multiple service providers, the network’s chance of an outage is practically zero. All 43 branches are now equipped with a fleet of Balance 380s, bonding a combination of DSL, cable and fiber-optic links together with an additional 4G USB modem for added resilience. These work together to create an Unbreakable VPN connection to the Balance 1350s at the corporate office, connecting the final dot.

**Dependable, Resilient Networking that's also Very Budget-friendly**

Harrington Industrial Plastics couldn’t be happier. They now benefit from an extremely reliable and cost-effective network. Supplying additional resilience is as easy as plugging in a 4G USB modem. Where the MPLS 768kb deployed previously had cost them $192000 a year for all 40 sites, their new solution is now only costing them $92000. Their total bandwidth has been bumped from 36 Mbps to 138 Mbps.
A Peplink customer since 2006, Pluss is a social enterprise that each year makes gainful employment a reality for more than 5000 disabled and disadvantaged UK citizens. With 37 locations and 300+ active users, Pluss makes heavy use of its WAN infrastructure, which until recently was built on managed MPLS lines.

Hoping to cut expenses and, if possible, boost performance at the same time, Steve Taylor, IT Manager at Pluss, set out to find a solution that would allow Pluss to replace costly MPLS service with a commodity alternative, such as DSL or EFM.

Steve found the solution Pluss needed in Peplink products, especially the Balance series of high-performance enterprise routers and SpeedFusion bonding technology. Pluss now powers its entire WAN infrastructure with simple-to-install, highly reliable, and cost-effective Peplink gear, which allows it to aggregate DSL and other commodity connections and replace expensive leased lines.
D.2 Colégio Next - Enabling eLearning

Colégio Next, a recognized Apple Distinguished School - deploys over 500 iPads to its 600 students as a teaching and learning tool.

Despite being equipped with iPads, teachers and students alike were not making use of them. The reason for this was because of the slow network access speeds. Apps would not download and course contents were inaccessible. Often, having more than a couple students connected to the same Wi-Fi access point was enough to bring it to its knees.

Colégio Next needed a unique solution, so they contacted Peplink.

Requirements
- Solve network congestion problem caused by 600 students over rural Internet connections
- Wi-Fi that can handle 50+ users per classroom
- An affordable network infrastructure that can provide simultaneous access to media-rich educational content

Solution
- Peplink MediaFast
- Multi-WAN Content-caching router, tailor-made for Education networking.
- AP One 300M
- Enterprise grade AP, 5GHz Wi-Fi, up to 60 concurrent users.

Benefits
- Instant, simultaneous access to media-rich educational content for 500+ iPads
- Wi-Fi connection stability for 50+ users per classroom, not achievable by other tested
equipment
- Teachers, students and guests can be assigned access priority to available bandwidth, further preventing congestion
- iOS updates (often 2GB size) no longer congest the network as they are downloaded only once, cached on the MediaFast and then distributed to all iOS devices
- AP Controller makes MAC Address Filtering easy. Students are assigned to designated APs by their devices' MAC Address in order to prevent saturating any single AP.
- Flawless iPad AirPlay mirroring at all times
- iPads are used all day, reaching their full potential with a fast and stable network all the time
- Students are far more engaged and teachers rely on their iPads all day
D.3 Performance Optimization

D.3.1 Scenario

In this scenario, email and web browsing are the two main Internet services used by LAN users. The mail server is external to the network. The connections are ADSL (WAN1, with slow uplink and fast downlink) and Metro Ethernet (WAN2, symmetric).

D.3.2 Solution

For optimal performance with this configuration, individually set the WAN load balance according to the characteristics of each service.

- Web browsing mainly downloads data; sending e-mails mainly consumes upload bandwidth.
- Both connections offer good download speeds; WAN2 offers good upload speeds.
- Define WAN1 and WAN2's inbound and outbound bandwidths to be 3M/512k and 4M/4M, respectively. This will ensure that outbound traffic is more likely to be routed through WAN2.
- For HTTP, set the weight to 3:4.
- For SMTP, set the weight to 1:8, such that users will have a greater chance to be routed via WAN2 when sending e-mail.
D.3.3 Settings

1. Add a new outbound traffic rule for HTTP.
2. Add a new outbound traffic rule for SMTP.

In general, to add a new outbound traffic rule, navigate to **Advanced>Outbound Policy**.

Click here and select **Managed by Custom Rules**.

Click **Add Rule** to add a new load distribution rule.
Settings for HTTP:

Set the weight of WAN1 and WAN2 for HTTP to 3 and 4, respectively.
Settings for SMTP:

Set the weight of WAN1 and WAN2 for SMTP to 1 and 8, respectively.
D.4 Maintaining the Same IP Address Throughout a Session

D.4.1 Scenario

Some IP address-sensitive websites (for example, Internet banking) use both client IP address and cookie matching for session identification. Since load balancing uses different IP addresses, the session is dropped when a mismatched IP is detected, resulting in frequent interruptions while visiting such sites.

D.4.2 Solution

Make use of the persistence functionality of the Peplink Balance. With persistence configured and the By Destination option selected, the Peplink Balance will use a consistent WAN connection for source-destination pairs of IP addresses, preventing sessions from being dropped.

With persistence configured and the option By Source is selected, the Peplink Balance uses a consistent WAN connection for same-source IP addresses. This option offers higher application compatibility but may inhibit the load balancing function unless there are many clients using the Internet.

D.4.3 Settings

Set persistence in at Advanced>Outbound Policy.

Click Add Rule, select HTTP (TCP port 80) for web service, and select Persistence. Click Save and then Apply Changes, located at the top right corner, to complete the process.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>HTTP Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Any</td>
</tr>
<tr>
<td>Destination</td>
<td>Any</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP: 80 HTTP</td>
</tr>
<tr>
<td>Port</td>
<td>Single Port: 80</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Persistence</td>
</tr>
<tr>
<td>Persistence Mode</td>
<td>By Source, By Destination</td>
</tr>
<tr>
<td>Load Distribution</td>
<td>Auto, Custom</td>
</tr>
<tr>
<td>Terminate Sessions on Link Recovery</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Tip

A network administrator can use the traceroute utility to manually analyze the connection path of a particular WAN connection.
D.5 Bypasing the Firewall to Access Hosts on LAN

D.5.1 Scenario

There are times when remote access to computers on the LAN is desirable; for example, when hosting web sites, online businesses, FTP download and upload areas, etc. In such cases, it may be appropriate to create an inbound NAT mapping for the network to allow some hosts on the LAN to be accessible from outside of the firewall.

D.5.2 Solution

The web admin interface can be used to add an inbound NAT mapping to a host and to bind the host to the WAN connection(s) of your choice. To begin, navigate to Network>NAT Mappings.

In this example, the host with an IP address of 192.168.1.102 is bound to 10.90.0.75 of WAN1:

Click **Save** and then **Apply Changes**, located at the top right corner, to complete the process.
D.6 Inbound Access Restriction

D.6.1 Scenario

A firewall is required in order to protect the network from potential hacker attacks and other Internet security threats.

D.6.2 Solution

Firewall functionality is built into the Peplink Balance. By default, inbound access is unrestricted. Enabling a basic level of protection involves setting up firewall rules.

For example, in order to protect your private network from external access, you can set up a firewall rule between the Internet and your private network. To do so, navigate to Advanced>Firwall>Access Rules. Then click the Add Rule button in the Inbound Firewall Rules table and change the settings according to the following screenshot:

![Add a New Inbound Firewall Rule](image)

After the fields have been entered as in the screenshot, click Save to add the rule. Afterwards, change the default inbound rule to Deny by clicking the default rule in the Inbound Firewall Rules table. Click Apply Changes on the top right corner to complete the process.
D.7 Outbound Access Restriction

D.7.1 Scenario

For security reasons, it may be appropriate to restrict outbound access. For example, you may want to prevent LAN users from using ftp to transfer files to and from the Internet. This can easily be achieved by setting up an outbound firewall rule with the Peplink Balance.

D.7.2 Solution

To setup a firewall between Internet and private network for outbound access, navigate to Advanced>Firewall>Access Rules. Click the Add Rule button in the Outbound Firewall Rules table, and then adjust settings according the screenshot:

![Add a New Outbound Firewall Rule](image)

After the fields have been entered as in the screenshot, click Save to add the rule. Click Apply Changes on the top right corner to complete the process.
Appendix E. Troubleshooting

Problem 1
Outbound load is only distributed over one WAN connection.

Solution
Outbound load balancing can only be distribute traffic evenly between available WAN connections if many outbound connections are made. If there is only one user on the LAN and only one download session is made from his/her browser, the WAN connections cannot be fully utilized.

For a single user, download management applications are recommended. The applications can split a file into pieces and download the pieces simultaneously. Examples include: DownThemAll (Firefox Extension), iGetter (Mac), etc.

If the outbound traffic is going across the SpeedFusion™ tunnel, (i.e., transferring a file to a VPN peer) the bandwidth of all WAN connections will be bonded. In this case, all bandwidth will be utilized and a file will be transferred across all available WAN connections.

For additional details, please refer to this FAQ:
http://www.peplink.com/knowledgebase/maximizing-your-wan-connections-without-speedfusion/

Problem 2
I am using a download manager program (e.g., Download Accelerator Plus, DownThemAll, etc.). Why is the download speed still only that of a single link?

Solution
First, check whether all WAN connections are up. Second, ensure your download manager application has split the file into 3 parts or more. It is also possible that all of 2 or even 3 download sessions were being distributed to the same link by chance.

Problem 3
I am using some websites to look up my public IP address, e.g., www.whatismyip.com. When I press the browser's Refresh button, the server almost always returns the same address. Isn’t the IP address supposed to be changing for every refresh?

Solution
The web server has enabled the Keep Alive function, which ensures that you use the same TCP session to query the server. Try to test with a website that does not enable Keep Alive.

For example, try http://private.dnsstuff.com/tools/aboutyou.ch. (This third-party web site is provided only for reference. Peplink has no association with the site and does not guarantee the site’s validity or availability.)
Problem 4
What can I do if I suspect a problem on my LAN connection?
Solution
You can test the LAN connection using ping. For example, if you are using DOS/Windows, at the command prompt, type ping 192.168.1.1. This pings the Peplink Balance device (provided that Peplink Balance’s IP is 192.168.1.1) to test whether the connection to the Peplink Balance is OK.

Problem 5
What can I do if I suspect a problem on my Internet/WAN connection?
Solution
You can test the WAN connection using ping, as in the solution to Problem 4. As we want to isolate the problems from the LAN, ping will be performed from the Peplink Balance. By using Ping/Traceroute under the Status tab of the Peplink Balance, you may able to find the source of problem.

Problem 6
When I upload files to a server via FTP, the transfer stalls after a few kilobytes of data are sent. What should I do?
Solution
The maximum transmission unit (MTU) or MSS setting may need to be adjusted. By default, the MTU is set at 1440. Choose Auto for all of your WAN connections. If that does not solve the problem, you can try the MTU 1492 if a connection is DSL. If problem still persists, change the size to progressive smaller values until your problem is resolved (e.g., 1462, 1440, 1420, 1400, etc).

Additional troubleshooting resources:
Peplink Knowledgebase: http://www.peplink.com/knowledgebase/
Peplink Community Forums: https://forum.peplink.com/

Appendix F. Declaration
1. CAUTION:
   RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
   DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

3. **Radiation Exposure Statement (for Balance One):**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

Note: The country code selection is for non-US models only and is not available to all US models. Per FCC regulation, all WiFi products marketed in US must fixed to US operation channels only.
Contact Us:

Sales
http://www.peplink.com/contact/sales/

Support
http://www.peplink.com/contact/

Certified Peplink Partner
http://www.peplink.com/partners/channel-partner-program/