

Peplink Balance Multi-WAN Bonding Routers

User Manual

For Models:

ONE AC/20/30/30 LTE/50/210/310/305/380/580/710/1350/2500

MediaFast 200/500/750

Peplink Balance Firmware 6.3

May 2016



Copyright & trademark specifications are subject to change without prior notice. Copyright © 2016 Peplink International Ltd. All Rights Reserved. Peplink and the Peplink logo are trademarks of Peplink International Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

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	USAGE SCENARIOS	19
7	PACKAGE CONTENTS	23
7.1	Peplink Balance One AC	23
7.2	Peplink Balance 20/30/30 LTE/50	23
7.3	Peplink Balance 210/310	23
7.4	Peplink Balance 305/380/580/710/1350/2500	23
7.5	Peplink MediaFast 200	23
7.6	Peplink MediaFast 500	23
8	PEPLINK BALANCE OVERVIEW	24
8.1	Peplink Balance One AC	24
8.2	Peplink Balance 20	26
8.3	Peplink Balance 30	28
8.4	Peplink Balance 30 LTE	30

8.5	Peplink Balance 50	32
8.6	Peplink Balance 210	34
8.7	Peplink Balance 310	36
8.8	Peplink Balance 305	38
8.9	Peplink Balance 380	41
8.10	Peplink Balance 580	44
8.11	Peplink Balance 710	47
8.12	Peplink Balance 1350	50
8.13	Peplink Balance 2500	53
8.14	Peplink MediaFast 500	57
9	INSTALLATION	60
9.1	Preparation	60
9.2	Constructing the Network	60
9.3	Configuring the Network Environment	62
10	BASIC CONFIGURATION	63
10.1	Connecting to the Web Admin Interface	63
10.2	Configuration with the Setup Wizard	64
10.3	Advanced Setup	68
10.4	Cellular WAN	69
11	MEDIAFAST CONFIGURATION	75
11.1	Setting Up MediaFast Content Caching	75
11.2	Scheduling Content Prefetching	76
11.3	MDM Settings	78
11.4	Viewing MediaFast Statistics	79
12	CONFIGURING THE LAN INTERFACE(S)	80
12.1	LAN Configuration with VLAN	87
13	DROP-IN MODE	92
14	CONFIGURING THE WAN INTERFACE(S)	96
14.1	Physical Interface Settings	98
14.2	Connection Method(s)	99
14.3	WAN Health Check	107
14.4	Bandwidth Allowance Monitor	110
14.5	Additional Public IP Settings	111
14.6	Dynamic DNS Settings	112
15	PEPVPN WITH SPEEDFUSION™ BANDWIDTH BONDING	115
15.1	SpeedFusion™ Settings	115
15.2	The Peplink Balance Behind a NAT Router	122

15.3	SpeedFusion™ Status	123
16	IPSEC VPN	124
16.1	IPsec VPN Settings	124
16.2	IPsec Status	128
17	OUTBOUND POLICY MANAGEMENT	129
17.1	Outbound Policy	130
17.2	Custom Rules for Outbound Policy	131
18	INBOUND ACCESS	139
18.1	Definition of Servers on LAN	139
18.2	Definition of Port Forwarding	140
18.3	Inbound Access Services	142
18.4	Reverse Lookup Zones	158
18.5	DNS Record Import Wizard	162
19	NAT MAPPINGS	166
20	CAPTIVE PORTAL	168
21	QOS	171
21.1	User Groups	171
21.2	Bandwidth Control	172
21.3	Application	173
22	FIREWALL	175
22.1	Outbound and Inbound Firewall Rules	175
23	OSPF & RIPV2	184
24	REMOTE USER ACCESS	187
MISCELLANEOUS SETTINGS		189
24.1	High Availability	189
24.2	Certificate Manager	192
24.3	Service Forwarding	192
24.4	Service Passthrough	194
25	AP	196
25.1	AP Controller	196
25.2	Wireless SSID	197
25.3	Profiles	203
25.4	Info	207
25.5	Usage	208
25.6	SSID	211
25.7	Wireless Client	211

25.8	Rogue AP	212
25.9	Toolbox	213
26	SYSTEM SETTINGS	214
26.1	Admin Security	214
26.2	Firmware	218
26.3	Schedule	219
26.4	Time	220
26.5	Email Notification.....	221
26.6	Event Log	223
26.7	SNMP	224
26.8	InControl.....	226
26.9	Configuration	227
26.10	Feature Add-ons.....	228
26.11	Reboot.....	228
27	TOOLS	229
27.1	Ping	229
27.2	Traceroute Test.....	230
27.3	Wake-on-LAN.....	230
27.4	CLI (Command Line Interface) Support.....	230
28	STATUS	232
28.1	Device	232
28.2	Active Sessions	234
28.3	Client List.....	236
28.4	WINS Client.....	236
28.5	OSPF & RIPv2	236
28.6	SpeedFusion™ Status	237
28.7	Event Log	240
28.8	Bandwidth.....	241
APPENDIX A. RESTORATION OF FACTORY DEFAULTS.....		246
APPENDIX C. ROUTING UNDER DHCP, STATIC IP, AND PPPOE		247
C.1	Routing Via Network Address Translation (NAT)	247
C.2	Routing Via IP Forwarding.....	248
APPENDIX D. CASE STUDIES		249
D.1	MPLS Alternative.....	249
D.2	Colégio Next - Enabling eLearning.....	256
D.3	Performance Optimization	258
D.4	Maintaining the Same IP Address Throughout a Session	262
D.5	Bypassing the Firewall to Access Hosts on LAN	263

D.6	Inbound Access Restriction	264
D.7	Outbound Access Restriction	265
APPENDIX E. TROUBLESHOOTING		266
APPENDIX F. DECLARATION		267
APPENDIX G: PRODUCT DATASHEETS		269

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.

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>.

2 Glossary

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

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

3 Product Comparison Chart

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

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

^Available as an optional feature

Full product comparison available at:
<http://www.peplink.com/products/balance/model-comparison/>

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

^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



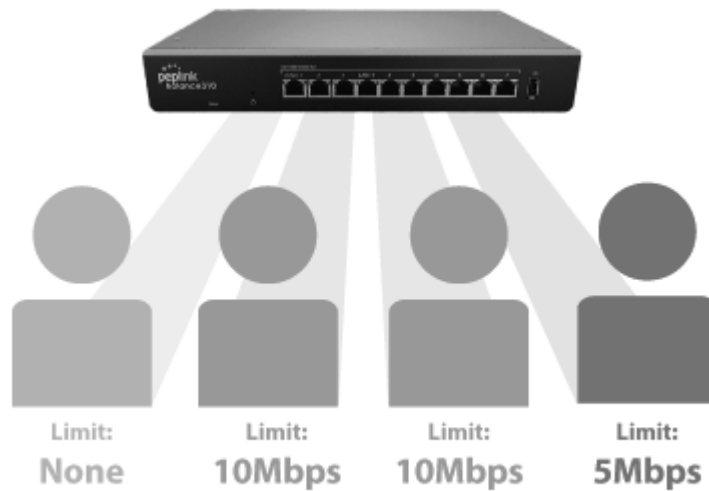
As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass**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



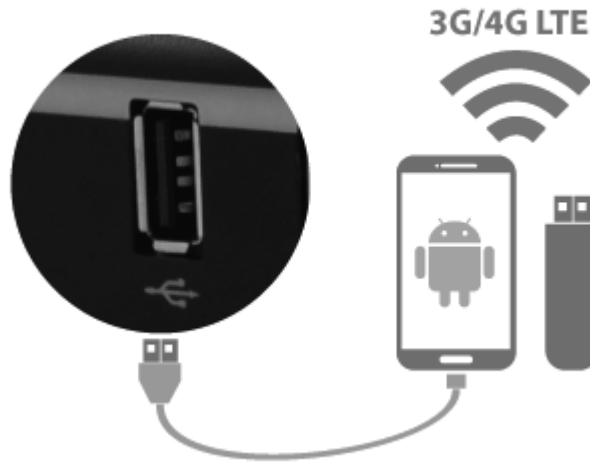
With per-user bandwidth control, you can define bandwidth control policies for up to 3 groups of users to prevent network congestion. Define groups by IP address and subnet, and set bandwidth limits for every user in the group.

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.

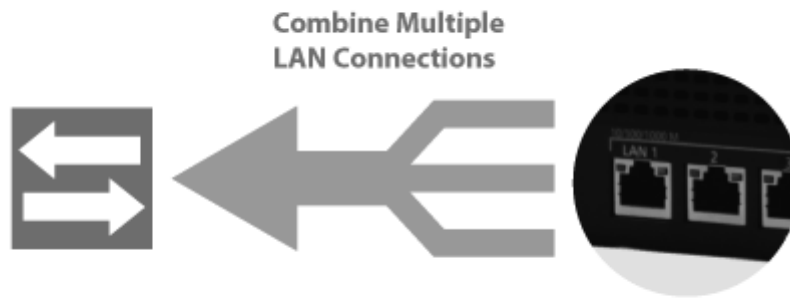
5.6 Built-In Remote User VPN Support



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 Usage Scenarios

The Balance SD-WAN router series has a wide range of products suitable for many different deployments and markets. Entry level SD-WAN models such as the Balance 30, and MediaFast 200 are suitable for SMEs or branch offices. High-capacity SD-WAN routers such as the Balance 580, Balance 2500, and MediaFast 750 are suitable for larger organizations and head offices.

Set out below are the major industries that have been using our SD-WAN routers:



Public Safety

Public safety sector has strict demand and review processes when procuring routers suitable for deployment. Our MAX BR1 are ruggedized and perform as required and have been used by police departments, fire departments and other emergency response units in different countries. The most common application is vehicular wireless connectivity, where multiple wireless employed to ensure service vehicles stay connected. Our wireless routers are also being used for adding wireless backhaul to remote CCTV networks.



Education

It is common for schools network to become slow and congested during classes due to students' simultaneous access. Our MediaFast routers can reduce network traffic to ease the load on the network. Teachers can store frequently accessed education content including high definition media, mobile applications, web content and mobile device updates in advance. This reduces network congestion during classes and provides students with a much improved education content user experience.



Retail

The retail sector generally has to keep their branch networks up and running for applications such as enterprise resource planning (ERP), terminal services and point-of-sale (POS) systems. By deploying wireless routers, our end users have been able to save significant amount of network costs at their branches by replacing or supplementing their MPLS lines with inexpensive WAN connections.



**Industrial
Construction
Utilities**

The industrial, construction and utilities sector typically have sites that are out of the way or temporary in nature. End uses in this sector have been deploying our wireless routers to quickly setup WAN connections through wireless connections. For areas where wireless connectivity coverage is intermittent, our customers have been deploying our MAX HD routers for more bandwidth and reliability by bonding multiple wireless networks through our SpeedFusion technology.



Hospitality

A hospitality customer usually needs a network infrastructure that can provide fast internet access to hundreds of guests. By deploying our Balance series routers, hospitality end-users are able to prioritize and separate network traffic to prevent congestion, and the ability to use 4G LTE USB modems for an additional resilience and bandwidth.



**Broadcasting
and Media**

Broadcasters, including journalists and reporters, usually rely on wireless networks to stream live content back to stations, especially for live broadcast and sports events. Our MAX HD2, MAX HD4 and MAX On-The-Go routers have been selected by end-users to employ multiple wireless networks to stream live multimedia contents.



Maritime

Vessels often roam between shore networks, wireless networks and satellite. Vessels which have been deploying our wireless routers to improve offshore communications, transmitting oceanographic research data and providing Internet access to its crew and passengers.



Transportation

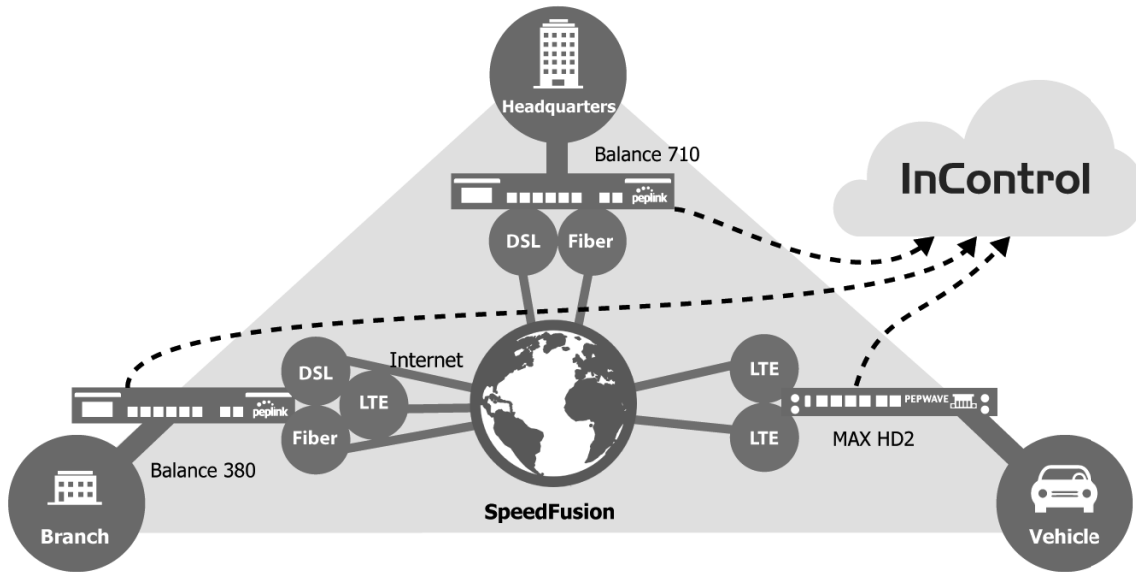
Our MAX HD series routers with its multiple embedded wireless modems can keep passengers connected to high speed Internet. Fleet management is also built-in and available to transportation operators via InControl.



Energy

It is crucial for stakeholders in energy sector to access their supervisory control and data acquisition systems reliably and remotely. Our wireless routers have been helping our customers modernize their networking communications part of their supervisory control and data acquisition systems, providing them with reliability and resiliency over wireless connections while enabling real-time monitoring and controls.

The diagram below illustrates how our SD-WAN routers, SpeedFusion technology and InControl cloud services can be used together.



Each of our SD-WAN routers (Balance 710, Balance 380 and MAX HD2) can form SpeedFusion with each other. Thus, secure connections can be established among the headquarters, branch and vehicle. Further Balance 710, Balance 380 and MAX HD2 can be managed by InControl to reduce administration effort.

7 Package Contents

The contents of Peplink Balance product packages are as follows:

7.1 Peplink Balance One AC

- Peplink Balance One
- Power adapter
- Information slip

7.2 Peplink Balance 20/30/30 LTE/50

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

7.3 Peplink Balance 210/310

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

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

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

7.5 Peplink MediaFast 200

- Peplink MediaFast 200
- Power adapter
- Information slip

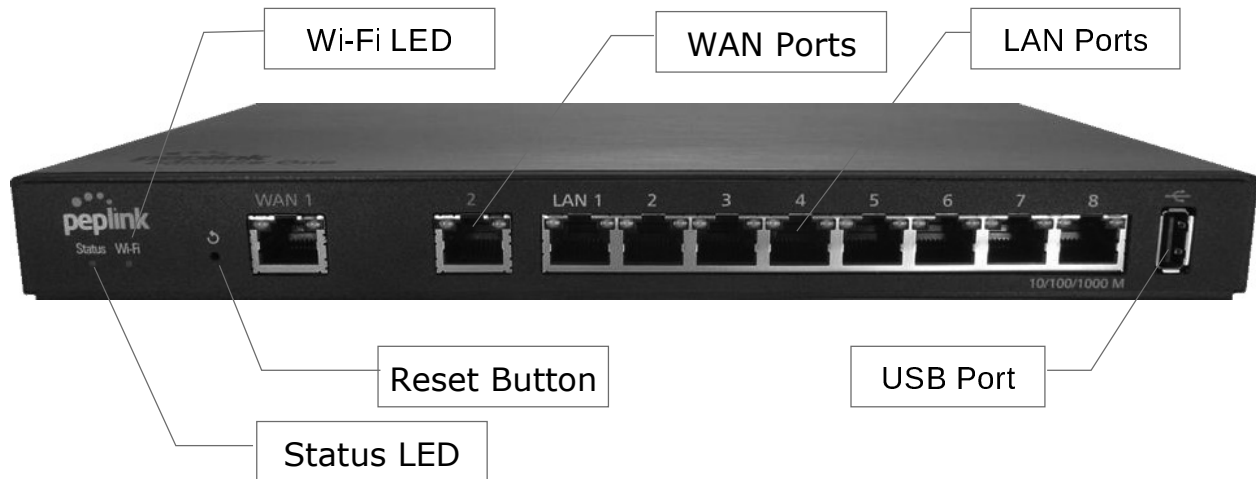
7.6 Peplink MediaFast 500

- Peplink MediaFast 500
- Power cord
- Information slip
- Rackmount kit

8 Peplink Balance Overview

8.1 Peplink Balance One AC

8.1.1 Front Panel Appearance



8.1.2 LED Indicators

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

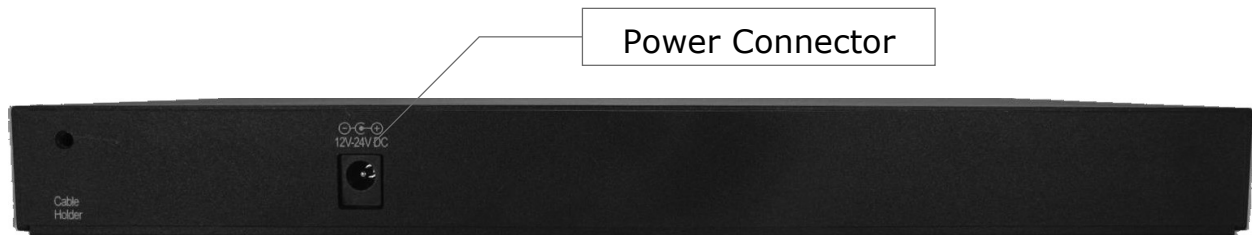
Power and Status Indicators	
Wi-Fi	OFF – Wi-Fi is off
	Green – Ready
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
----------	--

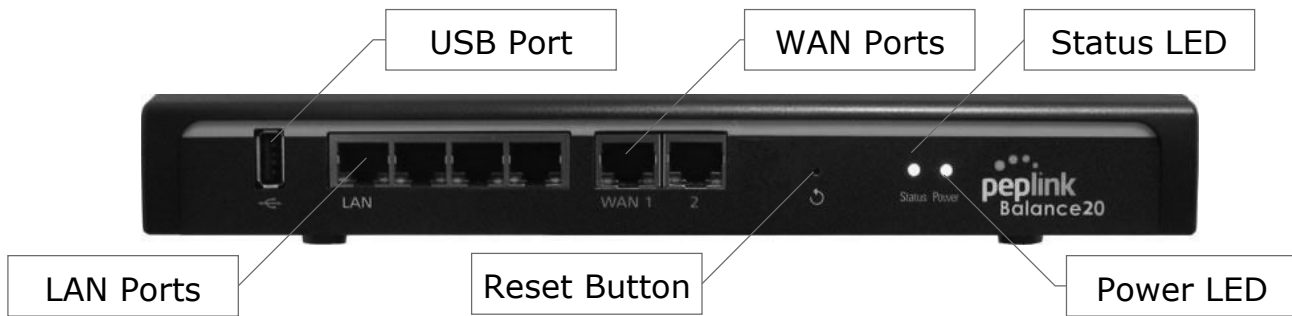
USB Ports For future functionality

8.1.3 Rear Panel Appearance



8.2 Peplink Balance 20

8.2.1 Front Panel Appearance



8.2.2 LED Indicators

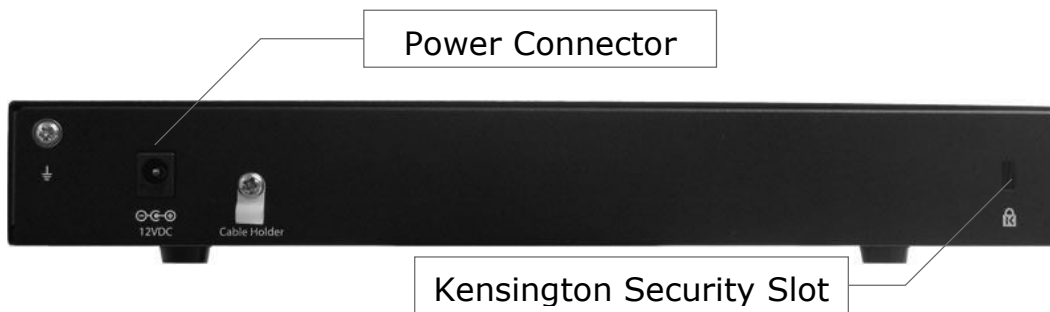
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

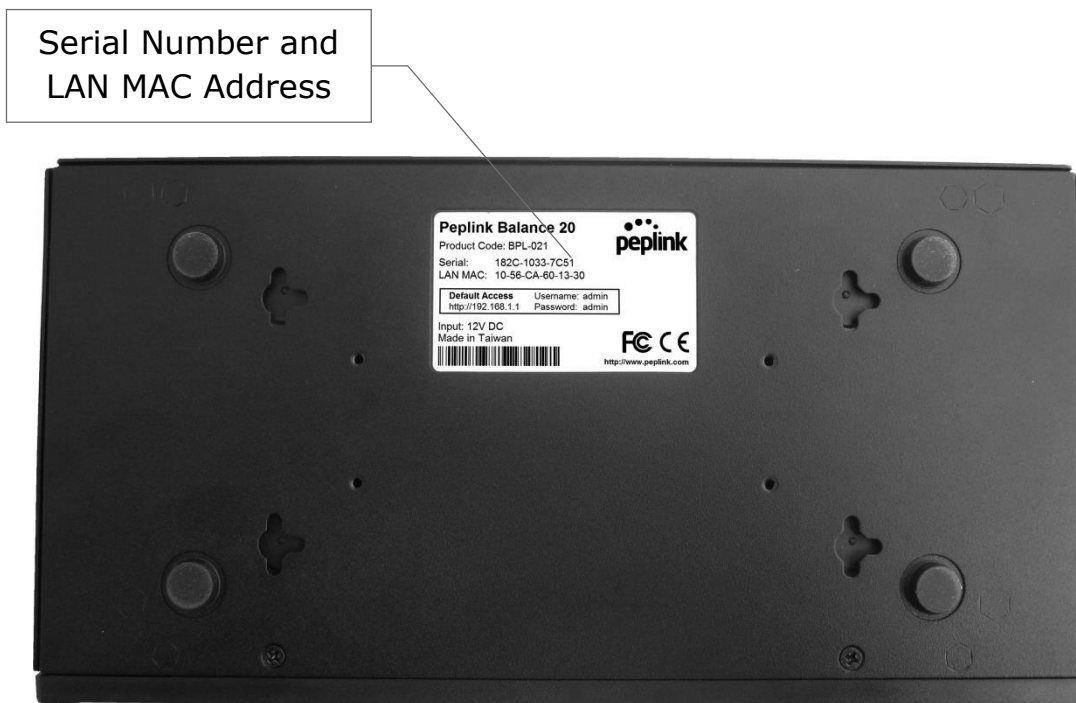
LAN and WAN Ports	
Green LED	ON – 10 / 100 / 1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

USB Port	
USB Ports	For connecting a 4G/3G USB modem

8.2.3 Rear Panel Appearance

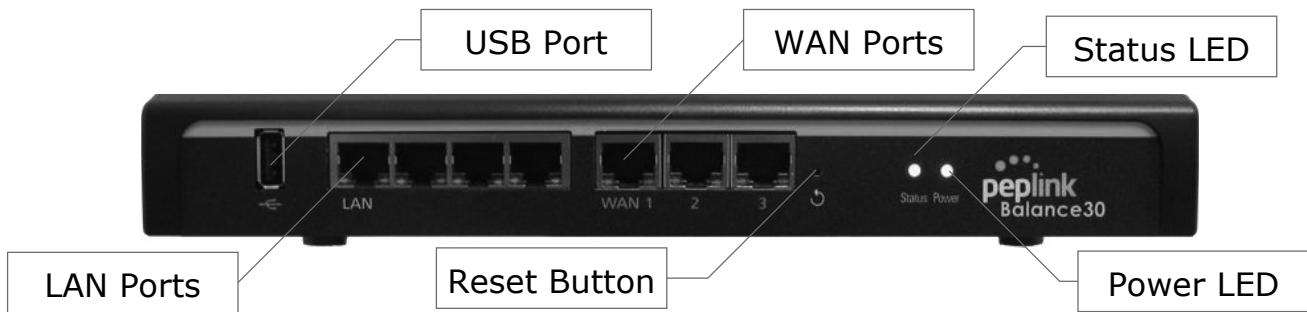


8.2.4 Unit Base Appearance



8.3 Peplink Balance 30

8.3.1 Front Panel Appearance



8.3.2 LED Indicators

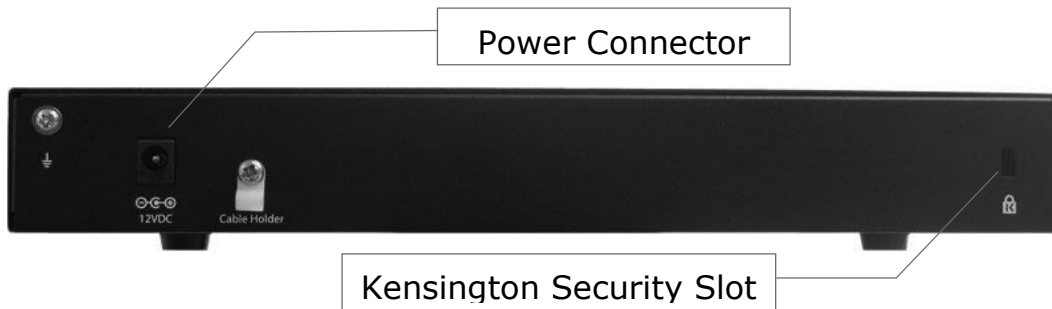
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

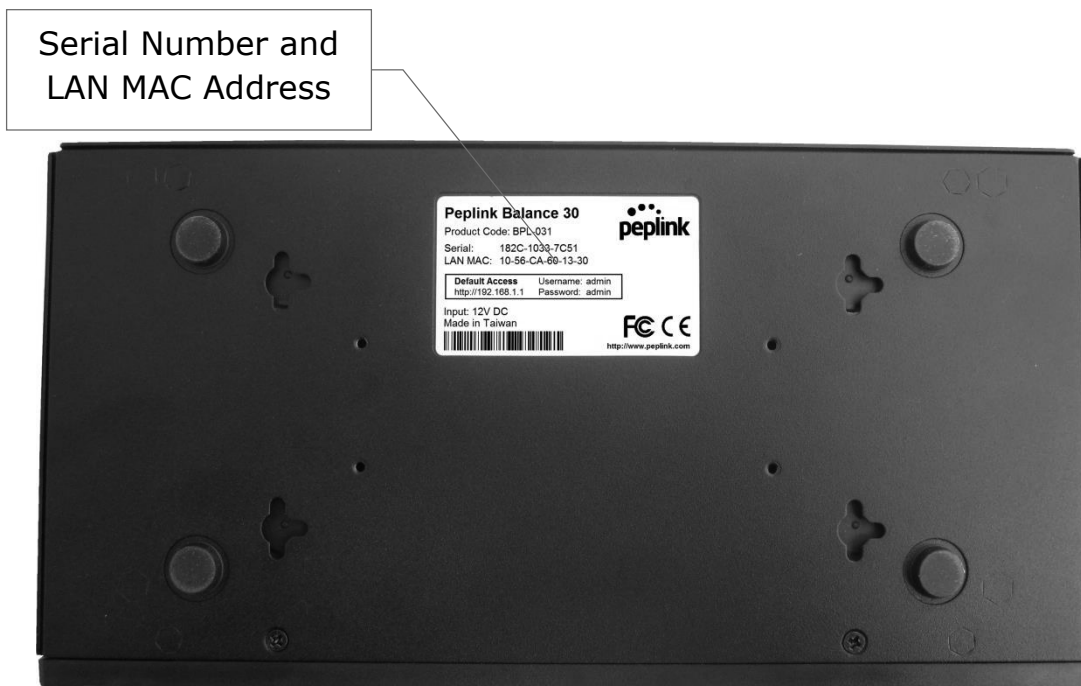
LAN and WAN Ports	
Green LED	ON – 10 / 100 /1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

USB Port	
USB Ports	For connecting a 4G/3G USB modem

8.3.3 Rear Panel Appearance

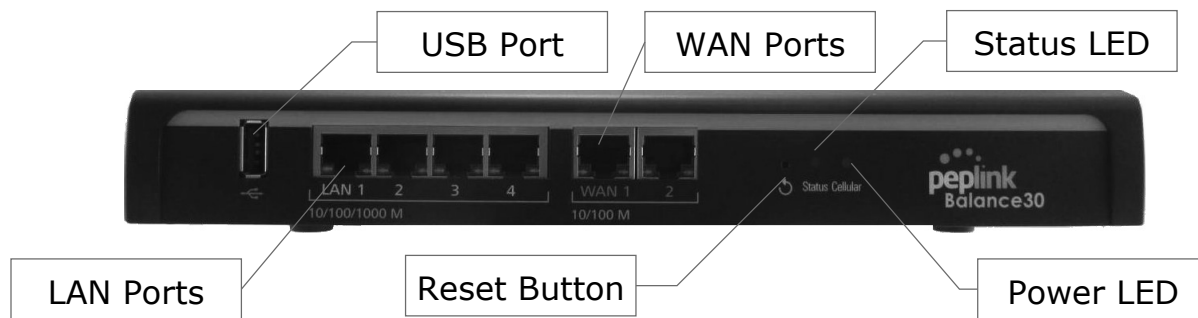


8.3.4 Unit Base Appearance



8.4 Peplink Balance 30 LTE

8.4.1 Front Panel Appearance



8.4.2 LED Indicators

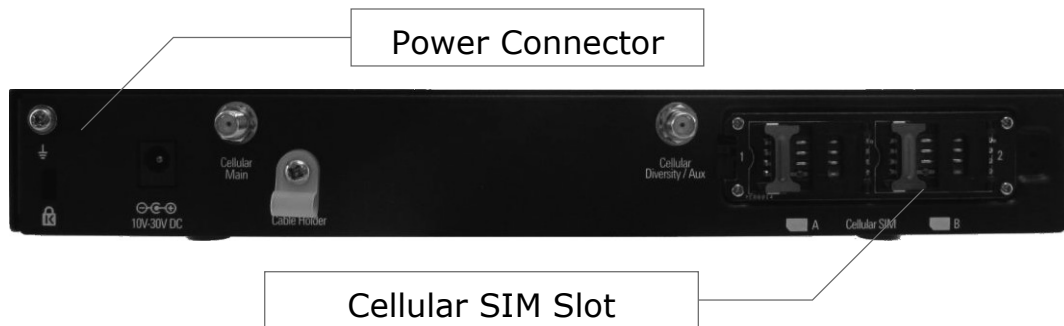
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

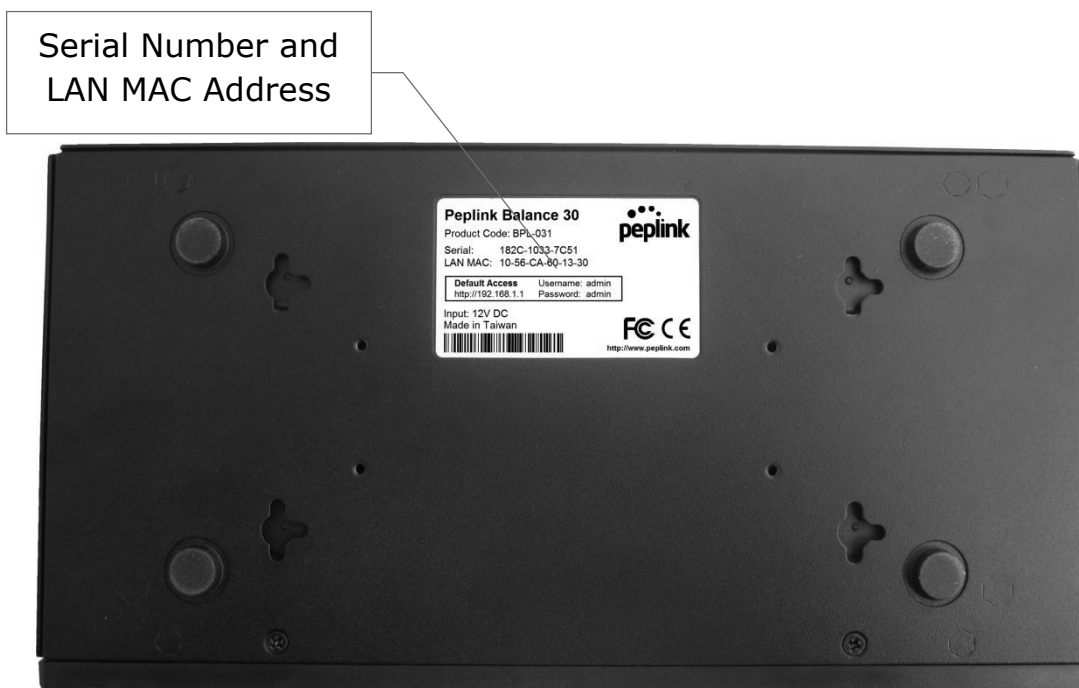
LAN and WAN Ports	
Green LED	ON – 10 / 100 /1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

USB Port	
USB Ports	For connecting a 4G/3G USB modem

8.4.3 Rear Panel Appearance

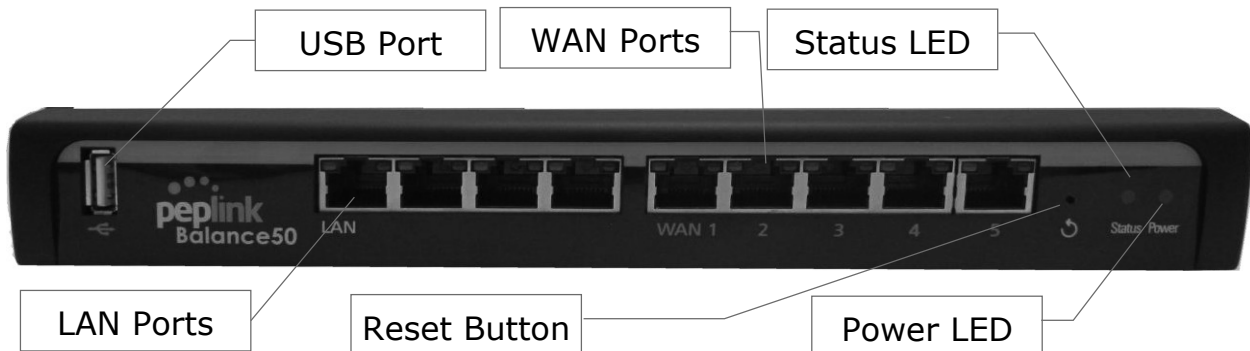


8.4.4 Unit Base Appearance



8.5 Peplink Balance 50

8.5.1 Front Panel Appearance



8.5.2 LED Indicators

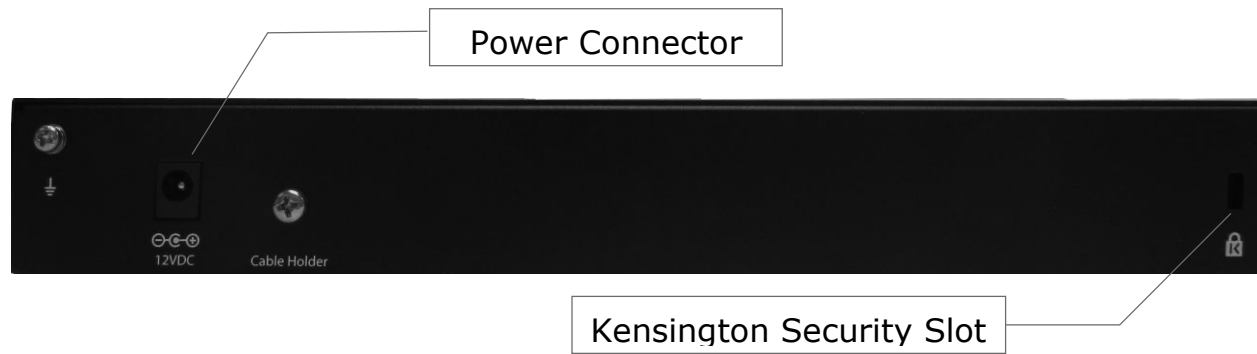
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

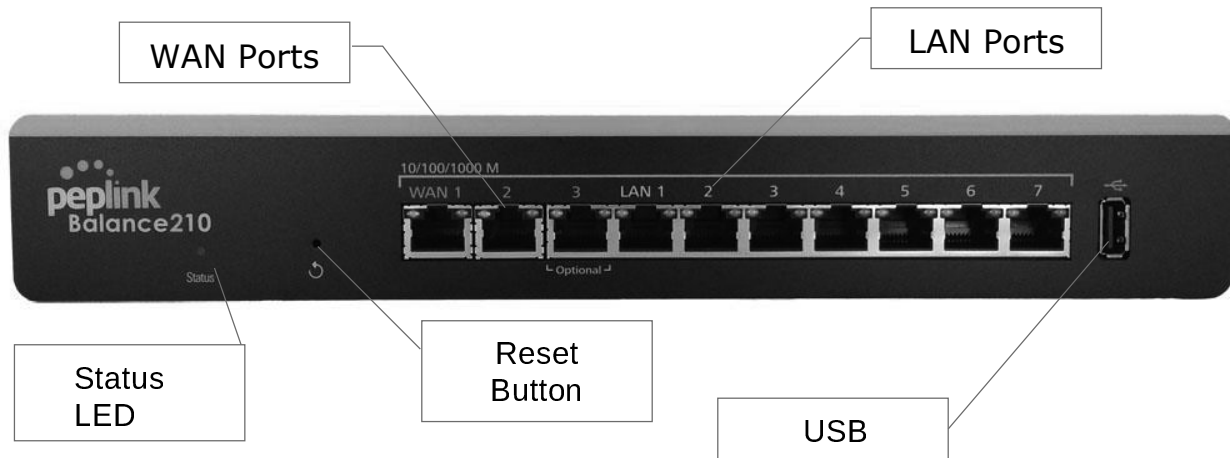
USB Port	
USB Ports	For connecting a 4G/3G USB modem

8.5.3 Rear Panel Appearance



8.6 Peplink Balance 210

8.6.1 Front Panel Appearance



8.6.2 LED Indicators

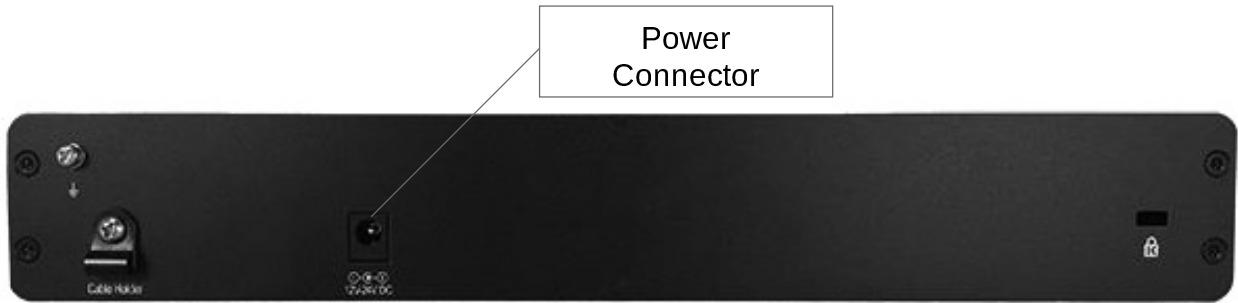
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
USB Ports	For connecting a 4G/3G USB modem

8.6.3 Rear Panel Appearance

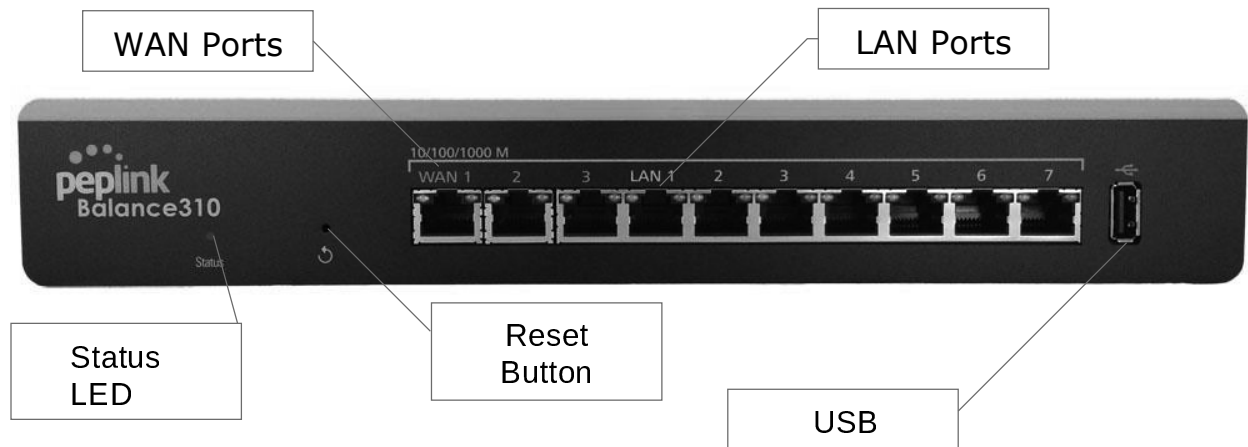


8.6.4 Unit Base Appearance



8.7 Peplink Balance 310

8.7.1 Front Panel Appearance



8.7.2 LED Indicators

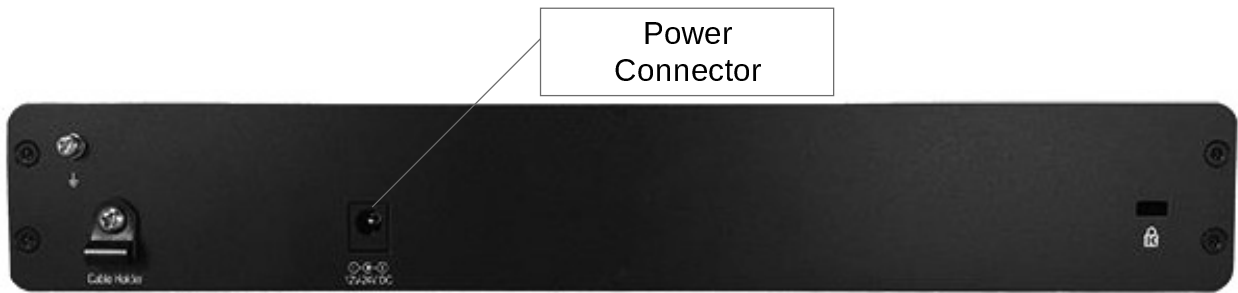
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
USB Ports	For connecting a 4G/3G USB modem

8.7.3 Rear Panel Appearance

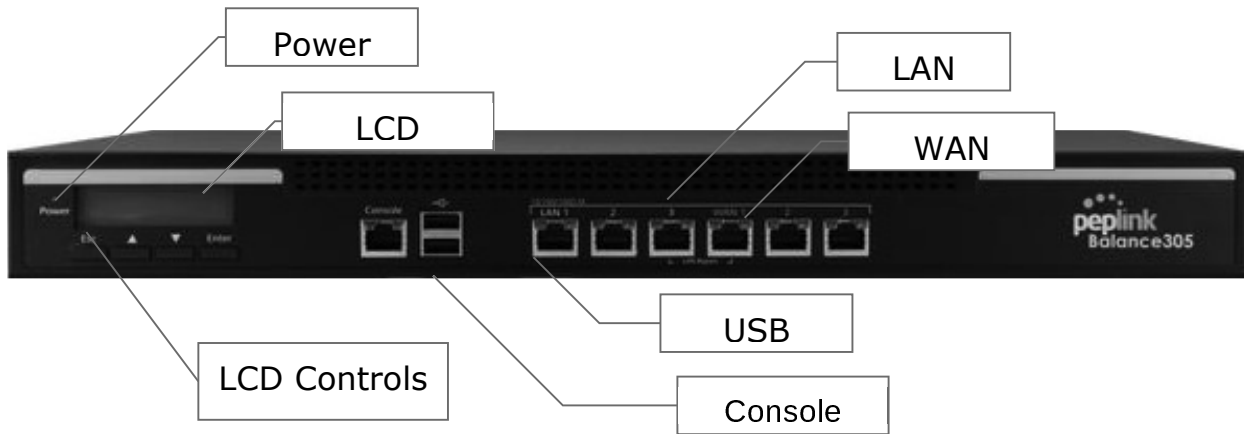


8.7.4 Unit Base Appearance



8.8 Peplink Balance 305

8.8.1 Front Panel Appearance



8.8.2 LED Indicators

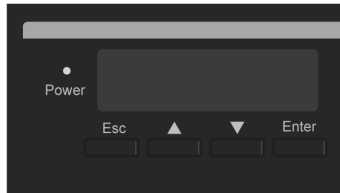
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Power LED	OFF – Power off
	GREEN – Power on

LAN Port, WAN 1 – 3 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

Console and USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

8.8.3 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)
 - > Link status (shows Connected/Disconnected, IP address list)
 - > WAN1
 - > WAN2
 - > WAN3
 - > VPN status (shows Connected/Disconnected)
 - >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, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
 - > LAN
 - > WAN1
 - > WAN2
 - > WAN3

8.8.4 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.

8.8.5 Unit Label Appearance

Peplink Balance 305


Product Code: BPL-305



Serial: 1824-A94A-3A4D

LAN MAC: 10-56-CA-07-3F-78

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

Input: 100V-240V AC
Made in Taiwan

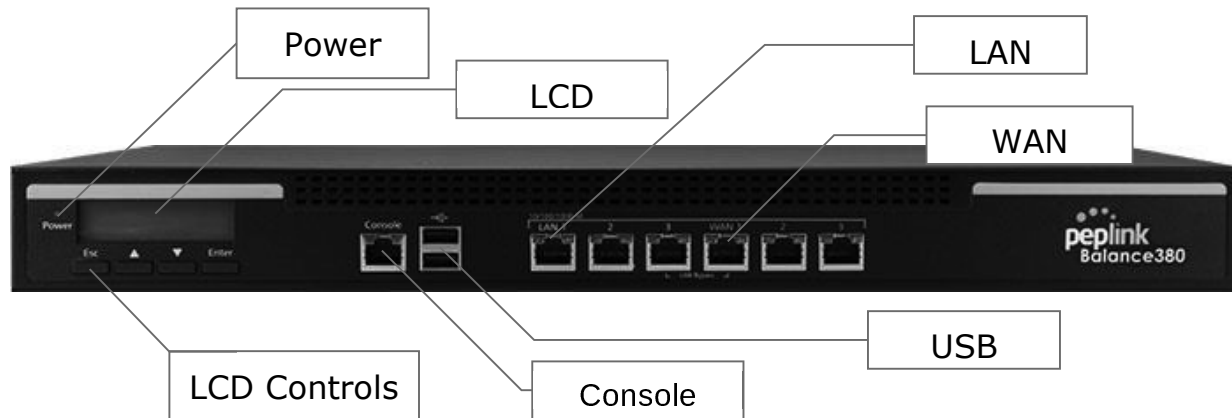




<http://www.peplink.com>

Serial Number
and
LAN MAC
Address

8.9 Peplink Balance 380

8.9.1 Front Panel Appearance

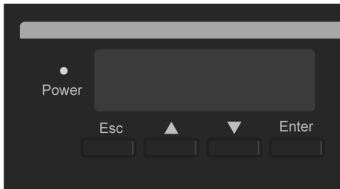


8.9.2 LED Indicators

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

Power and Status Indicators	
Power LED	OFF – Power off GREEN – Power on
LAN Port, WAN 1 – 3 Ports	
Right LED	ORANGE – 1000 Mbps GREEN – 100 Mbps OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic Blinking – Data is transferring OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports
Console and USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

8.9.3 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 (shows Connected/Disconnected, IP address list)
 - > WAN1
 - > WAN2
 - > WAN3
 - > VPN status (shows Connected/Disconnected)
 - >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, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
 - > LAN
 - > WAN1
 - > WAN2
 - > WAN3

8.9.4 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.

8.9.5 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
http://192.168.1.1	Password: admin

Made in Taiwan





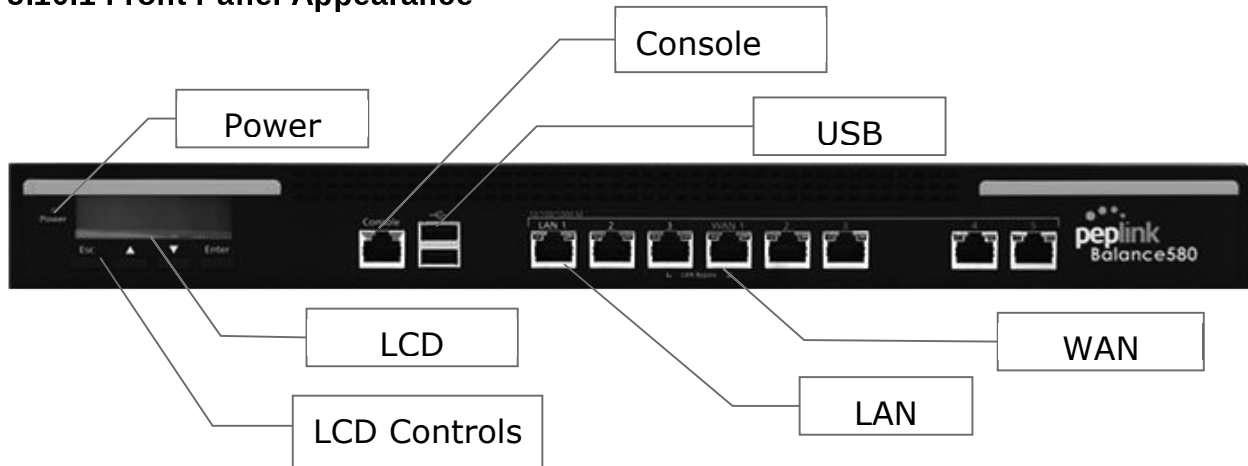


<http://www.peplink.com>

Serial Number and LAN MAC Address

8.10 Peplink Balance 580

8.10.1 Front Panel Appearance



8.10.2 LED Indicators

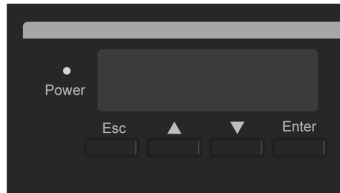
The statuses indicated by the front panel LEDs are as follows:

Power and Status Indicators	
Power LED	OFF – Power off
	GREEN – Power on

LAN Port, WAN 1 – 5 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

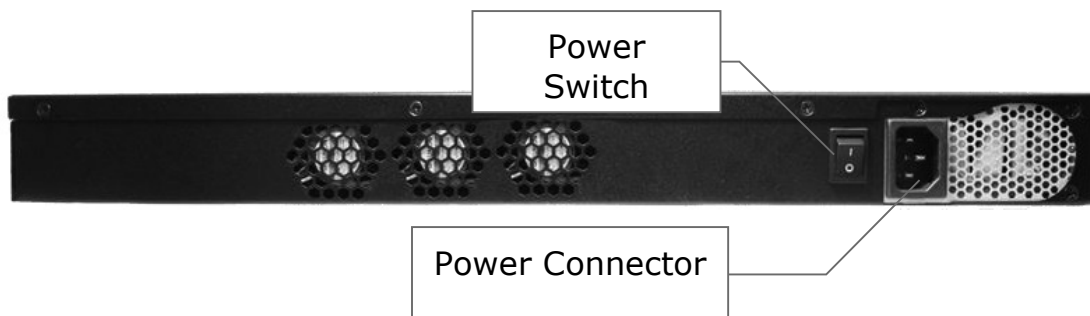
Console and USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

8.10.3 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 (shows Connected/Disconnected, IP address list)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN5
 - > VPN status (shows Connected/Disconnected)
 - > VPN Profile 1
 - > VPN Profile 2
 - > ...
 - > VPN Profile n
 - > Link usage
 - > Throughput in (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN5
 - > Throughput out (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN5
 - > Data Transfer'd (shows volume transferred since last reboot in MB)
 - > 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 (shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
 - > LAN
 - > WAN1
 - > WAN2
 - > ...
 - > WAN5

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.

8.10.4 Unit Label Appearance

Peplink Balance 580


Product Code: BPL-580



Serial: 1824-61DE-6B04

LAN MAC: 10-56-CA-03-E6-68

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

Made in Taiwan

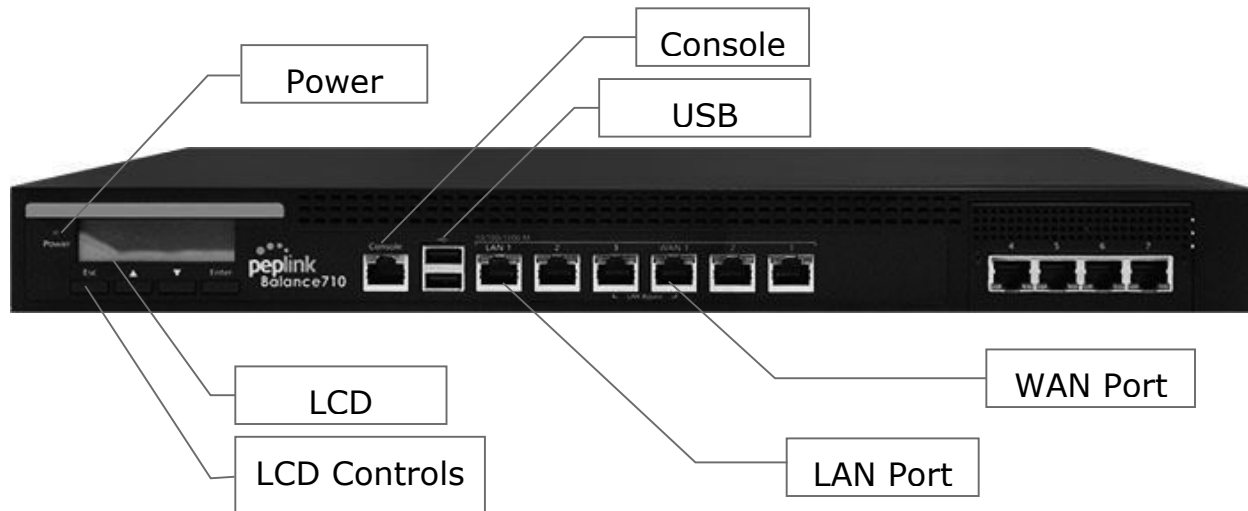




<http://www.peplink.com>

Serial Number
and
LAN MAC
Address

8.11 Peplink Balance 710

8.11.1 Front Panel Appearance



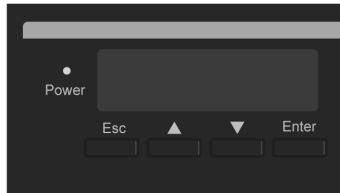
Status indicated in the front panel is as follows:

LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

LAN Port, WAN 1 – 7 Ports	
Green LED	ON – 1000 Mbps
	OFF – 100/10 Mbps
Orange LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

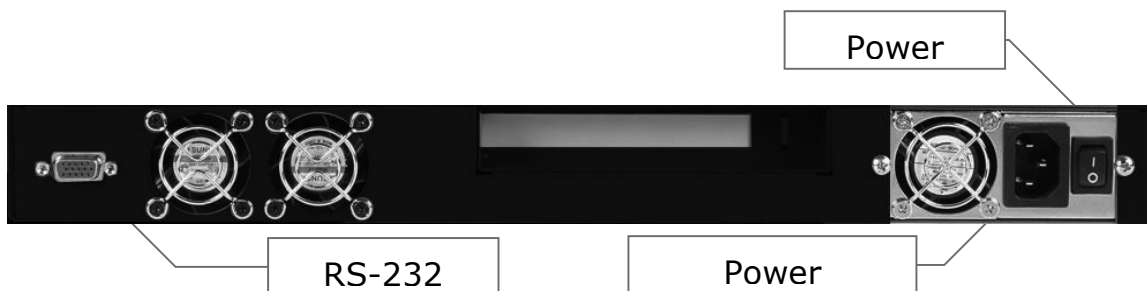
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

8.11.2 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 (shows Connected/Disconnected)
 - >VPN Profile 1
 - >VPN Profile 2
 - >...
 - >VPN Profile n
 - > Link usage
 - > Throughput in (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN7
 - > Throughput out (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN7
 - > Data Transfer'd (shows volume transferred since last reboot in MB)
 - > 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 (shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
 - > LAN
 - > WAN1
 - > WAN2
 - > ...
 - > WAN7

8.11.3 Rear Panel Appearance



Connector Ports	
RS-232 Port	Reserved for engineering use
Power Connector	AC input 110/220V

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.
Reset Switch	Press and release once to reset the system.


8.11.4 Unit Label Appearance



Peplink Balance 710
 Product Code: BPL-710
 Serial: 182C-1033-7C51
 LAN MAC: 10-56-CA-60-13-30

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

Serial Number
and
LAN MAC
Address

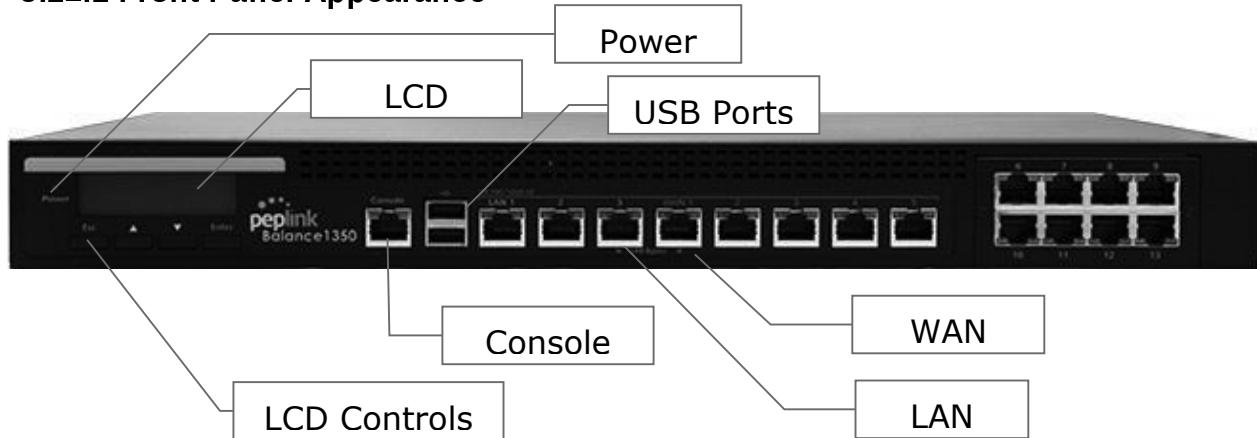
Made in Taiwan





<http://www.peplink.com>

8.12 Peplink Balance 1350

8.12.1 Front Panel Appearance



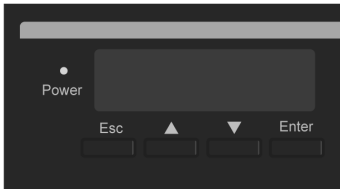
Status indicated in the front panel is as follows:

LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

LAN Port, WAN 1 – 13 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

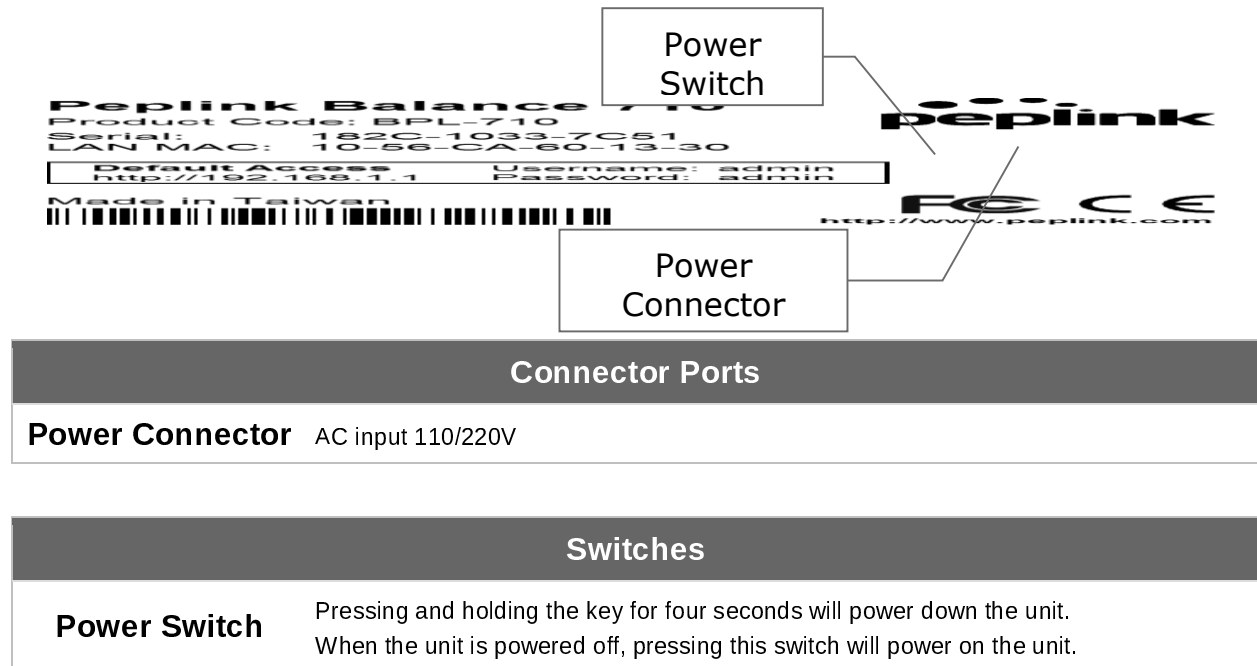
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

8.12.2 LCD Display Menu

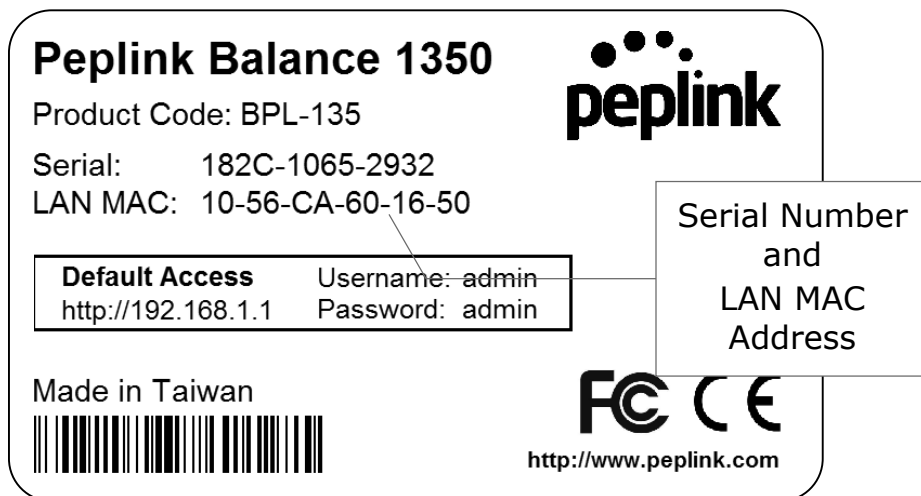


- > HA State: Master/Slave
 - > LAN IP
 - > VIP
- > System Status
 - > System
 - > Firmware ver. (shows firmware version)
 - > Serial number (shows serial number)
 - > System time (shows current time)
 - > System up time (shows system uptime since last reboot)
 - > CPU load (shows current CPU loading, 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 (shows Connected/Disconnected, IP address list)
 - > VPN status (shows Connected/Disconnected)
 - >VPN Profile 1
 - >VPN Profile 2
 - >...
 - >VPN Profile n
 - > Link usage
 - > Throughput in (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN13
 - > Throughput out (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN13
 - > Data Transfer'd (shows volume transferred since last reboot in MB)
 - > 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 (shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD,1000baseTx-FD)
 - > LAN
 - > WAN1
 - > WAN2
 - > ...
 - > WAN13

8.12.3 Rear Panel Appearance



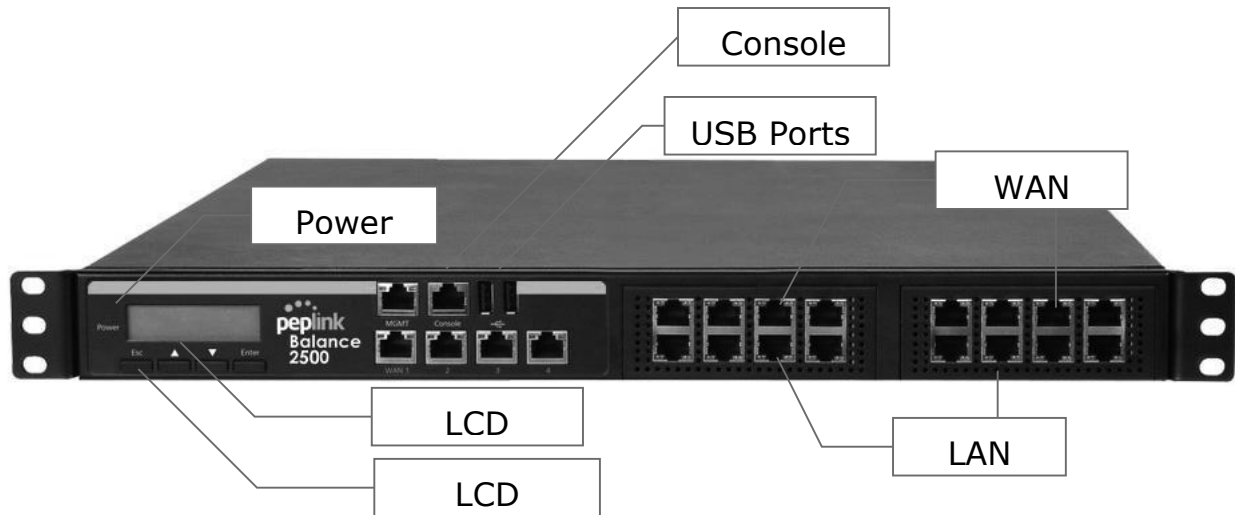
8.12.4 Unit Label Appearance



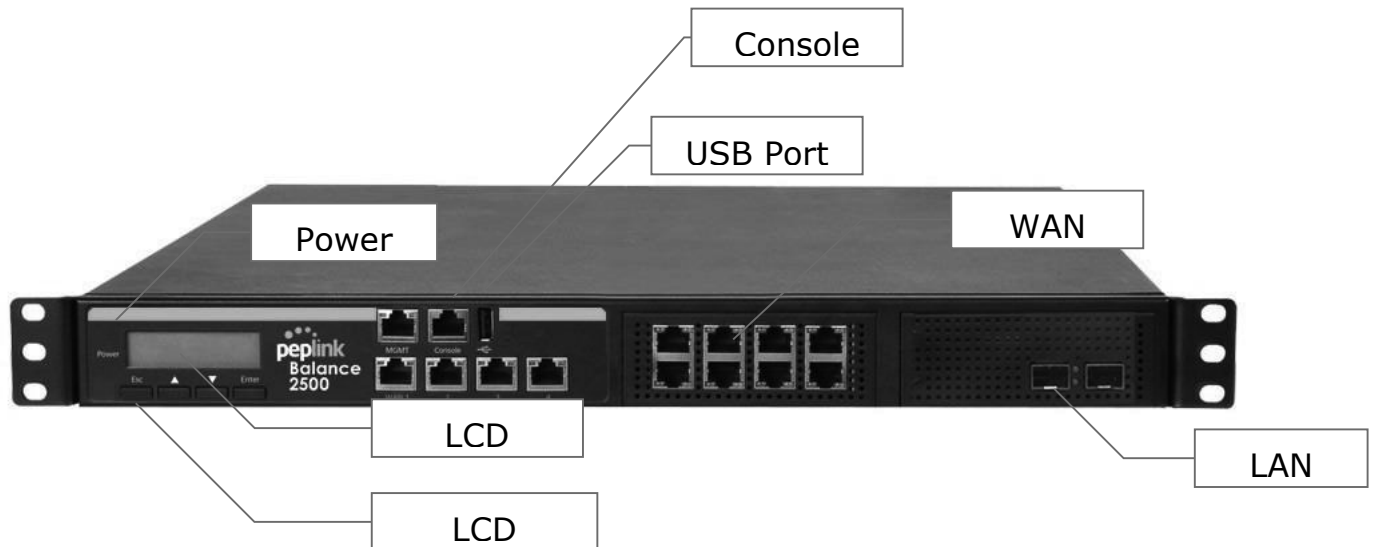
8.13 Peplink Balance 2500

8.13.1 Front Panel Appearance

BPL-2500



BPL-2500-SFP



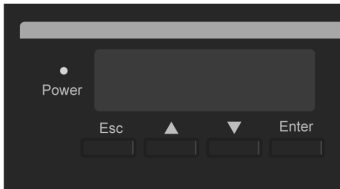
Status indicated in the front panel is as follows:

LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

LAN and WAN Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

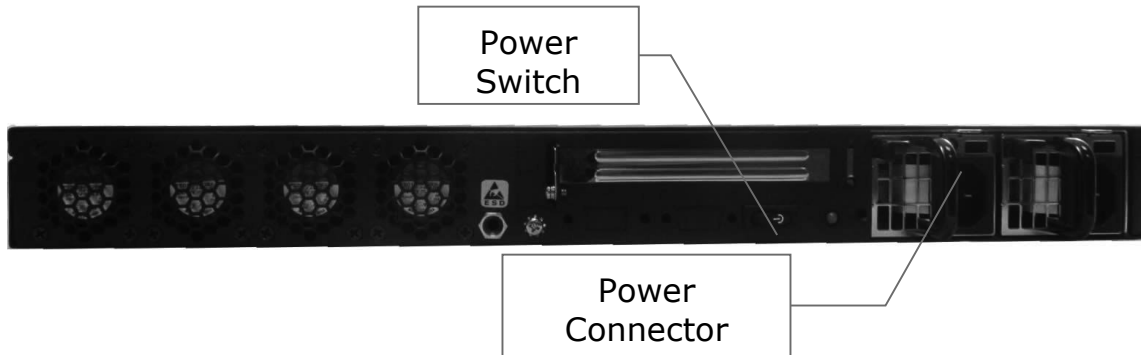
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

8.13.2 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 (shows Connected/Disconnected, IP address list)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN13
 - > VPN status (shows Connected/Disconnected)
 - >VPN Profile 1
 - >VPN Profile 2
 - >...
 - >VPN Profile n
 - > Link usage
 - > Throughput in (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN13
 - > Throughput out (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN13
 - > Data Transfer'd (shows volume transferred since last reboot in MB)
 - > 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 (shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD,1000baseTx-FD)
 - > LAN
 - > WAN1
 - > WAN2
 - > ...
 - > WAN13

8.13.3 Rear Panel Appearance



Connector Ports	
Power Connector	AC input 100-240V

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.



8.13.4 Unit Label Appearance

BPL-2500

Peplink Balance 2500
 Product Code: BPL-2500
 Serial: 1234-5678-9000
 LAN MAC: 11-22-33-44-55-66

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

Input: 100V-240V AC
 Made in Taiwan



<http://www.peplink.com>



Serial Number
and
LAN MAC
Address

BPL-2500-SFP

Peplink Balance 2500
 Product Code: BPL-2500-SFP
 Serial: 1234-5678-9000
 LAN MAC: 11-22-33-44-55-66

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

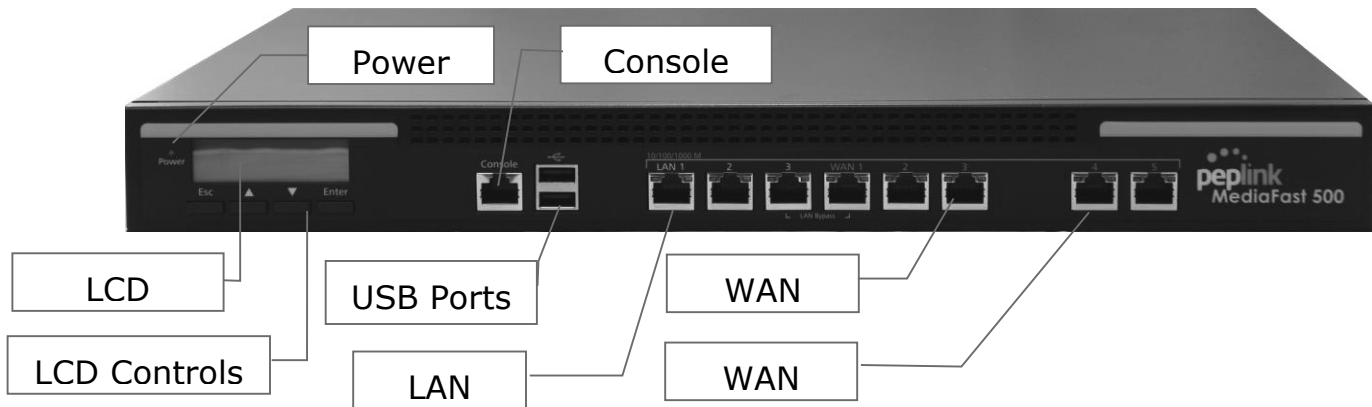
Input: 100V-240V AC
 Made in Taiwan



<http://www.peplink.com>

Serial Number
and
LAN MAC
Address

8.14 Peplink MediaFast 500

8.14.1 Front Panel Appearance



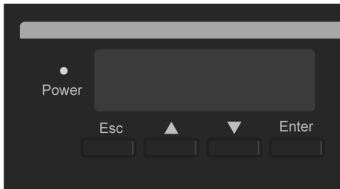
Status indicated in the front panel is as follows:

LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

LAN 1-3 Ports, WAN 1-5 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

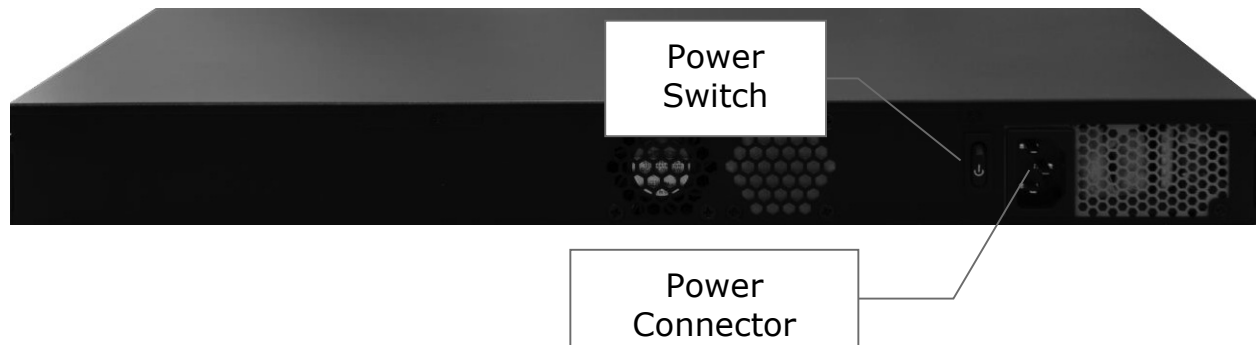
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting 4G/3G USB modems

8.14.2 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 (shows Connected/Disconnected, IP address list)
 - > VPN status (shows Connected/Disconnected)
 - > VPN Profile 1
 - > VPN Profile 2
 - > ...
 - > VPN Profile n
 - > Link usage
 - > Throughput in (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN5
 - > Throughput out (shows transfer rate in Kbps)
 - > WAN1
 - > WAN2
 - > ...
 - > WAN5
 - > Data Transfer'd (shows volume transferred since last reboot in MB)
 - > 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 (shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
 - > LAN
 - > WAN1
 - > WAN2
 - > ...
 - > WAN5

8.14.3 Rear Panel Appearance



Connector Ports	
Power Connector	AC input 100-240V

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.

9 Installation

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

9.1 Preparation

Before installing your Peplink Balance, please prepare the following:

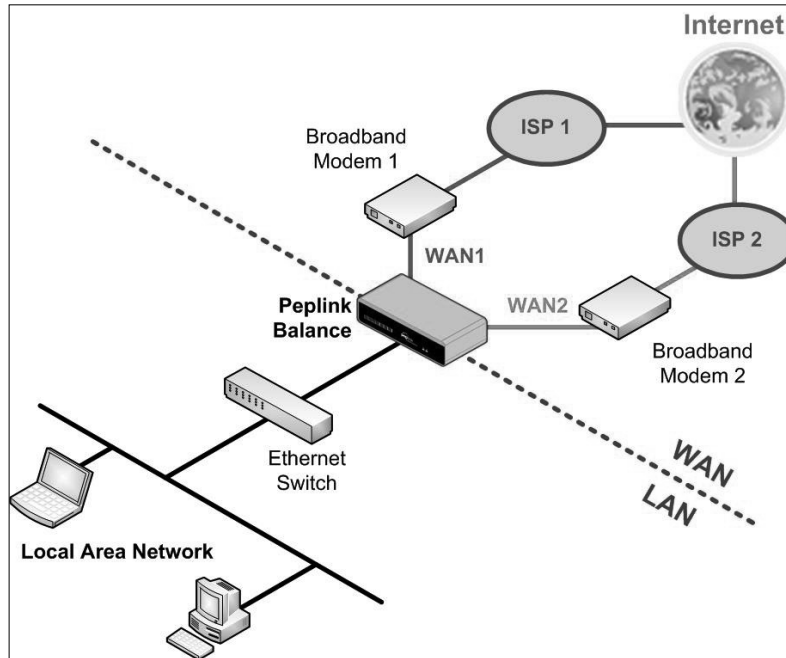
- At least one Internet/WAN access account
- For each network connection, one 10/100BaseT UTP cable with RJ45 connector, one 1000BaseT Cat5E UTP cable for the Gigabit port, or one USB modem for the USB WAN port
- A computer with the TCP/IP network protocol and a web browser installed—supported browsers 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

9.2 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:



9.3 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 10, Basic Configuration**.
For advanced configuration, refer to **Section 0, Configuring the LAN Interface(s)**.
- WAN configuration
For basic configuration, refer to **Section 10, Basic Configuration**.
For advanced configuration, refer to **Section 14, Configuring the WAN Interface(s)**.
- MediaFast configuration
For MediaFast configuration, refer to **Section 11, MediaFast Configuration**.

10 Basic Configuration

10.1 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.)

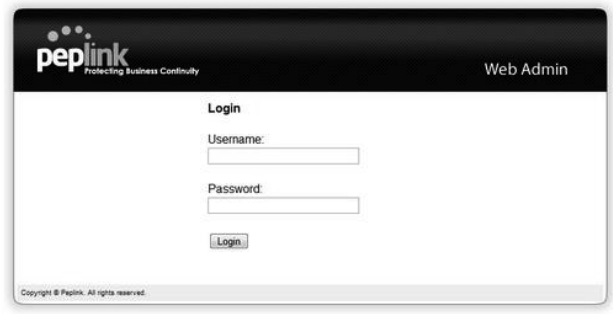
3. Enter the following to access the web admin interface.

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:

1 3G	
IP Address: 17.219.22.1 Details...	Status: <input type="checkbox"/> Connected Disconnect
2 Wi-Fi	
IP Address: 18.220.23.1 Details...	Status: <input type="checkbox"/> Connected Disconnect
3 FBB	
IP Address: 19.221.24.1 Details...	Status: <input type="checkbox"/> Connected Disconnect
4 WAN4	
IP Address: 123.203.209.47 Details...	Status: <input type="checkbox"/> Connected Disconnect
5 WAN5	
IP Address: 14.136.11.100 Details...	Status: <input type="checkbox"/> Connected Disconnect
6 WAN6	
IP Address: 213.141.82.11 Details...	Status: <input type="checkbox"/> Connected Disconnect
USB	
IP Address: (none)	Status: No Device Detected

LAN Interface	
Router IP Address: 192.168.1.1	

PepVPN with SpeedFusion™		Status
SDT	Established	
TPTTest		

AP Controller Information		Status
Access Point: 0 (Online: 0)		
Connected Clients: 0		

Device Information	
Model:	Peplink Balance 710
Firmware:	6.1.0 build 2863
Uptime:	38 days 22 hours 17 minutes
CPU Load:	<input type="text" value="5%"/>
Throughput:	0.0 Mbps ↑ 0.0 Mbps

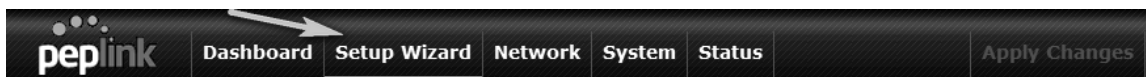
Important Note

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.

10.2 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.

Setup Wizard > WAN Setup > Step 1

Welcome to Setup Wizard!

The Setup Wizard will guide you through the WAN port(s) configuration step by step. This wizard is designed to simplify the process in configuring your device and connecting it to the Internet.

Click **Next** to begin.

Select **Yes** if you want to set up drop-in mode using the Setup Wizard.

Setup Wizard > WAN Setup > Step 2

Drop-in Mode	
Do you want to setup drop-in mode?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Which WAN port do you want to enable drop-in mode?	<div style="border: 1px solid black; padding: 2px;">WAN 1 ▼<ul style="list-style-type: none">WAN 1WAN 2WAN 3WAN 4WAN 5WAN 6WAN 7</div>

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.

Setup Wizard > WAN Setup > Step 3

Choose the WAN port(s) to be configured.

WAN Ports	
WAN 1 (Drop-in)	<input checked="" type="checkbox"/>
WAN 2	<input type="checkbox"/>
WAN 3	<input type="checkbox"/>
WAN 4	<input type="checkbox"/>
WAN 5	<input type="checkbox"/>
WAN 6	<input type="checkbox"/>
WAN 7	<input type="checkbox"/>
Mobile Internet	<input type="checkbox"/>

If drop-in mode is going to be configured, the setup wizard will move on to **Drop-in Settings**.

Setup Wizard > WAN Setup > Step 4


Enter the parameters of Drop-in Settings for WAN 1.

Drop-in Settings	
IP Address	<input type="text"/>
Subnet Mask	255.255.255.0 (/24) ▼
Default Gateway	<input type="text"/>
DNS Servers	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
Upload Bandwidth	1000 <input type="text"/> Mbps ▼
Download Bandwidth	1000 <input type="text"/> Mbps ▼

If you are not using drop-in mode, select the connection method for the WAN connection(s) from the following screen:

Setup Wizard > WAN Setup > Step 4

Choose a connection method for WAN 1.


Connection Method 	
Method	Select
Static IP	<input type="radio"/>
DHCP	<input checked="" type="radio"/>
PPPoE	<input type="radio"/>
Disable	<input type="radio"/>

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 14, 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**.

Setup Wizard > WAN Setup > Step 3


Select whether Operator Settings for Mobile Internet will be automatically detected or customized.

Operator Settings (for HSPA/EDGE/GPRS only) 	
Settings	Select
Auto	<input type="radio"/>
Custom	<input checked="" type="radio"/>

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.

Setup Wizard > WAN Setup > Step 4

Enter the parameters of Mobile Operator Settings for Mobile Internet.

Mobile Operator Settings 	
APN	<input type="text"/>
Login ID	<input type="text"/>
Password	<input type="text"/>
Dial Number	<input type="text"/>

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.

Setup Wizard > WAN Setup > Step 5

Choose the preferred WAN Port(s) that is to be used as primary connection. The port(s) not selected in this step will only be used when none of the connection of the preferred port is up.

Preferred WAN Port Selection	
Port	Preferred
WAN 1	<input checked="" type="checkbox"/>
WAN 2	<input checked="" type="checkbox"/>
Mobile Internet	<input type="checkbox"/>

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

Setup Wizard > WAN Setup > Step 6

Choose time zone of your Country / Region.

Time Zone Settings	
Time Zone	(GMT+07:00) Krasnoyarsk
	<input type="checkbox"/> Show all

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

Setup Wizard > WAN Setup > Final Step

Confirm the WAN connection(s) configuration below. Click *Back* to modify the configuration settings in previous steps. Click *Save Settings* when you are done.

Summary of WAN Port(s) Configuration	
WAN 1	
Connection Method	Drop-in Static IP
IP Address	192.22.22.1
Subnet Mask	255.255.255.0
Default Gateway	192.22.22.1
DNS Server	192.22.22.1
Upload Bandwidth	1000 Mbps
Download Bandwidth	1000 Mbps
Preferred WAN Port(s)	
Ports	WAN 1 WAN 2
Time Zone Settings	

<< Back Save Settings Cancel

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

10.3 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**.



Connection Name	Method	Routing Mode	Type
1. WAN_1	DHCP	NAT	Always-on
2. WAN_2	DHCP	NAT	Always-on
3. WAN_3	Not Configured	NAT	Always-on
4. WAN_4	Not Configured	NAT	Always-on
5. WAN_5	Not Configured	NAT	Always-on
6. WAN_6	Not Configured	NAT	Always-on
7. WAN_7	Not Configured	NAT	Always-on
8. WAN_8	Not Configured	NAT	Always-on
9. WAN_9	Not Configured	NAT	Always-on
10. WAN_10	Not Configured	NAT	Always-on
11. WAN_11	Not Configured	NAT	Always-on
12. WAN_12	Not Configured	NAT	Always-on
13. Mobile_Internet	ppp	NAT	Backup Group 1

IPv6
Disabled

Tip

Please refer to **Section 14, Configuring the WAN Interface(s)**, for details on setting up DHCP, static IP, PPPoE, L2TP, and mobile Internet connections.

10.4 Cellular WAN


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

WAN Connection Status ?		
Priority 1 (Highest)		
1 WAN 1	<input type="checkbox"/> Connected	Details
Priority 2		
2 WAN 2	<input checked="" type="checkbox"/> No Cable Detected	Details
1 Cellular 1	No Device Detected	Details
2 Cellular 2	<input checked="" type="checkbox"/> No SIM Card Detected Reload SIM	Details
Priority 3		
Drag desired (Priority 3) connections here		
Disabled		
WI-FI WAN	<input checked="" type="checkbox"/> Disabled	Details


Cellular 2 Status ?	
IMSI	(No SIM Card Detected)
MEID	HEX: A100001F7DB61E DEC: 270113180708238622
ESN	8075D998
IMEI	356144040003283
Network Mode	HSPA


Cellular Status	
IMSI	This is the International Mobile Subscriber Identity, which uniquely identifies the SIM card. This is applicable to 3G modems only.
MEID	Some 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.
ESN	This serves the same purpose as MEID HEX but uses an older format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.
Network Mode	This field displays the network mode, such as HSPA, for the listed cellular connection.


WAN Connection Settings	
WAN Connection Name	Cellular 1 Default
Network Mode	<input checked="" type="radio"/> HSPA <input type="radio"/> Sprint,EV-DO <input type="radio"/> Verizon Wireless,EV-DO
Routing Mode	<input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding ?
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Network Mode	Choose the appropriate network mode for the cellular connection.
Routing Mode	Select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (network address translation) or IP Forwarding . Click the  button to enable IP forwarding.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server 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.)</p> <p>When Use the following DNS server address(es) is selected, you can put custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields.</p>

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

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 on 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  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 	<input type="checkbox"/>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected
Idle Disconnect	<input type="checkbox"/>

General Settings

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).

IP Passthrough

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

Health Check Settings	
Heath 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 14.3 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	
Dynamic DNS Service Provider	<input type="text" value="changeip.com"/>
User ID	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Hosts	<input type="text"/>

Dynamic DNS Settings

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 14.6** for configuration details.

Dynamic DNS Service Provider

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

MTU

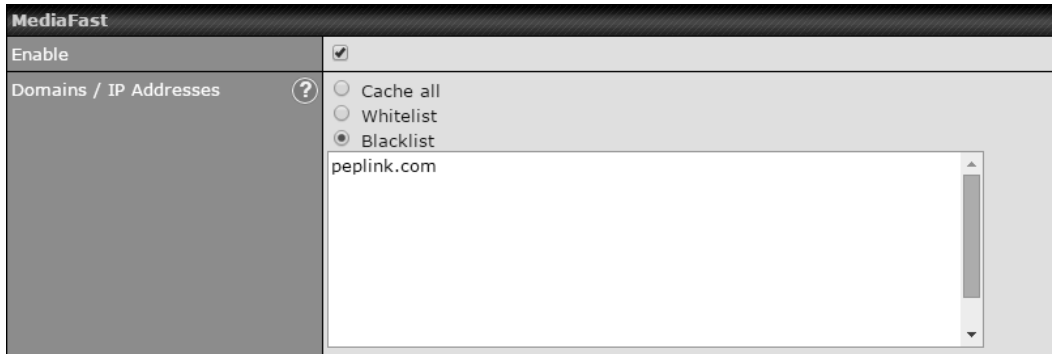
MTU MTU determines the maximum allowable size per packet, in bytes.

11 MediaFast Configuration

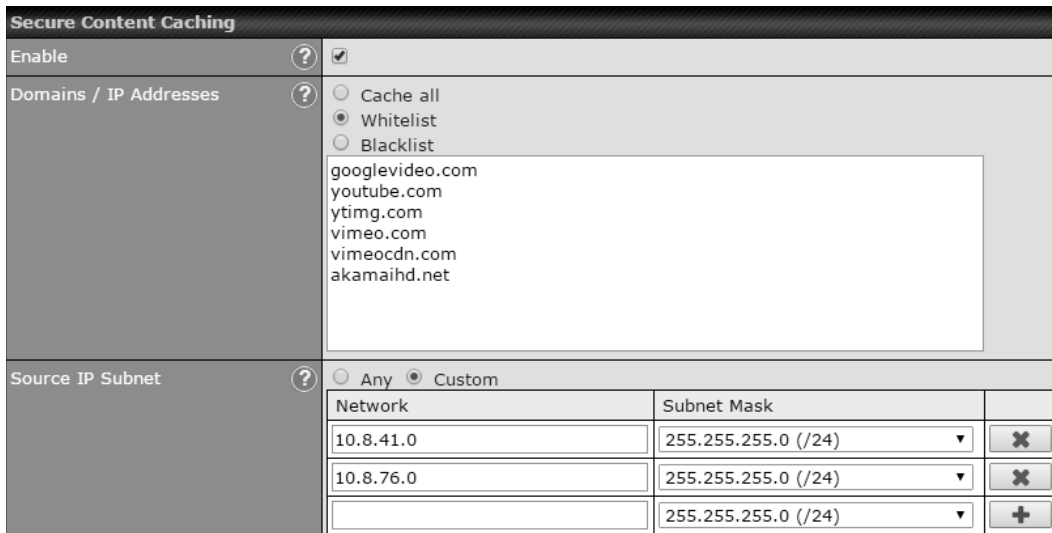
MediaFast settings can be configured from the **Network** menu.

11.1 Setting Up MediaFast Content Caching

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



MediaFast	
Enable	Click the checkbox to enable MediaFast content caching.
Domains / IP Addresses	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).



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

Cache Control		
Content Type	<input checked="" type="checkbox"/> Video	
	<input checked="" type="checkbox"/> Audio	
	<input checked="" type="checkbox"/> Images	
	<input checked="" type="checkbox"/> OS / Application Updates	
Cache Lifetime Settings	File Extension	Lifetime (days)
	<input type="text"/>	<input type="text"/>
		<input type="button" value="+"/>

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.

11.2 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							
Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
▶ Course Progress	Downloading	04-11 06:00	04-09 02:03	-		0 B	
▶ National Geog	Ready	04-11 00:00	04-09 00:00	00:01		4.98 kB	
▶ Syllabus	Downloading	04-11 06:00	04-09 06:00	-		0 B	
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01		115.91 kB	
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01		62.26 kB	

[New Schedule](#)

Tools	
Clear Web Cache	Clear Statistics

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

MediaFast Schedule							
Name (optional)	Cache Peplink Website						
Active	<input checked="" type="checkbox"/>						
URL	<table border="1"> <tr> <td>URL</td> <td></td> </tr> <tr> <td>www.peplink.com</td> <td><input type="button" value="x"/></td> </tr> <tr> <td>www.peplink.com/knowledgebase</td> <td><input type="button" value="+"/></td> </tr> </table>	URL		www.peplink.com	<input type="button" value="x"/>	www.peplink.com/knowledgebase	<input type="button" value="+"/>
	URL						
www.peplink.com	<input type="button" value="x"/>						
www.peplink.com/knowledgebase	<input type="button" value="+"/>						
Depth	2 levels Default						
Time Period	From 00:00 to 01:00						
Repeat	Everyday						
<input type="button" value="Save & Apply Now"/> <input type="button" value="Cancel"/>							

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.

11.3 MDM Settings

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

MDM Settings	
Enable	<input checked="" type="checkbox"/>
Account Settings	<input type="radio"/> Follow Web Admin Account <input checked="" type="radio"/> Custom
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

MDM Settings

Enable

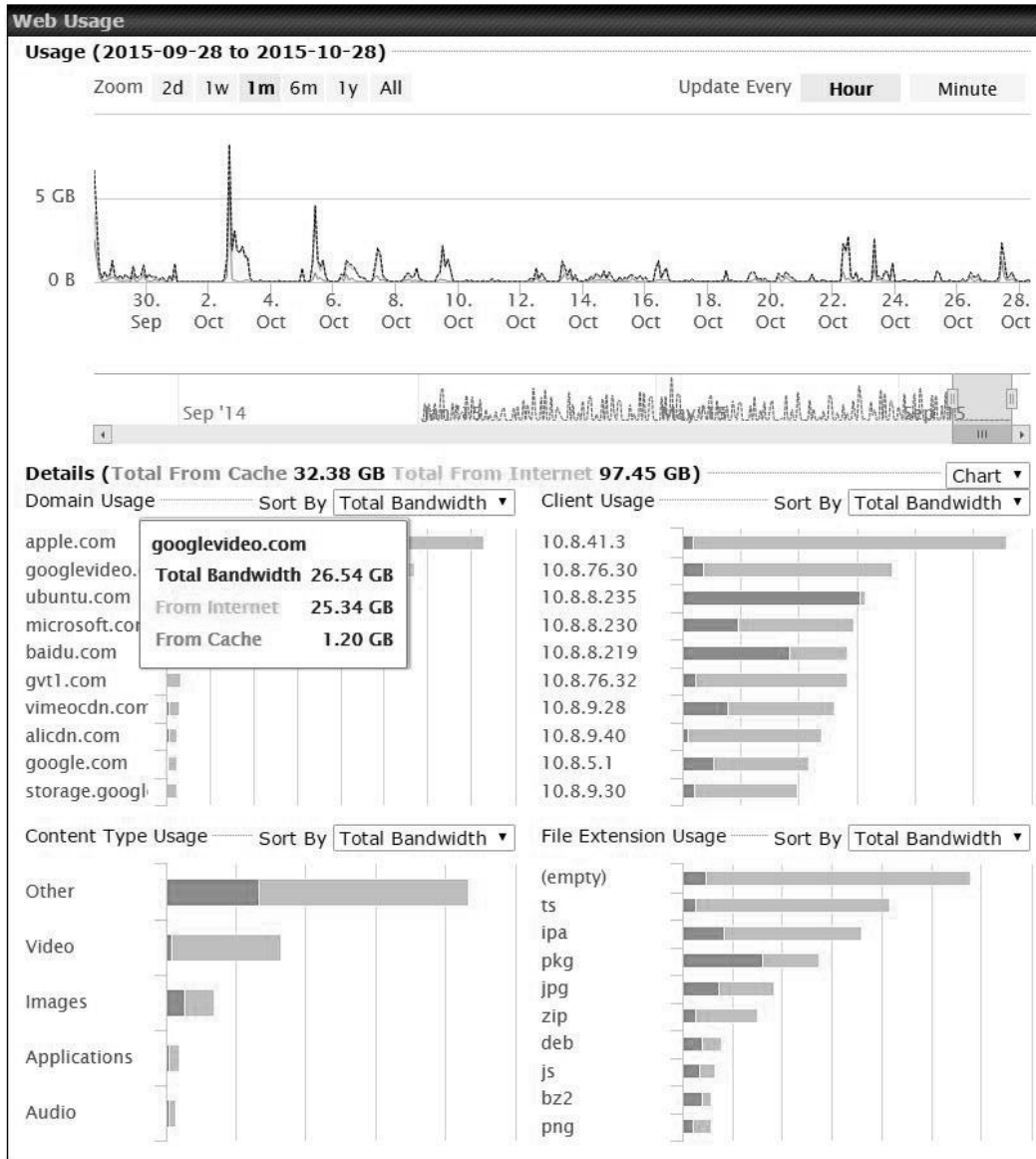
Click this checkbox to enable MDM on your router.

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.

11.4 Viewing MediaFast Statistics


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



12 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).


IP Settings	
IP Address	192.168.1.1 255.255.255.0 (/24) ▼

IP Settings	
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	
Enable	<input checked="" type="checkbox"/>
WAN for Drop-In Mode	WAN 1 with LAN bypass ▼
WAN Default Gateway	<input type="text"/> <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) <input type="text"/> - <input type="text"/> <input type="button" value="↓"/> <input type="text"/> <input type="button" value="Delete"/>
WAN DNS Servers	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
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.	

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 13, 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^A	<p>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.).</p> <p>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.).</p>
Shared IP Address^A	<p>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.).</p>
WAN Default Gateway	<p>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 I have other host(s) on WAN segment box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.</p>
WAN DNS Servers	<p>Enter the selected WAN's corresponding DNS server IP addresses.</p>

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



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

Layer 2 PepVPN Bridging Settings	
PepVPN Profiles to Bridge	<p>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.</p>
Remote Network Isolation	<p>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.</p>
Spanning Tree Protocol	<p>Click this checkbox to enable spanning tree protocol in your L2 PepVPN.</p>
Override IP Address when bridge connected	<p>Select Do not override if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.</p> <p>If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.</p>

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

DHCP Server											
DHCP Server	<input checked="" type="checkbox"/>	Enable									
DHCP Server Logging	<input type="checkbox"/>										
IP Range	192.168.1.10 - 192.168.1.250	255.255.255.0 (/24)									
Lease Time	1 Days 0 Hours 0 Mins										
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically										
WINS Servers	<input checked="" type="checkbox"/> Assign WINS server <input type="radio"/> Built-in <input checked="" type="radio"/> External WINS Server 1: <input type="text"/> WINS Server 2: <input type="text"/>										
BOOTP	<input checked="" type="checkbox"/> Server IP Address: <input type="text"/> Boot File: <input type="text"/> Server Name: <input type="text"/> (Optional)										
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		<input type="button" value="Add"/>			
Option	Value										
No Extended DHCP Option											
<input type="button" value="Add"/>											
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>00:00:00:00:00:00</td> <td></td> <td style="text-align: center;">+</td> </tr> </tbody> </table>			Name	MAC Address	Static IP			00:00:00:00:00:00		+
Name	MAC Address	Static IP									
	00:00:00:00:00:00		+								

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	<p>In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.</p> <p>To define an extended DHCP option, click the Add button, choose the option to define, and 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.</p>
DHCP Reservation	<p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses.</p> <p>The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p>Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in 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 28.3.</p>


Next, choose port settings.

LAN Physical Settings	
Ports	<input checked="" type="checkbox"/> LAN Auto <input type="checkbox"/> WAN 3
IEEE 802.3ad Link Aggregation	LAN: 1 2 3 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> WAN: 3 <input type="checkbox"/>

LAN Physical Settings	
Speed	<p>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.</p>
IEEE 802.3ad Link Aggregation	<p>Choose the interfaces that you wish to aggregate here if needed.</p>

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

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

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

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

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			
Static Route	Destination Network	Subnet Mask	Gateway
		255.255.255.0 (/24) ↓	
			+
Note: Static routes will be advertised to remote PepVPN peers			




Static Route Settings	
Static Route	<p>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 <i>w.x.y.z</i> format.</p> <p>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 <input type="button" value="+"/> to create a new route. Click <input type="button" value="x"/> to remove a route.</p>

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

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

Enter any needed DNS proxy settings. Once all settings have been entered, click **Save** to store your changes.

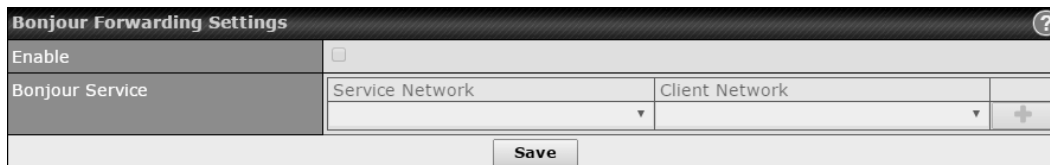
DNS Proxy Settings			
Enable	<input checked="" type="checkbox"/>		
DNS Caching	<input type="checkbox"/>		
Include Google Public DNS Servers	<input type="checkbox"/>		
Local DNS Records	Host Name	IP Address	TTL
			3600 +
Domain Lookup Policy	Domain	Connection	
		: +	
DNS Resolvers	WAN Connection		DNS Servers
	<input type="checkbox"/> WAN 1	10.88.3.1 168.95.1.1	
	<input type="checkbox"/> WAN 2		
	<input type="checkbox"/> WAN 3		
	<input type="checkbox"/> Mobile Internet		
	LAN Connection		DNS Servers
<input type="checkbox"/> Untagged LAN			
Preferred connections are shown with <input checked="" type="checkbox"/>			



DNS Proxy Settings	
Enable	<p>To enable the DNS proxy feature, check this box, and then set up the feature at Network>LAN>DNS Proxy Settings.</p> <p>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.</p>
DNS Caching	<p>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.</p>
Include Google Public DNS Servers	<p>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.</p>
Local DNS Records	<p>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.</p>
Domain Lookup Policy	<p>DNS proxy will look up the domain names defined here using only the specified connections.</p>
DNS Resolvers^A	<p>Check the box to enable the WINS server. A list of WINS clients will be displayed at Network>LAN>DNS Proxy Settings>DNS Resolvers.</p> <p>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</p>

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.



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

12.1 LAN Configuration with VLAN

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

IP Settings	
IP Address	192.168.222.1 255.255.255.0 (/24) ▼

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

LAN	VLAN	Network
Untagged LAN ←	None	192.168.222.1/24

New LAN

The following settings are displayed:

LAN


IP Settings	
IP Address	192.168.222.1 255.255.255.0 (/24) ▼

IP Settings	
IP Address	Enter the Peplink Balance's IP address and subnet mask values to be used on the LAN.

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


Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a 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	<input checked="" type="checkbox"/>
WAN for Drop-In Mode	WAN 1 with LAN bypass
WAN Default Gateway	<input type="text"/> <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) <input type="text"/> - <input type="text"/> <input type="button" value="↓"/> <input type="text"/> <input type="button" value="Delete"/>
WAN DNS Servers	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
<p>NOTE: The DHCP Server Settings will be overwritten.</p> <p>The following WAN 1 with LAN bypass settings will be overwritten: Enable, Connection Method, Routing Mode, Connection Type, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.</p> <p>The PPTP Server will be disabled. High Availability will be disabled.</p> <p>Tip: please review the DNS Forwarding setting under the Service Forwarding section.</p>	


Drop-in Mode Settings	
Enable	<p>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.</p> <p>Please refer to Section 13, Drop-in Mode for details.</p>
WAN for Drop-In Mode	<p>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.</p>
Shared Drop-In IP^A	<p>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.).</p> <p>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.).</p>
Shared IP Address^A	<p>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.)</p>
WAN Default Gateway	<p>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 I have other host(s) on WAN segment box and enter the IP address of the hosts that</p>

	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 	<input type="text" value="-----"/>
Remote Network Isolation 	<input type="checkbox"/>
Spanning Tree Protocol	<input type="checkbox"/>
Override IP Address when bridge connected 	<input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None

Layer 2 PepVPN Bridging ^A	
PepVPN Profiles to Bridge^A	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^A	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^A	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^A	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	<input checked="" type="checkbox"/>	Enable							
IP Range	192.168.222.10 - 192.168.222.250	255.255.255.0 (/24)							
Lease Time	1 Days 0 Hours 0 Mins								
DNS Servers	<input checked="" type="checkbox"/>	Assign DNS server automatically							
WINS Servers	<input type="checkbox"/>	Assign WINS server							
BOOTP	<input type="checkbox"/>								
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;">Add</td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		Add	
Option	Value								
No Extended DHCP Option									
Add									
DHCP Reservation	<input checked="" type="checkbox"/>	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>		Name	MAC Address	Static IP			
Name	MAC Address	Static IP							

DHCP Server Settings	
DHCP Server	When this setting is enabled, the 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 28.3**.

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.

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

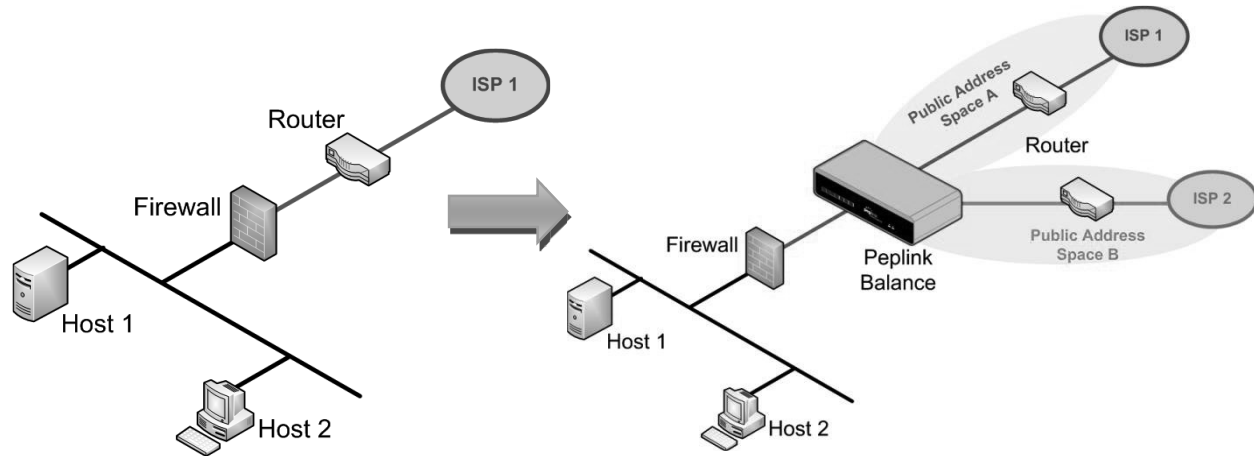
DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active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

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.

13 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.

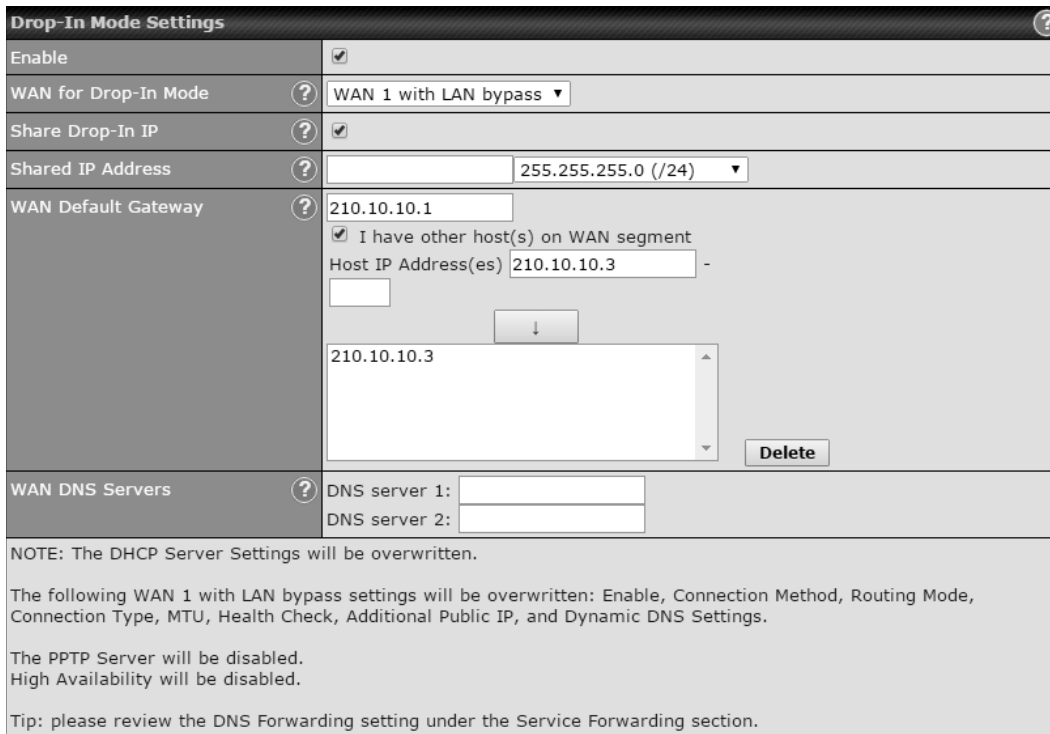
IMPORTANT NOTE for customers using drop-in mode and planning to upgrade from Firmware 4.8.2 or below to 5.0+

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:

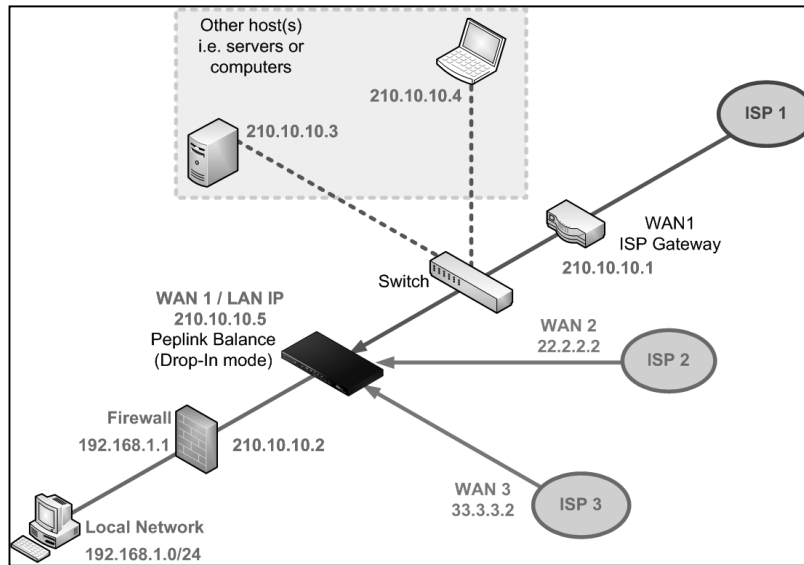


Drop-In Mode Settings	
Enable	<input checked="" type="checkbox"/>
WAN for Drop-In Mode	WAN 1 with LAN bypass ▾
Share Drop-In IP	<input checked="" type="checkbox"/>
Shared IP Address	255.255.255.0 (/24) ▾
WAN Default Gateway	210.10.10.1 <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) 210.10.10.3 - [] ↓ 210.10.10.3 Delete
WAN DNS Servers	DNS server 1: [] DNS server 2: []

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.

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:

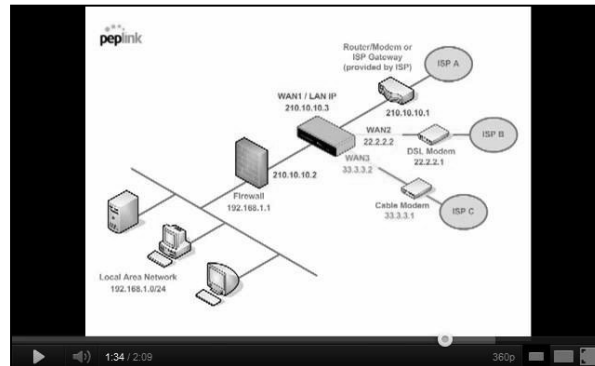


Important Note

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!




<http://youtu.be/lZG2-VPml5w>

14 Configuring the WAN Interface(s)

WAN interface settings are located at **Network>WAN**.

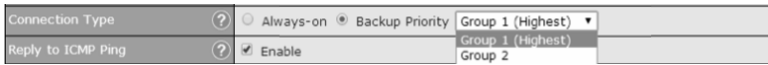
Connection Name	Method	Routing Mode	Type
1. WAN 1	Static IP	NAT	Always-on
2. WAN 2	Static IP	NAT	Always-on
3. WAN 3	Static IP	NAT	Always-on
4. WAN 4	Not Configured	NAT	Always-on
5. WAN 5	Not Configured	NAT	Always-on
6. WAN 6	Not Configured	NAT	Always-on
7. WAN 7	Not Configured	NAT	Always-on
8. WAN 8	Not Configured	NAT	Always-on
9. WAN 9	Not Configured	NAT	Always-on
10. WAN 10	Not Configured	NAT	Always-on
11. WAN 11	Not Configured	NAT	Always-on
12. WAN 12	Not Configured	NAT	Always-on
13. Mobile Internet	PPP	NAT	Backup Group 1

IPv6
Disabled 

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	<input type="text" value="WAN 1"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Connection Method	<input type="text" value="DHCP"/> ▾ Click here to edit Connection settings
Routing Mode	<input checked="" type="radio"/> NAT
Connection Type	<input checked="" type="radio"/> Always-on <input type="radio"/> Backup Priority
Reply to ICMP Ping	<input type="checkbox"/> Enable
Upload Bandwidth	<input type="text" value="1"/> Gbps ▾
Download Bandwidth	<input type="text" value="1"/> Gbps ▾

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: <ol style="list-style-type: none"> DHCP Static IP PPPoE L2TP

	<p>5. GRE</p> <p>See Sections 14.2.1, 14.2.2, 14.2.3, 14.2.4 and 14.2.5 for configuration details pertaining to each connection method.</p>
Routing Mode	<p>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.</p>
Connection Type	<p>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).</p>  <p>The default and recommended connection type is Always-on.</p>
Reply to ICMP Ping	<p>If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.</p>
Upload Bandwidth	<p>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.</p>
Download Bandwidth	<p>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.</p>

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.



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.

14.1 Physical Interface Settings

Physical Interface Settings	
Speed	<input type="text" value="Auto"/>
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="1440"/> <input type="button" value="Default"/>
MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>
MAC Address Clone	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="10 :56 :CA :06 :08 :09"/>
VLAN	<input type="checkbox"/> Enable

Physical Interface Settings	
Speed	This setting specifies port speed and duplex configurations of the WAN port. By default, Auto 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 Advertise Speed .
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to Custom 1440 . You may adjust the MTU value by editing the text field. Click Default to restore the default MTU value. Select Auto , and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes.
MSS	This setting should be configured based on the maximum payload size that the local system can handle. The MSS (maximum segment size) is computed by taking the MTU and subtracting 40 bytes for TCP over IPv4. If MTU is set to Auto , MSS will also be set automatically. By default, MSS is set to Auto .
MAC Address Clone	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 Default button restores the MAC address to the default value.
VLAN	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 VLAN ID that the provider requires. Note: leave this field disabled if you are not sure.

14.2 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)

14.2.1 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	
Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

DHCP Settings	
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with a hostname, you can safely bypass this option.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>

Please refer to **Sections 14.3, 14.4, 14.5, and 14.6** for details about **WAN Health Check, Bandwidth Allowance Monitor, Additional Public IP Settings, and Dynamic DNS Settings**.

14.2.2 Static IP Connection

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

Static IP Settings	
IP Address	<input type="text"/>
Subnet Mask	255.255.255.0 (/24) ▾
Default Gateway	<input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

Static IP Settings	
IP Address / Subnet Mask / Default Gateway	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.
DNS Servers	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.

14.2.3 PPPoE Connection

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

PPPoE Settings	
PPPoE User Name	<input type="text"/>
PPPoE Password	<input type="password"/>
Confirm PPPoE Password	<input type="password"/>
Service Name (Optional)	<input type="text"/> <small>Leave it blank unless it is provided by ISP</small>
IP Address (Optional)	<input type="text"/> <small>Leave it blank unless it is provided by ISP</small>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

PPPoE Settings	
PPPoE User Name / Password	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.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Server Name (Optional)	Server name is a PPPoE parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
IP Address	PPPoE server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)</p> <p>When Use the following DNS server address(es) is selected, you can enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>

Please refer to **Sections 14.3, 14.4, 14.5, and 14.6** for details about **WAN Health Check, Bandwidth Allowance Monitor, Additional Public IP Settings, and Dynamic DNS Settings**.

Note
A PPPoE connection made from a firewall does not work with drop-in mode.

14.2.4 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 Settings	
L2TP User Name	<input type="text"/>
L2TP Password	<input type="password"/>
Confirm L2TP Password	<input type="password"/>
Server IP Address / Host	<input type="text"/>
Address Type	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically
	<input checked="" type="checkbox"/> Use the following DNS server address(es)
	DNS Server 1: <input type="text"/>
	DNS Server 2: <input type="text"/>

L2TP Settings	
L2TP User Name / Password	Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.
Confirm L2TP Password	Verify your password by entering it again in this field.
Server IP Address / Host	L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
Address Type	Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)</p> <p>When Use the following DNS server address(es) is selected, you can enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>

14.2.5 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>.

Connection Settings	
WAN Connection Name	Mobile Internet
Enable	<input checked="" type="checkbox"/>
Connection Type	<input type="radio"/> Always-on <input checked="" type="radio"/> Backup Priority Group 1 (Highest) ▾
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Idle Disconnect	<input checked="" type="checkbox"/> 3 minutes <small>Time value is global. A change will affect all WAN profiles.</small>
Reply to ICMP Ping	<input checked="" type="checkbox"/> Enable
Operator Settings (for HSPA/EDGE/GPRS only)	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Mobile Operator Settings APN: <input type="text"/> Login ID: <input type="text"/> Password: <input type="text"/> Dial Number: <input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>

Mobile Internet Connection Settings	
WAN Connection Name	Enter a name for this WAN connection.
Enable	Click the box to enable the connection.
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 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 Always-on .
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 and this WAN connection is made active, the WAN connection will be immediately available for use.
Idle Disconnect	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.
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.

Operator Settings	<p>This setting applies to 3G/LTE/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems.</p> <p>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.</p>
SIM PIN (Optional)	<p>This is an optional field which is only needed when there is SIM lock for your SIM card service.</p>
DNS Servers	<p>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.</p>

Please refer to **Sections 14.3, 14.4, 14.5, and 14.6** for details about **WAN Health Check, Bandwidth Allowance Monitor, Additional Public IP Settings, and Dynamic DNS Settings**.

14.2.5.1 Modem Specific Custom Settings

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

Modem Specific Custom Settings	
Modem Model	xxx Modem
IMSI	123400005678900
Network Type	? 3G preferred ▾
GSM Frequency Band	All Bands ▾

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	<p>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.</p> <p>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.</p> <p>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.</p> <p>The default network type is 3G preferred.</p>
GSM Frequency Band	<p>This setting allows you to specify which GSM frequency band will be used.</p> <p>GSM1900 is used in the United States, Canada, and many other countries in the Americas.</p> <p>GSM900 / GSM1800 / GSM2100 are used in Europe, the Middle East, Africa, Asia, Oceania, and Brazil.</p> <p>If All Bands is chosen, the appropriate frequency band will be used automatically.</p> <p>The default GSM frequency band is All Bands.</p>

14.2.5.2 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.

Modem Specific Custom Settings	
Modem Model	Sprint Modem
ESN	C7B1C7B1
Network Type	4G only <input type="button" value="v"/> 4G only 3G only

Modem Specific Custom Settings	
Modem Model	The brand of the modem is automatically detected and appears here.
ESN	The modem's electronic serial number (ESN) is also auto-detected and appears here.
Network Type	This is to specify the network type (e.g., 3G or 4G) to be used with the modem.

14.3 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**.

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

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

Health Check Settings

Method

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

Health Check Disabled

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

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

Health Check Method: PING

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

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

PING Hosts

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

Health Check Method: DNS Lookup

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

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

**Health Check
 DNS Servers**

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

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

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

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

Health Check Method: HTTP

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

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

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1





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

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

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

Other Health Check Settings

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

Timeout This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.

Health Check Interval This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.

Health Check Retries This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.

Recovery Retries This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink Balance treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.


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.**

14.4 Bandwidth Allowance Monitor

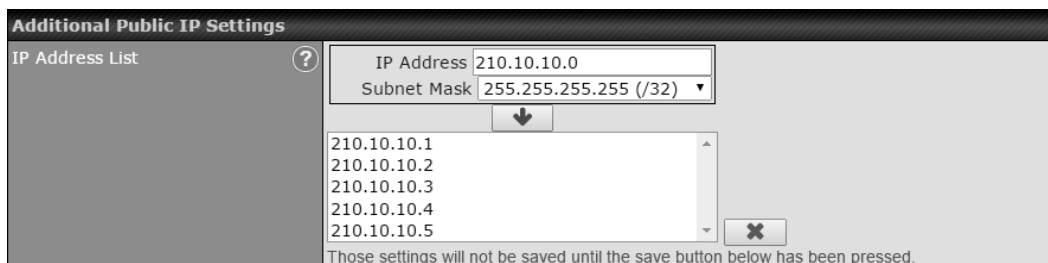
The Bandwidth Allowance Monitor helps track your network usage. Please refer to **Section 28.8** to view usage statistics.

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

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

Disclaimer	
<p>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.</p>	

14.5 Additional Public IP Settings



Additional Public IP Settings

IP Address List

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**.

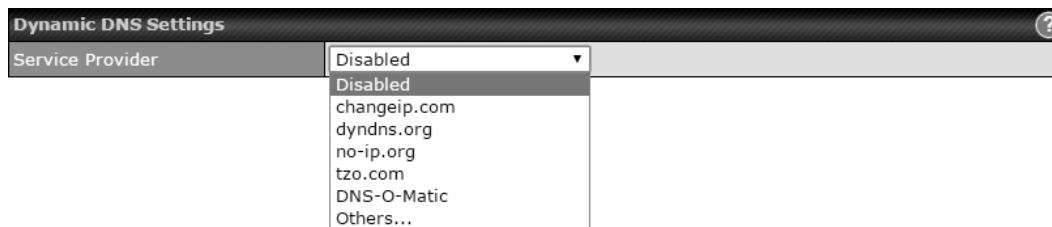
14.6 Dynamic DNS Settings

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

Dynamic DNS Settings	
Service Provider	<p>This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:</p> <ul style="list-style-type: none"> • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic • Others... <p style="margin-left: 20px;">support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.</p> <p>Select Disabled to disable this feature.</p>
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.
Password / Pass / TZO Key	This setting specifies the password for the dynamic DNS service.
Update All Hosts	Check this box to automatically update all hosts.
Hosts / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

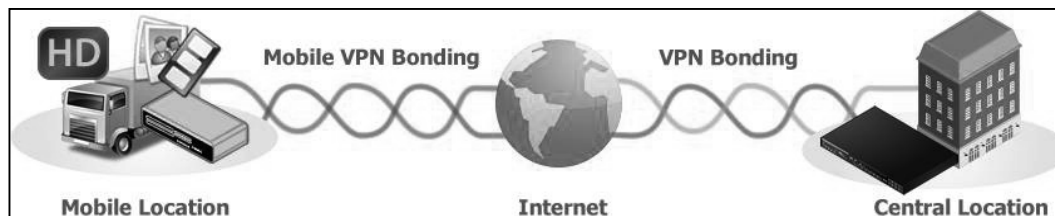
Important Note

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

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

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

15 PepVPN with SpeedFusion™ Bandwidth Bonding



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.

15.1 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](#).

Profile	Remote ID	Remote Address(es)	
FL_Office	Balance_20D3		
NY_Office	Balance_FBDB		
<input type="button" value="New Profile"/>			

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

To configure a new SpeedFusion profile, navigate to **Network>Interfaces>SpeedFusion>New Profile**.

PepVPN Profile					
Name	<input type="text" value="Balance 2942-1257-1241"/>				
Active	<input checked="" type="checkbox"/>				
SpeedFusion	Supported				
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF				
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key <input type="radio"/> X.509				
Remote ID / Pre-shared Key	<table border="1"> <tr> <th>Remote ID</th> <th>Pre-shared Key</th> </tr> <tr> <td>Balance 9875-A63D-92AS</td> <td>.....</td> </tr> </table>	Remote ID	Pre-shared Key	Balance 9875-A63D-92AS
Remote ID	Pre-shared Key				
Balance 9875-A63D-92AS				
NAT Mode	<input type="checkbox"/>				
Remote IP Address / Host Names (Optional)	<input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small>				
Data Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>				
Bandwidth Limit	<input type="checkbox"/>				
Cost	<input type="text" value="10"/>				
WAN Smoothing	<input type="text" value="Off"/>				
Use IP ToS	<input type="checkbox"/>				

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

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

	<p>This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.</p> <p>Click the  icon to customize the handshake port (TCP)</p>
Data Port	<p>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.</p>
Bandwidth Limit	<p>Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.</p>
Cost	<p>Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10</p>
WAN Smoothing^A	<p>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.</p> <p>Off - Disable WAN Smoothing.</p> <p>Normal - The total bandwidth consumption will be at most 2x of the original data traffic.</p> <p>Medium - The total bandwidth consumption will be at most 3x of the original data traffic.</p> <p>High - The total bandwidth consumption depends on the number of connected active tunnels.</p>

^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.

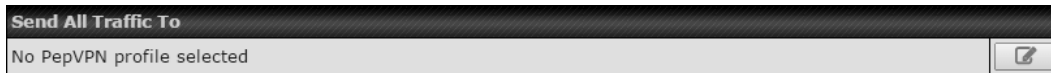
WAN Connection Priority		
1. WAN1	Priority: 1 (Highest)	Connect to Remote: All
2. WAN2	Priority: 1 (Highest)	Connect to Remote: All
3. WAN3	Priority: 1 (Highest)	Connect to Remote: All
4. WAN4	Priority: 1 (Highest)	Connect to Remote: All
5. WAN5	Priority: 1 (Highest)	Connect to Remote: All
6. WAN6	Priority: 1 (Highest)	Connect to Remote: All
7. WAN7	Priority: 1 (Highest)	Connect to Remote: All
8. Mobile Internet	Priority: 1 (Highest)	Connect to Remote: All

WAN Connection Priority

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.

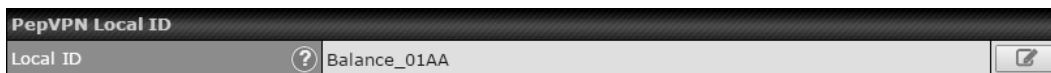
To allow connection mapping to remote WANs, click the question mark icon found at the top right of this section, and then click the displayed link to reveal the **Connect to Remote** drop-down menu.



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:

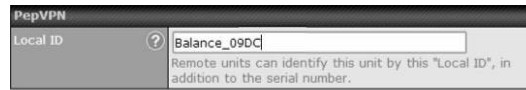
You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main PepVPN connection fail.



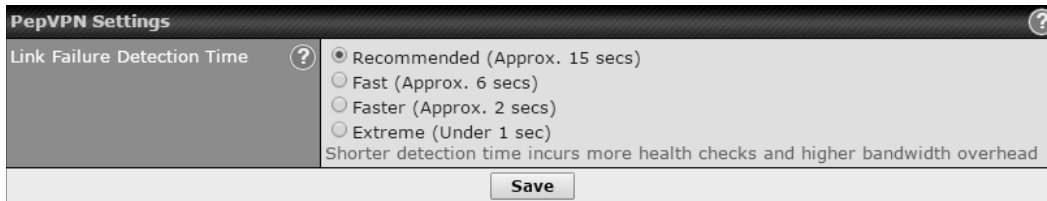
PepVPN Local ID

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:



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.

When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds.

Link Failure Detection Time

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.

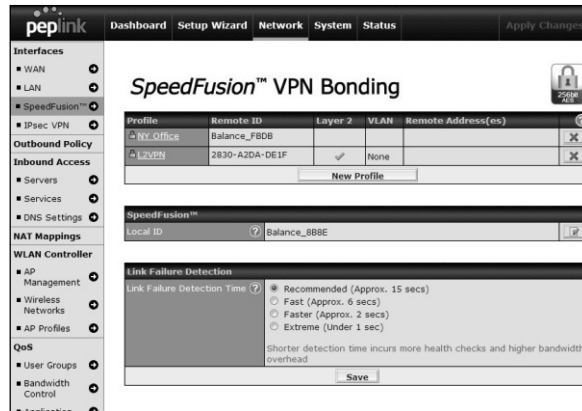
When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

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

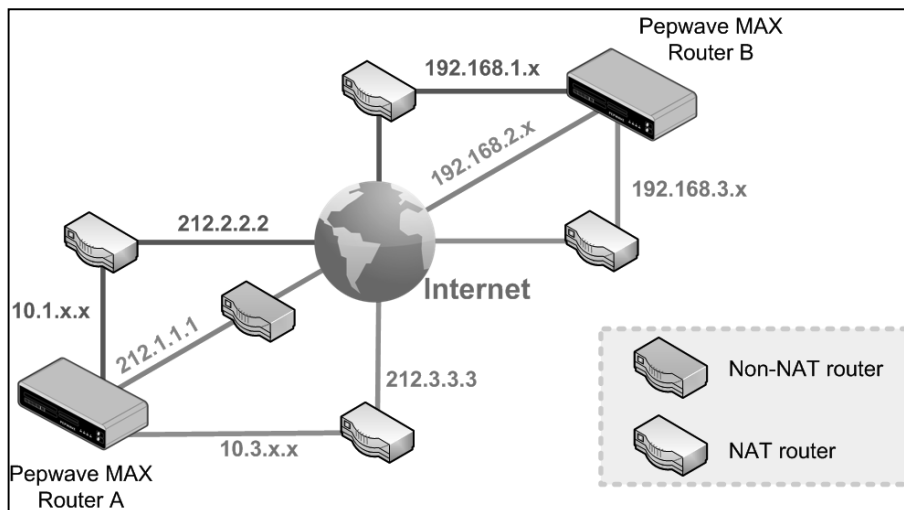
15.2 The Peplink Balance Behind a NAT Router

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:





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.

15.3 SpeedFusion™ Status

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

PepVPN with SpeedFusion		Status
FL Office	<input type="checkbox"/>	Established
NY Office	<input checked="" type="checkbox"/>	Starting...

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 28.6** for details.

PepVPN with SpeedFusion - Remote Peer Details		Show disconnected profiles
Search <input type="text"/>		
Remote Peer	Profile	Information
<input checked="" type="checkbox"/> FL Office B380	FL Office	Bridged to Untagged LAN with IP address 10.7.2.4  
<input type="checkbox"/> via Provider	Rx: < 1 kbps Tx: 1.8 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms

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.

16 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.



16.1 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**.

NAT-Traversal		Enabled (required by L2TP with IPsec)	
IPsec VPN Profiles	Remote Networks		
Profile 1	192.168.11.193/24		
New Profile			


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 ✕

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

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

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	
Priority	WAN Selection
1	WAN 1 ▼
2	----- ▼

WAN Connection Priority

This feature enables you to prioritize the WAN connections used by this VPN profile.

16.2 IPsec Status

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

17 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 Policy [?]

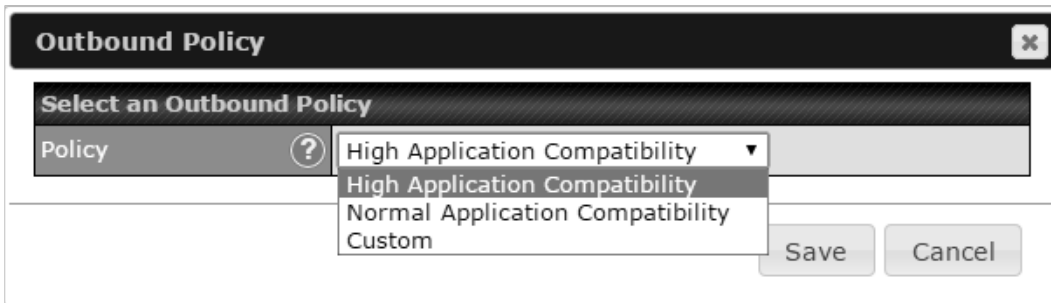
Custom [edit icon]

Rules (Drag and drop rows to change rule order) [?]

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

[Add Rule]

Outbound policies for managing and load balancing outbound traffic are located at **Network>Outbound Policy>** [edit icon].



Outbound Policy [X]

Select an Outbound Policy

Policy [?] High Application Compatibility [v]
High Application Compatibility
Normal Application Compatibility
Custom

[Save] [Cancel]

17.1 Outbound Policy

There are three main selections for the outbound traffic policy:

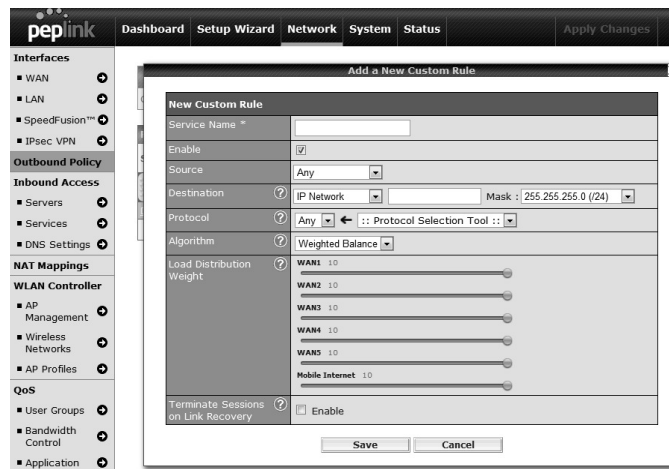
- High Application Compatibility
- Normal Application Compatibility
- Custom

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

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


Tip

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



http://youtu.be/rKH4AS_bQnE

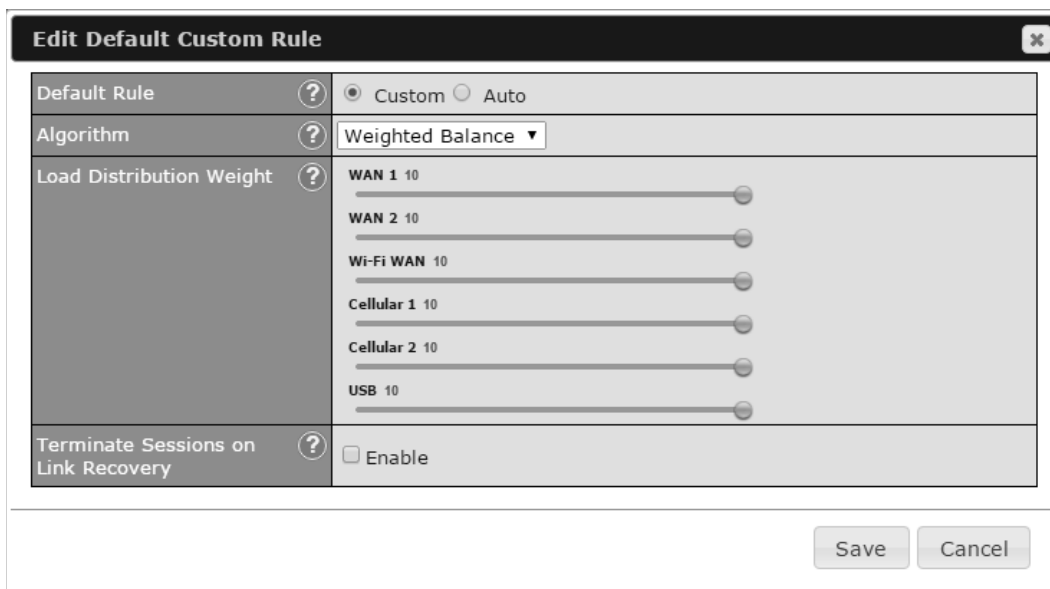
17.2 Custom Rules for Outbound Policy

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



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

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.



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

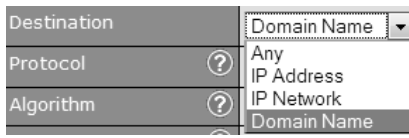
By default, **Auto** is selected for as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

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

Add a New Custom Rule ✕

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

New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	<p>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.</p> <p>Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.</p>
Source	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.

Destination	<p>This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.</p>  <p>If Domain Name is chosen and a domain name, such as <i>foobar.com</i>, is entered, any outgoing accesses to <i>foobar.com</i> and <i>*.foobar.com</i> will match this criterion. You may enter a wildcard (.) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter <i>foobar.*</i>, for example, <i>www.foobar.com</i>, <i>www.foobar.co.jp</i>, or <i>foobar.co.uk</i> will also match. Placing wildcards in any other position is not supported.</p> <p>NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.</p>
Protocol and Port	<p>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.</p>
Algorithm	<p>This setting specifies the behavior of the Peplink Balance for the custom rule. One of the following values can be selected:</p> <ul style="list-style-type: none">• Weighted Balance• Persistence• Enforced• Priority• Overflow• Least Used• Lowest Latency <p>The upcoming sections detail the listed algorithms.</p>
Terminate Sessions on Link Recovery	<p>This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the Weighted, Persistence, and Priority algorithms.</p> <p>By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.</p>

17.2.1 Algorithm: Weighted Balance

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

Algorithm ?	Weighted Balance ▾
Load Distribution Weight ?	WAN 1 10 WAN 2 10 WAN 3 10 Mobile Internet 10

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 $40\% = (10 / 25) \times 100\%$.

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

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

17.2.2 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.

Algorithm	<input type="text" value="Persistence"/>
Persistence Mode	<input type="radio"/> By Source <input checked="" type="radio"/> By Destination
Load Distribution	<input type="radio"/> Auto <input checked="" type="radio"/> Custom
Load Distribution Weight	<p>WAN 1 10 <input type="range"/></p> <p>WAN 2 10 <input type="range"/></p> <p>WAN 3 10 <input type="range"/></p> <p>Mobile Internet 10 <input type="range"/></p>

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

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

The default mode is **By Source**.

When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. If you choose **Auto** in **Load Distribution**, the weights will be automatically adjusted according to each WAN's **Download Bandwidth**, which is specified in the WAN settings page (see **Section 14, Configuring the WAN Interface(s)**). If you choose **Custom**, you can customize the weight of each WAN manually using the provided sliders.

17.2.3 Algorithm: Enforced

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

Algorithm	<input type="text" value="Enforced"/>
Enforced Connection	<input type="text" value="WAN: WAN 1"/> <ul style="list-style-type: none"> WAN: WAN 1 WAN: WAN 2 WAN: WAN 3 WAN: Mobile Internet VPN: FL_Office VPN: NY_Office

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.

17.2.4 Algorithm: Priority

This setting specifies the priority of the WAN connections used to route the specified