

Peplink Balance Multi-WAN Bonding Routers

User Manual

For Models:

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

MediaFast 200/500/750

Peplink Balance Firmware 6.3

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	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	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 268

1 Introduction and Scope

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

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

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

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

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

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

Important Note to Users Upgrading from Firmware 4.7 or below

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

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

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

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	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 802.11a/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
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



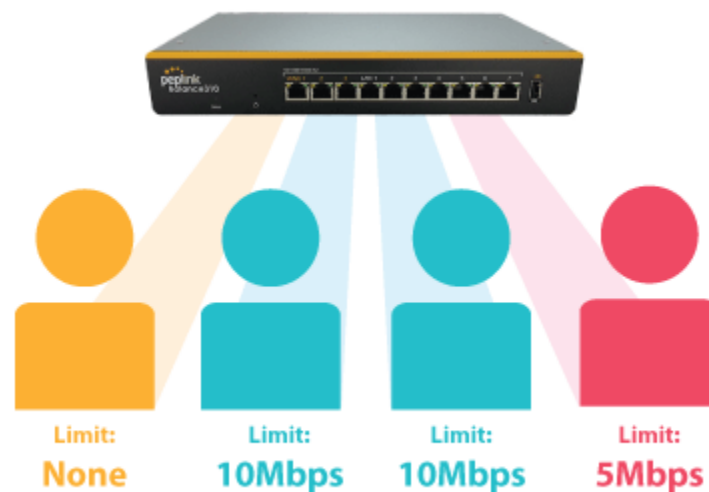
As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass**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

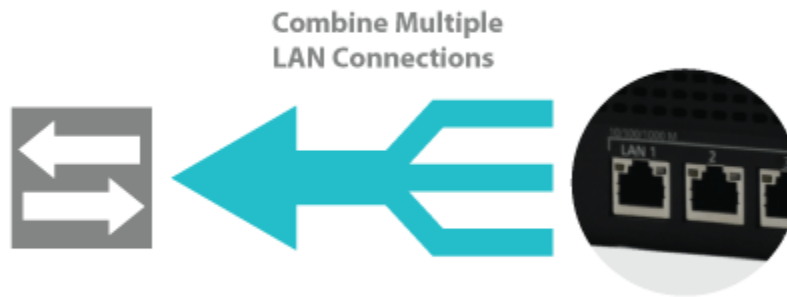
5.6 Built-In Remote User VPN Support



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

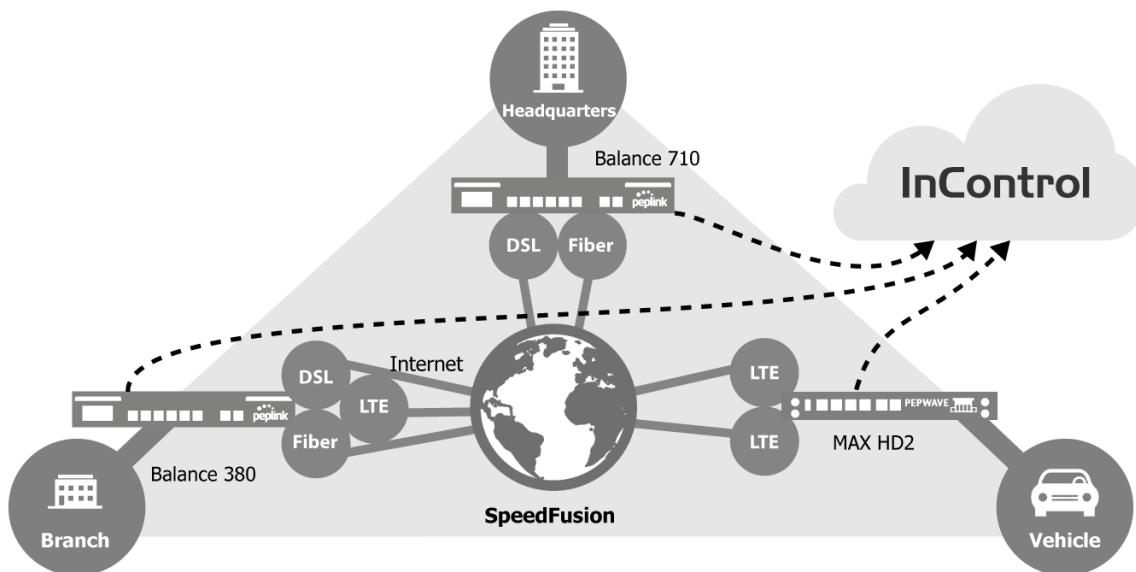
Our MAX HD series routers with its multiple embedded wireless modems can keep passengers connected to high speed Internet. Fleet management is also built-in and available to transportation operators via InControl.



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

- 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

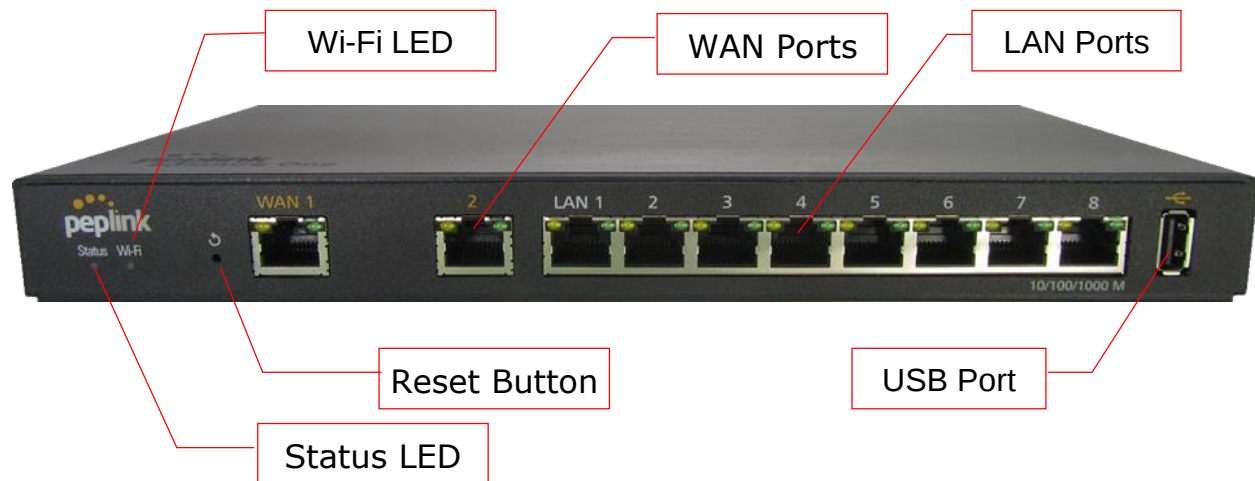
7.6 Peplink MediaFast 500

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

8 Peplink Balance Overview

8.1 Peplink Balance One

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

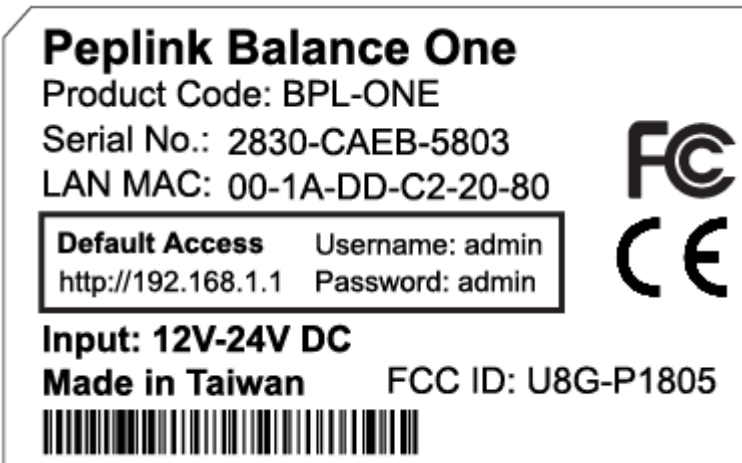
USB Ports

For future functionality

8.1.3 Rear Panel Appearance

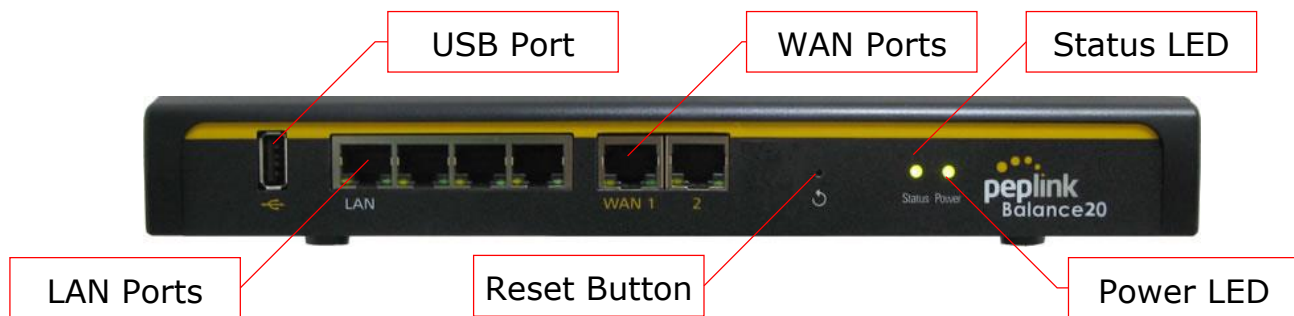


8.1.4 Product Label



8.2 Peplink Balance 20

8.2.1 Front Panel Appearance



8.2.2 LED Indicators

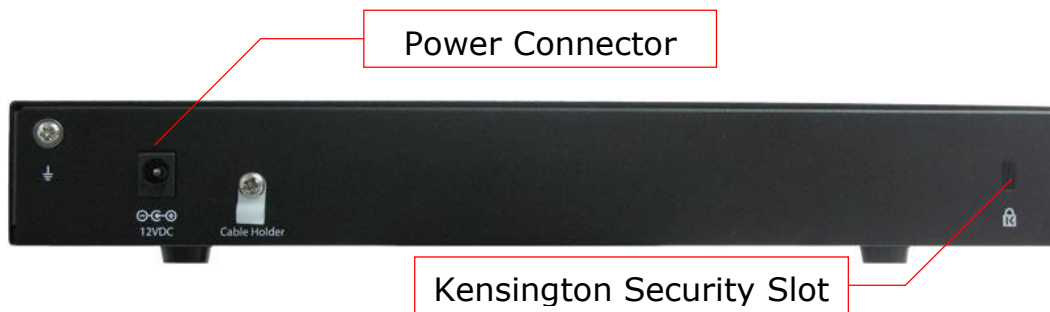
The statuses indicated by the front panel LEDs are as follows:

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

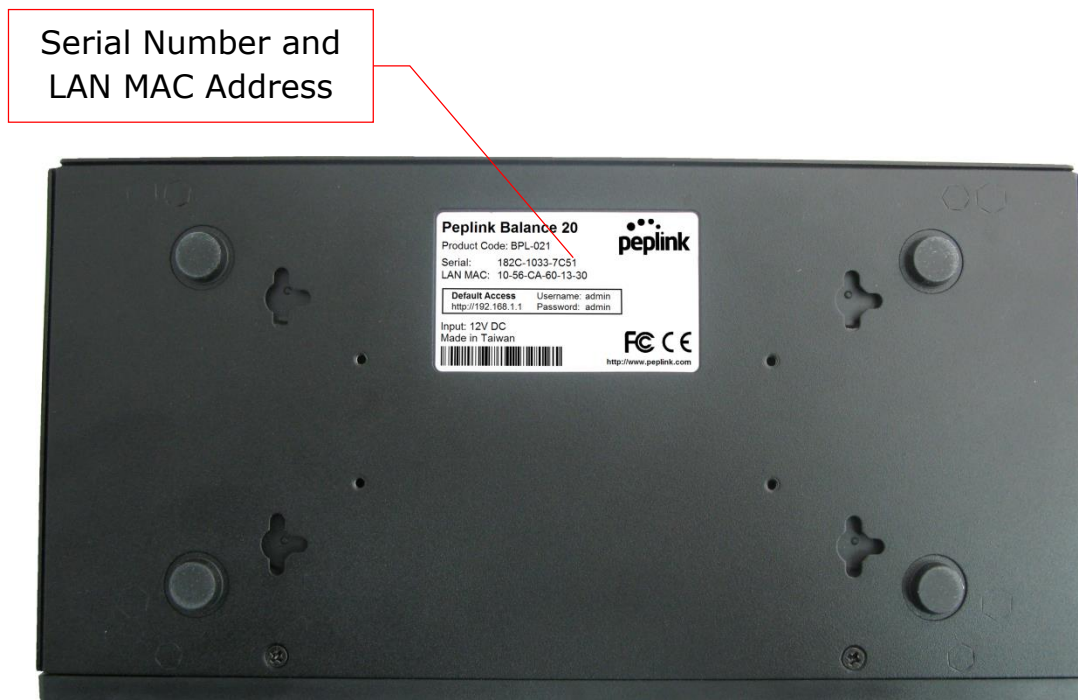
LAN and WAN Ports	
Green LED	ON – 10 / 100 / 1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

8.2.3 Rear Panel Appearance

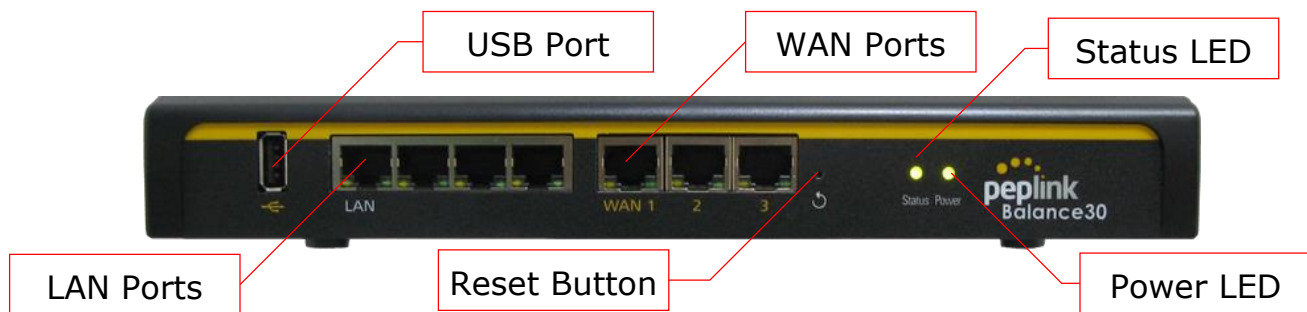


8.2.4 Unit Base Appearance



8.3 Peplink Balance 30

8.3.1 Front Panel Appearance



8.3.2 LED Indicators

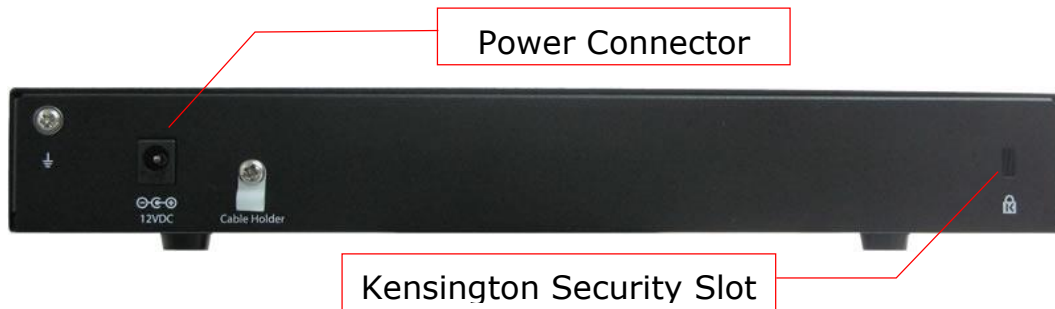
The statuses indicated by the front panel LEDs are as follows:

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

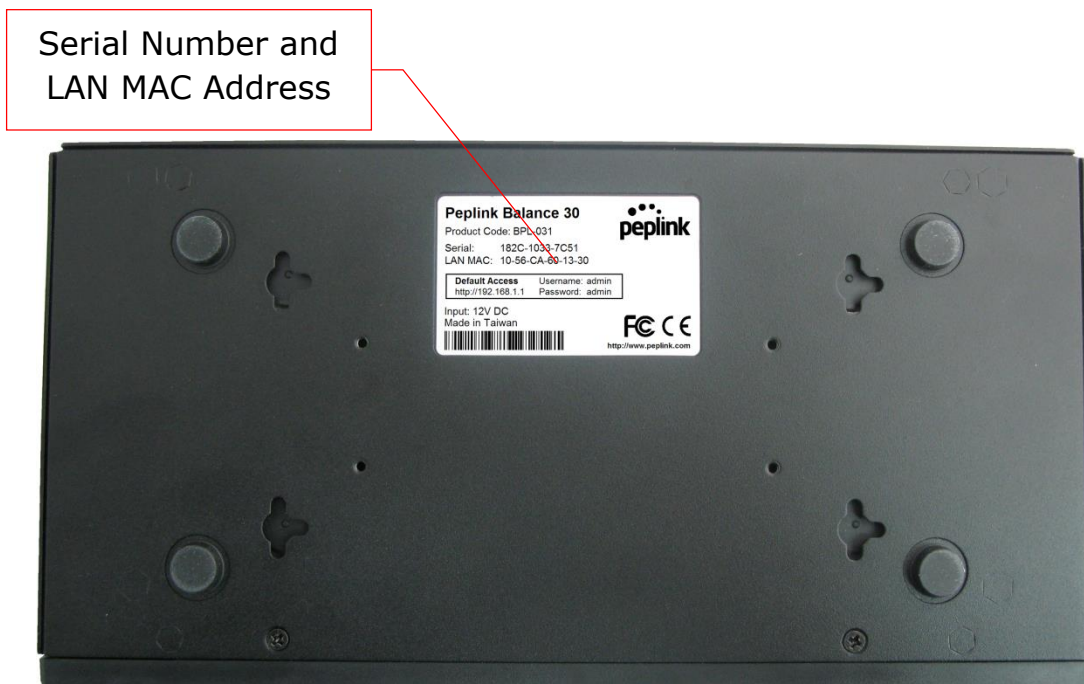
LAN and WAN Ports	
Green LED	ON – 10 / 100 /1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

8.3.3 Rear Panel Appearance

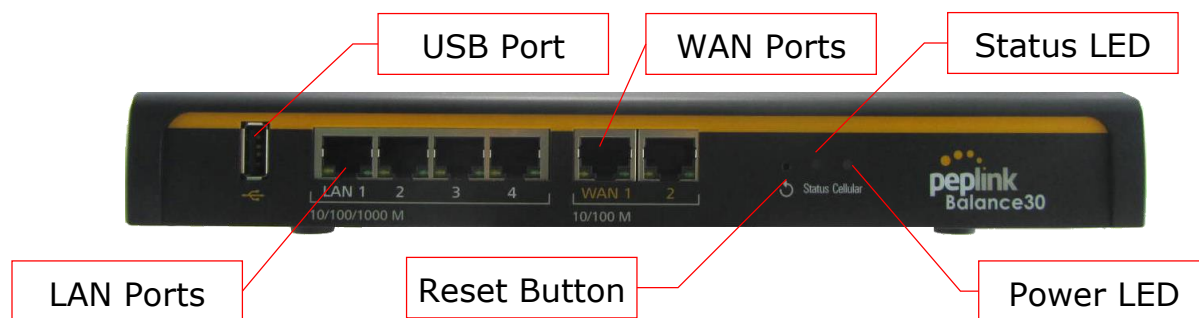


8.3.4 Unit Base Appearance



8.4 Peplink Balance 30 LTE

8.4.1 Front Panel Appearance



8.4.2 LED Indicators

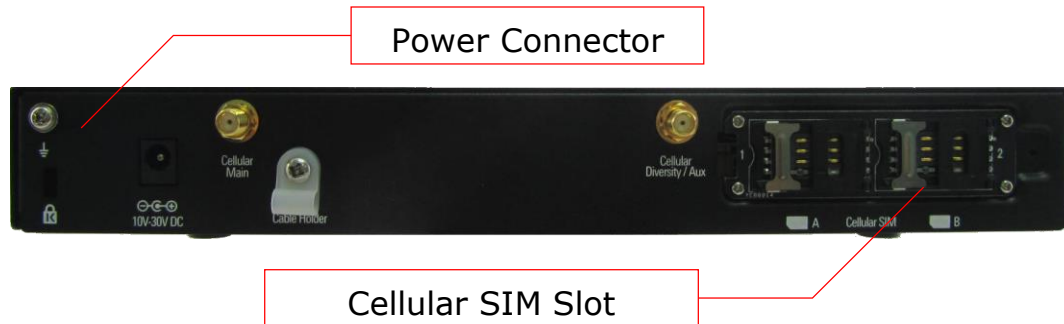
The statuses indicated by the front panel LEDs are as follows:

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

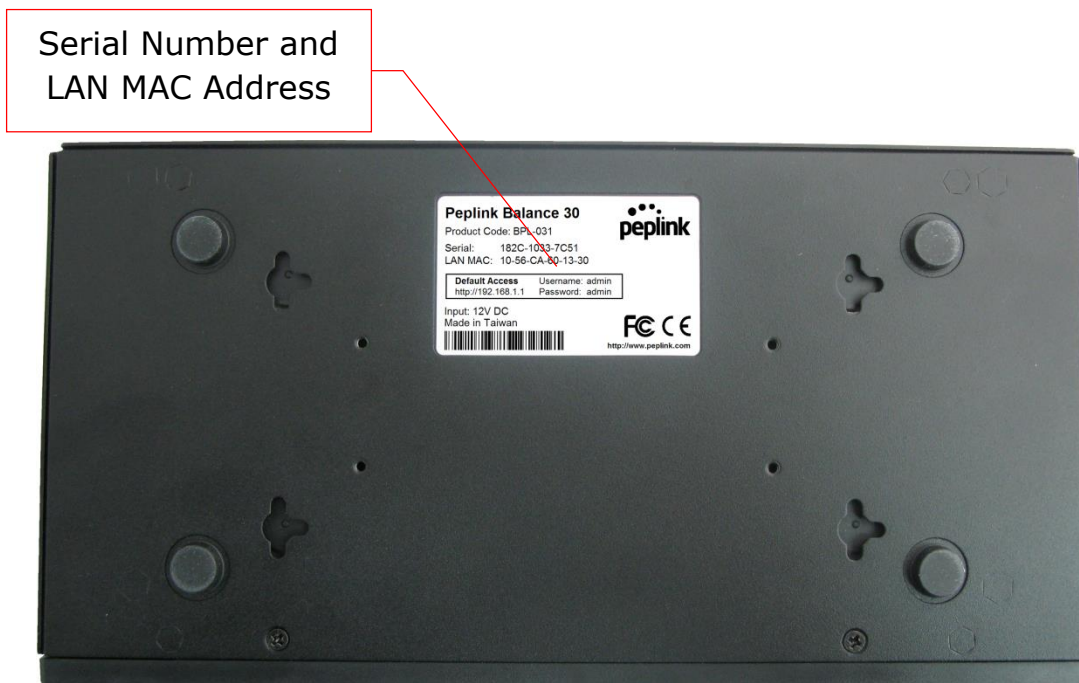
LAN and WAN Ports	
Green LED	ON – 10 / 100 /1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

8.4.3 Rear Panel Appearance

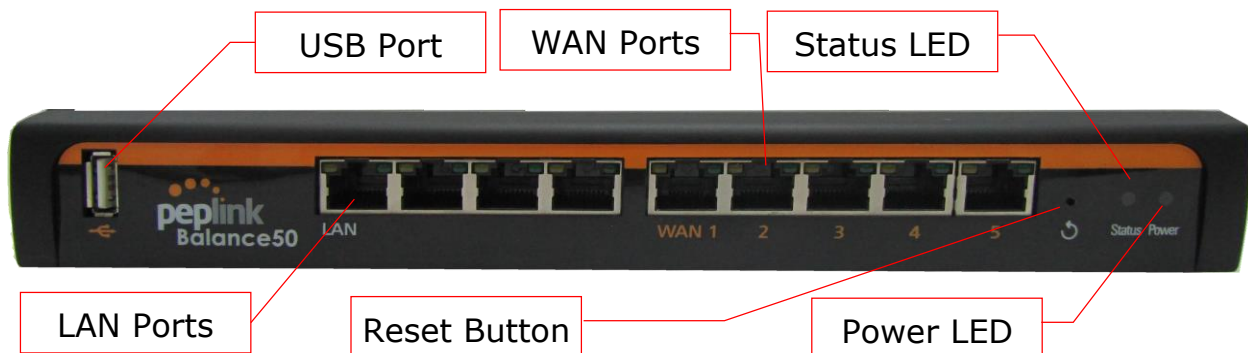


8.4.4 Unit Base Appearance



8.5 Peplink Balance 50

8.5.1 Front Panel Appearance



8.5.2 LED Indicators

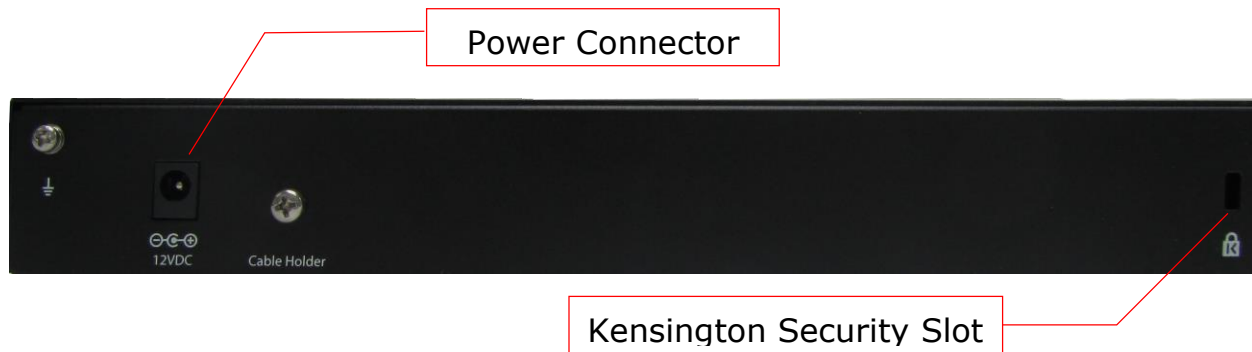
The statuses indicated by the front panel LEDs are as follows:

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

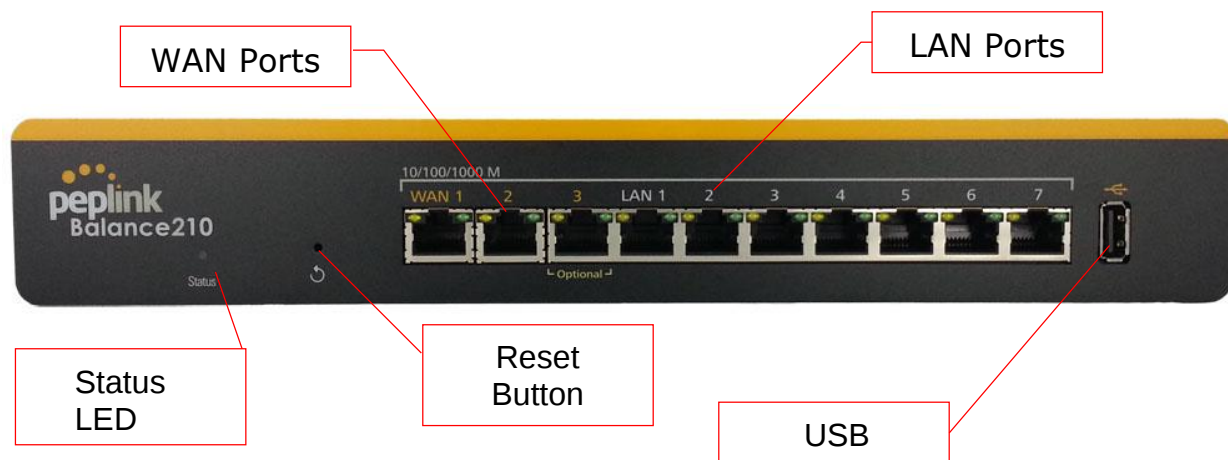
USB Port	
USB Ports	For connecting a 4G/3G USB modem

8.5.3 Rear Panel Appearance



8.6 Peplink Balance 210

8.6.1 Front Panel Appearance



8.6.2 LED Indicators

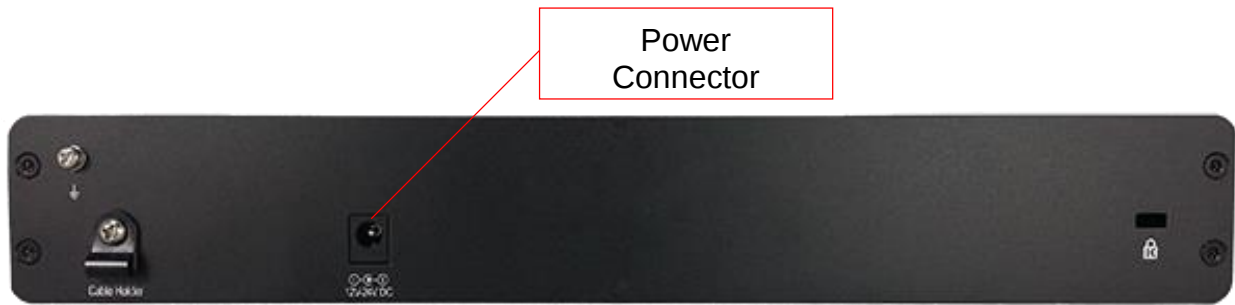
The statuses indicated by the front panel LEDs are as follows:

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

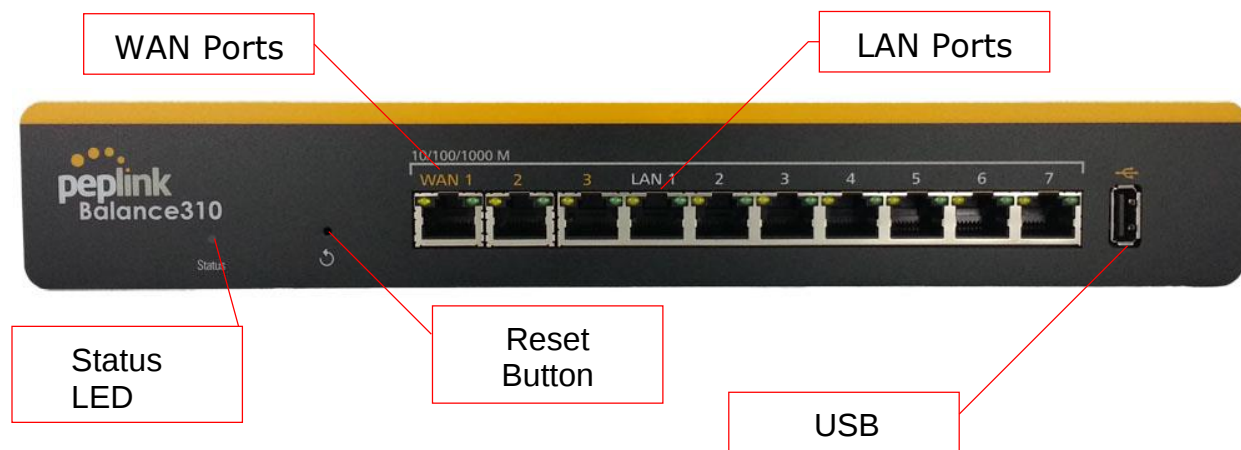


8.6.4 Unit Base Appearance



8.7 Peplink Balance 310

8.7.1 Front Panel Appearance



8.7.2 LED Indicators

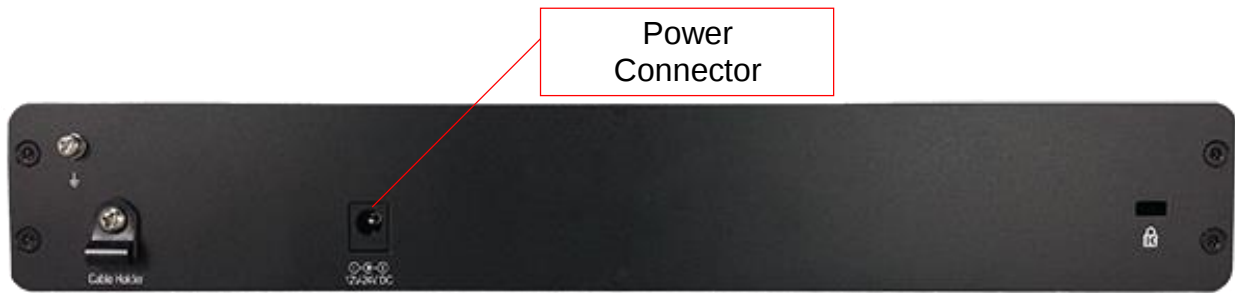
The statuses indicated by the front panel LEDs are as follows:

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

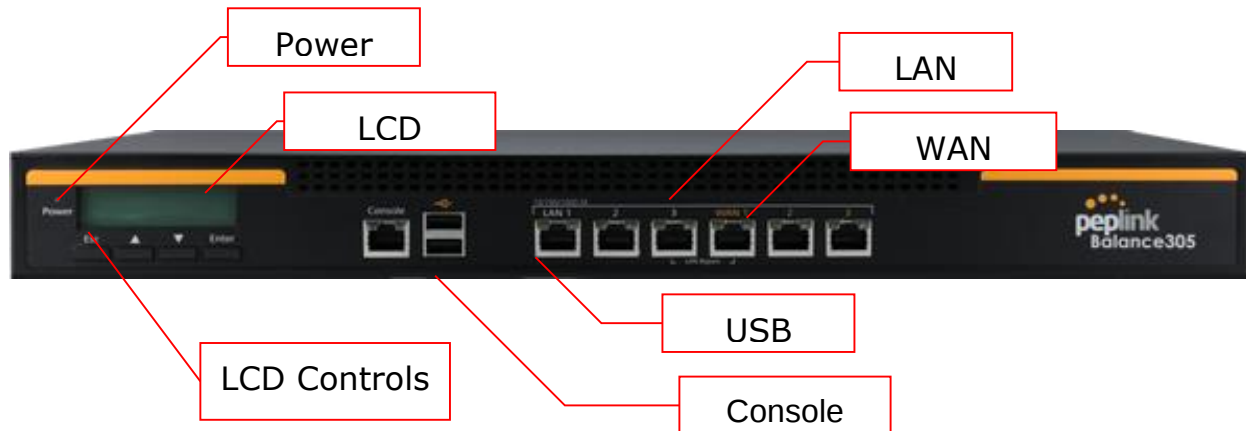


8.7.4 Unit Base Appearance



8.8 Peplink Balance 305

8.8.1 Front Panel Appearance



8.8.2 LED Indicators

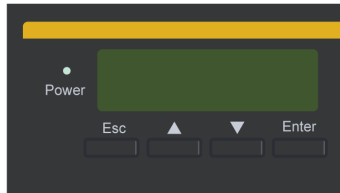
The statuses indicated by the front panel LEDs are as follows:

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

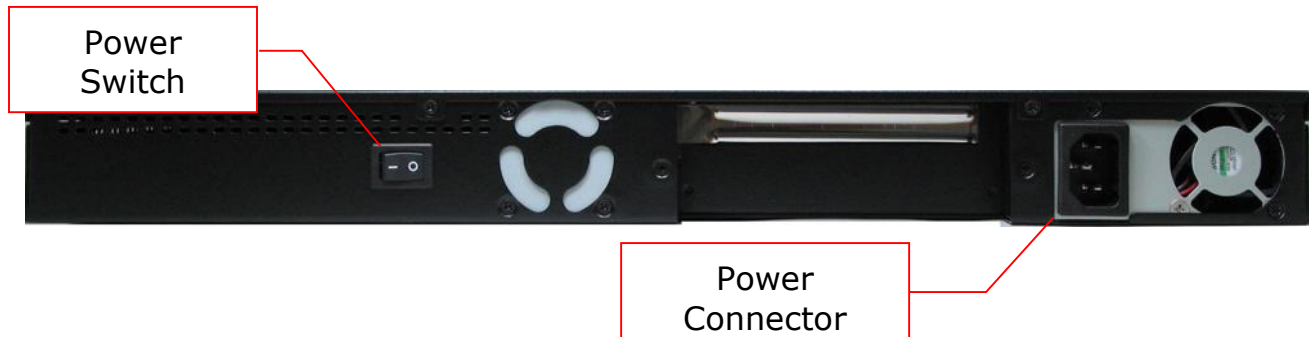
Console and USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

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



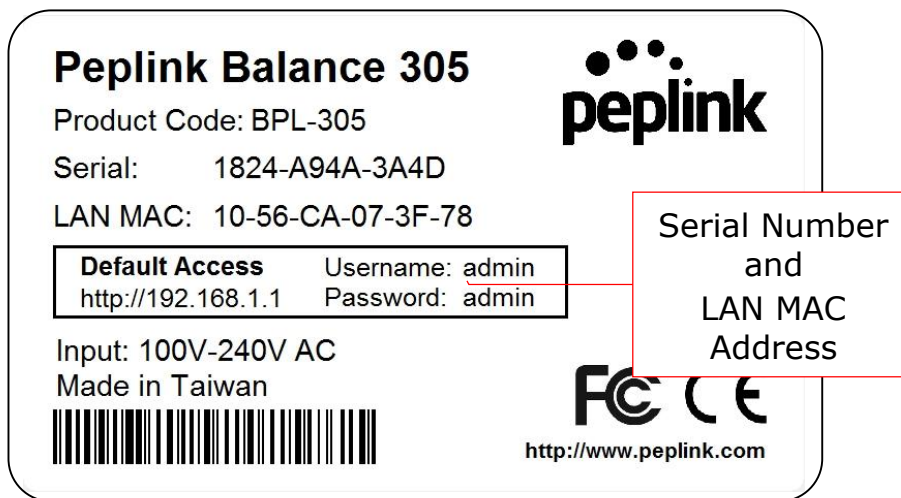
Connector Ports

Power Connector AC input 110/220V

Switch

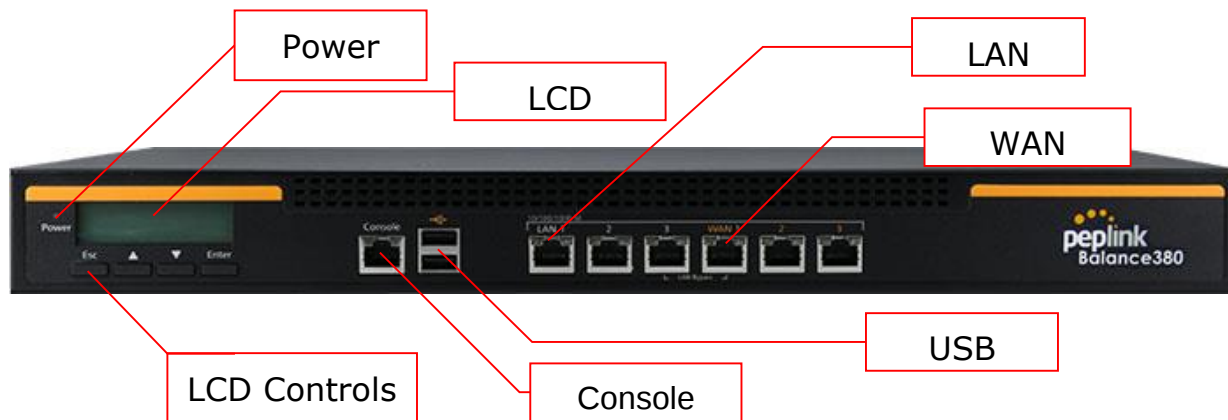
Power Switch Pressing and holding the key for four seconds will power down the unit.
When the unit is powered off, pressing this switch will power on the unit.

8.8.5 Unit Label Appearance



8.9 Peplink Balance 380

8.9.1 Front Panel Appearance



8.9.2 LED Indicators

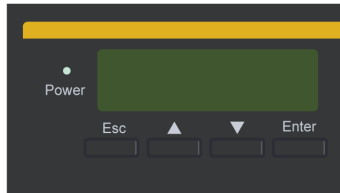
The statuses indicated by the front panel LEDs are as follows:

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

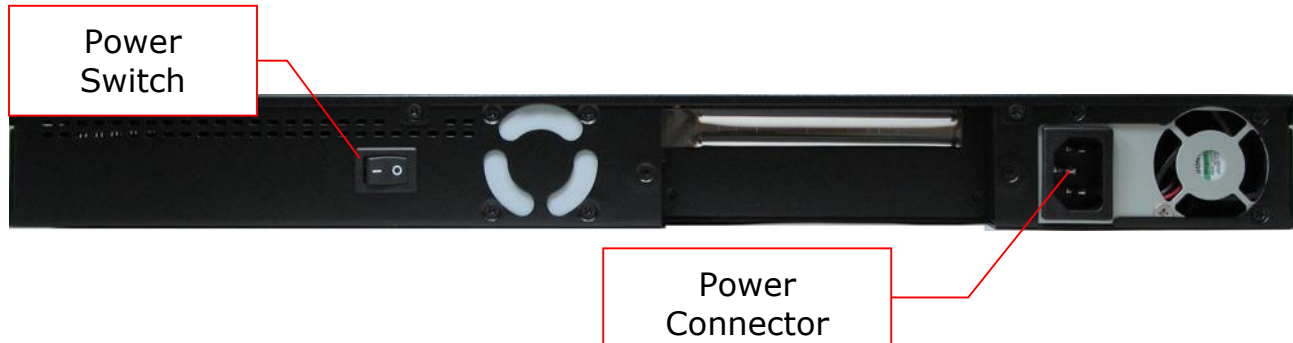
Console and USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

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



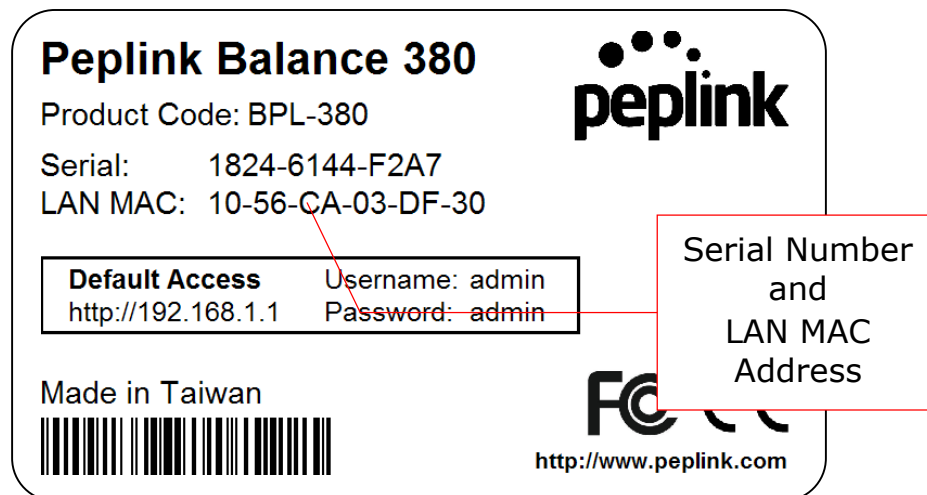
Connector Ports

Power Connector AC input 110/220V

Switch

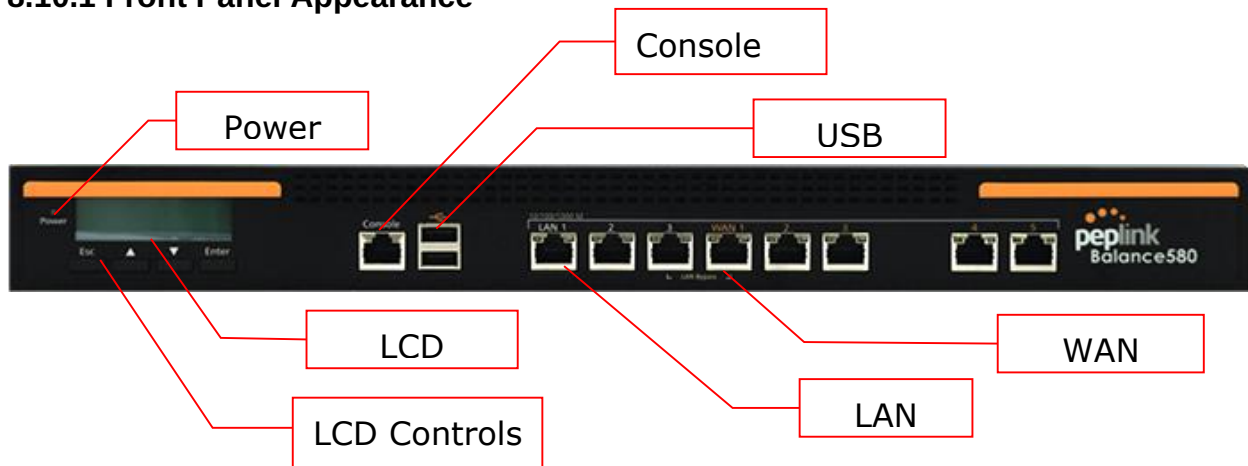
Power Switch Pressing and holding the key for four seconds will power down the unit.
When the unit is powered off, pressing this switch will power on the unit.

8.9.5 Unit Label Appearance



8.10 Peplink Balance 580

8.10.1 Front Panel Appearance



8.10.2 LED Indicators

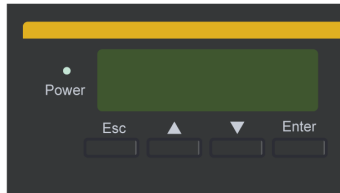
The statuses indicated by the front panel LEDs are as follows:

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

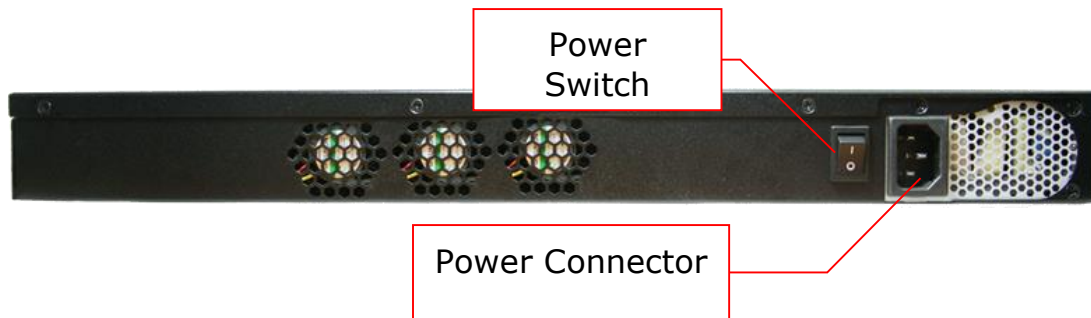
Console and USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

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



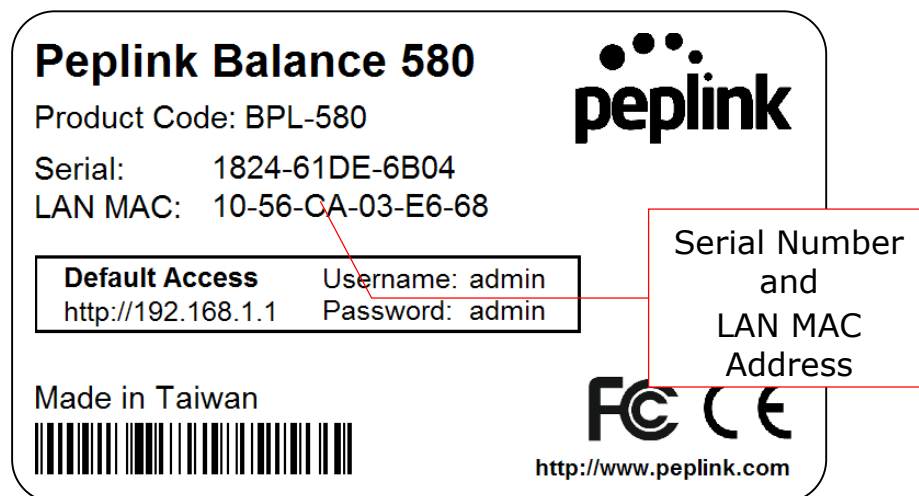
Connector Ports

Power Connector AC input 110/220V

Switch

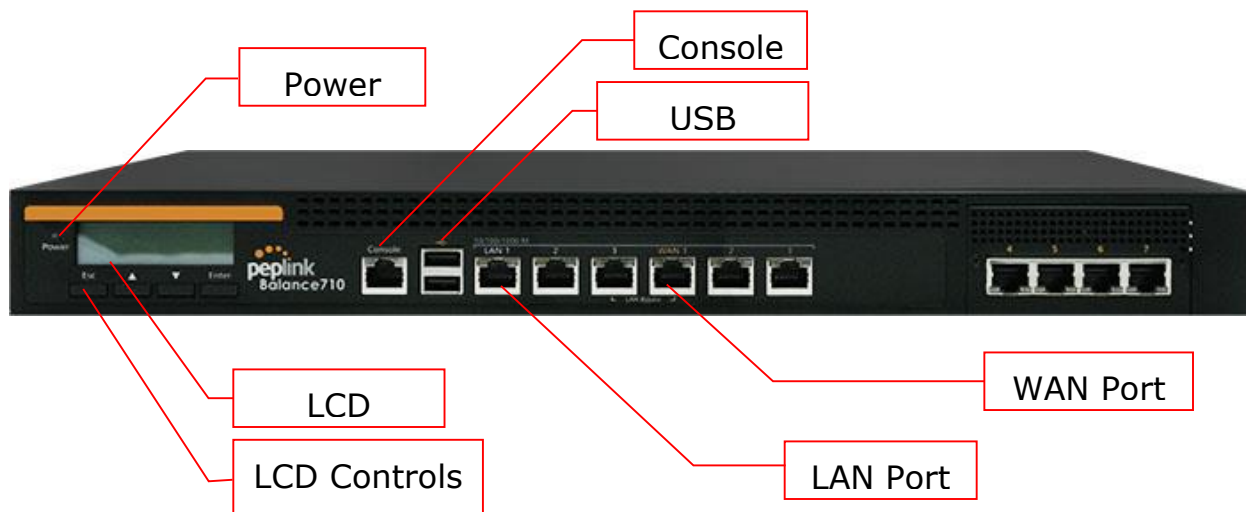
Power Switch Pressing and holding the key for four seconds will power down the unit.
When the unit is powered off, pressing this switch will power on the unit.

8.10.4 Unit Label Appearance



8.11 Peplink Balance 710

8.11.1 Front Panel Appearance



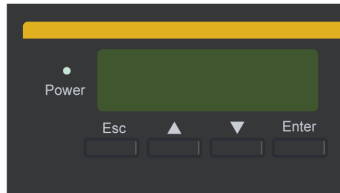
Status indicated in the front panel is as follows:

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 (shows Connected/Disconnected, IP address list)
 - > 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

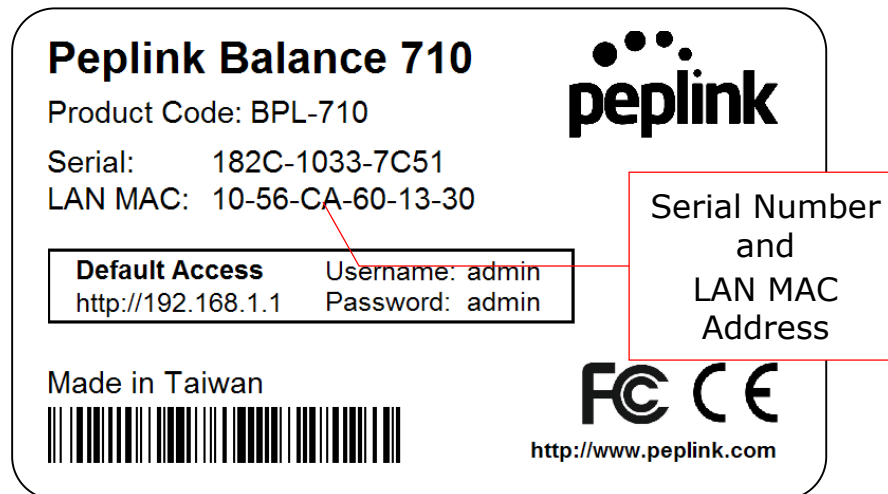
8.11.3 Rear Panel Appearance



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

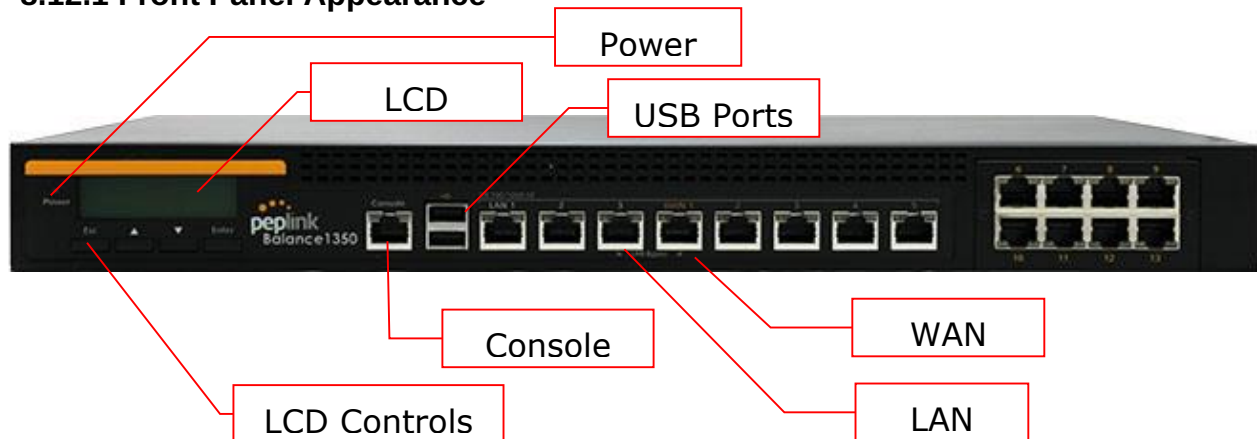
Switches	
Power Switch	Pressing and holding the key for four seconds will power down the unit. When the unit is powered off, pressing this switch will power on the unit.
Reset Switch	Press and release once to reset the system.

8.11.4 Unit Label Appearance



8.12 Peplink Balance 1350

8.12.1 Front Panel Appearance



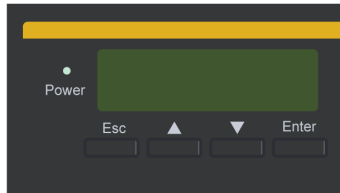
Status indicated in the front panel is as follows:

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

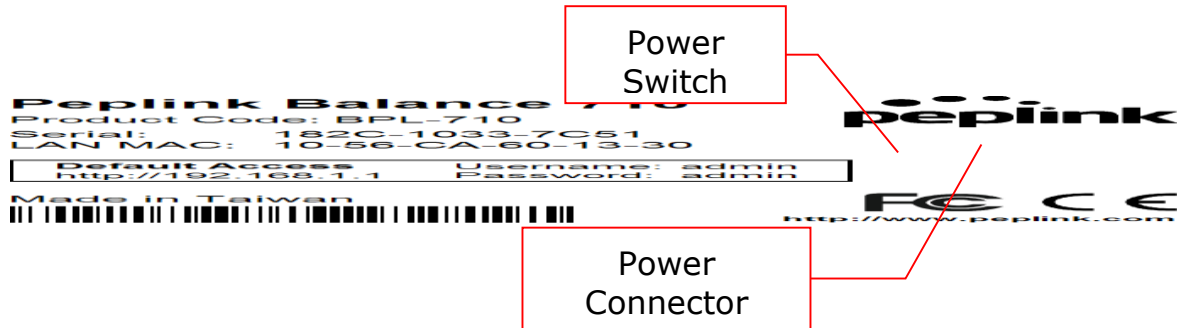
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

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 (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

8.12.3 Rear Panel Appearance



Connector Ports

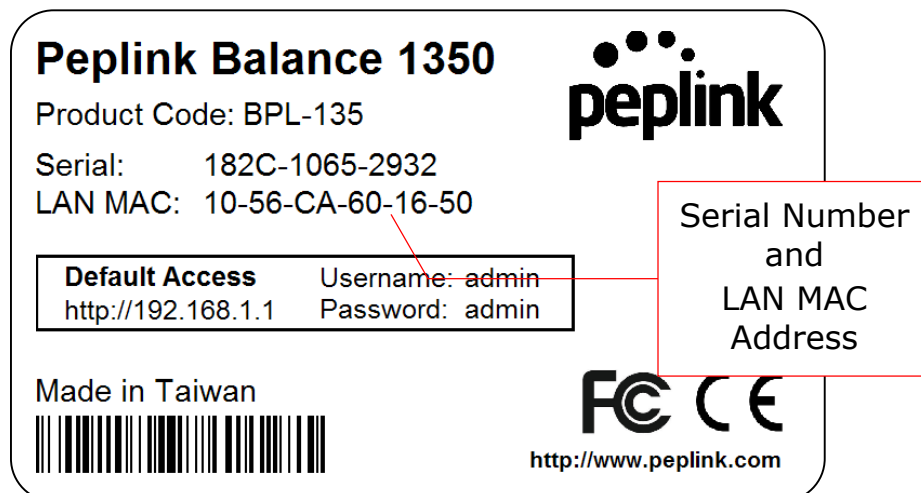
Power Connector AC input 110/220V

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.

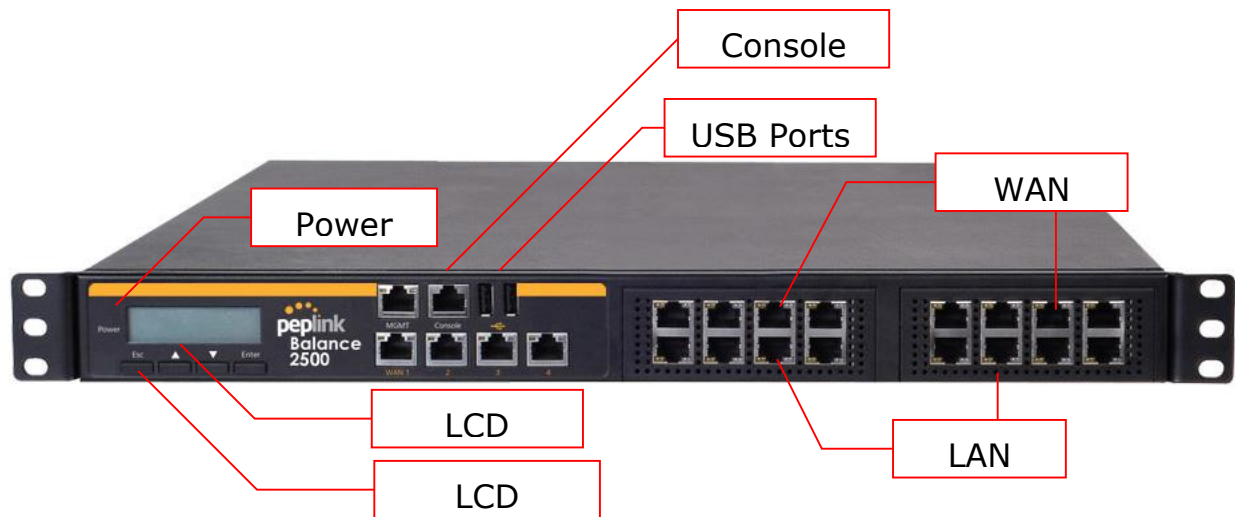
8.12.4 Unit Label Appearance



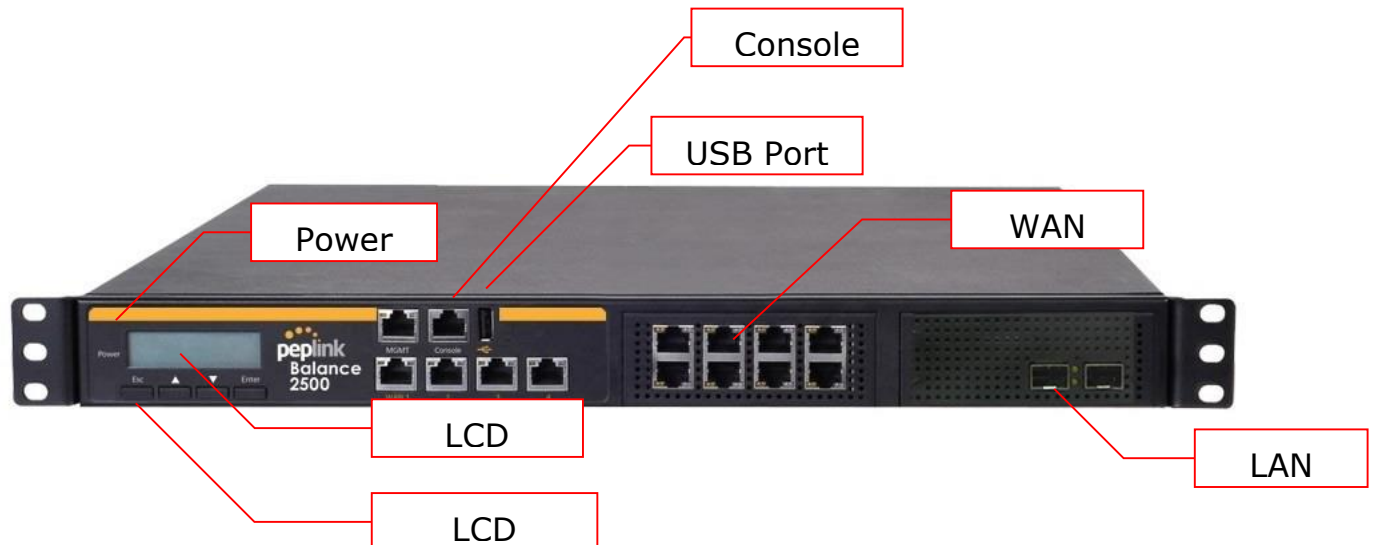
8.13 Peplink Balance 2500

8.13.1 Front Panel Appearance

BPL-2500



BPL-2500-SFP



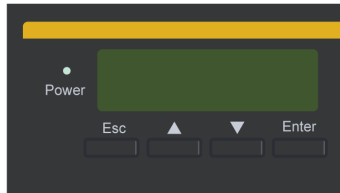
Status indicated in the front panel is as follows:

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

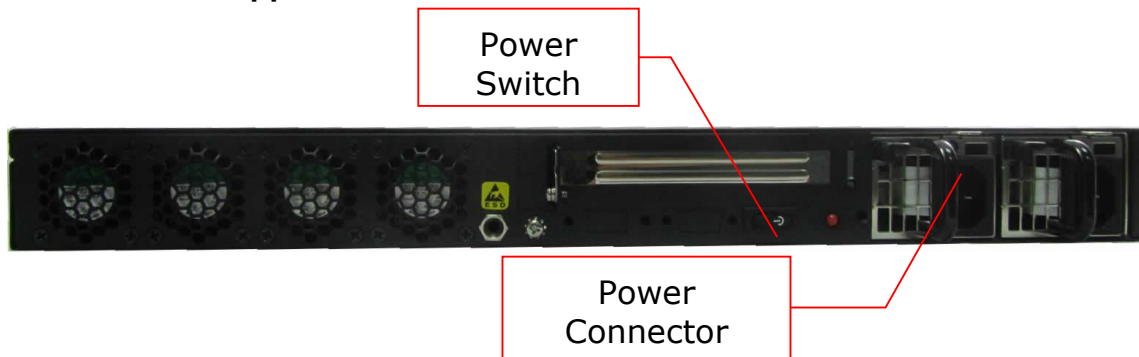
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

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



Serial Number
and
LAN MAC
Address

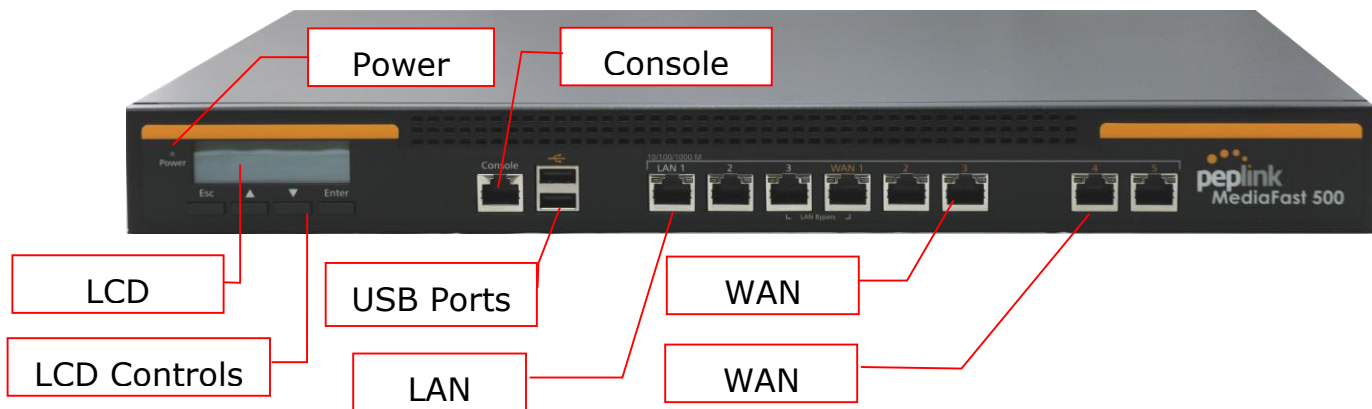
BPL-2500-SFP



Serial Number
and
LAN MAC
Address

8.14 Peplink MediaFast 500

8.14.1 Front Panel Appearance



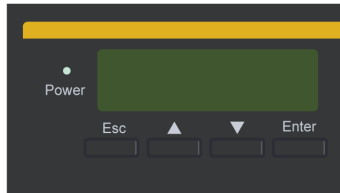
Status indicated in the front panel is as follows:

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

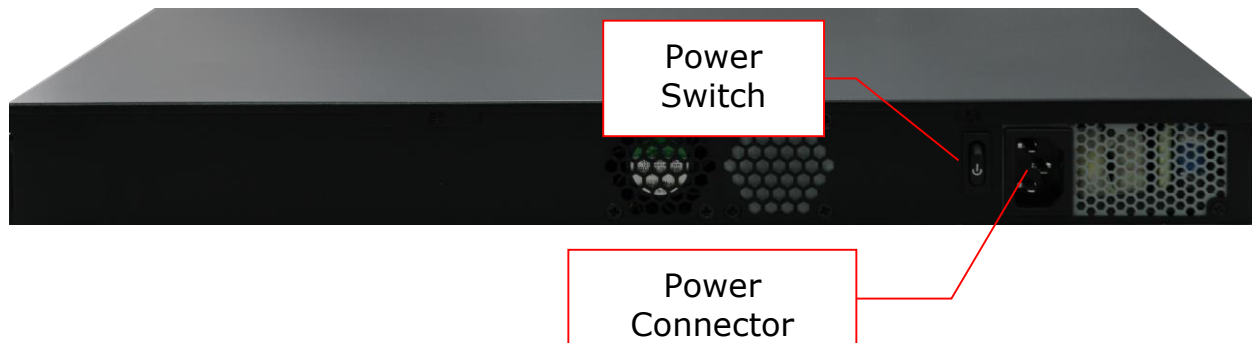
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting 4G/3G USB modems

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 (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

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:

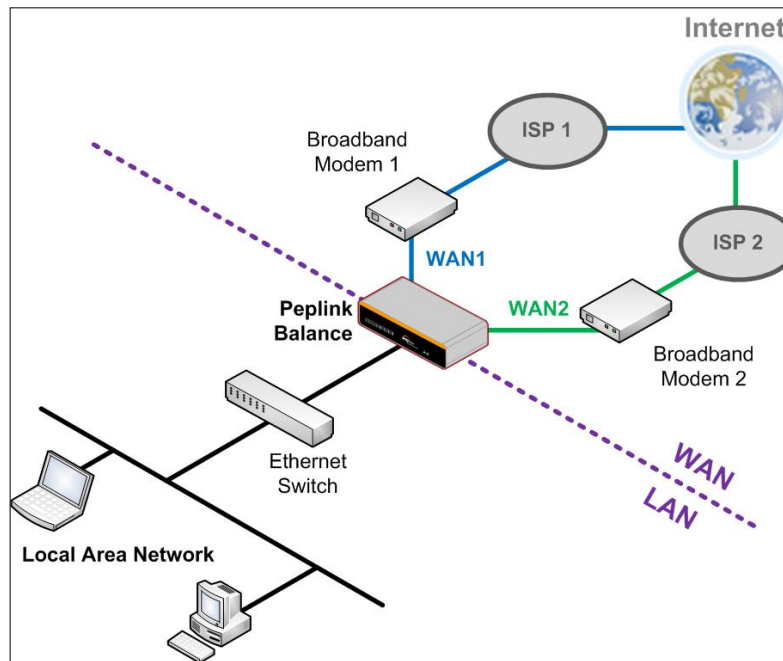
- At least one Internet/WAN access account
- For each network connection, one 10/100BaseT UTP cable with RJ45 connector, one 1000BaseT Cat5E UTP cable for the Gigabit port, or one USB modem for the USB WAN port
- A computer with the TCP/IP network protocol and a web browser installed—supported browsers 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	Status: ● Connected	Details... Disconnect
2 Wi-Fi		
IP Address: 18.220.23.1	Status: ● Connected	Details... Disconnect
3 FDD		
IP Address: 19.221.24.1	Status: ● Connected	Details... Disconnect
4 WAN1		
IP Address: 123.203.209.47	Status: ● Connected	Details... Disconnect
5 WAN5		
IP Address: 14.136.11.100	Status: ● Connected	Details... Disconnect
6 WAN6		
IP Address: 213.141.82.11	Status: ● Connected	Details... 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	● m	
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:	<div style="width: 5%;"></div> 5%	
Throughput:	↓ 0.0 Mbps ↑ 0.0 Mbps	

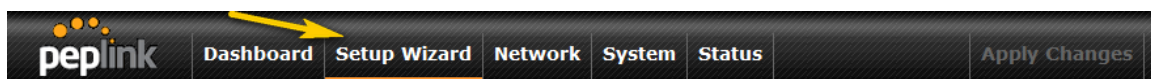
Important Note

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>WAN 1 ▼ WAN 1 WAN 2 WAN 3 WAN 4 WAN 5 WAN 6 WAN 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 Mbps ▼
Download Bandwidth	1000 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

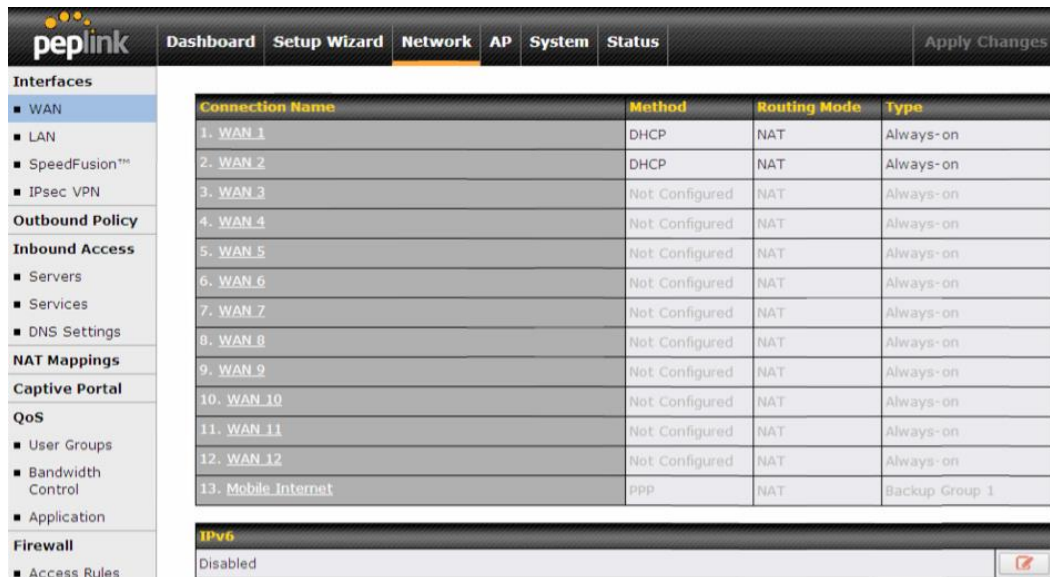
Save Settings

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**.



The screenshot shows the Peplink web interface with the 'Network' tab selected. The left sidebar contains a tree view with 'Interfaces' expanded, showing 'WAN' as the selected option. The main content area displays a table of WAN connections and an IPv6 status section.

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

Below the table, the 'IPv6' status is shown as 'Disabled' with a red status icon.

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	Connected	Details
Priority 2		
2 WAN 2	No Cable Detected	Details
1 Cellular 1	No Device Detected	Details
2 Cellular 2	No SIM Card Detected Reload SIM	Details
Priority 3		
Drag desired (Priority 3) connections here		
Disabled		
WI-FI WAN	Disabled	Details

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	? Auto
Authentication	Auto
Band Selection	<input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (800 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (850 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (900 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (1700 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (1900 MHz) <input checked="" type="checkbox"/> WCDMA / HSDPA / HSUPA / HSPA+ (2100 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (850 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (900 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (1800 MHz) <input checked="" type="checkbox"/> GSM / GPRS / EDGE (1900 MHz)
Data Roaming	<input type="checkbox"/>
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	
Username	
Password	
SIM PIN (Optional)	?
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable
Action	? <input type="checkbox"/> Disconnect when usage hits 100% Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification .
Start Day	On 1st of each month
Monthly Allowance	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	<p>This setting applies to 3G / EDGE / GPRS modems only. It does not apply to EVDO / EVDO Rev. A modems.</p> <p>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.</p>

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	
IP Passthrough	<p>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.</p> <p>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).</p> <p>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).</p> <p>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.</p>

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	 SmartCheck ▼
Timeout	 5 ▼ second(s)
Health Check Interval	 10 ▼ second(s)
Health Check Retries	 3 ▼
Recovery Retries	 3 ▼

Health Check Settings	
Health Check Method	This setting allows you to specify the health check method for the cellular connection. 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="password"/>
Confirm Password	<input type="password"/>
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.

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 ☒

Domains / IP Addresses ☐ Cache all
☐ Whitelist
☒ Blacklist
 peplink.com

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).

Secure Content Caching

Enable ☒

Domains / IP Addresses ☐ Cache all
☒ Whitelist
☐ Blacklist
 googlevideo.com
 youtube.com
 yting.com
 vimeo.com
 vimeocdn.com
 akamaihd.net

Source IP Subnet ☐ Any ☒ Custom

Network	Subnet Mask	
10.8.41.0	255.255.255.0 (/24)	✖
10.8.76.0	255.255.255.0 (/24)	✖
	255.255.255.0 (/24)	+

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

Cache Control								
Content Type	<div><input checked="" type="checkbox"/> Video</div> <div><input checked="" type="checkbox"/> Audio</div> <div><input checked="" type="checkbox"/> Images</div> <div><input checked="" type="checkbox"/> OS / Application Updates</div>							
Cache Lifetime Settings	<table border="1"><thead><tr><th>File Extension</th><th>Lifetime (days)</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr><tr><td colspan="2"><div><input type="button" value="+"/></div></td></tr></tbody></table>		File Extension	Lifetime (days)	<input type="text"/>	<input type="text"/>	<div><input type="button" value="+"/></div>	
File Extension	Lifetime (days)							
<input type="text"/>	<input type="text"/>							
<div><input type="button" value="+"/></div>								

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, administering 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="password"/>
Confirm Password	<input type="password"/>

MDM Settings

Enable

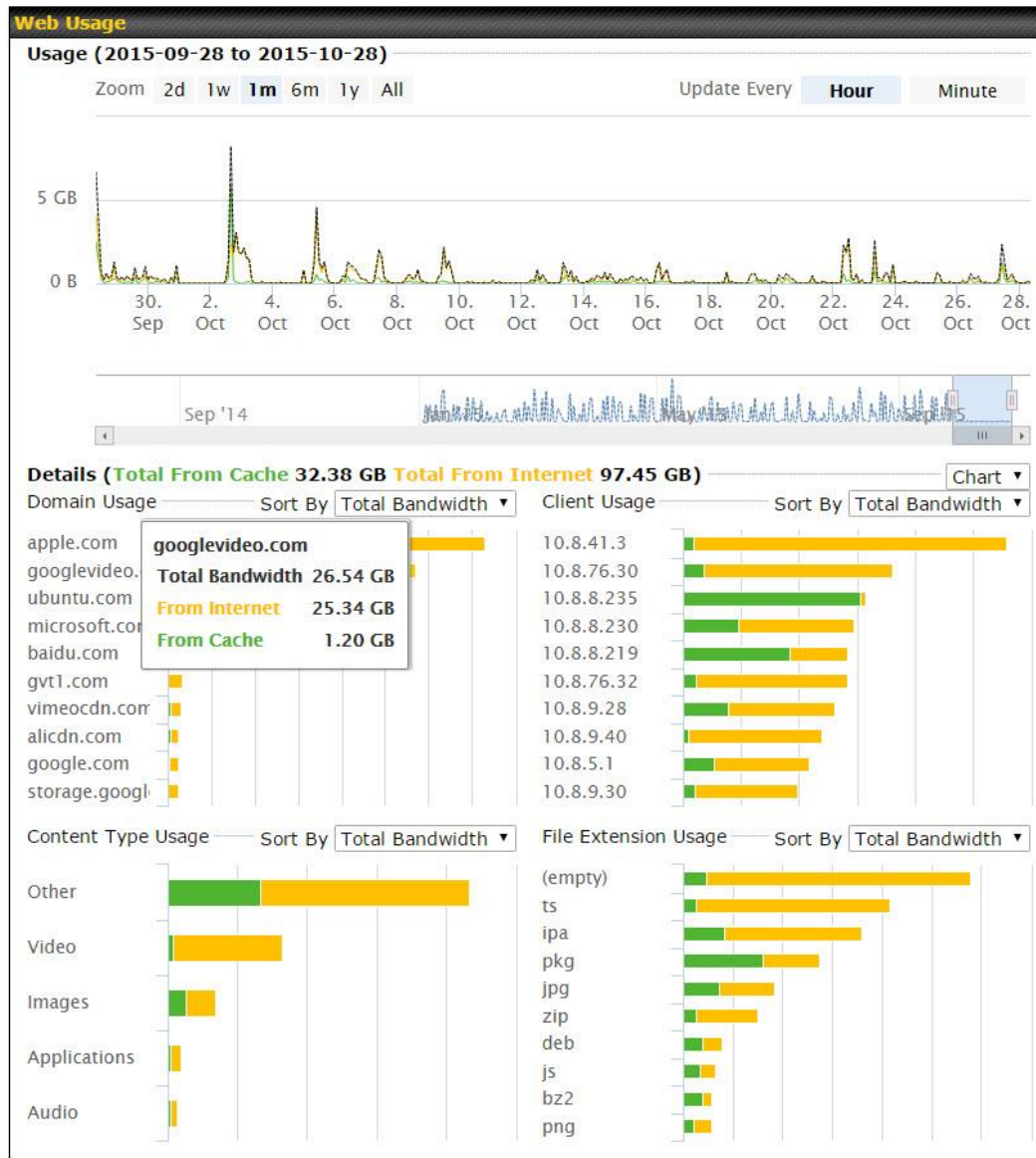
Click this checkbox to enable MDM on your router.

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"/>
<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	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">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;">Add</td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		Add			
Option	Value										
No Extended DHCP Option											
Add											
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>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	<p>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.</p> <p>When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP WINS 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.</p>
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: <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 WAN: <input type="checkbox"/> 3

LAN Physical Settings	
Speed	The default speed setting is Auto , which allows the Balance to detect and apply an appropriate speed setting. You can also set the speed manually, as well as specify whether the speed will be advertised on the network. Generally, advertising port speed is necessary only when the port experiences difficulty negotiating speeds with peer devices.
IEEE 802.3ad Link Aggregation	Choose the interfaces that you wish to aggregate here if needed.



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

Static Route Settings										
Static Route		<table border="1"> <thead> <tr> <th>Destination Network</th> <th>Subnet Mask</th> <th>Gateway</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>255.255.255.0 (/24)</td> <td></td> <td></td> </tr> </tbody> </table>	Destination Network	Subnet Mask	Gateway			255.255.255.0 (/24)		
Destination Network	Subnet Mask	Gateway								
	255.255.255.0 (/24)									



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 w.x.y.z 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  to create a new route. Click  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	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> <th>TTL</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>3600</td> <td>+</td> </tr> </tbody> </table>	Host Name	IP Address	TTL				3600	+								
Host Name	IP Address	TTL															
		3600	+														
Domain Lookup Policy	<table border="1"> <thead> <tr> <th>Domain</th> <th>Connection</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Domain	Connection														
Domain	Connection																
DNS Resolvers	<table border="1"> <thead> <tr> <th>WAN Connection</th> <th>DNS Servers</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> WAN 1</td> <td>10.88.3.1 168.95.1.1</td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 3</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Mobile Internet</td> <td></td> </tr> <tr> <th>LAN Connection</th> <th>DNS Servers</th> </tr> <tr> <td><input type="checkbox"/> Untagged LAN</td> <td></td> </tr> </tbody> </table>			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	
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"/>																	

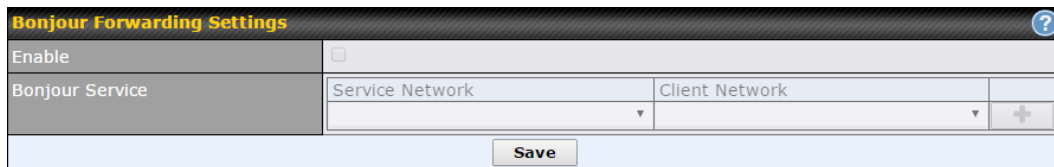
DNS Proxy Settings	
Enable	<p>To enable the DNS proxy feature, check this box, and then set up the feature at Network>LAN>DNS Proxy Settings.</p> <p>A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the DNS servers/resolvers 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

☒

WAN for Drop-In Mode

WAN 1 with LAN bypass

WAN Default Gateway

☒ I have other host(s) on WAN segment
Host IP Address(es) -

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.




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">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;">Add</td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		Add			
Option	Value										
No Extended DHCP Option											
Add											
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td style="text-align: center;">+</td> </tr> </tbody> </table>			Name	MAC Address	Static IP					+
Name	MAC Address	Static IP									
			+								

DHCP Server Settings	
DHCP Server	When this setting is enabled, the 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	<p>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.</p> <p>When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP WINS 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.</p>
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

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	 <div> <div>DHCP Server 1: <input type="text"/></div> <div>DHCP Server 2: <input type="text"/></div> </div>
DHCP Option 82	 <input type="checkbox"/>

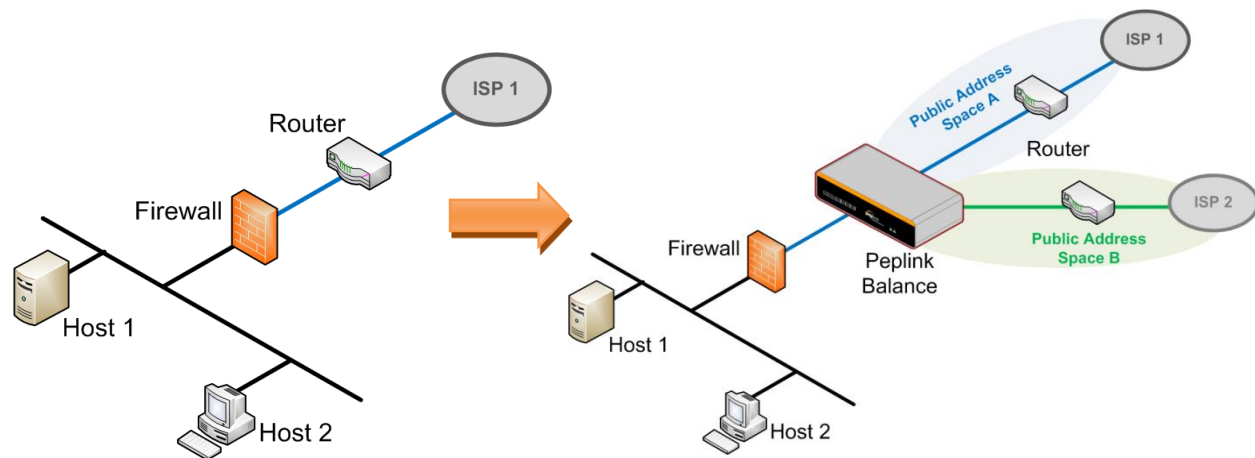
DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active 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

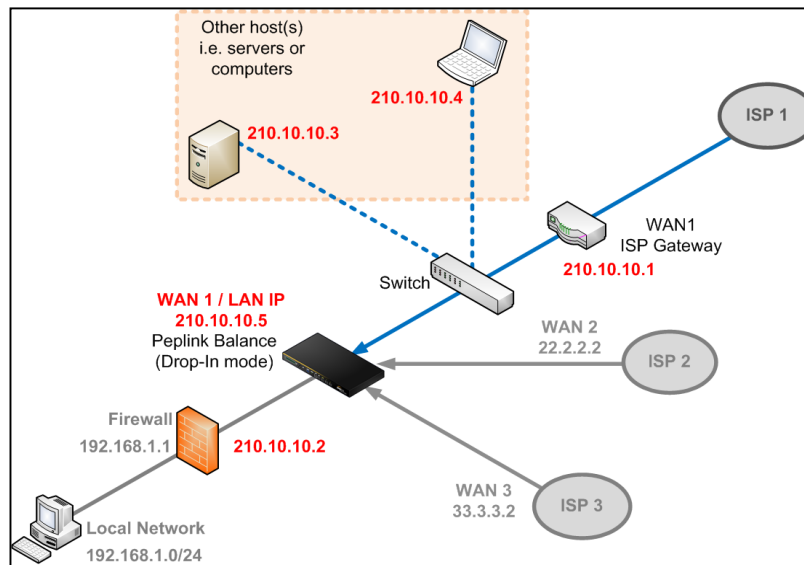
The PPTP server will be disabled in drop-in mode.

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	<input type="text"/> 255.255.255.0 (/24) ▼
WAN Default Gateway	<input type="text"/> 210.10.10.1 <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) <input type="text"/> 210.10.10.3 - <input type="text"/> <input type="button" value="↓"/> <input type="text"/> 210.10.10.3 <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>	

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:

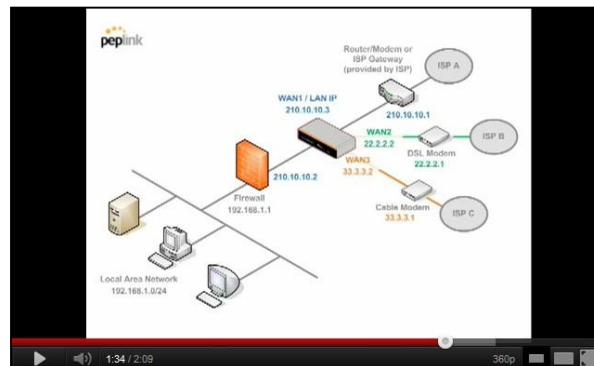


Important Note

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/IZG2-VPml5w>

14 Configuring the WAN Interface(s)

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

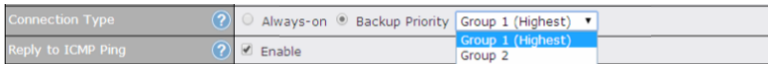
Connection Name	Method	Routing Mode	Type
1. WAN 1	Static IP	NAT	Always-on
2. WAN 2	Static IP	NAT	Always-on
3. WAN 3	Static IP	NAT	Always-on
4. WAN 4	Not Configured	NAT	Always-on
5. WAN 5	Not Configured	NAT	Always-on
6. WAN 6	Not Configured	NAT	Always-on
7. WAN 7	Not Configured	NAT	Always-on
8. WAN 8	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

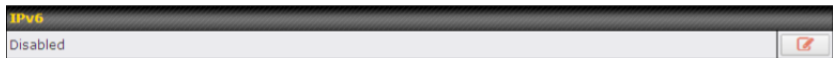
IPv6	Disabled	
-------------	----------	---

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="button" 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	<p>This option allows you to select the connection method for this WAN connection. Available options are:</p> <ol style="list-style-type: none"> 1. DHCP 2. Static IP 3. PPPoE 4. 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.</p> <p>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	<p>IPv6 support can be enabled on one of the available Ethernet WAN ports. On this screen, you can choose which WAN will support IPv6.</p>  <p>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.</p>

14.1 Physical Interface Settings

Physical Interface Settings	
Speed	<input data-bbox="570 296 594 327" type="button" value="?"/> Auto
MTU	<input data-bbox="570 331 594 363" type="button" value="?"/> <input type="radio"/> Auto <input checked="" type="radio"/> Custom 1440 <input data-bbox="1008 331 1081 363" type="button" value="Default"/>
MSS	<input data-bbox="570 367 594 399" type="button" value="?"/> <input checked="" type="radio"/> Auto <input type="radio"/> Custom
MAC Address Clone	<input data-bbox="570 403 594 434" type="button" value="?"/> <input checked="" type="radio"/> Default <input type="radio"/> Custom 10 : 56 : CA : 06 : 08 : 09
VLAN	<input data-bbox="570 438 594 470" type="button" value="?"/> <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	<p>These settings specify the information required in order to communicate on the Internet via a fixed Internet IP address.</p> <p>The information is typically determined by and can be obtained from your ISP.</p>
DNS Servers	<p>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.</p> <p>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>

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	<div>4G only ▼</div> <div>4G only</div> <div>3G only</div>

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	<div>? Disabled</div> <div>Health Check disabled. Network problem cannot be detected.</div>

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					
<table border="1"><thead><tr><th colspan="2">Health Check Settings</th></tr></thead><tbody><tr><td>Health Check Method</td><td><div>? Disabled</div><div>Health Check disabled. Network problem cannot be detected.</div></td></tr></tbody></table>		Health Check Settings		Health Check Method	<div>? Disabled</div> <div>Health Check disabled. Network problem cannot be detected.</div>
Health Check Settings					
Health Check Method	<div>? Disabled</div> <div>Health Check disabled. Network problem cannot be detected.</div>				
When Disabled is chosen in the Method field, the WAN connection will always be considered as up. The connection will NOT be treated as down in the event of IP routing errors.					
Health Check Method: PING					
<table border="1"><tbody><tr><td>Health Check Method</td><td><div>? PING</div></td></tr><tr><td>PING Hosts</td><td><div><div><div>? Host 1:</div><div></div></div><div><div>? Host 2:</div><div></div></div></div><div><input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts</div></td></tr></tbody></table>		Health Check Method	<div>? PING</div>	PING Hosts	<div><div><div>? Host 1:</div><div></div></div><div><div>? Host 2:</div><div></div></div></div> <div><input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts</div>
Health Check Method	<div>? PING</div>				
PING Hosts	<div><div><div>? Host 1:</div><div></div></div><div><div>? Host 2:</div><div></div></div></div> <div><input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts</div>				
ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.					
PING Hosts	This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If Use first two DNS servers as Ping Hosts is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.				
Health Check Method: DNS Lookup					
<table border="1"><tbody><tr><td>Health Check Method</td><td><div>? DNS Lookup</div></td></tr><tr><td>Health Check DNS Servers</td><td><div><div><div>? Host 1:</div><div></div></div><div><div>? Host 2:</div><div></div></div></div><div><input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers</div><div><input type="checkbox"/> Include public DNS servers</div></td></tr></tbody></table>		Health Check Method	<div>? DNS Lookup</div>	Health Check DNS Servers	<div><div><div>? Host 1:</div><div></div></div><div><div>? Host 2:</div><div></div></div></div> <div><input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers</div> <div><input type="checkbox"/> Include public DNS servers</div>
Health Check Method	<div>? DNS Lookup</div>				
Health Check DNS Servers	<div><div><div>? Host 1:</div><div></div></div><div><div>? Host 2:</div><div></div></div></div> <div><input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers</div> <div><input type="checkbox"/> Include public DNS servers</div>				
DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.					

Health Check DNS Servers




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

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

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

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

Health Check Method: HTTP

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

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

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1





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

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

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

Other Health Check Settings

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

Timeout

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

Health Check Interval

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

Health Check Retries

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

Recovery Retries

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


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

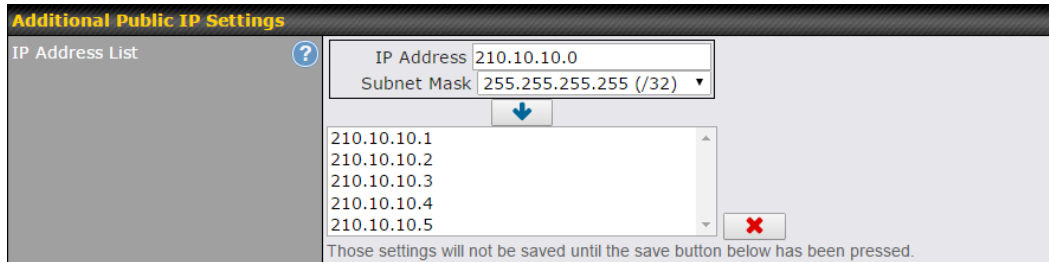
The Bandwidth Allowance Monitor helps track your network usage. Please refer to **Section 28.8** to view usage statistics.

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

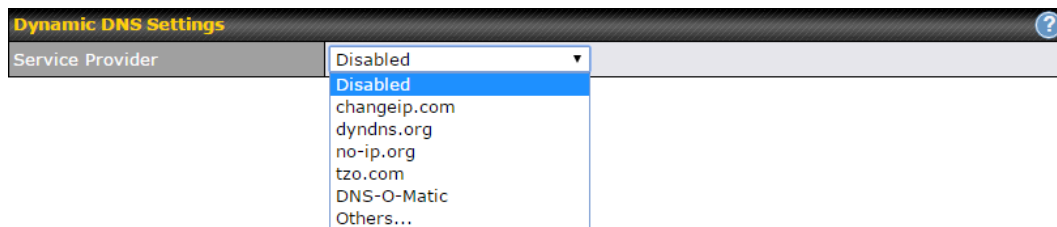
14.6 Dynamic DNS Settings

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**.



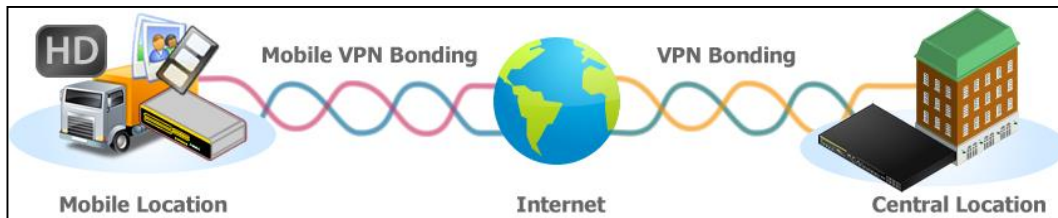
If your desired provider is not listed, you may check with **DNS-O-Matic**. This service supports updating 30 other dynamic DNS service providers. (Note: Peplink is not affiliated with DNS-O-Matic.)

Dynamic DNS Settings	
Service Provider	DNS-O-Matic
Username	
Password	
Confirm Password	
Update All Hosts	<input type="checkbox"/>
Hosts / IDs	

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

Important Note	
<p>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.</p> <p>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.</p> <p>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.</p>	

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		
New Profile			

Send All Traffic To	No PepVPN profile selected	
----------------------------	----------------------------	--



PepVPN Local ID	Local ID	Balance_01AA	
------------------------	----------	--------------	--


PepVPN Settings	Link Failure Detection Time <ul style="list-style-type: none"> <input checked="" type="radio"/> Recommended (Approx. 15 secs) <input type="radio"/> Fast (Approx. 6 secs) <input type="radio"/> Faster (Approx. 2 secs) <input type="radio"/> Extreme (Under 1 sec) Shorter detection time incurs more health checks and higher bandwidth overhead	
Save		

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

PepVPN Profile		
Name	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	Remote ID	Pre-shared Key
	Balance 9875-A63D-92AS
NAT Mode	<input type="checkbox"/>	
Remote IP Address / Host Names (Optional)	<input type="text"/> If this field is empty, this field on the remote unit must be filled	
Data Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>	
Bandwidth Limit	<input type="checkbox"/>	
Cost	10	
WAN Smoothing	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

No PepVPN profile selected

Send All Traffic To

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

Send All Traffic

Send All Traffic To ? Balance 2942-1257-1241

DNS Server
8.8.8.8
8.8.4.4

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

DNS Server
8.8.8.8
8.8.4.4

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

PepVPN Local ID

Local ID ? Balance_01AA

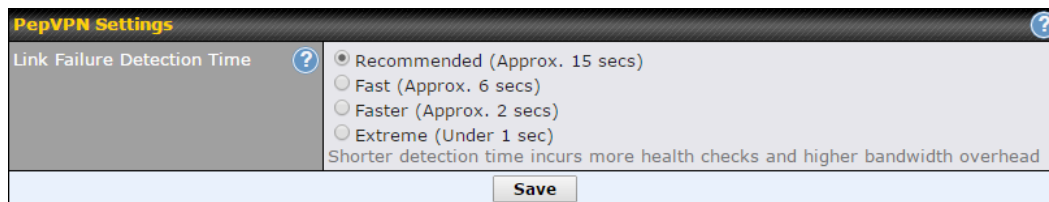
PepVPN Local ID

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

Link Failure Detection Time

The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed.

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

When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds.

When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds.

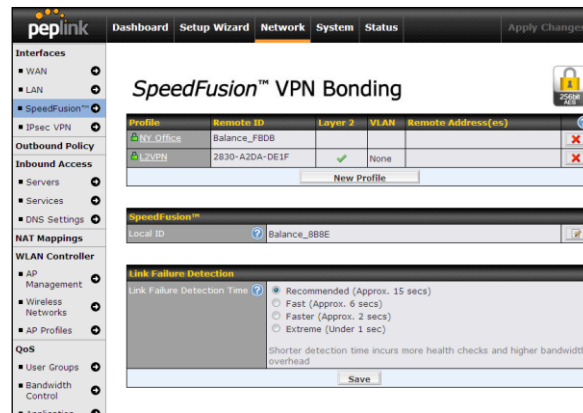
When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

Important Note

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

Tip

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



http://youtu.be/xNaq13FWu_g

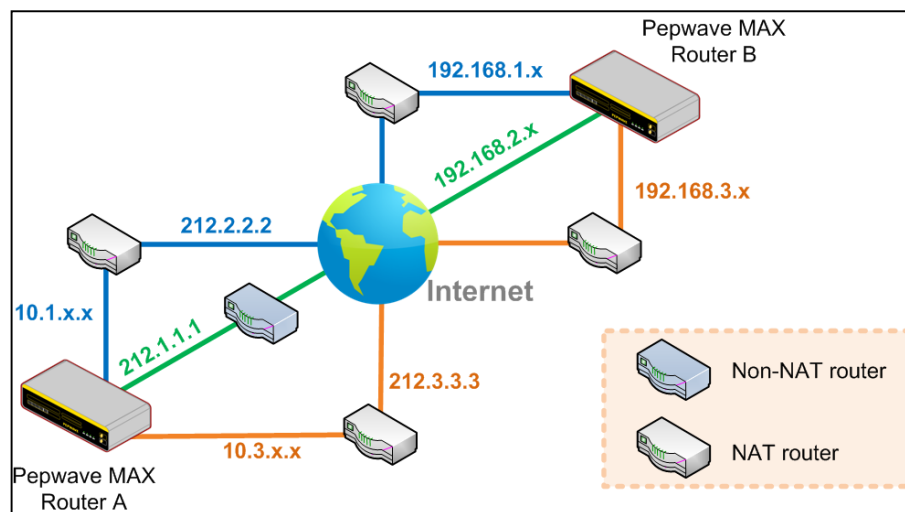
15.2 The Peplink Balance Behind a NAT Router

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		Established
NY Office		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
 FL Office B380	FL Office	Bridged to Untagged LAN with IP address 10.7.2.4  
 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	<input type="text" value="Profile 1"/>								
Active	<input checked="" type="checkbox"/>								
Connect Upon Disconnection of	<input checked="" type="checkbox"/>	<input type="text" value="WAN 2"/>							
Remote Gateway IP Address / Host Name	<input type="text" value="12.12.12.12"/>								
Local Networks	<p>Propose the following networks to remote gateway:</p> <p><input type="checkbox"/> 172.16.1.1/24</p> <p><input type="checkbox"/> 172.16.2.1/24</p> <p><input type="checkbox"/> 172.16.3.1/24</p> <p><input checked="" type="checkbox"/> 10.10.0.1/32</p> <p><input checked="" type="checkbox"/> 192.168.10.0/24</p> <p><input checked="" type="checkbox"/> 192.168.11.0/24</p> <p><input type="checkbox"/> <input type="text" value=""/></p> <p>Apply the following NAT policies:</p> <p><input checked="" type="checkbox"/> 172.16.1.0/24 <input checked="" type="checkbox"/> 192.168.10.0/24</p> <p><input checked="" type="checkbox"/> 172.16.2.0/24 <input checked="" type="checkbox"/> 10.10.0.1/32</p> <p><input checked="" type="checkbox"/> 172.16.3.11/32 <input checked="" type="checkbox"/> 192.168.11.101/32</p> <p><input checked="" type="checkbox"/> 172.16.3.21/32 <input checked="" type="checkbox"/> 192.168.11.201/32</p> <p><input type="checkbox"/> Local Network <input checked="" type="checkbox"/> NAT Network</p>								
Remote Networks	<table border="1"> <thead> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text" value="192.167.11.193"/></td> <td><input type="text" value="255.255.255.0 (/24)"/></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Network	Subnet Mask		<input type="text" value="192.167.11.193"/>	<input type="text" value="255.255.255.0 (/24)"/>	<input type="button" value="+"/>		
Network	Subnet Mask								
<input type="text" value="192.167.11.193"/>	<input type="text" value="255.255.255.0 (/24)"/>	<input type="button" value="+"/>							
Authentication	<input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate								
Mode	<input checked="" type="radio"/> Main Mode (All WANs need to have Static IP) <input type="radio"/> Aggressive Mode								
Force UDP Encapsulation	<input type="checkbox"/>								
Preshared Key	<input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters								
Local ID	<input type="text"/>								
Remote ID	<input type="text"/>								
Phase 1 (IKE) Proposal	1 <input type="text" value="AES-256 & SHA1"/> 2 <input type="text" value="-----"/>								
Phase 1 DH Group	<input checked="" type="checkbox"/> Group 2: MODP 1024 <input type="checkbox"/> Group 5: MODP 1536								
Phase 1 SA Lifetime	<input type="text" value="3600"/>	seconds	<input type="button" value="Default"/>						
Phase 2 (ESP) Proposal	1 <input type="text" value="AES-256 & SHA1"/> 2 <input type="text" value="-----"/>								
Phase 2 PFS Group	<input checked="" type="radio"/> None <input type="radio"/> Group 2: MODP 1024 <input type="radio"/> Group 5: MODP 1536								
Phase 2 SA Lifetime	<input type="text" value="28800"/>	seconds	<input type="button" value="Default"/>						

IPsec VPN Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected. 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**.

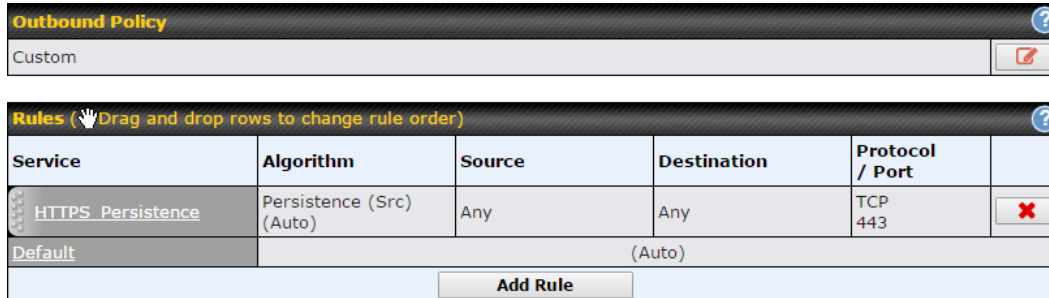
17 Outbound Policy Management


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**.




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

Add Rule

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



Select an Outbound Policy

Policy  High Application Compatibility

High Application Compatibility
Normal Application Compatibility
Custom

Save Cancel

17.1 Outbound Policy

There are three main selections for the outbound traffic policy:

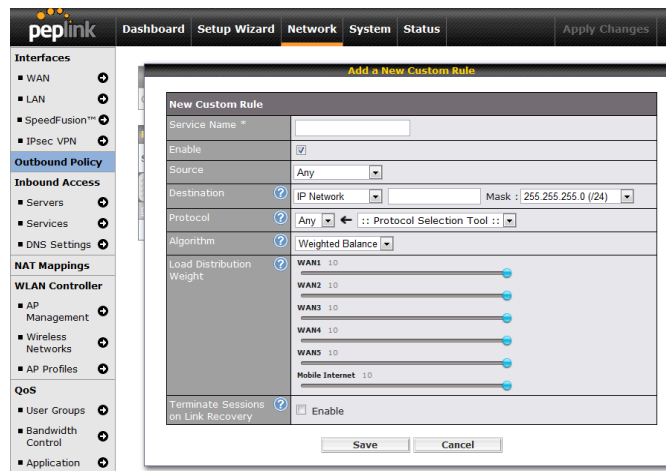
- High Application Compatibility
- Normal Application Compatibility
- Custom

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

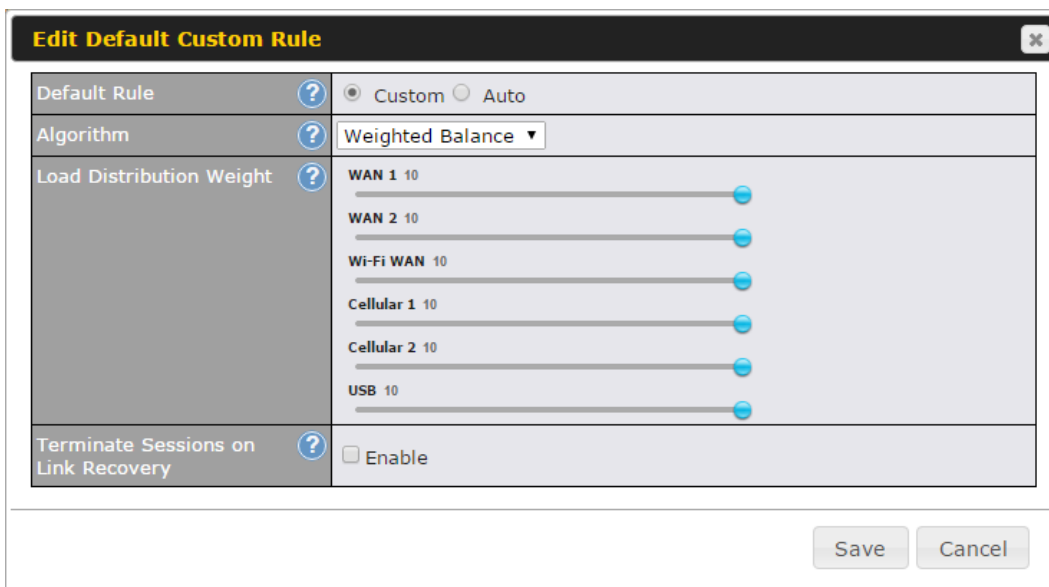
Click  in the **Outbound Policy** form. Choose **Custom** and press the **Save** button. The following screen will then be displayed:



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

Add Rule

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.



Edit Default Custom Rule

Default Rule: ☒ Custom ☐ 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: ☐ Enable

Save Cancel

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.

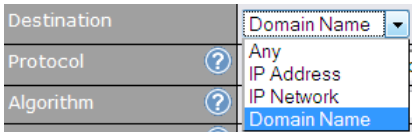
To create a custom rule, click **Add Rule** at the bottom of the table. The following window will be displayed:

Add a New Custom Rule

Service Name *	<input type="text"/>		
Enable	<input checked="" type="checkbox"/>	Always on	▼
Source	Any ▼		
Destination	?	IP Network ▼	Mask: <input type="text"/> 255.255.255.0 (/24) ▼
Protocol	?	Any ▼	← :: Protocol Selection Tool :: ▼
Algorithm	?	Weighted Balance ▼	
Load Distribution Weight	?	<div>WAN 1 10 <input type="range"/></div> <div>WAN 2 10 <input type="range"/></div> <div>Wi-Fi WAN 10 <input type="range"/></div> <div>Cellular 1 10 <input type="range"/></div> <div>Cellular 2 10 <input type="range"/></div> <div>USB 10 <input type="range"/></div>	
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.

<p>Destination</p>	<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>
<p>Protocol and Port</p>	<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>
<p>Algorithm</p>	<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>
<p>Terminate Sessions on Link Recovery</p>	<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 ?	<div>WAN 1 10 </div> <div>WAN 2 10 </div> <div>WAN 3 10 </div> <div>Mobile Internet 10 </div>

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

For example, with the following weight settings 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	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	<div> <div>WAN 1 10</div> <div>WAN 2 10</div> <div>WAN 3 10</div> <div>Mobile Internet 10</div> </div>

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

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

The default mode is **By Source**.

When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. If you choose **Auto** in **Load Distribution**, the weights will be automatically adjusted according to each WAN's **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	Enforced
Enforced Connection	<div> <div>WAN: WAN 1</div> <div>WAN: WAN 1</div> <div>WAN: WAN 2</div> <div>WAN: WAN 3</div> <div>WAN: Mobile Internet</div> <div>VPN: FL_Office</div> <div>VPN: NY_Office</div> </div>










Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection.

Starting from Firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

17.2.4 Algorithm: Priority

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

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

Algorithm		Priority 	
Priority Order		Highest Priority	Not In Use
		 WAN: WAN 1	 VPN: FL_Office
		 WAN: WAN 2	 VPN: NY_Office
		 WAN: WAN 3	
		 WAN: Mobile Internet	
		Lowest Priority	







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

Tip

Configure multiple distribution rules to accommodate different kinds of services.

17.2.5 Algorithm: Overflow

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

Algorithm		Overflow
Overflow Order		<div>Highest Priority</div> <div><div></div>WAN: WAN 1</div> <div><div></div>WAN: WAN 2</div> <div><div></div>WAN: WAN 3</div> <div><div></div>WAN: Mobile Internet</div> <div>Lowest Priority</div>


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

17.2.6 Algorithm: Least Used

Algorithm	 Least Used ▼
Connection	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> Mobile Internet

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

17.2.7 Algorithm: Lowest Latency

Algorithm	 Lowest Latency ▼ <small>Note: Use of Lowest Latency will incur additional network usage.</small>
Connection	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> Mobile Internet

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

Tip

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

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

17.2.8 Expert Mode

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

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

Help




Close

This table allows you to fine tune how the outbound traffic should be distributed to the WAN connections.

Click the **Add Rule** button to add a new rule. Click the 'X' button to remove a rule. Drag a rule to promote or demote its precedence. A higher position of a rule signifies a higher precedence. You may change the default outbound policy behavior by clicking the **Default** link.

If you require advanced control of S2S VPN traffic, [turn on Expert Mode](#).

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

Custom Rules  Drag and drop rows to change rule order) 					
Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS Persis...	Persistence (Src) (Auto)	Any	IP Network 192.168.50.0/24	TCP 443	
Site-to-Site VPN Routes					
Default	Lowest Latency				
<div>Add Rule</div>					

18 Inbound Access

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

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

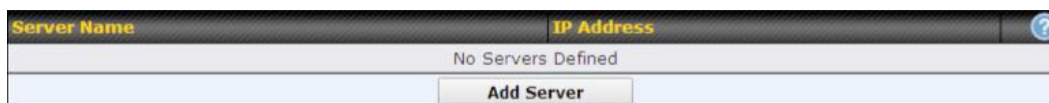
Important Note

Inbound access applies only to WAN connections that operate in NAT mode. For WAN connections that operate in drop-in mode or IP forwarding, inbound traffic is forwarded to the LAN by default.

18.1 Definition of Servers on LAN

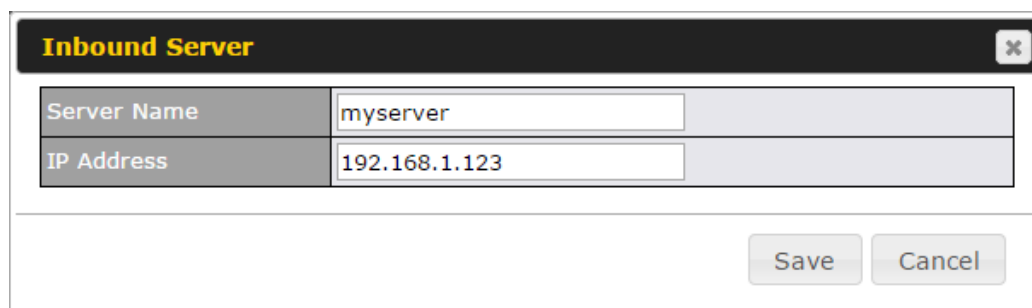
The settings to configure servers on the LAN are located at **Network>Inbound Access>Servers**.

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



Server Name	IP Address
No Servers Defined	
Add Server	

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



Inbound Server [X]

Server Name	myserver
IP Address	192.168.1.123

[Save](#) [Cancel](#)

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



Server Name	IP Address
myserver	192.168.1.123
Add Server	

To define additional servers, click **Add Server** and repeat the above steps.

18.2 Definition of Port Forwarding

Inbound port forwarding rules are defined at **Network>Inbound Access>Services**.

Service	IP Address(es)	Server	Protocol	Action
Web	WAN1: Interface IP	192.168.10.1	TCP:80	<button>Delete</button>
<button>Add Service</button>				

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

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Service Name *	Web	
IP Protocol	TCP ← HTTP	
Port	Single Port Service Port: 80	
Inbound IP Address(es) * (Require at least one IP address)	<div> <div>Connection / IP Address(es)</div> <div> <input checked="" type="checkbox"/> WAN1 <div> <input checked="" type="checkbox"/> 218.100.66.100 (Interface IP) <input type="checkbox"/> 218.100.66.66 <input type="checkbox"/> 218.100.66.103 </div> </div> <div> <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> Mobile Internet </div> </div>	
Server IP Address	192.168.1.10	
* Required Fields		
<div>Save</div> <div>Cancel</div>		

Port Forwarding Settings

Enable

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

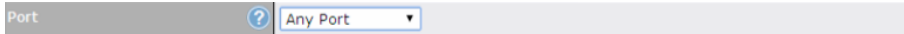
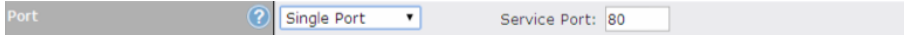
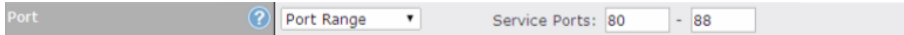
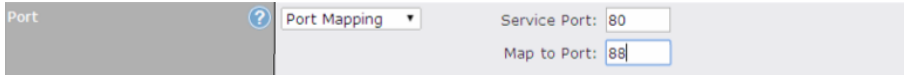
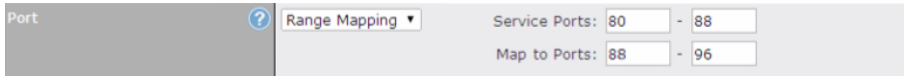
Service Name

This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.

IP Protocol

The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Peplink Balance via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings.

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

	<p>The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p> <p>Any Port, Single Port, Port Range, Port Map, and Range Mapping</p> <div data-bbox="410 315 1308 348">  </div> <p>Any Port: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the Servers setting. For example, with IP Protocol set to TCP, and Port set to Any Port, all TCP traffic is forwarded to the configured servers.</p> <div data-bbox="410 459 1308 493">  </div> <p>Single Port: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the Servers setting. For example, with IP Protocol set to TCP, and Port set to Single Port and Service Port 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.</p> <div data-bbox="410 638 1308 672">  </div> <p>Port Range: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the Servers setting. For example, with IP Protocol set to TCP, and Port set to Port Range and Service Ports 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.</p> <div data-bbox="410 850 1308 924">  </div> <p>Port Mapping: traffic that is received by Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the Servers setting. For example, with IP Protocol set to TCP, and Port set to Port Mapping, Service Port 80, and Map to Port 88, TCP traffic on Port 80 is forwarded to the configured servers via Port 88. (Please see below for details on the Servers setting.)</p> <div data-bbox="410 1104 1308 1178">  </div> <p>Range Mapping: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the Servers setting.</p>
<p>Inbound IP Address(es)</p>	<p>This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.</p>
<p>Server IP Address</p>	<p>This setting specifies the LAN IP address of the server that handles the requests for the service.</p>

18.3 Inbound Access Services

18.3.1 Definition of Services

Services are defined at **Network>Inbound Access>Services**.

Service	IP Address(es)	Server	Protocol
No Services Defined			
Add Service			

Tip

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

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

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Service Name	Web
IP Protocol	TCP <input type="button" value="Protocol Selection Tool"/>
Port	Single Port <input type="button" value="Service Port: 80"/>
Inbound IP Address(es) (Require at least one IP address)	<div> <div>Connection / IP Address(es)</div> <div> <input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> 10.88.3.184 (Interface IP) </div> <div> <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> Mobile Internet </div> </div>
Included Server(s) (Require at least one IP address)	<div> <div>Server</div> <div> <input checked="" type="checkbox"/> myserver (192.168.1.123) <input type="button" value="Weight 10"/> </div> </div>

Services Settings

Enable

This setting specifies whether the inbound service rule takes effect.

When **Yes** is selected, the inbound service rule takes effect. If the inbound traffic matches the specified IP protocol and port, action will be taken by the Peplink Balance based on the other parameters of the rule.

When **No** is selected, the inbound service rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.

Service Name

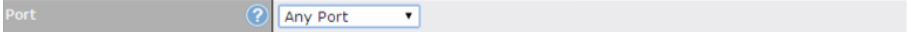
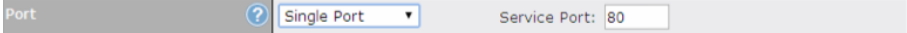
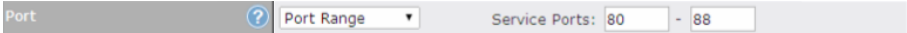
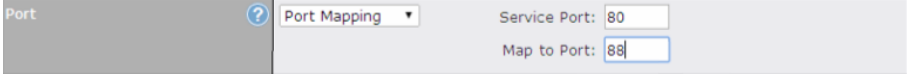
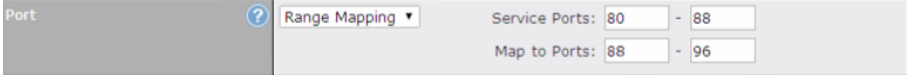
This setting identifies the service to the system administrator. Only alphanumeric and the underscore “_” characters are valid.

IP Protocol

The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Inbound traffic that matches the specified **IP Protocol** and **Port(s)** will be forwarded to the LAN hosts specified by the **Servers** setting.

Upon choosing a protocol, the **Protocol Selection Tool** drop-down menu can be used to automatically the port information of common Internet services (e.g. HTTP, HTTPS, etc.).

After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and the port number will remain manually modifiable.

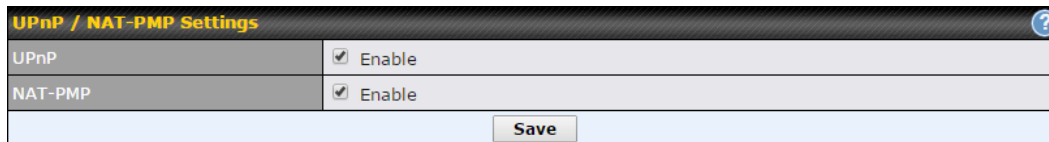
	<p>The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p> <p>Any Port, Single Port, Port Range, Port Map, and Range Mapping</p>  <p>Any Port: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP and Port is set to Any Port, then all TCP traffic will be forwarded to the configured servers.</p>  <p>Single Port: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP, Port is set to Single Port, and Service Port is set to 80, then TCP traffic received on Port 80 will be forwarded to the configured servers via port 80.</p>  <p>Port Range: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP, Port is set to Port Range, and Service Port set to 80-88, then TCP traffic received on ports 80 through 88 will be forwarded to the configured servers via the respective ports.</p>  <p>Port Mapping: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP, Port is set to Port Mapping, Service Port is set to 80, and Map to Port is set to 88, then TCP traffic on port 80 is forwarded to the configured servers via port 88.</p> <p>(Please see below for details on the Servers setting.)</p>  <p>Range Mapping: traffic that is received by Peplink Balance via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the Servers setting.</p>
<p>Inbound IP Address(es)</p>	<p>This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.</p>
<p>Included Server(s)</p>	<p>This setting specifies the LAN servers that handle requests for the service, and the relative weight values. The amount of traffic that is distributed to a server is proportional to the weight value assigned to the server relative to the total weight.</p> <p>Example:</p> <p>With the following weight settings on a Peplink Balance:</p> <ul style="list-style-type: none"> demo_server_1: 10 demo_server_2: 5 <p>The total weight is 15 = (10 + 5)</p> <p>Matching traffic distributed to demo_server_1: 67% = (10 / 15) x 100%</p> <p>Matching traffic distributed to demo_server_2: 33% = (5 / 15) x 100%</p>

18.3.2 UPnP / NAT-PMP SETTINGS

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

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

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



UPnP / NAT-PMP Settings	
UPnP	<input checked="" type="checkbox"/> Enable
NAT-PMP	<input checked="" type="checkbox"/> Enable
<div>Save</div>	

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

18.3.3 Definition of DNS Records

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




For example:

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

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

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

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


DNS Server	<input type="checkbox"/> Disabled	
Zone Transfer	<input type="checkbox"/> Disabled	
Default SOA / NS	<input type="checkbox"/> Undefined	
Default Connection Priority 		
Priority 1: WAN 1, WAN 2, WAN 3, WAN 4, WAN 5, WAN 6, WAN 7, WAN 8, WAN 9, WAN 10, WAN 11, WAN 12, Mobile Internet 		
Domain Names 		
Domain Name		
These is currently no DNS domains.		
<input type="button" value="New Domain Name"/>		
Reverse Lookup Zones 		
Zone Name		
There is currently no Reverse Lookup Zones.		
<input type="button" value="New Reverse Lookup Zone"/>		

[Import records via zone transfer...](#)


DNS Settings

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

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

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

DNS Servers

DNS Servers 

<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> Interface IP
<input 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"/> WAN 8	
<input type="checkbox"/> WAN 9	
<input type="checkbox"/> WAN 10	
<input type="checkbox"/> WAN 11	
<input type="checkbox"/> WAN 12	
<input type="checkbox"/> Mobile Internet	

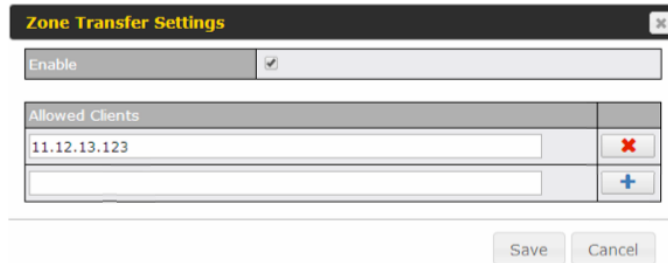
To specify the Internet IP addresses on which the DNS server should listen, select the desired WAN connection then select the desired associated IP addresses. (Multiple items in the list can be selected by holding CTRL and clicking on the items.)

Click **Save** to save the settings when configuration is complete.

Zone Transfer

This setting specifies the IP address(es) of the secondary DNS server(s) authorized to retrieve zone records from the DNS server of the Peplink Balance.

The zone transfer server of the Peplink Balance listens on TCP port 53.



The dialog box titled "Zone Transfer Settings" contains an "Enable" checkbox which is checked. Below it is a table for "Allowed Clients". The first row contains the IP address "11.12.13.123" and a red "X" button. The second row is empty and has a blue "+" button. At the bottom of the dialog are "Save" and "Cancel" buttons.


Zone Transfer Settings	
Enable	<input checked="" type="checkbox"/>
Allowed Clients	
11.12.13.123	

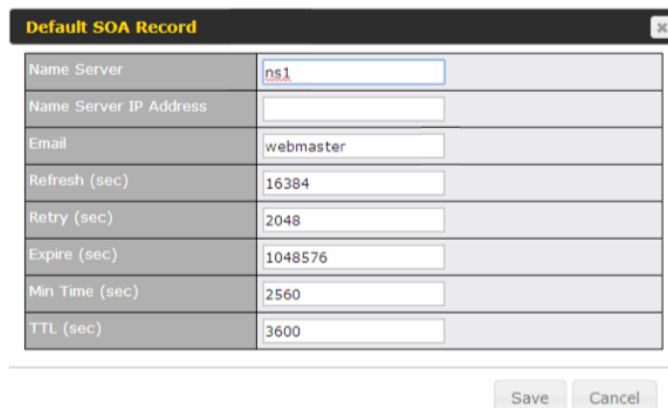
The Peplink Balance serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing its LAN interface.

Routing Control by Subnet Database

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

Default SOA / NS

Click the  button to define a default SOA / NS record for all domain names. For configuration details please refer to **Section 18.3.5**.



The dialog box titled "Default SOA Record" contains a table with the following fields: Name Server (ns1), Name Server IP Address (empty), Email (webmaster), Refresh (sec) (16384), Retry (sec) (2048), Expire (sec) (1048576), Min Time (sec) (2560), and TTL (sec) (3600). At the bottom are "Save" and "Cancel" buttons.

Default SOA Record	
Name Server	ns1
Name Server IP Address	
Email	webmaster
Refresh (sec)	16384
Retry (sec)	2048
Expire (sec)	1048576
Min Time (sec)	2560
TTL (sec)	3600


When defining a default SOA record, **Name Server IP Address** is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain.

For defining default NS records, the host *[domain]* indicates that this record is for the domain name itself without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the **Host** field left empty. When the entered name server is a fully qualified domain name (FQDN), the **IP Address** field will be disabled.

Default Connection Priority

Default Connection Priority defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the **Connection Priority** set to **Default**. Please refer to **Section 18.3.9** for details.

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


To specify the primary and backup connections, click the  button that corresponds to **Default Connection Priority**. The following screen will appear:

Default Connection Priority

Connection	Priority
WAN 1	1 (Highest) ▼
WAN 2	1 (Highest) ▼
WAN 3	1 (Highest) ▼
WAN 4	1 (Highest) ▼
WAN 5	1 (Highest) ▼
WAN 6	1 (Highest) ▼
WAN 7	1 (Highest) ▼
WAN 8	1 (Highest) ▼
WAN 9	1 (Highest) ▼
WAN 10	1 (Highest) ▼
WAN 11	1 (Highest) ▼
WAN 12	1 (Highest) ▼
Mobile Internet	1 (Highest) ▼

Each WAN connection is associated with a priority number. Click **Save** to save the settings when configuration is complete.

Domain name

This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its "NS", "MX" and "TXT" records, and its sub-domains' "A" and "CNAME" records. Add a new record by clicking the **New Domain Name** button. Click on a domain name to edit. Press  to remove a domain name.

18.3.4 Creating DNS Records

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

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

peplink.com

SOA Record
?

Use Default SOA and NS Records

NS Records
?

Host	Name Server	TTL (sec)	
There is currently no NS records.			
<div>New NS Records</div>			

MX Records
?

Host	Priority	Mail Server	TTL (sec)	
There is currently no MX records.				
<div>New MX Records</div>				

CNAME Records
?

Host	Points To	TTL (sec)	
There is currently no CNAME records.			
<div>New CNAME Record</div>			

A Records
?

Host	Included IP Address(es)	TTL (sec)	
There is currently no A records.			
<div>New A Record</div>			

TXT Records
?

Host	TXT Value	TTL (sec)	
There is currently no default TXT records.			
<div>New TXT Record</div>			

SRV Records
?

Service	Priority	Weight	Target	Port	TTL (sec)	
There is currently no SRV records						
<div>New SRV Record</div>						

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

18.3.5 SOA Records


Default / Custom SOA Record

Policy









☒ Use Default SOA and NS Records
☐ Customize SOA Record for this domain

Save

Cancel

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

SOA Record

Name Server		ns1
Name Server IP Address		
Email		webmaster
Refresh (sec)		14400
Retry (sec)		900
Expire (sec)		1209600
Min Time (sec)		3600
TTL (sec)		3600

Save

Cancel

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

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

Default values are set for SOA and NS records,

- **Name Server IP Address:** This is the IP address of the authoritative name server. An entry in this field is optional. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically. If it is left blank, the A record for the name server must be created manually.

- **E-mail:** Defines the e-mail address of the person responsible for this zone. Note: format should be *mailbox-name.domain.com*, e.g., *hostmaster.example.com*.
- **Refresh:** Indicates the length of time (in seconds) when the slave will try to refresh the zone from the master.
- **Retry:** Defines the duration (in seconds) between retries if the slave (secondary) fails to contact the master and the refresh (above) has expired.
- **Expire:** Indicates the time (in seconds) when the zone data is no longer authoritative. This option applies to slave DNS servers only.
- **Min Time:** Is the negative caching time which defines the time (in seconds) after an error record is cached.
- **TTL (Time-to-Live):** Defines the duration (in seconds) that the record may be cached.

18.3.6 NS Records


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

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

The screenshot shows a web interface for managing NS Records. At the top is a header bar labeled "NS Records" with a close button. Below this is a form with a "Host" input field. Underneath is a table with two columns: "Name Server" and "TTL (sec)". The "Name Server" column has an empty input field, and the "TTL (sec)" column has a value of "3600". To the right of the table is a blue "+" button. At the bottom right of the form are "Save" and "Cancel" buttons.

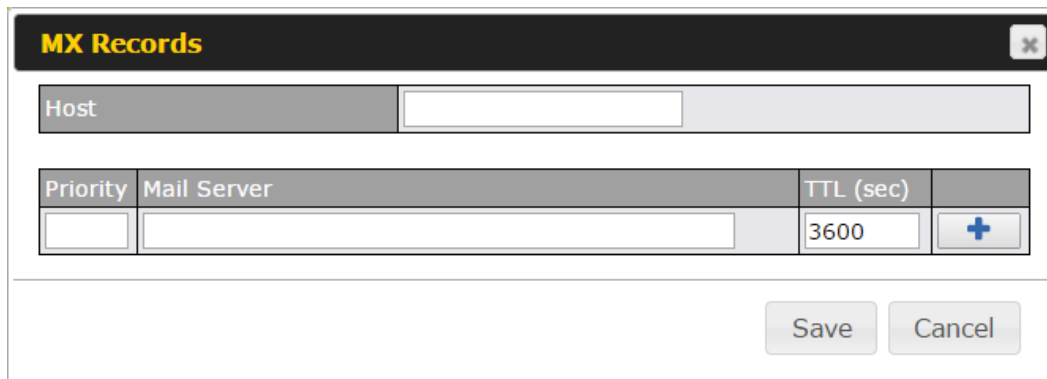
Name Server	TTL (sec)
<input type="text"/>	3600

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

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

18.3.7 MX Records

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



The MX Records form is a modal window titled "MX Records" with a close button in the top right corner. It contains a "Host" input field. Below it is a table with four columns: "Priority", "Mail Server", "TTL (sec)", and an empty column. The "Priority" column has a small input field with a value of 10. The "Mail Server" column has a text input field. The "TTL (sec)" column has a text input field with a value of 3600. The empty column contains a blue plus button. At the bottom right of the form are "Save" and "Cancel" buttons.

Host

Priority	Mail Server	TTL (sec)	
10		3600	+

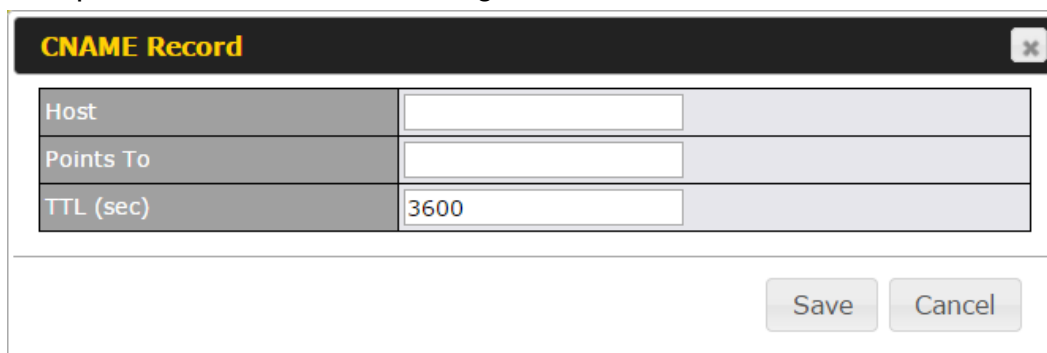
Save Cancel

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

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

18.3.8 CNAME Record

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



The CNAME Record form is a modal window titled "CNAME Record" with a close button in the top right corner. It contains a "Host" input field, a "Points To" input field, and a "TTL (sec)" input field with a value of 3600. At the bottom right of the form are "Save" and "Cancel" buttons.

Host	Points To	TTL (sec)
		3600

Save Cancel

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

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

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

18.3.9 A Record

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


A Record
✕

Host	<input type="text" value="www"/>
TTL (sec)	<input type="text" value="3600"/>
Priority	<input checked="" type="radio"/> Default <input type="radio"/> Custom

Included IP Address(es)
<input type="checkbox"/> WAN 1
<input 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"/> WAN 8
<input type="checkbox"/> WAN 9
<input type="checkbox"/> WAN 10
<input type="checkbox"/> WAN 11
<input type="checkbox"/> WAN 12
<input type="checkbox"/> Mobile Internet
<input type="checkbox"/> Custom IP Address

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

A Record	
Host Name	This field specifies the A record of this sub-domain to be served by the Peplink Balance. The wildcard character "*" is supported. The IP addresses of "*.domain.name" will be returned for every name ending with ".domain.name" except names that have their own records.
TTL	This setting specifies the time to live of this record in external DNS caches. In order to reflect any dynamic changes on the IP addresses in case of link failure and


	recovery, this value should be set to a smaller value, e.g., 5 secs, 60 secs, etc.
Priority	<p>This option specifies the priority of different connections.</p> <p>Select the Default option to apply the Default Connection Priority (refer to the table shown on the main DNS settings page) to an A record. To customize priorities, choose the Custom option and a priority selection table will be shown at the bottom.</p>
Included IP Address(es)	<p>This setting specifies lists of WAN-specific Internet IP addresses that are candidates to be returned when the Peplink Balance responds to DNS queries for the domain name specified by Host Name.</p> <p>The IP addresses listed in each box as default are the Internet IP addresses associated with each of the WAN connections. Static IP addresses that are not associated with any WAN can be entered into the Custom IP list. A PTR record is also created for each custom IP.</p> <p>For WAN connections that operate under drop-in mode, there may be other routable IP addresses in addition to the default IP address. Therefore, the Peplink Balance allows custom Internet IP addresses to be added manually via filling the text box on the right-hand side and clicking the  button.</p> <p>Only the checked IP addresses in the lists are candidates to be returned when responding to a DNS query.</p> <p>If a WAN connection is down, the corresponding set of IP addresses will not be returned. However, the IP addresses in the Custom IP Address field will always be returned.</p> <p>If the Connection Priority field is set to Custom, you can also specify the usage priority of each WAN connection. Only selected IP address(es) of available connection(s) with the highest priority, and custom IP addresses will be returned. By default, Connection Priority is set to Default.</p>

18.3.10 PTR Records

PTR records are created along with A records pointing to custom IPs. Please refer to **Section 18.3.9** for details. For example, if you created an A record *www.mydomain.com* pointing to *11.22.33.44*, then a PTR record *44.33.22.11.in-addr.arpa* pointing to *www.mydomain.com* will also be created. When there are multiple host names pointing to the same IP address, only one PTR record for the IP address will be created. In order for PTR records to function, you also need to create NS records. For example, if the IP address range *11.22.33.0* to *11.22.33.255* is delegated to the DNS server on the Peplink Balance, you will also have to create a domain *33.22.11.in-addr.arpa* and have its NS records pointing to your DNS server's (the Peplink Balance's) public IP addresses. With the above records created, the PTR record creation is complete.

18.3.11 TXT Records

This table shows the TXT record of the domain name.

TXT Record 

Host	<input type="text"/>
TXT Value	<input type="text"/>
TTL (sec)	<input type="text" value="3600"/>

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


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

The maximum size of the TXT Value is 255 bytes.

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

18.3.12 SRV Records

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

SRV Records 

Priority	Weight	Target	Port	TTL (sec)	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="3600"/>	<input type="button" value="+"/>

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

Domain Delegation

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

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

Domain Names	
Domain Name	
peplink.com	
New Domain Name	

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

SOA Record			
Use Custom SOA and NS Records			
Name Server	Details	IP Address	TTL (sec)
ns1	Email: webmaster Refresh (sec): 16384 Retry (sec): 2048 Expire (sec): 1048576 Min Time (sec): 2560	220.246.168.80	3600

NS Records		
Host	Name Server	TTL (sec)
peplink.com	ns1	3600 (SOA)
New NS Records		

- Then create an A record with an empty host name.

A Record

Host	<input type="text"/>
TTL (sec)	3600
Priority	<input checked="" type="radio"/> Default <input type="radio"/> Custom

Included IP Address(es)

<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> Interface IP	<input type="text"/>	+
<input 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"/> WAN 8			
<input type="checkbox"/> WAN 9			
<input type="checkbox"/> WAN 10			
<input type="checkbox"/> WAN 11			
<input type="checkbox"/> WAN 12			
<input type="checkbox"/> Mobile Internet			
<input type="checkbox"/> Custom IP Address			

Save Cancel

A Records			
Host	Included IP Address(es)	TTL (sec)	
ns1	220.246.168.80	3600	(SOA)
New A Record			

If ISC BIND 8 or 9 is being utilized in the zone file mycompany.com, add the following lines:

```

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

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


Hosting the complete domain at Peplink Balance

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

- Under **Network>Inbound Access>DNS Settings**, create a new domain (e.g., mycompany.com).
- Create NS records named ns1, ns2, etc. The IP addresses are the Balance's DNS server addresses (same

as above).

3. Create the corresponding A, CNAME, MX, and TXT records as you wish. The A record resembles the one below:

A Records			
Host	Included IP Address(es)	TTL (sec)	
www	WAN1:default WAN2:default	3600	
New A Record			

Testing the DNS Configuration

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

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

An nslookup in Windows will appear as follows:

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

Please note that the values of the IP addresses are fictitious and for illustration only.

18.4 Reverse Lookup Zones

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



Reverse lookup refers to performing a DNS query to find one or more DNS names associated with a given IP address.

The DNS stores IP addresses in the form of specially formatted names as pointer (PTR) records using special domains/zones. The zone is *in-addr.arpa*.

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

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

33.22.11.in-addr.arpa

SOA Record

WARNING: You should define SOA record in your zone!
[Click here to define SOA Record](#)

NS Records

Host	Name Server	TTL (sec)
WARNING: You should define NS records in your zone!		
New NS Records		

CNAME Records

Host	Points To	TTL (sec)
There is currently no CNAME records.		
New CNAME Record		

PTR Records

Host IP Number	Points To	TTL (sec)
There is currently no PTR records.		
New PTR Record		

Close

18.4.1 SOA Record

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

SOA Record

Name Server	
Email	webmaster
Refresh (sec)	14400
Retry (sec)	900
Expire (sec)	1209600
Min Time (sec)	3600
TTL (sec)	3600

Save
Cancel

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

For example:

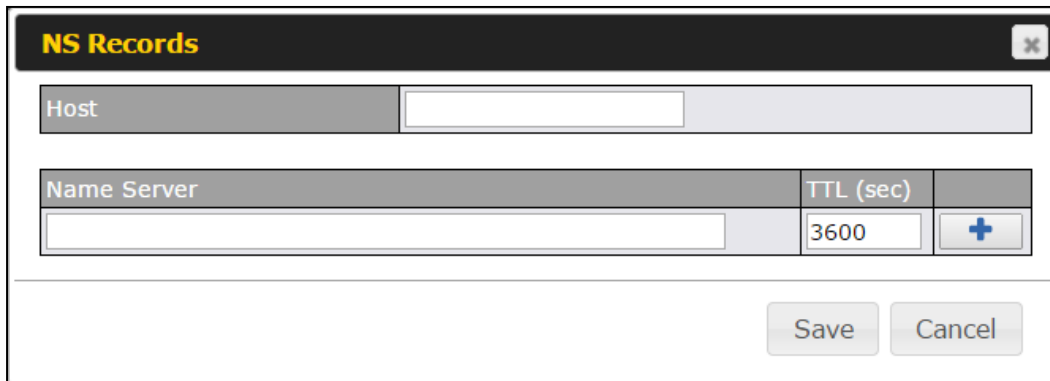
"ns1.mydomain.com" (equivalent to "www.1stdomain.com.")

"ns2.mydomain.com."

Email, Refresh, Retry, Expire, Min Time, and TTL are entered in the same way as in

the forward zone. Please refer to **Section 18.3.5** for details.

18.4.2 NS Records

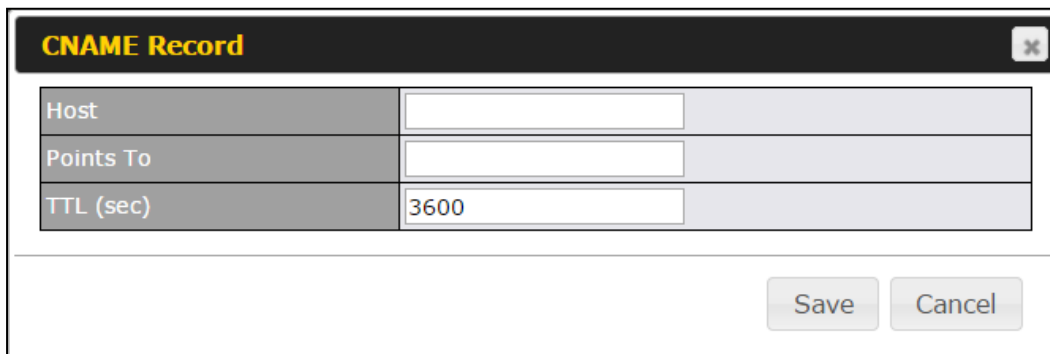


The **NS Records** dialog box contains a 'Host' field, a 'Name Server' field, a 'TTL (sec)' field with a value of 3600, and a '+' button. At the bottom are 'Save' and 'Cancel' buttons.

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

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

18.4.3 CNAME Records



The **CNAME Record** dialog box contains a 'Host' field, a 'Points To' field, a 'TTL (sec)' field with a value of 3600, and a '+' button. At the bottom are 'Save' and 'Cancel' buttons.

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

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

18.4.4 PTR Records

PTR Record ✕

Host IP Number	<input type="text"/>
Points To	<input type="text"/>
TTL (sec)	<input type="text" value="3600"/>

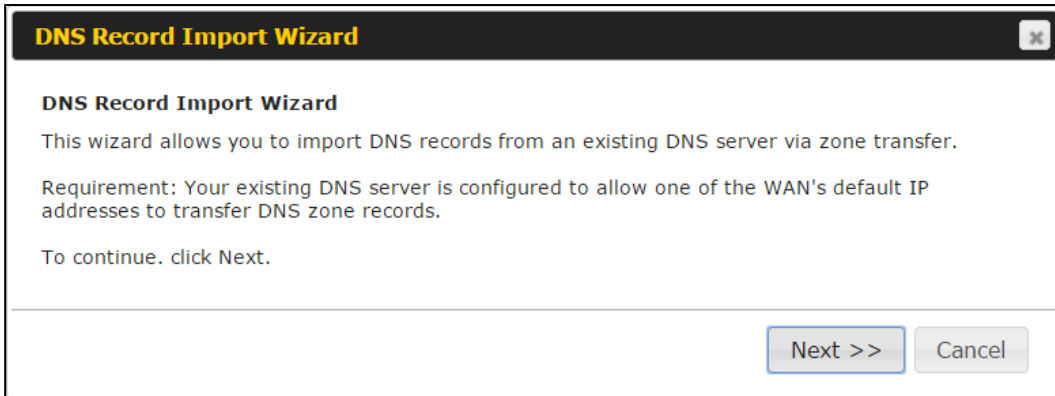
To create a new PTR record, click the **New PTR Record** button.

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

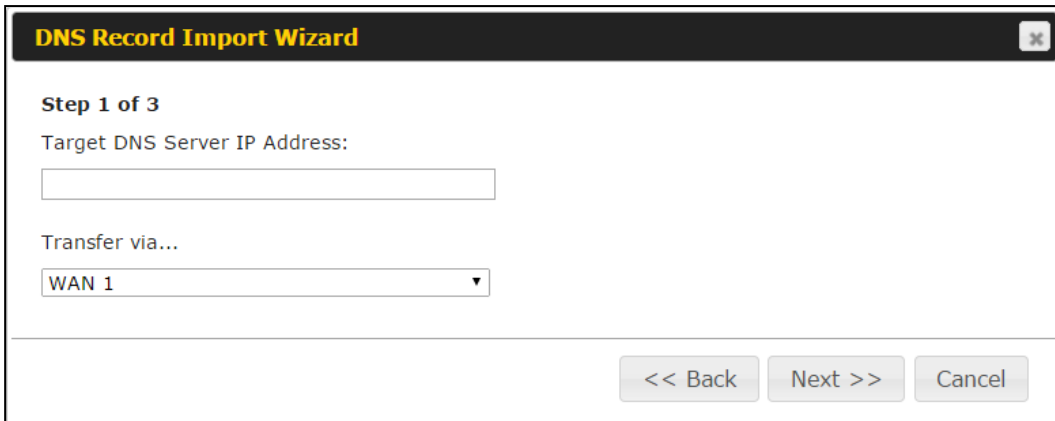
The **Points To** field defines the host name which the PTR record should be pointed to. It must be a FQDN.

18.5 DNS Record Import Wizard

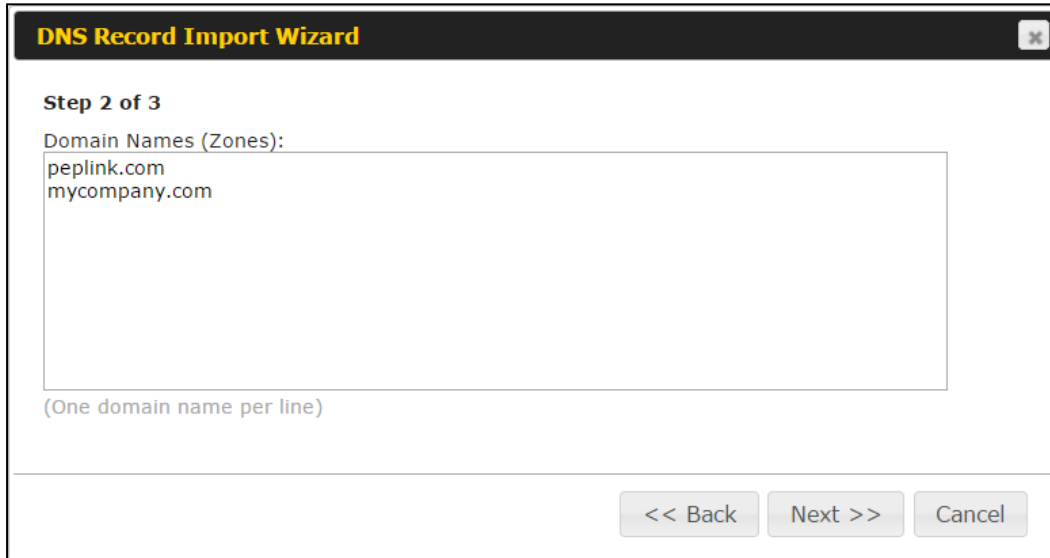
At the bottom of the DNS settings page, the link **Import records via zone transfer...** is used to import DNS record using an import wizard.



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



- In the **Target DNS Server IP Address** field, enter the IP address of the DNS server.
- In the **Transfer via...** field, choose the connection which you would like to transfer through.
- Select **Next >>** to continue.



DNS Record Import Wizard

Step 2 of 3

Domain Names (Zones):

peplink.com
mycompany.com

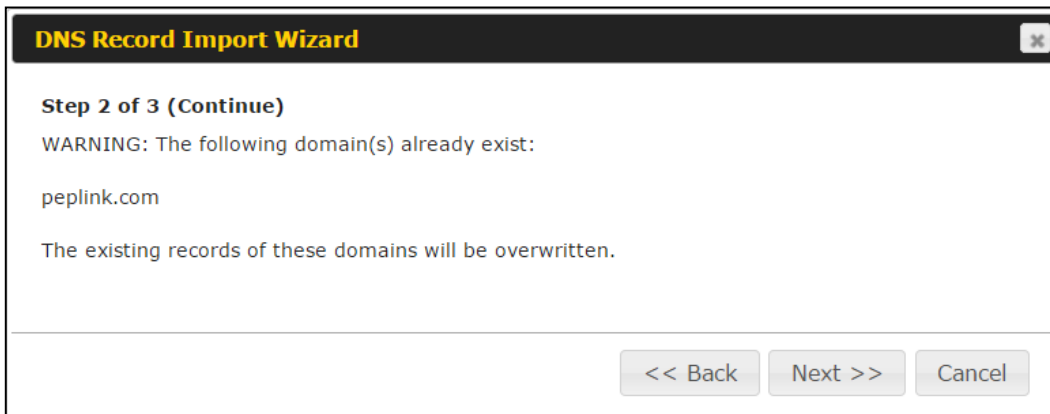
(One domain name per line)

<< Back Next >> Cancel

- In the blank space, enter the **Domain Names (Zones)** which you would like to assign the IP address entered in the previous step. Enter one domain name per line.
- Select **Next >>** to continue.

Important Note

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



DNS Record Import Wizard


Step 2 of 3 (Continue)

WARNING: The following domain(s) already exist:

peplink.com


The existing records of these domains will be overwritten.

<< Back Next >> Cancel

DNS Record Import Wizard 

Fetching zone records...

Abort

DNS Record Import Wizard 

Step 3 of 3

Fetch Results

Domain	Result	Details
peplink.com	Ok	
mycompany.com	Ok	

Cancel

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

Zone: mytest.com		
Record Type	Name	Value
SOA	mytest.com	ns1.mytest.com.
NS	mytest.com	ns1.mytest.com.
NS	mytest.com	ns2.mytest.com.
NS	mytest.com	ns3.mytest.com.
NS	mytest.com	ns4.mytest.com.
MX	mytest.com	mail01.mytest.com.
MX	mytest.com	1.us.testinglabs.com.
MX	mytest.com	backup.mytest.com.
MX	mytest.com	2.us.testinglabs.com.
A	backup.mytest.com	210.120.111.12
A	download.mytest.com	33.11.22.33
A	guest.mytest.com	126.132.111.0

19 NAT Mappings

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

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

LAN Clients	Inbound Mappings	Outbound Mappings	
192.168.1.123	(WAN 1):10.91.137.1 (Interface IP)	Use Interface IP only	
Add NAT Rule			

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

LAN Client(s)	IP Address
Address	192.168.1.123
Inbound Mappings	<div> <div>Connection / Inbound IP Address(es)</div> <div> <input checked="" type="checkbox"/> WAN 1 <div>10.91.137.1 (Interface IP)</div> </div> <div> <input 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"/> WAN 8 <input type="checkbox"/> WAN 9 <input type="checkbox"/> WAN 10 <input type="checkbox"/> WAN 11 <input type="checkbox"/> WAN 12 <input type="checkbox"/> Mobile Internet </div> </div>
Outbound Mappings	<div> <div>Connection / Outbound IP Address</div> <div> <div>WAN 1</div> <div>10.91.137.1 (Interface IP)</div> </div> <div> <div>WAN 2</div> <div>10.91.138.1 (Interface IP)</div> </div> <div> <div>WAN 3</div> <div>10.91.139.1 (Interface IP)</div> </div> <div> <div>WAN 4</div> <div>Interface IP</div> </div> <div> <div>WAN 5</div> <div>Interface IP</div> </div> <div> <div>WAN 6</div> <div>Interface IP</div> </div> <div> <div>WAN 7</div> <div>Interface IP</div> </div> <div> <div>WAN 8</div> <div>Interface IP</div> </div> <div> <div>WAN 9</div> <div>Interface IP</div> </div> <div> <div>WAN 10</div> <div>Interface IP</div> </div> <div> <div>WAN 11</div> <div>Interface IP</div> </div> <div> <div>WAN 12</div> <div>Interface IP</div> </div> <div> <div>Mobile Internet</div> <div>Interface IP</div> </div> </div>

NAT Mapping Settings	
LAN Client(s)	NAT Mapping rules can be defined for a single LAN IP Address , an IP Range , or an IP Network .
Address	This refers to the LAN host's private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when IP Address is selected.
Range	The IP range is a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when IP Range is selected.
Network	The IP network refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when IP Network is selected.
Inbound Mappings	<p>This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when IP Address is selected in the LAN Client(s) field.</p> <p>Note 1: Inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode.</p> <p>Note 2: Each WAN IP address can be associated to one NAT mapping only.</p>
Outbound Mappings	<p>This setting specifies the WAN IP addresses should be used when an IP connection is made from a LAN host to the Internet.</p> <p>Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility).</p> <p>Note 1: If you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the Outbound Policy section.</p> <p>Note 2: WAN connections in drop-in mode or IP forwarding mode are not shown here.</p>

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

Important Note
Inbound firewall rules override inbound mapping settings.

20 Captive Portal

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

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

Captive Portal Settings																													
Enable	Check Enable and then, optionally, select the LANs/VLANs that will use the captive portal.																												
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click Default .																												
Access Mode	Click Open Access to allow clients to freely access your router. Click User Authentication to force your clients to authenticate before accessing your router.																												
RADIUS Server	<p>This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:</p> <table border="1"> <tbody> <tr> <td>Authentication</td> <td colspan="3">RADIUS Server ▼</td> </tr> <tr> <td>Auth Server</td> <td><input type="text"/></td> <td>Port 1812</td> <td>Default</td> </tr> <tr> <td>Auth Server Secret</td> <td><input type="text"/></td> <td colspan="2"><input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>CoA-DM</td> <td colspan="3"><input type="checkbox"/></td> </tr> <tr> <td>Accounting Server</td> <td><input type="text"/></td> <td>Port 1813</td> <td>Default</td> </tr> <tr> <td>Accounting Server Secret</td> <td><input type="text"/></td> <td colspan="2"><input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Accounting Interim Interval</td> <td><input type="text"/></td> <td>seconds</td> <td>?</td> </tr> </tbody> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	RADIUS Server ▼			Auth Server	<input type="text"/>	Port 1812	Default	Auth Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters		CoA-DM	<input type="checkbox"/>			Accounting Server	<input type="text"/>	Port 1813	Default	Accounting Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters		Accounting Interim Interval	<input type="text"/>	seconds	?
Authentication	RADIUS Server ▼																												
Auth Server	<input type="text"/>	Port 1812	Default																										
Auth Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters																											
CoA-DM	<input type="checkbox"/>																												
Accounting Server	<input type="text"/>	Port 1813	Default																										
Accounting Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters																											
Accounting Interim Interval	<input type="text"/>	seconds	?																										

LDAP Server

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

Authentication	LDAP Server		
LDAP Server		Port 389	Default
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server		
Base DN			
Base Filter			

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



Access Quota

Set a time and data cap to each user's Internet usage.



Quota Reset Time

This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.

Allowed Networks



To whitelist a network, enter the domain name / IP address here and click . To delete an existing network from the list of allowed networks, click the  button next to the listing.

Allowed Clients

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

Splash Page

Here, you can choose between using the Balance's built-in captive portal and redirecting clients to a URL you define.

The **Portal Customization** menu has two options: **Preview** and . Clicking **Preview** will result in a pop-up previewing the captive portal that your clients will see. Clicking  will result in the appearance of following menu:

Portal Customization	
Logo Image	<input checked="" type="radio"/> No image [Use default Logo Image] <input type="radio"/> Choose File No file chosen <small>NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.</small>
Message	<div></div>
Terms & Conditions	<div>[Use default Terms & Conditions]</div>
Custom Landing Page	<input checked="" type="checkbox"/> <input type="text" value="http://"/>


Portal Customization	
Logo Image	Click the Choose File button to select an logo to use for the built-in portal.
Message	If you have any additional messages for your users, enter them in this field.
Terms & Conditions	If you would like to use your own set of terms and conditions, please enter them here. If left empty, the built-in portal will display the default terms and conditions.
Custom Landing Page	Fill in this field to redirect clients to an external URL.

21 QoS

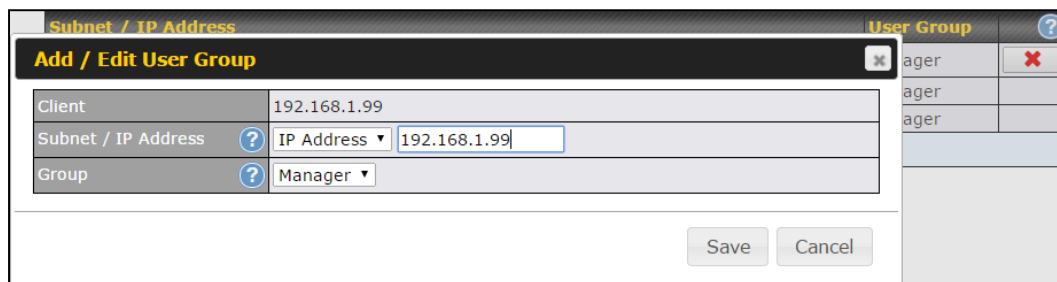
21.1 User Groups

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

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

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

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



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

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

21.2 Bandwidth Control

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

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

Group Bandwidth Reservation				
Enable	<input checked="" type="checkbox"/>			
Group Reserved Bandwidth		Manager	Staff	Guest
	% BW	50%	30%	20%
	WAN1	50.0M/50.0M	30.0M/30.0M	20.0M/20.0M
	WAN2	3.9M/4.0M	2.3M/2.4M	1.6M/1.6M
	WAN3	750k/1.0M	450k/614k	300k/410k

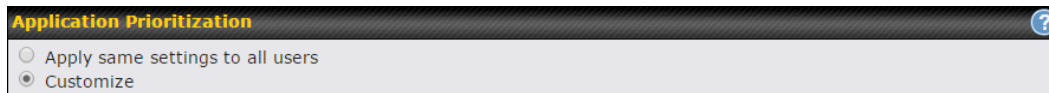
You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Managers. By default, download and upload bandwidth limits are set to unlimited (set as **0**).

Individual Bandwidth Limit				
Enable	<input checked="" type="checkbox"/>			
User Bandwidth Limit	Download		Upload	
	Manager: Unlimited		Unlimited	
	Staff:	20 Mbps	10 Mbps	(0: unlimited)
	Guest:	500 Mbps	100 Mbps	(0: unlimited)

21.3 Application

21.3.1 Application Prioritization

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



Application Prioritization [?]

☐ Apply same settings to all users

☒ Customize

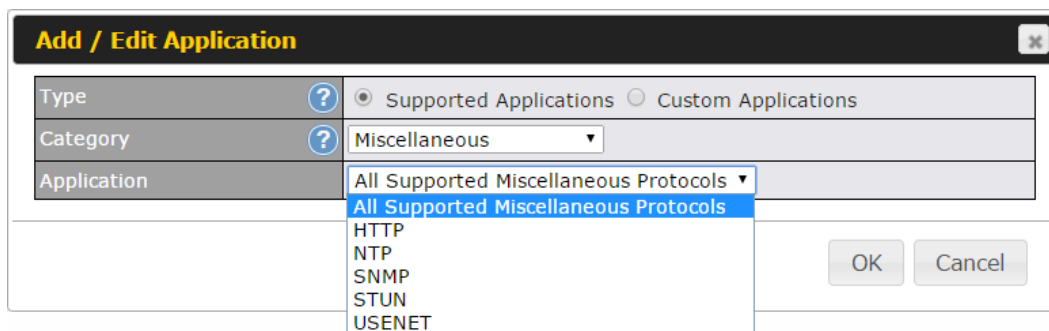
Three priority levels can be set for application prioritization: **↑ High**, **— Normal**, and **↓ Low**. The Peplink Balance can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually.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

Application	Priority			Action
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High	— Normal	↑ High	✖
All Email Protocols	↑ High	↑ High	↑ High	✖
MySQL	↑ High	— Normal	↓ Low	✖
SIP	↑ High	↓ Low	↓ Low	✖
Add				

21.3.2 Prioritization for Custom Application

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

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



Add / Edit Application [X]

Type: ☒ Supported Applications ☐ Custom Applications

Category: Miscellaneous

Application: All Supported Miscellaneous Protocols

- All Supported Miscellaneous Protocols
- HTTP
- NTP
- SNMP
- STUN
- USENET

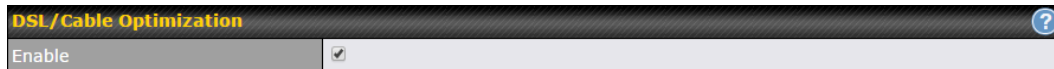
OK Cancel

Category and **Application** availability will be different across different Peplink Balance models.

21.3.3 DSL/Cable Optimization

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

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



22 Firewall

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

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

Outbound (LAN to WAN)

Inbound (WAN to LAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

Outbound Firewall Rules (🖱️ Drag and drop rows to change rule order) ?

Rule	Protocol	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Allow

Add Rule

Inbound Firewall Rules (🖱️ Drag and drop rows to change rule order) ?

Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Any	Allow

Add Rule

Apply Firewall Rules to PepVPN Traffic ?

Enabled

Intrusion Detection and DoS Prevention ?

Disabled

22.1 Outbound and Inbound Firewall Rules

22.1.1 Access Rules

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

Outbound Firewall Rules (🖱️ Drag and drop rows to change rule order) ?

Rule	Protocol	Source IP Port	Destination IP Port	Policy
Default	Any	Any	Any	Allow

Add Rule

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on
Protocol	Any <input type="button" value="Protocol Selection Tool"/>
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save

Cancel

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

Inbound Firewall Rules <small>(Drag and drop rows to change rule order)</small>						
Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy	
Default	Any	Any	Any	Any	Allow	
Add Rule						

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

Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	<input checked="" type="checkbox"/> Always on
WAN Connection	<input type="text" value="Any"/>
Protocol	<input type="text" value="Any"/> <input type="button" value="Protocol Selection Tool"/>
Source IP & Port	<input type="text" value="Any Address"/>
Destination IP & Port	<input type="text" value="Any Address"/>
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save

Cancel

Inbound / Outbound Firewall Settings

Rule Name

This setting specifies a name for the firewall rule.

Enable

This setting specifies whether the firewall rule should take effect.

If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule.

If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.

Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.

WAN Connection (Inbound)

Select the WAN connection that this firewall rule should apply to.

Protocol

This setting specifies the protocol to be matched.

Via a drop-down menu, the following protocols can be specified:

- TCP
- UDP
- ICMP
- IP

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

After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.

Source IP & Port

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

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

Destination IP & Port

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

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

Action

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

- Source IP & port
- Destination IP & port

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

Event Logging

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

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

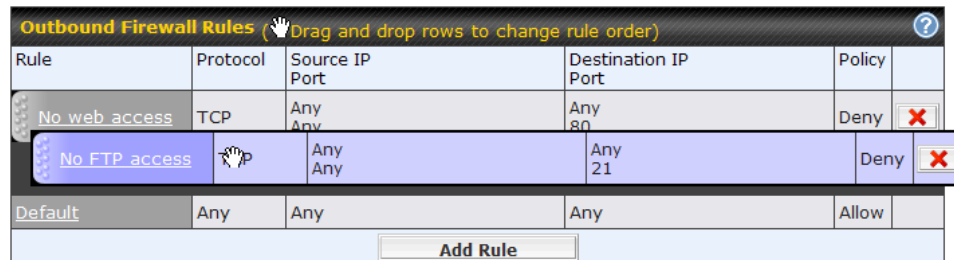
- **CONN:** The connection where the log entry refers to
- **SRC:** Source IP address
- **DST:** Destination IP address
- **LEN:** Packet length

- **PROTO:** Protocol
- **SPT:** Source port
- **DPT:** Destination port

Click **Save** to store your changes. To create an additional firewall rule, click **Add Rule** and repeat the above steps.

To change a rule's priority, simply drag and drop the rule:

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



To remove a rule, click the  button.

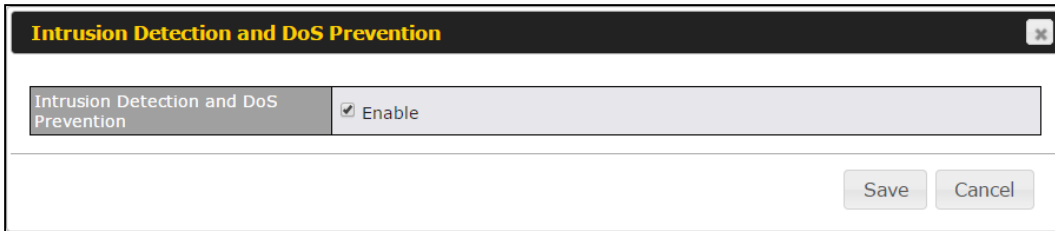
Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default** rule will be applied.


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

Tip

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

22.1.2 Intrusion Detection and DoS Prevention



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

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

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

22.1.3 Content Blocking

Application Blocking	
Please Select Application... +	

Web Blocking	
Preset Category	
<input type="radio"/> High <input type="radio"/> Moderate <input type="radio"/> Low <input checked="" type="radio"/> Custom	<div> <input type="checkbox"/> Abortion <input type="checkbox"/> Alcohol <input type="checkbox"/> Dating <input type="checkbox"/> Entertainment <input type="checkbox"/> Gambling <input type="checkbox"/> Instant Messaging <input type="checkbox"/> Lingerie <input type="checkbox"/> Nudity <input type="checkbox"/> Phishing <input type="checkbox"/> Radio <input type="checkbox"/> Search Engines <input type="checkbox"/> Sports <input type="checkbox"/> Update Sites <input type="checkbox"/> Viruses <input type="checkbox"/> Webmail </div> <div> <input type="checkbox"/> Adware <input type="checkbox"/> Anti-Spyware <input type="checkbox"/> Drugs <input type="checkbox"/> File Hosting <input type="checkbox"/> Games <input type="checkbox"/> Job Search/Employment <input type="checkbox"/> Malware <input type="checkbox"/> News/Media <input type="checkbox"/> Pornography <input type="checkbox"/> Remote Access <input type="checkbox"/> Sexuality Education <input type="checkbox"/> Spyware <input type="checkbox"/> Vacation <input type="checkbox"/> Weapons <input type="checkbox"/> WebTV </div> <div> <input type="checkbox"/> Aggressive <input type="checkbox"/> Chatroom <input type="checkbox"/> Ecommerce/Shopping <input type="checkbox"/> P2P/File sharing <input type="checkbox"/> Hacking <input type="checkbox"/> Kids Time Wasting <input type="checkbox"/> Manga/Anime/Webcomic <input type="checkbox"/> Auctions <input type="checkbox"/> Proxy/Anonymizer <input type="checkbox"/> Ringtones <input type="checkbox"/> Social Networking <input type="checkbox"/> Tobacco <input type="checkbox"/> Violence <input type="checkbox"/> Weather </div>
Customized Domains	
cbs.com	✖
	+
Exempted Domains from Web Blocking	
	+

Exempted User Groups	
Manager	<input type="checkbox"/> Exempt
Staff	<input type="checkbox"/> Exempt
Guest	<input type="checkbox"/> Exempt

Exempted Subnets	
Network	Subnet Mask
	255.255.255.0 (/24) +

URL Logging	
Enable	<input type="checkbox"/>
Log Server Host	Port: <input type="text"/>

22.1.3.1 Application Blocking

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

22.1.3.2 Web Blocking

Defines web site domain names to be blocked from LAN/PPTP/PepVPN peer clients'

access except for those on the Exempted User Groups or Exempted Subnets defined below.

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

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

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

22.1.3.3 Customized Domains

Enter an appropriate website address, and the Peplink Balance will block and disallow LAN/PPTP/SpeedFusion™ peer clients to access these websites. Exceptions can be added using the instructions in **Sections 22.1.3.4** and **22.1.3.5**.

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

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

22.1.3.4 Exempted User Groups

Check and select pre-defined user group(s) who can be exempted from the access blocking rules. User groups can be defined at **QoS>User Groups** section. Please refer to **Section 21.1** for details.

22.1.3.5 Exempted Subnets

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

22.1.3.6 URL Logging

Click **enable**, and then enter the ip address and port (if applicable) where your remote syslog server is located.

23 OSPF & RIPv2

The Peplink Balance supports OSPF and RIPv2 dynamic routing protocols. Click the **Network** tab from the top bar, and then click the **OSPF & RIPv2** item on the sidebar to reach the following menu:

OSPF	
Router ID	<input checked="" type="radio"/> LAN IP Address <input type="radio"/> Custom: <input type="text"/>
Area	Interfaces
0	PepVPN
<input type="button" value="Add"/>	

RIPv2	
No RIPv2 Defined. <input type="button" value="Add"/>	

OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the LAN IP address. If you want to specify your own ID, enter it in the Custom field.
Area	This is an overview of the OSPFv2 areas you have defined. Click on the area name to configure it. To set a new area, click Add . To delete an existing area, click <input type="button" value="X"/> .

OSPF Settings

Area ID

Link Type

☒ Broadcast
☐ Point-to-Point

Authentication

MD5


Interfaces


☐ LAN (192.168.168.1/24)
☐ V167 (192.168.167.1/24)
☐ WAN 1 (10.91.137.1/24)
☐ WAN 2 (10.91.138.1/24)
☐ WAN 3 (10.91.139.1/24)
☐ WAN 4
☐ WAN 5
☐ WAN 6
☐ WAN 7
☐ WAN 8
☐ WAN 9
☐ WAN 10
☐ WAN 11
☐ WAN 12

OK

Cancel

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

To access RIPv2 settings, click .

RIPv2 Settings 

Authentication	None ▾
Interfaces	<div><input type="checkbox"/> LAN (192.168.168.1/24) <input type="checkbox"/> V167 (192.168.167.1/24) <input type="checkbox"/> WAN 1 (10.91.137.1/24) <input type="checkbox"/> WAN 2 (10.91.138.1/24) <input type="checkbox"/> WAN 3 (10.91.139.1/24) <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input type="checkbox"/> WAN 6 <input type="checkbox"/> WAN 7 <input type="checkbox"/> WAN 8 <input type="checkbox"/> WAN 9 <input type="checkbox"/> WAN 10 <input type="checkbox"/> WAN 11 <input type="checkbox"/> WAN 12</div>

OK

Cancel

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


24 Remote User Access

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

Remote User Access Settings											
Enable	<input checked="" type="checkbox"/>										
VPN Type	<input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <small>IPsec NAT-Traversal will be enabled to ensure compatibility for most of the devices</small>										
Preshared Key	<input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters										
Listen On	Connection / IP Address(es)										
	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> 10.10.12.47 (Interface IP)									
	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> Interface IP									
	<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> Interface IP									
	<input checked="" type="checkbox"/> Mobile Internet	<input checked="" type="checkbox"/> Interface IP									
User Accounts	<table border="1"> <thead> <tr> <th>Username</th> <th>Password</th> <th></th> </tr> </thead> <tbody> <tr> <td>admin</td> <td>.....</td> <td>X</td> </tr> <tr> <td></td> <td></td> <td>+</td> </tr> </tbody> </table>	Username	Password		admin	X			+	
	Username	Password									
	admin	X								
		+									

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

corresponding row.

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

Miscellaneous Settings

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

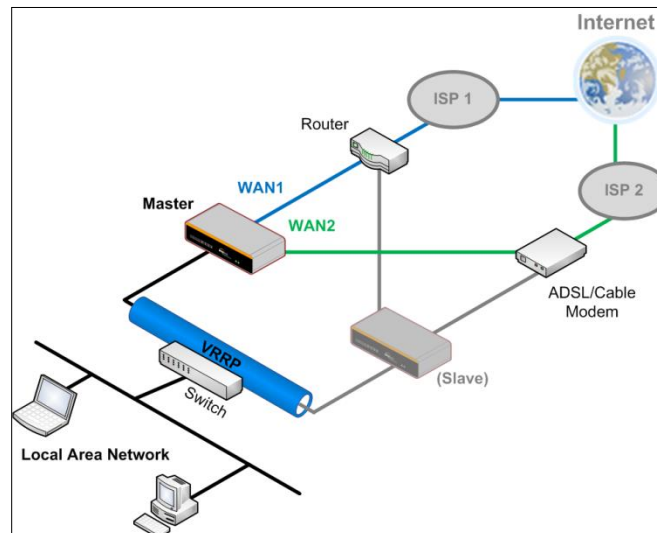
24.1 High Availability

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

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

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

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



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

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

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

once again become active.

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

Interface for Master Router

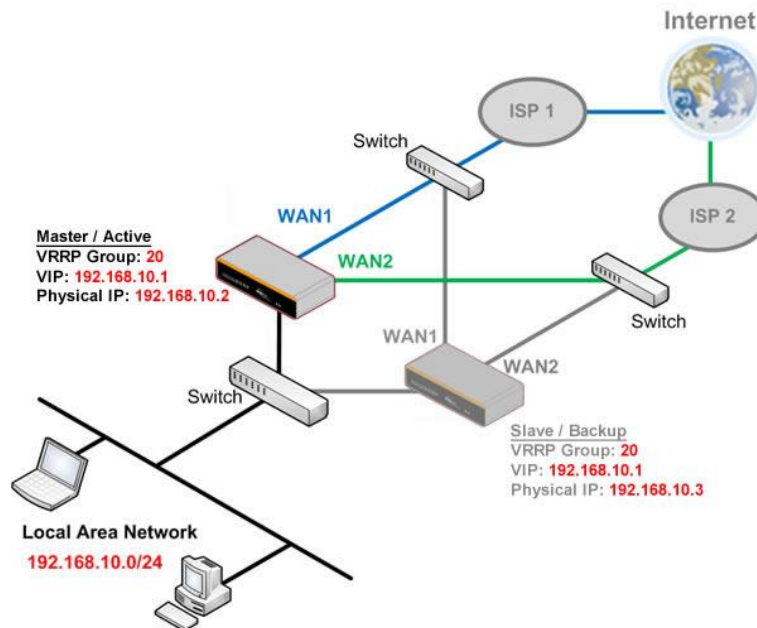
Interface for Slave Router

High Availability		High Availability	
Enable	<input checked="" type="checkbox"/>	Enable	<input checked="" type="checkbox"/>
Group Number	5	Group Number	5
Preferred Role	<input checked="" type="radio"/> Master <input type="radio"/> Slave	Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/> Slave
Resume Master Role Upon Recovery	<input checked="" type="checkbox"/>	Configuration Sync.	<input type="checkbox"/> Master Serial Number: 54BF-5WEY-E37Q
Virtual IP		Virtual IP	
LAN Administration IP	192.168.1.1	LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0

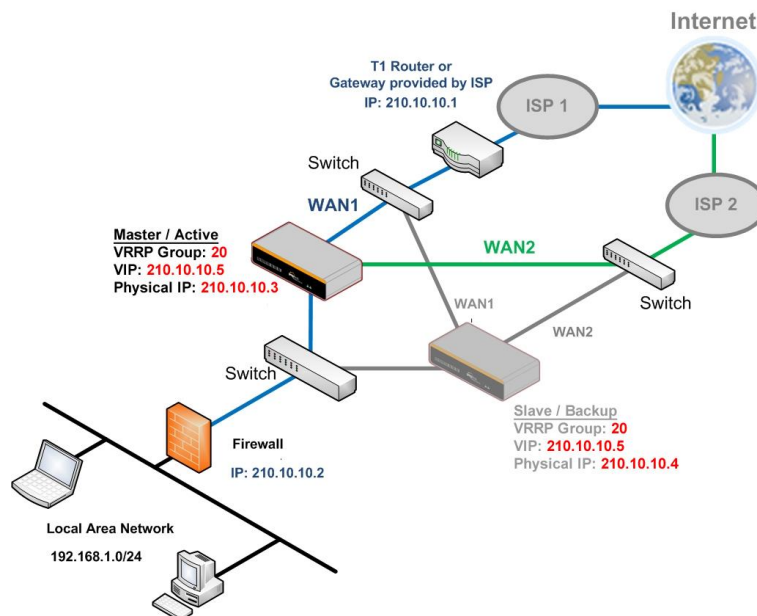
High Availability	
Enable	Checking this box specifies that the Peplink Balance unit is part of a high availability configuration.
Group Number	This number identifies a pair of Peplink Balance units operating in a high availability configuration. The two Peplink Balance units in the pair must have the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

Important Note

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




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



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




24.2 Certificate Manager

Certificate Manager		
VPN Certificate	 No Certificate	Assign
Web Admin SSL Certificate	 No Certificate	Assign
Captive Portal SSL Certificate	No Certificate	Assign

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

24.3 Service Forwarding

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

SMTP Forwarding Setup 	
SMTP Forwarding	<input type="checkbox"/> Enable
Web Proxy Forwarding Setup 	
Web Proxy Forwarding	<input type="checkbox"/> Enable
DNS Forwarding Setup 	
Forward Outgoing DNS Requests to Local DNS Proxy	<input type="checkbox"/> Enable
Custom Service Forwarding Setup	
Custom Service Forwarding	<input type="checkbox"/> Enable

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

24.3.1 SMTP Forwarding

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

SMTP Forwarding Setup			
SMTP Forwarding		<input checked="" type="checkbox"/> Enable	
Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	<input type="checkbox"/>		
WAN 2	<input checked="" type="checkbox"/>	22.2.2.2	25
WAN 3	<input checked="" type="checkbox"/>	33.3.3.2	25
WAN 4	<input type="checkbox"/>		

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

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

Note

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see **Section 17.1**).

24.3.2 Web Proxy Forwarding

Web Proxy Forwarding Setup			
Web Proxy Forwarding		<input checked="" type="checkbox"/> Enable	
Web Proxy Interception Settings			
Proxy Server		IP Address <input type="text" value="123.123.11.22"/> Port <input type="text" value="8080"/> (Current settings in users' browser)	
Connection	Enable Forwarding?	Proxy Server IP Address : Port	
WAN 1	<input type="checkbox"/>		
WAN 2	<input checked="" type="checkbox"/>	22.2.2.2 : 8765	
WAN 3	<input checked="" type="checkbox"/>	33.3.3.2 : 8080	
WAN 4	<input type="checkbox"/>		

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

destination.

24.3.3 DNS Forwarding

DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	<input checked="" type="checkbox"/> Enable

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

24.3.4 Custom Service Forwarding

Custom Service Forwarding Setup			
Custom Service Forwarding	<input checked="" type="checkbox"/> Enable		
Settings	TCP Port	Server IP Address	Server Port
	<input type="text"/>	<input type="text"/>	<input type="text"/> <input type="button" value="+"/>

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

24.4 Service Passthrough

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

Service Passthrough Support	
SIP	<input checked="" type="radio"/> Standard Mode <input type="radio"/> Compatibility Mode <input checked="" type="checkbox"/> Define custom signal ports 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>
H.323	<input checked="" type="checkbox"/> Enable
FTP	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Define custom control ports 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>
TFTP	<input checked="" type="checkbox"/> Enable
IPsec NAT-T	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Define custom ports 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> <input checked="" type="checkbox"/> Route IPsec Site-to-Site VPN via <input type="text" value="WAN 1"/>

(Registered trademarks are copyrighted by their respective owner)

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

Service Passthrough Support	
SIP	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Peplink Balance can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets

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

25 AP

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

Special Note

With the installation of Firmware 6.2.1 and upwards, full AP support is included free.

25.1 AP Controller

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

AP Controller	
AP Management	<input checked="" type="checkbox"/>
Support Remote AP	<input checked="" type="checkbox"/>
Permitted AP	<input type="radio"/> Any <input checked="" type="radio"/> Approved List <div style="border: 1px solid black; height: 100px; width: 100%;"></div> <p>(One serial number per line)</p>

AP Controller

AP Management

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

Support Remote AP

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

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

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

DNS Proxy Settings					
Enable	<input checked="" type="checkbox"/>				
DNS Caching	<input type="checkbox"/>				
Include Google Public DNS Servers	<input type="checkbox"/>				
Local DNS Records	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td>wlancontroller</td> <td>10.10.10.1</td> </tr> </tbody> </table>	Host Name	IP Address	wlancontroller	10.10.10.1
Host Name	IP Address				
wlancontroller	10.10.10.1				

Permitted AP

Access points to manage can be specified here. If **Any** is selected, the AP controller will manage any AP that reports to it. If **Approved List** is selected, only APs with serial numbers listed in the provided text box will be managed.

25.2 Wireless SSID

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

SSID	Security Policy
PEPLINK_E73D	WPA/WPA2 - Personal
<input type="button" value="New SSID"/>	


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


SSID
✕

SSID Settings	
SSID	<input type="text"/>
VLAN ID	LAN (No VLAN) ▼
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Multicast Filter	<input type="checkbox"/>
Multicast Rate	MCS8/MCS0/6M ▼
IGMP Snooping	<input type="checkbox"/>
Layer 2 Isolation	<input type="checkbox"/>
Band Steering	Disable ▼

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
VLAN ID	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is 0 , which means VLAN tagging is disabled (instead of tagged with zero).

Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate ^A	Select Auto to allow the Peplink Balance to set the data rate automatically, or select Fixed and choose a rate from the displayed drop-down menu.
Multicast Filter ^A	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate ^A	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected Protocol and Channel Bonding settings will affect the rate options and values available here.
IGMP Snooping ^A	To allow the Peplink Balance to listen to internet group management protocol (IGMP) network traffic, select this option.
DHCP Option 82 ^A	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
Network Priority (QoS) ^A	Select from Gold , Silver , and Bronze to control the QoS priority of this wireless network's traffic.
Layer 2 Isolation ^A	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
Band Steering ^A	Band steering allows the Peplink Balance to steer AP clients from the 2.4 GHz band to the 5GHz band for better usage of bandwidth. To make steering mandatory, select Enforce . To cause the Peplink Balance to preferentially choose steering, select Prefer . The default for this setting is Disable .

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

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Shared Key	<input type="text"/> <div>  <input checked="" type="checkbox"/> Hide Characters </div>

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

Access Control	
Restricted Mode	None

Access Control

Restricted Mode

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

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

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

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

MAC Address List

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

RADIUS Server Settings	Primary Server	Secondary Server
Host	<input type="text"/>	<input type="text"/>
Secret	<input type="text"/>	<input type="text"/>
Authentication Port	1812 <input type="button" value="Default"/>	1812 <input type="button" value="Default"/>
Accounting Port	1813 <input type="button" value="Default"/>	1813 <input type="button" value="Default"/>

RADIUS Server Settings

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

Guest Protect			
Block All Private IP	<input type="checkbox"/>		
Custom Subnet	Network	Subnet Mask	
	<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>
Block Exception	Network	Subnet Mask	
	<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>
Block PepVPN	<input type="checkbox"/>		

Guest Protect	
Block All Private IP	Check this box to deny all connection attempts by private IP addresses.
Custom Subnet	To create a custom subnet for guest access, enter the IP address and choose a subnet mask from the drop-down menu. To add the new subnet, click <input type="button" value="+"/> . To delete a custom subnet, click <input type="button" value="X"/> .
Block Exception	To block access from a particular subnet, enter the IP address and choose a subnet mask from the drop-down menu. To add the new subnet, click <input type="button" value="+"/> . To delete a blocked subnet, click <input type="button" value="X"/> .
Block PepVPN	To block PepVPN access, check this box.

Bandwidth Management	
Upstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)
Downstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)
Client Upstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)
Client Downstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)
Max Number of Clients	<input type="text" value="0"/> (0: Unlimited)

Bandwidth Management	
Upstream Limit	Enter a value in kbps to limit the wireless network's upstream bandwidth. Enter 0 to allow unlimited upstream bandwidth.
Downstream Limit	Enter a value in kbps to limit the wireless network's downstream bandwidth. Enter 0 to allow unlimited downstream bandwidth.
Client Upstream Limit	Enter a value in kbps to limit connected clients' upstream bandwidth. Enter 0 to allow unlimited upstream bandwidth.
Client	Enter a value in kbps to limit connected clients' downstream bandwidth. Enter 0 to allow


Downstream Limit unlimited downstream bandwidth.

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

Firewall Settings			
Firewall Mode	Lockdown - Block all except... ▼		
Firewall Exceptions	Name	Type	Item
New Rule			

Firewall Settings

Firewall Mode

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

Firewall Rule	
Name	<input type="text"/>
Type	Port ▼
Protocol	TCP ▼
Port	Any Port ▼
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Firewall Rule

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

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

Protocol / Port

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

IP Address / Subnet Mask

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

MAC Address

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

25.3 Profiles

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

Name	Used by	Action
1. Default	(None)	Clone
New AP Profile		

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


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

AP Profile

AP Settings

AP Profile Name		
SSID	<input type="checkbox"/> 2.4 GHz <input type="checkbox"/> 5 GHz <input type="checkbox"/> PEPLINK_01AA	
Operating Country	United States	
Preferred Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz	
5 GHz Protocol	802.11n/ac	
5 GHz Channel Width	20 MHz	
5 GHz Channel	Auto	<input type="button" value="Edit"/> Channels: 36 40 44 48 ...
2.4 GHz Protocol	802.11ng	
2.4 GHz Channel Width	20 MHz	
2.4 GHz Channel	1 (2.412 GHz)	
Management VLAN ID	0	(0: Untagged)
Power Boost	<input type="checkbox"/>	
Output Power	Dynamic: Auto	
Operating Schedule	<input checked="" type="radio"/> Always On <input type="radio"/> Custom Schedule	
Max number of Clients	0	(0: Unlimited)
Client Signal Strength Threshold	0	(0: Unlimited)
Beacon Rate	1Mbps	<input type="button" value="Default"/>
Beacon Interval	100ms	
DTIM	1	<input type="button" value="Default"/>
RTS Threshold	0	<input type="button" value="Default"/>
Slot Time	9 μ s	<input type="button" value="Default"/>
ACK Timeout	48 μ s	<input type="button" value="Default"/>
Frame Aggregation	<input checked="" type="checkbox"/>	
Frame Length	50000	<input type="button" value="Default"/>


AP Settings	
AP Profile Name	This field specifies the name of this AP profile.
SSID	These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Peplink Balance does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.
Operating Country	<p>This drop-down menu specifies the national / regional regulations which the AP should follow.</p> <ul style="list-style-type: none"> • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). <p>NOTE: Users are required to choose an option suitable to local laws and regulations. Per FCC regulation, the country selection is not available on all models marketed in US. All US models are fixed to US channels only.</p>
Preferred Frequency	These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies.
5 GHz Protocol	This section displays the 5 GHz protocols your APs are using.
5GHz Channel Bonding	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
5 GHz Channel	This drop-down menu selects the 5 GHz 802.11 channel to be utilized. If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
2.4 GHz Protocol	This section displays the 2.4 GHz protocols your APs are using.
2.4 GHz Channel Bonding	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
2.4 GHz Channel	This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is 0 by default, meaning that no VLAN tagging will be applied. NOTE: change this value with caution as alterations may result in loss of connection to the AP controller.
Power Boost^A	With this option enabled, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to

	increased interference.
Output Power^A	<p>This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When Dynamic settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance.</p> <p>The Dynamic: Auto setting will set the AP to do this automatically. Otherwise, the Dynamic: Manual setting will set the AP to dynamically adjust only of instructed to do so. If you have set Dynamic:Manual, you can go to AP>Toolbox>Auto Power Adj. to give your AP further instructions.</p>
Operating Schedule^A	<p>These buttons determine the time period at which the AP under this profile will be activated. Clicking the Custom Schedule option will open the following diagram:</p>  <p>Click the desired time periods to toggle the activation state of APs under this profile.</p>
Max number of Clients^A	This field determines the maximum clients that can be connected to APs under this profile.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Beacon Rate^A	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are 1Mbps , 2Mbps , 5.5Mbps , 6Mbps , and 11Mbps .
Beacon Interval^A	This drop-down menu provides the option to set the time between each beacon send. Available options are 100ms , 250ms , and 500ms .
DTIM^A	This field provides the option to set the frequency for beacon to include delivery traffic indication messages (DTIM). The interval unit is measured in milliseconds.
RTS Threshold^A	This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.
Slot Time^A	This field provides the option to modify the unit wait time before it transmits. The default value is 9μs .
ACK Timeout^A	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is 48μs .
Frame	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.

Aggregation^A

Frame Length

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

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

Web Administration Settings (on External AP)	
Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	443
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username	admin
Admin Password	ebb7a61c9901 <input type="button" value="Generate"/>

Web Administration Settings

Enable

Check the box to allow Peplink Balance to manage the web admin access information of the AP.

Web Access Protocol

These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are **HTTP** and **HTTPS**.

Management Port

This field specifies the management port used for accessing the device.

HTTP to HTTPS Redirection

This option will be available if you have chosen **HTTPS** as the **Web Access Protocol**. With this enabled, any HTTP access to the web admin will redirect to HTTPS automatically.

Admin User Name

This field specifies the administrator username of the web admin. It is set as *admin* by default.

Admin Password

This field allows you to specify a new administrator password. You may also click the **Generate** button and let the system generate a random password automatically.

AP Time Settings	
Time Zone	<input type="radio"/> Follow controller time zone selection <input checked="" type="radio"/> (GMT-08:00) Pacific Time (US & Canada)
Time Server	<input checked="" type="radio"/> Follow controller NTP server selection <input type="radio"/>

AP Time Settings

Time Zone

Check the box to allow the Peplink Balance to manage the web admin access information of the AP.

Time Server

These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are **HTTP** and **HTTPS**.

AP Controller Settings	
Client Load Balancing	<input checked="" type="checkbox"/>
Coverage Redundancy	High

AP Controller Settings	
Client Load Balancing	Check the box to turn on client load balancing.
Coverage Redundancy	Select the degree of coverage redundancy to use. Available values are Low , Medium , and High .

25.4 Info

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



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

SSID	The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs.
No. of APs	This pie chart and table indicates how many APs are online and how many are offline.
No. of Clients	This graph displays the number of clients connected to each network at any given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time.
Data Usage	This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to Zoom to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
		More...

Events

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

25.5 Usage

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

Search Filter						
AP Name / Serial Number / SSID	<input type="text" value="All"/> <input type="checkbox"/> Include Offline APs					
Search Result						

Managed APs						
						Expand Collapse
Name	IP Address	MAC	Location	Firmware Pack ID	Configuration	
▼ Default (8/9 online)						
<input type="checkbox"/> JES-A817-BCC	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None	<input checked="" type="checkbox"/> - View Edit



Usage




AP Name/Serial Number


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

Online Status

This button toggles whether your search will include offline devices.


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

On the right of the table, you will see the following icons:   .

Click the  icon to see a usage table for each client:


Client List						
MAC Address	IP Address	Type	Signal	SSID	Upload	Download
80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB

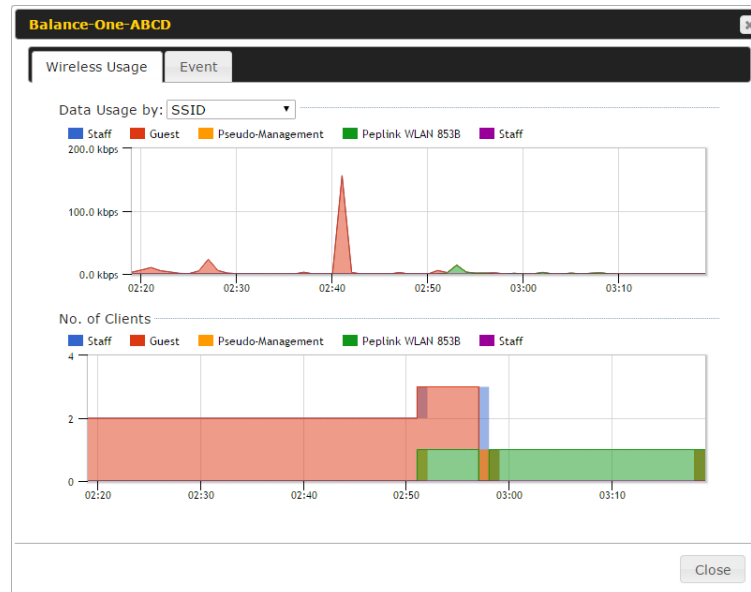
Managed Wireless Devices

Click the  icon to configure each client

AP Details	
Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:E0
Product Name	Pepwave AP Pro Duo
Name	<input type="text"/>
Location	<input type="text"/>
Firmware Version	3.5.2
Firmware Pack	Default (None) ▼
AP Client Limit	<input checked="" type="radio"/> Follow AP Profile <input type="radio"/> Custom
2.4 GHz SSID List	T4Open
5 GHz SSID List	T4Open
Last config applied by controller	Mon Nov 23 11:25:03 HKT 2015
Uptime	Wed Nov 11 15:00:27 HKT 2015
Current Channel	1 (2.4 GHz) 153 (5 GHz)
Channel	2.4 GHz: Follow AP Profile ▼ 5 GHz: Follow AP Profile ▼
Output Power	2.4 GHz: Follow AP Profile ▼ 5 GHz: Follow AP Profile ▼

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

Click the  icon to see a graph displaying usage:



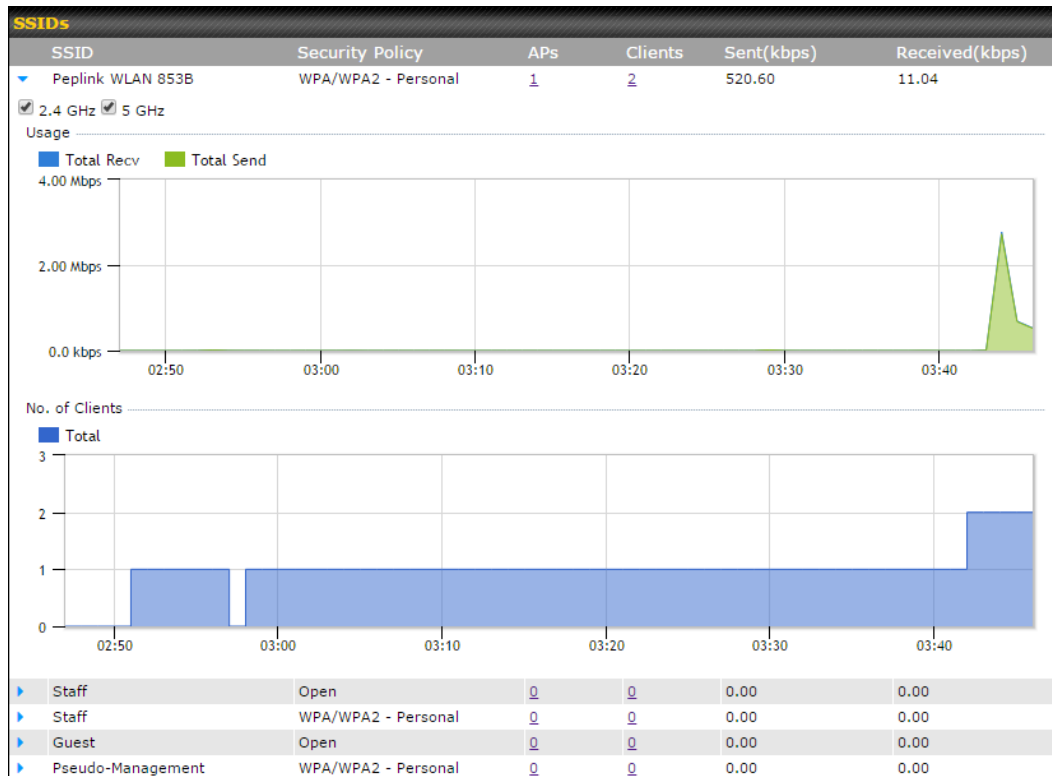
Click any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can display the information by SSID or by AP send/receive rate.

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

Event Information	
Events	
Jan 2 11:53:39	Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 11:39:31	Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:16:55	Client A8:BB:CF:E1:0F:1E disassociated from Balance_11a
Jan 2 11:11:54	Client A8:BB:CF:E1:0F:1E associated with Balance_11a
Jan 2 11:10:45	Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 11:00:36	Client 00:21:6A:35:59:A4 associated with Balance_11a
Jan 2 11:00:20	Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 10:59:09	Client 00:21:6A:35:59:A4 disassociated from Balance_11a
Jan 2 10:42:28	Client F4:B7:E2:16:35:E9 associated with Balance_11a
Jan 2 10:29:12	Client 84:7A:88:78:1E:4B associated with Balance_11a
Jan 2 10:24:27	Client 90:B9:31:0D:11:EC disassociated from Marketing_11a
Jan 2 10:24:27	Client 90:B9:31:0D:11:EC roamed to Marketing_11a at 2830-BFC8-D230
Jan 2 10:13:22	Client E8:8D:28:A8:43:93 associated with Balance_11a
Jan 2 10:13:22	Client E8:8D:28:A8:43:93 roamed to Balance_11a from 2830-BF7F-694C
Jan 2 10:07:52	Client CC:3A:61:89:07:F3 associated with Wireless_11a
Jan 2 10:04:35	Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 10:03:38	Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 09:58:27	Client 00:26:BB:08:AC:FD disassociated from Wireless_11a
Jan 2 09:52:46	Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 09:20:26	Client 8C:3A:E3:3F:17:62 associated with Balance_11a
More...	

25.6 SSID

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



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

25.7 Wireless Client

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

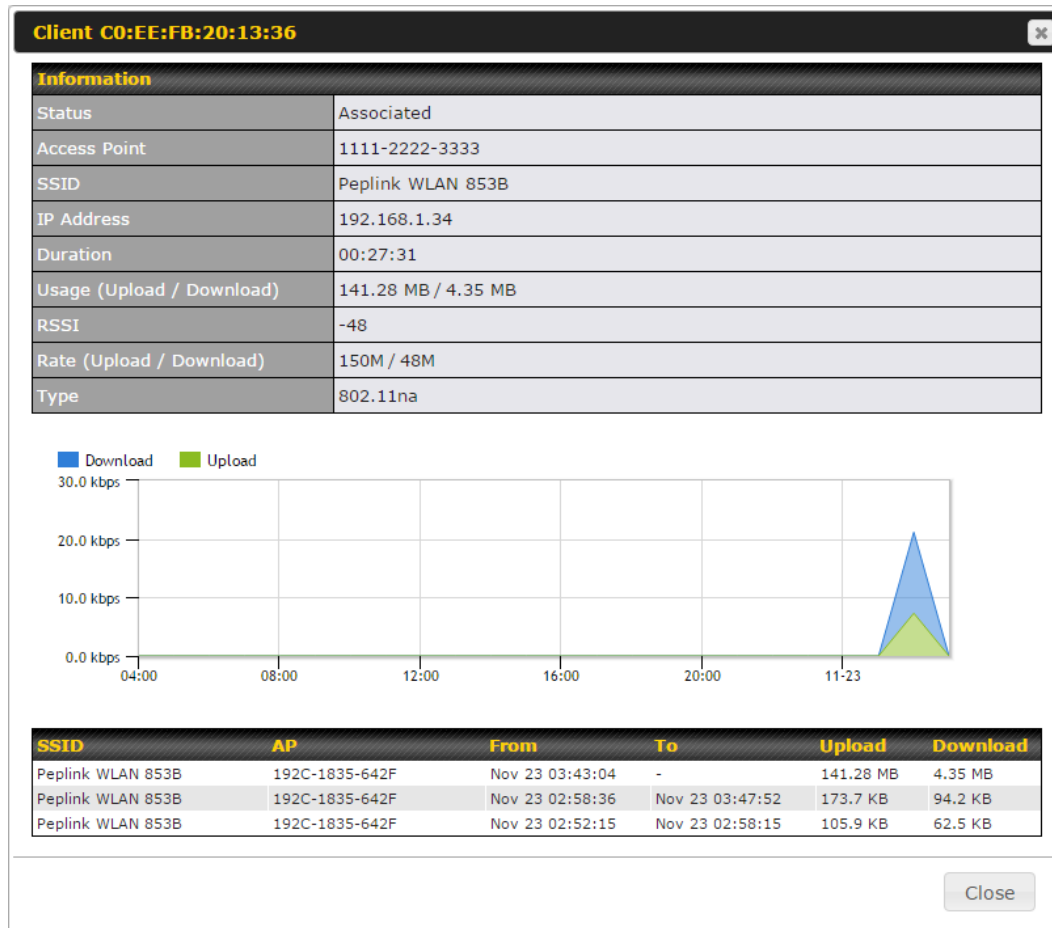
Search Filter

Client MAC / SSID / AP Serial Number	<input type="text"/>
Maximum Result (1-256)	<input type="text" value="50"/>
Search Result	<input type="button" value="Search"/>

Top 10 Clients of last hour (Updated at 03:00)

Client MAC Address	Upload	Download	
C0:EE:FB:20:13:36	53.5 KB	101.4 KB	☆

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





25.8 Rogue AP

A listing of suspected rogue devices can be accessed by navigating to **AP>Rogue AP**.

Suspected Rogue APs					
BSSID	SSID	Channel	Encryption	Last Seen	Mark as
00:1A:DD:EC:25:22	Wireless	11	WPA2	10 hours ago	✓ ⊗
00:1A:DD:EC:25:23	Accounting	11	WPA2	10 hours ago	✓ ⊗
00:1A:DD:EC:25:24	Marketing	11	WPA2	11 hours ago	✓ ⊗
00:03:7F:00:00:00	MYB1PUSH	1	WPA & WPA2	11 minutes ago	✓ ⊗
00:03:7F:00:00:01	MYB1	1	WPA2	15 minutes ago	✓ ⊗
00:1A:DD:B9:60:88	PEPWAVE_CB7E	1	WPA & WPA2	5 minutes ago	✓ ⊗
00:1A:DD:BB:09:C1	Micro_S1_1	6	WPA & WPA2	1 hour ago	✓ ⊗
00:1A:DD:BB:52:A8	MAX HD2 Gobi	11	WPA & WPA2	2 minutes ago	✓ ⊗
00:1A:DD:BF:75:81	PEPLINK_05B5	4	WPA & WPA2	1 minute ago	✓ ⊗
00:1A:DD:BF:75:82	LK_05B5	4	WPA2	1 minute ago	✓ ⊗
00:1A:DD:BF:75:83	LK_05B5_VLAN22	4	WPA2	1 minute ago	✓ ⊗
00:1A:DD:C1:ED:E4	dev_captive_portal_test	1	WPA & WPA2	3 minutes ago	✓ ⊗
00:1A:DD:C2:E4:C5	PEPWAVE_7052	11	WPA & WPA2	2 hours ago	✓ ⊗
00:1A:DD:C3:F1:64	dev_captive_portal_test	6	WPA & WPA2	6 minutes ago	✓ ⊗
00:1A:DD:C4:DC:24	ssid_test	8	WPA & WPA2	2 minutes ago	✓ ⊗
00:1A:DD:C4:DC:25	SSID New	8	WPA & WPA2	2 minutes ago	✓ ⊗
00:1A:DD:C5:46:04	Guest SSID	9	WPA2	2 minutes ago	✓ ⊗
00:1A:DD:C5:47:04	PEPWAVE_67B8	1	WPA & WPA2	5 minutes ago	✓ ⊗
00:1A:DD:C5:4E:24	G BR1 Portal	2	WPA2	2 minutes ago	✓ ⊗
00:1A:DD:C6:9A:48	ssid_test	8	WPA & WPA2	2 hours ago	✓ ⊗

Suspected Rogue Devices

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



25.9 Toolbox

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

Firmware Packs

Auto Power Adj.

Dynamic Channel Assignment

Pack ID	Release Date	Details	Action
1126	2013-08-26		



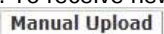

Check for Updates

Manual Upload

Default...

No default defined.

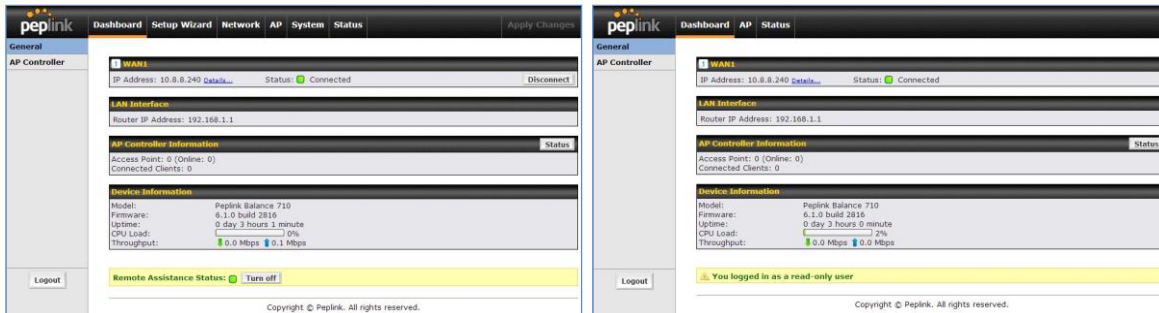
Firmware Packs

This is the first menu that will appear. Here, you can manage the firmware of your AP. Clicking on  will display information regarding each firmware pack. To receive new firmware packs, you can either press  to download new packs or you can press  to manually upload a firmware pack. Press  to define which firmware pack is default.

26 System Settings

26.1 Admin Security

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



Admin account
UI

User account
UI

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

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

Default: 4 hours 0 minutes.

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

Admin Settings ?		
Router Name	182C-124B-09DC	hostname: 182c-124b-09dc
Admin User Name	admin	
Admin Password	••••••••	
Confirm Admin Password	••••••••	
Read-only User Name	user	
User Password		
Confirm User Password		
Front Panel Passcode	<input type="checkbox"/>	
Web Session Timeout	4 Hours 0 Minutes	
Authentication by RADIUS	<input checked="" type="checkbox"/> Enable	
Auth Protocol	MS-CHAP v2	
Auth Server		Port <input type="text"/> Default
Auth Server Secret		<input checked="" type="checkbox"/> Hide Characters
Auth Timeout	3 seconds	
Accounting Server		Port <input type="text"/> Default
Accounting Server Secret		<input checked="" type="checkbox"/> Hide Characters
Restricted Admin Access	<input type="checkbox"/> by Management Port Only	
CLI SSH	<input checked="" type="checkbox"/> Enable	
CLI SSH Port	8822	Default
CLI SSH Access	LAN/WAN	
Security	HTTP	
Web Admin Port	80	Default
Web Admin Access	LAN/WAN	

Admin Settings	
Router Name	This field allows you to define a name for this Peplink Balance unit. By default, Router Name is set as Balance_XXXX , where XXXX refers to the last 4 digits of the serial number of that balance unit.
Admin User Name	Admin User Name is set as admin by default, but can be changed, if desired.
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	Read-only User Name is set as user by default, but can be changed, if desired.
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm User	This field allows you to verify and confirm the new user password.

Password	
Front Panel Passcode	To require a 4-digit passcode to access front panel controls, check this box and then select the code from the drop-down menus.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Balance terminates its access to the web admin interface. By default, it is set to 4 hours .
Authentication by RADIUS	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.
Auth Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.
Network Connection	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
Restricted Admin Access	Check this box to restrict management to administrators connected to the management port.
CLI SSH & Console	The CLI (command line interface) can be accessed via SSH. It can also be accessed from the serial console port on some Peplink Balance models. This field enables CLI support. For additional information regarding CLI, please refer to Section 22.5 .
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
Security	<p>This option is for specifying the protocol(s) through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> • HTTP • HTTPS

- HTTP/HTTPS

Web Admin Port

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

Web Admin Access

This option is for specifying the network interfaces through which the web admin interface can be accessed:

- LAN only
- LAN/WAN

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

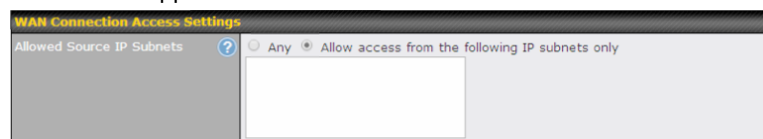


WAN Connection Access Settings

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

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

Allowed Source IP Subnets



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

To define multiple subnets, separate each IP subnet, one per line. For example:

192.168.0.0/24

10.8.0.0/16


Allowed WAN IP Address(es)

This is to choose which WAN IP address(es) the web server should listen on.


Allowed WAN IP Address(es)	Connection / IP Address(es)	All	Clear
	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.91.137.1 (Interface IP)	
	<input checked="" type="checkbox"/> WAN 2	<input checked="" type="checkbox"/> 10.91.138.1 (Interface IP)	
	<input checked="" type="checkbox"/> WAN 3	<input checked="" type="checkbox"/> 10.91.139.1 (Interface IP)	

26.2 Firmware

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

Firmware Upgrade 

Current firmware version: 6.2.1
Firmware check pending

Manual Firmware Upgrade 

Firmware Image No file chosen

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

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

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

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

Firmware Upgrade Status

Status LED Information during firmware upgrade:

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

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

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

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

<http://www.peplink.com> -219 / 269 - Copyright © 2016 Peplink

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

26.4 Time

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

Time Settings	
Time Zone	(GMT+07:00) Krasnoyarsk <input type="checkbox"/> Show all
Time Server	0.peplink.pool.ntp.org <input type="button" value="Default"/>
<input type="button" value="Save"/>	

Time Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme) in which Peplink Balance operates. The Time Zone value affects the time stamps in the event log of the Peplink Balance and e-mail notifications. Check Show all to show all time zone options.
Time Server	This setting specifies the NTP network time server to be utilized by the Peplink Balance.

26.5 Email Notification

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

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	smtp.mycompany.com <input checked="" type="checkbox"/> Require authentication
SSL Encryption	<input checked="" type="checkbox"/> (Note: any server certificate will be accepted)
SMTP Port	465 <input type="button" value="Default"/>
SMTP User Name	smtpuser
SMTP Password	•••••
Confirm SMTP Password	•••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

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

Recipient's Email Address

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

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

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Send Test Notification

Cancel

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

Test email sent. Email notification settings are not saved, it will be saved after clicked the 'Save' button.

Test Result


```
[INFO] Try email through connection #3
[<-] 220 ESMTP
[->] EHLO balance
[<-] 250-smtp Hello balance [210.210.210.210]
250-SIZE 100000000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250-UTF8
```

26.6 Event Log

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

Send Events to Remote Syslog Server	
Remote Syslog	<input checked="" type="checkbox"/>
Remote Syslog Host	<input type="text"/>

Push Events to Mobile Devices	
Push Events	<input checked="" type="checkbox"/>

Remote Syslog Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
The Peplink Balance can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature.	
Push Events	<div><div>For more information on the Router Utility, go to: www.peplink.com/products/router-utility</div></div>

26.7 SNMP

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

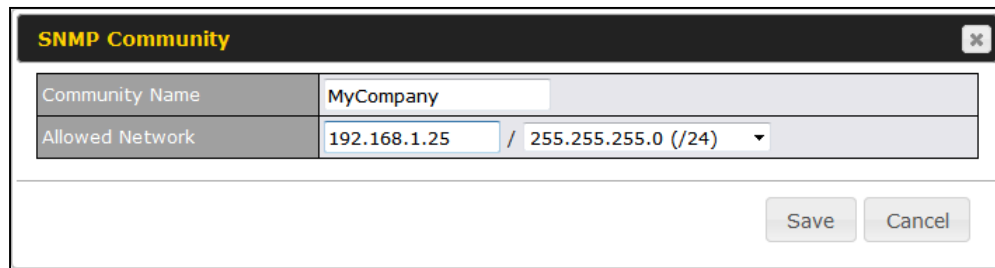
SNMP Settings	
SNMP Device Name	Balance_OD84
SNMP Port	161 <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

Community Name	Allowed Source Network	Access Mode	
MyCompany	192.168.1.20/24	Read Only	<input type="button" value="X"/>
<input type="button" value="Add SNMP Community"/>			

SNMPv3 User Name	Authentication / Privacy	Access Mode	
SNMPUser	SHA / DES	Read Only	<input type="button" value="X"/>
<input type="button" value="Add SNMP User"/>			

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

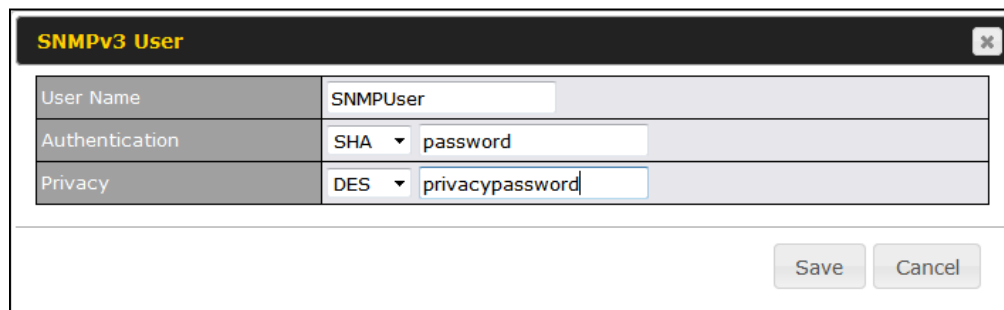
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:



The dialog box titled "SNMP Community" contains two input fields: "Community Name" with the value "MyCompany" and "Allowed Network" with the value "192.168.1.25 / 255.255.255.0 (/24)". At the bottom right are "Save" and "Cancel" buttons.

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

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



The dialog box titled "SNMPv3 User" contains three input fields: "User Name" with the value "SNMPUser", "Authentication" with a dropdown menu set to "SHA" and a password field containing "password", and "Privacy" with a dropdown menu set to "DES" and a privacy password field containing "privacypassword". At the bottom right are "Save" and "Cancel" buttons.

SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	<p>This setting specifies via a drop-down menu one of the following valid authentication protocols:</p> <ul style="list-style-type: none"> • NONE • MD5 • SHA <p>When MD5 or SHA is selected, an entry field will appear for the password.</p>
Privacy Protocol	<p>This setting specifies via a drop-down menu one of the following valid privacy protocols:</p> <ul style="list-style-type: none"> • NONE • DES <p>When DES is selected, an entry field will appear for the password.</p>

26.8 InControl

InControl Management	
InControl Management	<input checked="" type="checkbox"/> Allow InControl Management
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/> <input type="text"/>

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

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

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

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

26.9 Configuration

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

Restore Configuration to Factory Settings

Restore Factory Settings

Download Active Configurations

Download

Upload Configurations

Configuration File

Browse...

No file selected.

Upload

Upload Configurations from High Availability Pair

Configuration File

Browse...

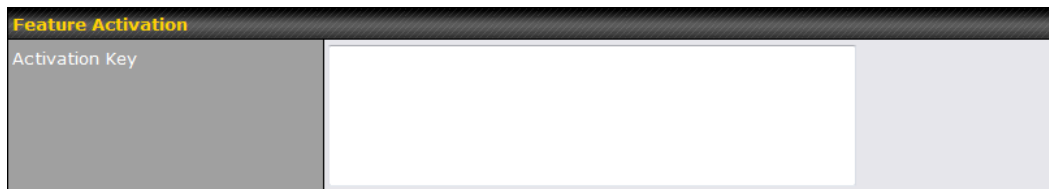
No file selected.

Upload

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

26.10 Feature Add-ons

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

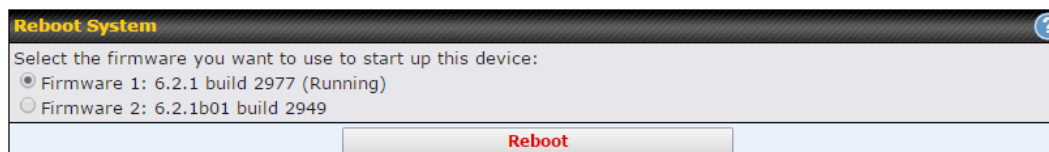


The image shows a web form titled "Feature Activation". It has a label "Activation Key" on the left and a large, empty text input field on the right.

26.11 Reboot

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

Please note that a firmware upgrade will always replace the inactive firmware partition.

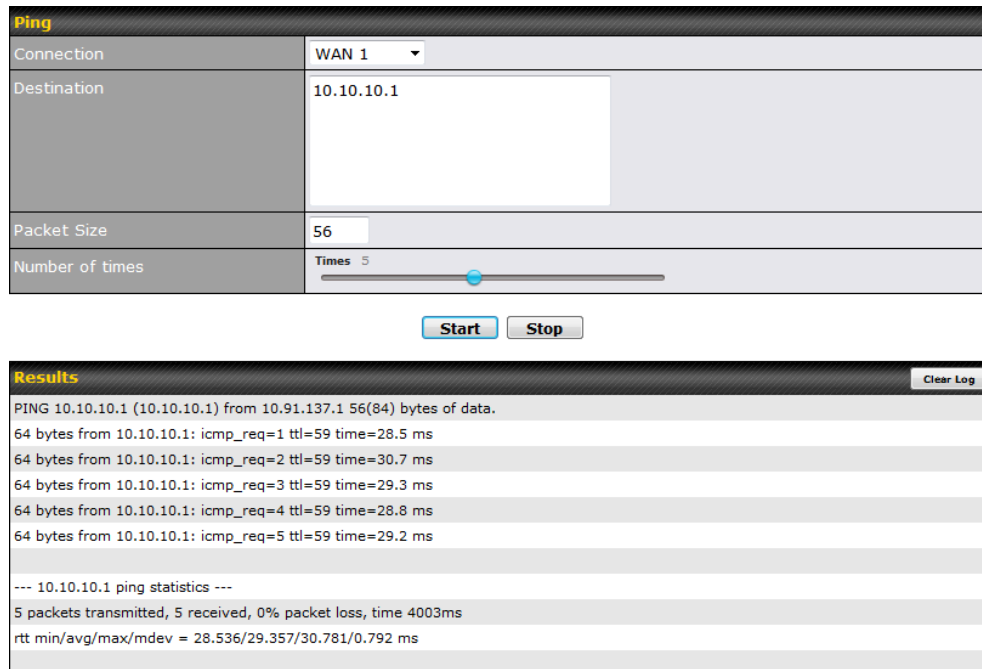


The image shows a web form titled "Reboot System" with a help icon (question mark) in the top right corner. The text inside says "Select the firmware you want to use to start up this device:". There are two radio button options: "Firmware 1: 6.2.1 build 2977 (Running)" which is selected, and "Firmware 2: 6.2.1b01 build 2949". At the bottom right, there is a button labeled "Reboot" in red text.

27 Tools

27.1 Ping

The ping test tool sends pings through a specified Ethernet interface or a SpeedFusion™ VPN connection. You can specify the number of pings in the field **Number of times** to a maximum number of 10 times. **Packet Size** can be set to a maximum of 1472 bytes. The ping utility is located at **System>Tools>Ping**, illustrated below:



Ping	
Connection	WAN 1
Destination	10.10.10.1
Packet Size	56
Number of times	Times 5

Results	
PING 10.10.10.1 (10.10.10.1) from 10.91.137.1 56(84) bytes of data.	
64 bytes from 10.10.10.1: icmp_req=1 ttl=59 time=28.5 ms	
64 bytes from 10.10.10.1: icmp_req=2 ttl=59 time=30.7 ms	
64 bytes from 10.10.10.1: icmp_req=3 ttl=59 time=29.3 ms	
64 bytes from 10.10.10.1: icmp_req=4 ttl=59 time=28.8 ms	
64 bytes from 10.10.10.1: icmp_req=5 ttl=59 time=29.2 ms	

--- 10.10.10.1 ping statistics ---	
5 packets transmitted, 5 received, 0% packet loss, time 4003ms	
rtt min/avg/max/mdev = 28.536/29.357/30.781/0.792 ms	

Tip

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

27.2 Traceroute Test

The traceroute test tool traces the routing path to the destination through a particular Ethernet interface or a SpeedFusion™ connection. The traceroute test utility is located at **System>Tools>Traceroute**.

Traceroute	
Connection	WAN 1
Destination	64.233.189.99
<div>Start Stop</div>	

Results	
<div>Clear Log</div>	
<pre> Traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 100 bytes packet size 0 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 2 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 3 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 4 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 5 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 6 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 7 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 8 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 9 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 11 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 12 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 13 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 14 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 15 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 16 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 17 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 18 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 19 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 20 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 21 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 22 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 23 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 24 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 25 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 26 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 27 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 28 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 29 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 30 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1 </pre>	

Tip

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

27.3 Wake-on-LAN

Peplink routers can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**

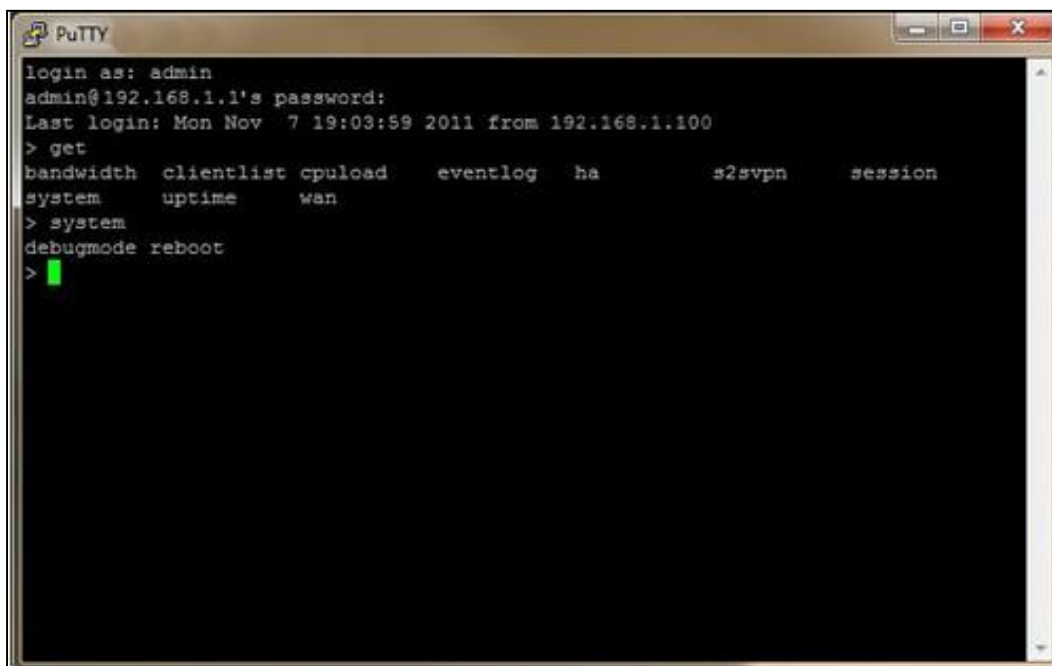
Wake-on-LAN	
Wake-on-LAN Target	Surf_SOHO (00:90:0B:36:3C:8C) <div>Send</div>

Select a client from the drop-down list and click **Send** to send a “magic packet”

27.4 CLI (Command Line Interface) Support

The serial console connector on some Peplink Balance units is RJ-45. To access the serial console port, prepare a RJ-45 to DB-9 console cable. Connect the RJ-45 end to the unit's console port and the DB-9 end to a terminal's serial port. The port setting will be **115200,8N1**.

The serial console connector on other Peplink Balance units is a DB-9 male connector. To access the serial console port, connect a null modem cable with a DB-9 connector on both ends to a terminal with the port setting of *115200,8N1*.



28 Status

28.1 Device

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

System Information	
Router Name	1824-6C65-DDB9
Model	Peplink Balance 30
Hardware Revision	2
Serial Number	1824-6C65-DDB9
Firmware	6.2.1 build 2977
PepVPN Version	4.0.0
Modem Support Version	1018 (Modem Support List)
Host Name	1824-6c65-ddb9
Uptime	8 days 1 hour 12 minutes
System Time	Sun Jun 21 07:51:07 WET 2015
Diagnostic Report	Download
Remote Assistance	Turn on

Interface	MAC Address
LAN	10:56:CA:04:64:BC
WAN 1	10:56:CA:04:64:BD
WAN 2	10:56:CA:04:64:BE
WAN 3	10:56:CA:04:64:BF

System Information	
Router Name	This is the name specified in the Router Name field located at System>Admin Security .
Model	This shows the model name and number of this device.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version this device is currently running.
Uptime	This shows the length of time since the device has been rebooted.
System Time	This shows the current system time.
Diagnostic Report	The Download link is for exporting a diagnostic report file required for system investigation.
Remote Assistance	Click Turn on to enable remote assistance.

The second table shows the MAC address of each LAN/WAN interface connected.

Important Note
If you encounter issues and would like to contact the Peplink Support Team (http://www.peplink.com/contact/), please download the diagnostic report file and attach it along with a description of your issue. In Firmware 5.1 or before, the diagnostic report file can be obtained at System>Reboot .

28.2 Active Sessions

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

Overview		
Session data captured within one minute. Refresh		
Service	Inbound Sessions	Outbound Sessions
AIM/ICQ	0	1
Bittorrent	0	32
DNS	0	51
Flash	0	1
HTTPS	0	76
Jabber	0	5
MSN	0	11
NTP	0	4
QQ	0	1
Remote Desktop	0	3
SSH	0	12
SSL	0	64
XMPP	0	4
Yahoo	0	1

Interface	Inbound Sessions	Outbound Sessions
WAN1	0	219
WAN2	0	0
WAN3	0	0
Mobile Internet	0	0

Top Clients

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

This screen displays the number of sessions initiated by each application. Click on each service listing for additional information. This screen also indicates the number of sessions initiated by each WAN port. Finally, you can see which clients are initiating the most sessions.

In addition, you can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to **Status>Active Sessions>Search**.

Overview

Search

Session data captured 1 min ago. [Refresh](#)

IP / Subnet	Source or Destination ▾ / 255.255.255.255 (/32) ▾		
Port	Source or Destination ▾		
Protocol / Service	SSL ▾		
Interface	<div><div><input type="checkbox"/> 1 WAN 1</div><div><input type="checkbox"/> 4 WAN 4</div><div><input type="checkbox"/> 7 WAN 7</div><div><input type="checkbox"/> 10 WAN 10</div><div><input type="checkbox"/> Mobile Internet</div></div> <div><div><input type="checkbox"/> 2 WAN 2</div><div><input type="checkbox"/> 5 WAN 5</div><div><input type="checkbox"/> 8 WAN 8</div><div><input type="checkbox"/> 11 WAN 11</div><div><input type="checkbox"/> VPN</div></div> <div><div><input type="checkbox"/> 3 WAN 3</div><div><input type="checkbox"/> 6 WAN 6</div><div><input type="checkbox"/> 9 WAN 9</div><div><input type="checkbox"/> 12 WAN 12</div></div>		

Search

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Transit


Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0







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

28.3 Client List

The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses, names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address.

Clients can be imported into the DHCP reservation table by clicking the  button on the right. Further update the record after the import by going to **Network>LAN**.

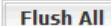
Filter	<input type="checkbox"/> Online Clients Only <input type="checkbox"/> DHCP Clients Only				
--------	--	--	--	--	--

Client List					
IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
 192.168.167.10		0	0	10:56:CA:0A:56:58	
 192.168.167.11	PogoU64-2-1	0	0	00:50:56:99:49:1A	
 192.168.167.12	PogoU64-2-2	0	0	00:50:56:99:32:75	

If the PPTP server (see **Section Error! Reference source not found.**), SpeedFusion™ (see **Section 12.1**), or AP controller (see **Section 20**) is enabled, you may see the corresponding connection name listed in the **Name** field.

28.4 WINS Client

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

WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4
	

The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server (see **Section 10**). The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush All** to flush all WINS client records.

28.5 OSPF & RIPv2

Information on OSPF and RIPv2 routing setup can be found at **Status>OSPF & RIPv2**.

28.6 SpeedFusion™ Status

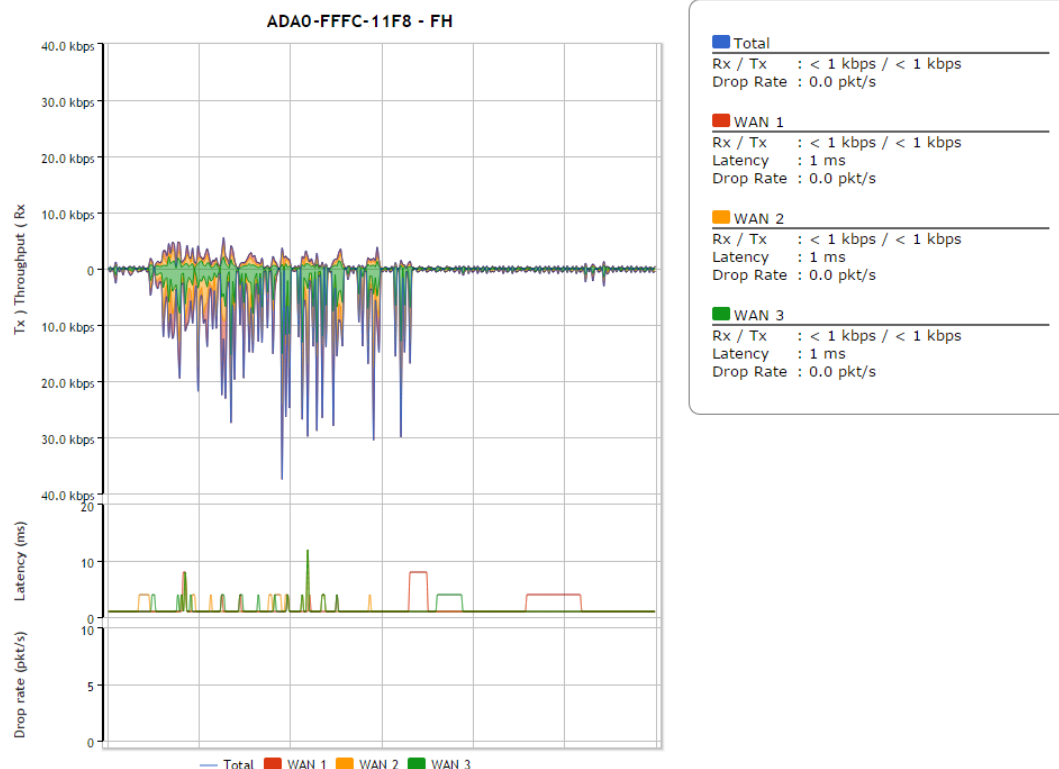
Current SpeedFusion™ status information is located at **Status>SpeedFusion™**. Details about SpeedFusion™ connection peers appears as below:


PepVPN with SpeedFusion - Remote Peer Details			<input type="checkbox"/> Show disconnected profiles
Search	<input type="text"/>		
Remote Peer ▲	Profile	Information	
ADA0-FFFC-11F8	FH	192.168.77.0/24	
3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24	

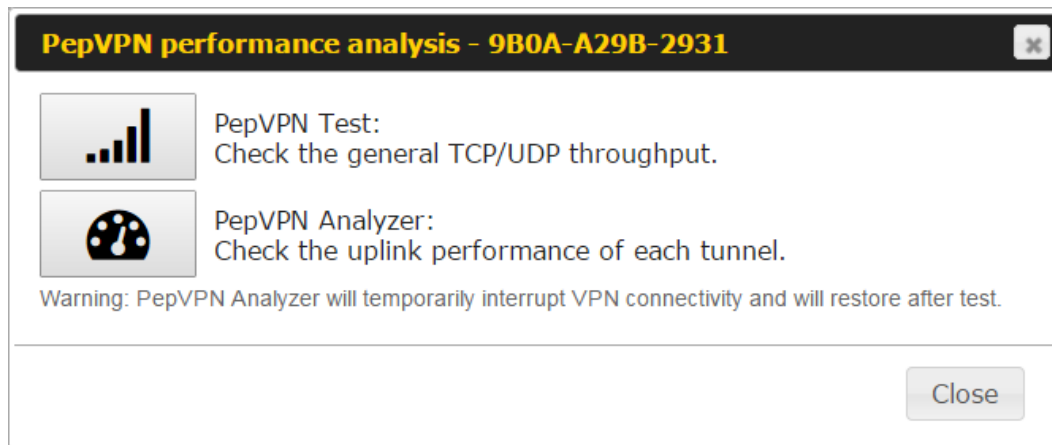
Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.

Remote Peer ▲	Profile	Information	
ADA0-FFFC-11F8	FH	192.168.77.0/24	
WAN 1	Rx: < 1 kbps Tx: < 1 kbps Drop rate: 0.0 pkt/s Latency: 1 ms		
WAN 2	Rx: < 1 kbps Tx: < 1 kbps Drop rate: 0.0 pkt/s Latency: 1 ms		
WAN 3	Rx: < 1 kbps Tx: < 1 kbps Drop rate: 0.0 pkt/s Latency: 1 ms		
Total	Rx: < 1 kbps Tx: 1.1 kbps Drop rate: 0.0 pkt/s		
3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24	
WAN 1	Rx: < 1 kbps Tx: < 1 kbps Drop rate: 0.0 pkt/s Latency: 4 ms		
WAN 2	Rx: < 1 kbps Tx: < 1 kbps Drop rate: 0.0 pkt/s Latency: 4 ms		
WAN 3	Rx: < 1 kbps Tx: < 1 kbps Drop rate: 0.0 pkt/s Latency: 4 ms		
Total	Rx: 1.6 kbps Tx: < 1 kbps Drop rate: 0.0 pkt/s		

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

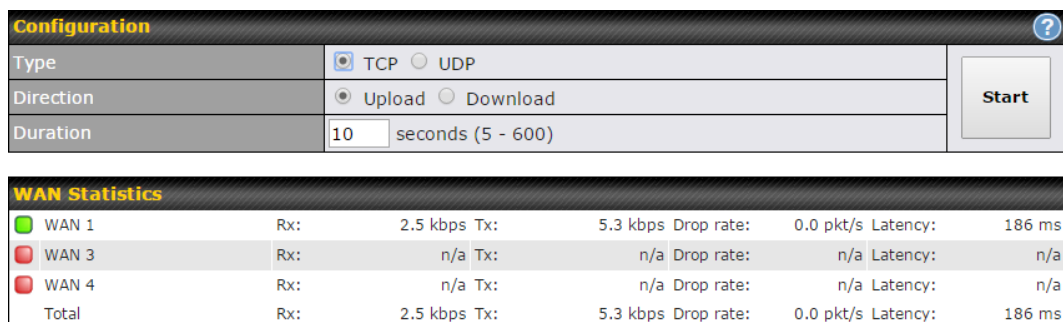


When pressing the  button, the following menu will appear:



PepVPN Test:
Check the general TCP/UDP throughput.

After clicking the icon, the following menu appears:



WAN Statistics						
WAN 1	Rx:	2.5 kbps	Tx:	5.3 kbps	Drop rate:	0.0 pkt/s Latency: 186 ms
WAN 3	Rx:	n/a	Tx:	n/a	Drop rate:	n/a Latency: n/a
WAN 4	Rx:	n/a	Tx:	n/a	Drop rate:	n/a Latency: n/a
Total	Rx:	2.5 kbps	Tx:	5.3 kbps	Drop rate:	0.0 pkt/s Latency: 186 ms

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

Results		
0.1250 MB / 1.00 sec =	1.0485 Mbps	
1.0000 MB / 1.00 sec =	8.3888 Mbps	
1.3125 MB / 1.00 sec =	11.0098 Mbps	
3.0000 MB / 1.00 sec =	25.1465 Mbps	
5.6875 MB / 1.00 sec =	47.7473 Mbps	
6.0625 MB / 1.00 sec =	50.8562 Mbps	
4.9375 MB / 1.00 sec =	41.4188 Mbps	
4.5000 MB / 1.00 sec =	37.7487 Mbps	
5.0000 MB / 1.00 sec =	41.9438 Mbps	
5.6875 MB / 1.00 sec =	47.7099 Mbps	
37.3167 MB / 10.05 sec = 31.1504 Mbps 8 %TX 9 %RX 47 retrans 132.62 msRTT		
TEST DONE		



PepVPN Analyzer:
Check the uplink performance of each tunnel.

The bandwidth bonding feature of PepVPN occurs when multiple WAN lines from one end merge with multiple WAN lines from the other end. For this to happen, each WAN line needs to form a connection with all the WAN lines on the opposite end. The function of the PepVPN analyzer is to report the throughput, packet loss, and latency of all possible combinations of connections. **Please note that the PepVPN Analyzer will temporarily interrupt VPN connectivity and will restore after test.**

After clicking the icon, the analyzer will require several minutes to perform its analysis depending the number of WAN links in the SpeedFusion™ Tunnel. Once the test the complete, the report will appear:

Results							
Estimated time: 150 s							
Time remaining: 0 s							
100%							
Local WAN1 > Remote WAN3	Local WAN1 > Remote WAN4	Local WAN1 > Remote WAN5	Local WAN1 > Remote WAN6	Tx Avg. (Mbps)	Tx Max. (Mbps)	Packet loss (%)	RTT (ms)
0				5.87	16.95	0.76	420.51
	0			20.72	26.39	1.59	29.89
		0		30.10	43.69	2.24	29.61
			0	45.01	55.93	2.16	28.24
0	0			24.87	33.56	0.86	49.86
0		0		19.30	31.28	0.01	49.78
	0	0		18.59	30.41	2.08	39.78
0	0	0		20.56	34.60	0.00	38.11
0			0	36.70	59.16	2.64	42.06
	0		0	19.98	30.40	4.40	38.01
0	0		0	31.63	42.99	0.72	37.99
		0	0	36.88	55.78	2.60	33.89
0		0	0	38.30	47.89	0.01	29.98
	0	0	0	33.21	55.23	2.69	30.48
0	0	0	0	30.02	46.66	3.77	28.68

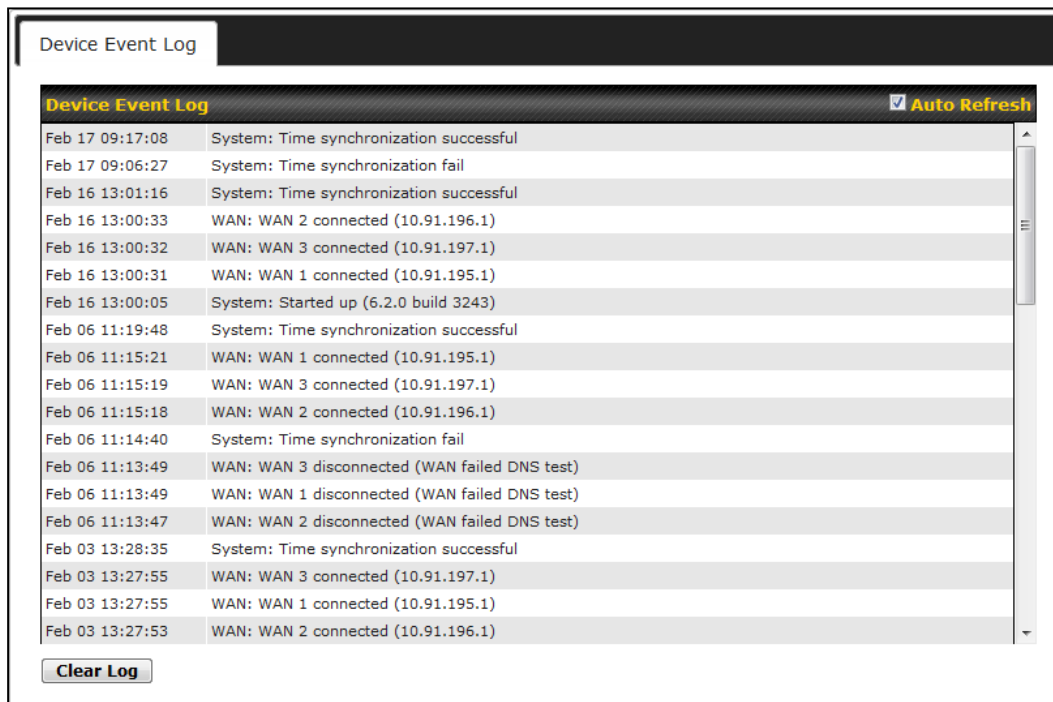
"O" indicates that specific WAN / Tunnel is active for that particular test.

"Tx Avg." is the averaged throughput across the full 10 seconds time, while "Tx Max." is the averaged throughput of the fastest 30% of time.

28.7 Event Log

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

28.7.1 Device Event Log



The screenshot shows the 'Device Event Log' tab selected. It features a table with event details, an 'Auto Refresh' checkbox, and a 'Clear Log' button.

Device Event Log		<input checked="" type="checkbox"/> Auto Refresh
Feb 17 09:17:08	System: Time synchronization successful	
Feb 17 09:06:27	System: Time synchronization fail	
Feb 16 13:01:16	System: Time synchronization successful	
Feb 16 13:00:33	WAN: WAN 2 connected (10.91.196.1)	
Feb 16 13:00:32	WAN: WAN 3 connected (10.91.197.1)	
Feb 16 13:00:31	WAN: WAN 1 connected (10.91.195.1)	
Feb 16 13:00:05	System: Started up (6.2.0 build 3243)	
Feb 06 11:19:48	System: Time synchronization successful	
Feb 06 11:15:21	WAN: WAN 1 connected (10.91.195.1)	
Feb 06 11:15:19	WAN: WAN 3 connected (10.91.197.1)	
Feb 06 11:15:18	WAN: WAN 2 connected (10.91.196.1)	
Feb 06 11:14:40	System: Time synchronization fail	
Feb 06 11:13:49	WAN: WAN 3 disconnected (WAN failed DNS test)	
Feb 06 11:13:49	WAN: WAN 1 disconnected (WAN failed DNS test)	
Feb 06 11:13:47	WAN: WAN 2 disconnected (WAN failed DNS test)	
Feb 03 13:28:35	System: Time synchronization successful	
Feb 03 13:27:55	WAN: WAN 3 connected (10.91.197.1)	
Feb 03 13:27:55	WAN: WAN 1 connected (10.91.195.1)	
Feb 03 13:27:53	WAN: WAN 2 connected (10.91.196.1)	

Clear Log

The log section displays a list of events that has taken place on the Peplink Balance unit. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

28.7.2 IPsec Event Log



The screenshot shows the 'IPsec VPN Event Log' tab selected. It features a table with event details, an 'Auto Refresh' checkbox, and an 'End of log' indicator.

IPsec VPN Event Log		<input checked="" type="checkbox"/> Auto Refresh
Dec 30 08:32:26	IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...	
Dec 30 08:31:46	IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...	
Sep 04 01:01:29	IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...	

End of log

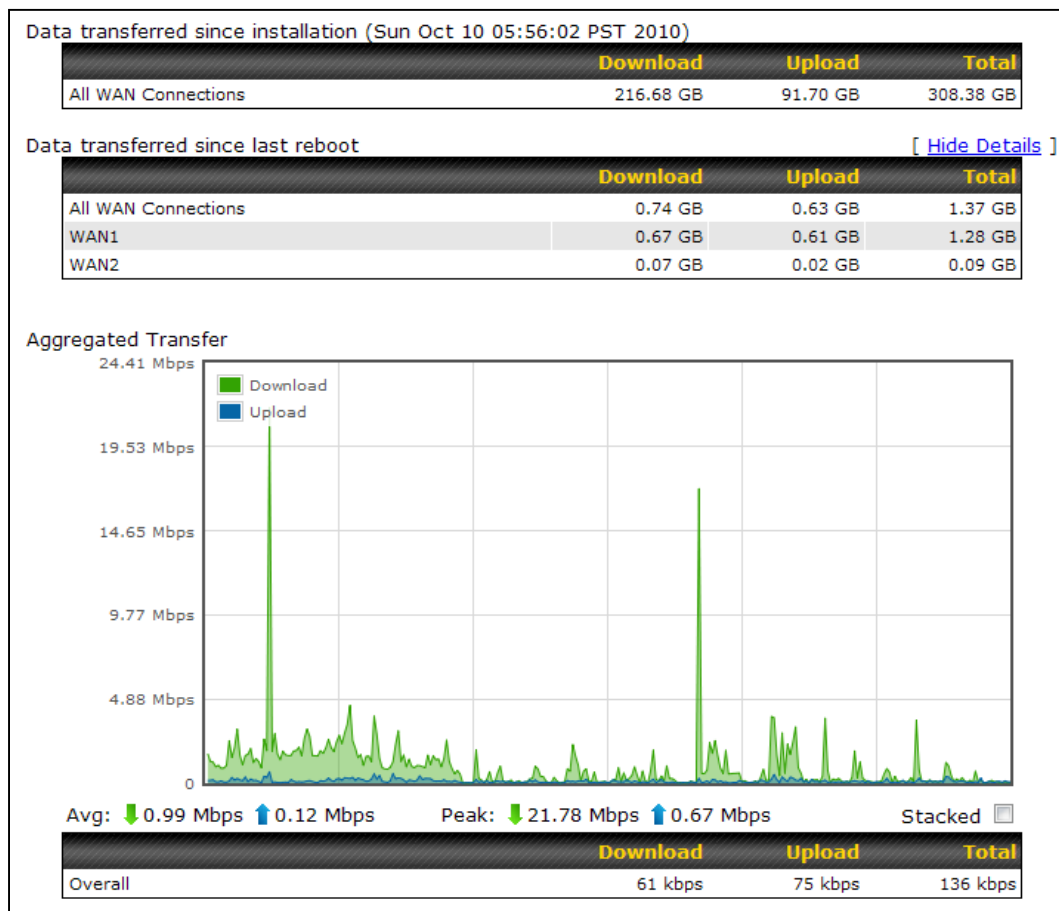
This section displays a list of events that has taken place within an IPsec VPN connection. Check the box next to **Auto Refresh** and the log will be refreshed automatically. For an AP event log, navigate to **AP>Info**.

28.8 Bandwidth

This section shows the bandwidth usage statistics, located at **Status>Bandwidth**. Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

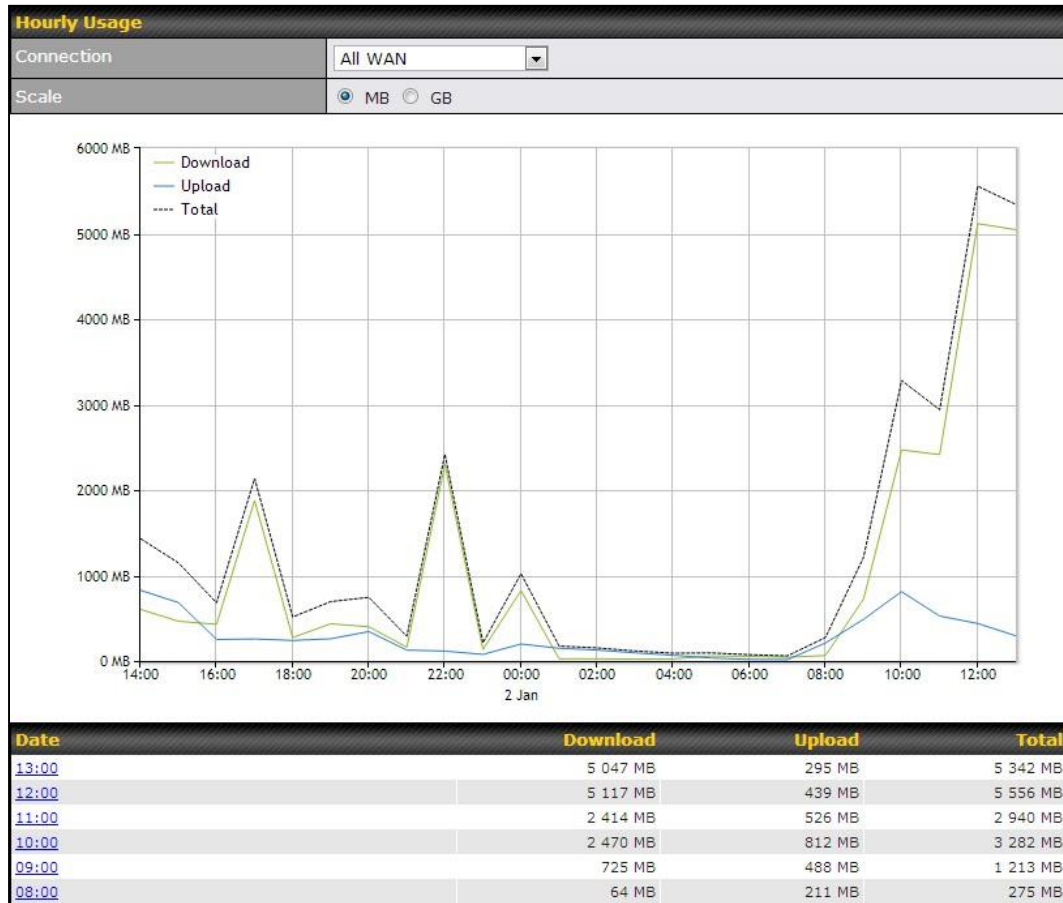
28.8.1 Real-Time

The **Data transferred since installation** table indicates how much network traffic has been processed by the device since the first bootup. The **Data transferred since last reboot** table indicates how much network traffic has been processed by the device since the last bootup.



28.8.2 Hourly

This page shows the hourly bandwidth usage for all WAN connections, with the option of viewing each individual connection. Select the desired connection to check from the drop-down menu.



28.8.3 Daily

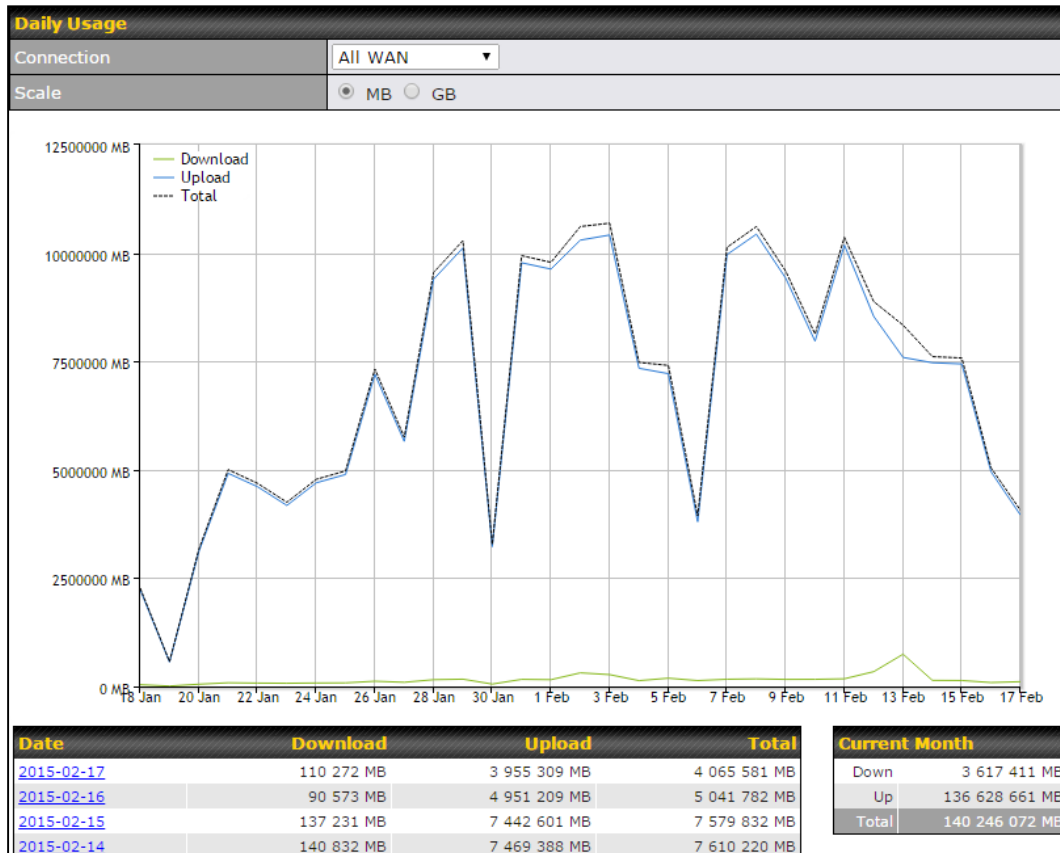
This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature as shown in **Section 14.4**, the **Current Billing Cycle** table for that WAN connection will be displayed.

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (MB) or gigabytes (GB).



Status



Click on a specific date to receive a breakdown of all client usage for that date.

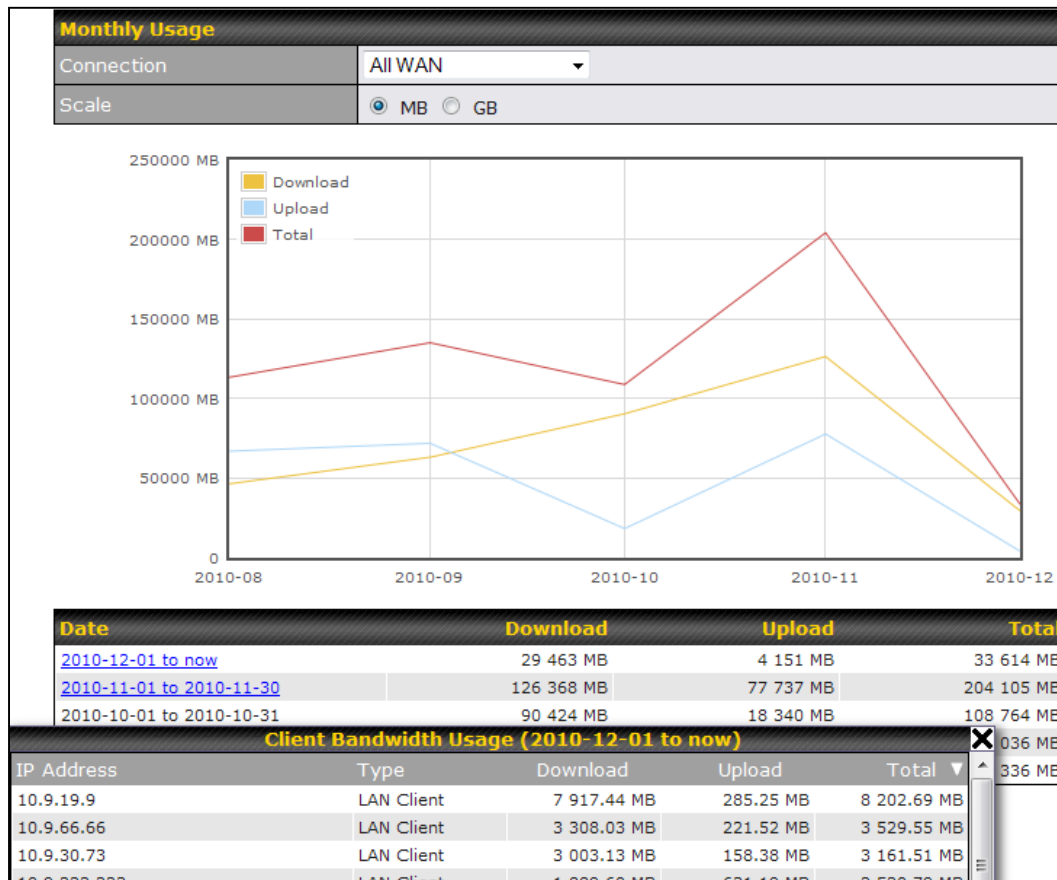
Client Bandwidth Usage (2015-02-15)

IP Address	Type	Download	Upload	Total
192.168.168.15	LAN Client	7 972.69 MB	1 217 122.81 MB	1 225 095.50 MB
192.168.168.14	LAN Client	7 432.25 MB	1 197 380.53 MB	1 204 812.79 MB
192.168.168.22	LAN Client	5 676.90 MB	617 109.49 MB	622 786.39 MB
192.168.168.21	LAN Client	5 693.38 MB	615 629.07 MB	621 322.46 MB
192.168.168.12	LAN Client	2 156.79 MB	339 779.46 MB	341 936.25 MB
192.168.168.16	LAN Client	2 107.10 MB	333 980.14 MB	336 087.23 MB
192.168.168.18	LAN Client	16.75 MB	9.50 MB	26.25 MB
192.168.167.14	LAN Client	4.74 MB	8.35 MB	13.09 MB
192.168.167.13	LAN Client	4.73 MB	8.35 MB	13.08 MB
192.168.168.19	LAN Client	0.02 MB	0.02 MB	0.03 MB
192.168.168.20	LAN Client	0.00 MB	0.00 MB	0.00 MB
192.168.168.11	LAN Client	0.00 MB	0.00 MB	0.00 MB

28.8.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection. If you have enabled **Bandwidth Monitoring** feature as shown in **Section 14.4**, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

Click the first two rows to view the client bandwidth usage in the last two months. This feature is not available if you have chosen to view the bandwidth of an individual WAN connection. The scale of the graph can be set to display megabytes (MB) or gigabytes (GB).



Click on a specific month to receive a breakdown of all client usage for that month.

Appendix A. Restoration of Factory Defaults

To restore the factory default settings on a Peplink Balance unit, perform the following:

For Balance models with a reset button:

1. Locate the reset button on the Peplink Balance unit.
2. With a paper clip, press and keep the reset button pressed for at least 10 seconds, until the unit reboots itself.

For Balance/MediaFast models with an LCD menu:

- Use the buttons on front panel to control the LCD menu to go to **Maintenance>Factory Defaults**, and then choose **Yes** to confirm.

Afterwards, the factory default settings will be restored.

Important Note

All user settings will be lost after restoring the factory default settings. Regular backup of configuration parameters is strongly recommended.

Appendix C. Routing under DHCP, Static IP, and PPPoE

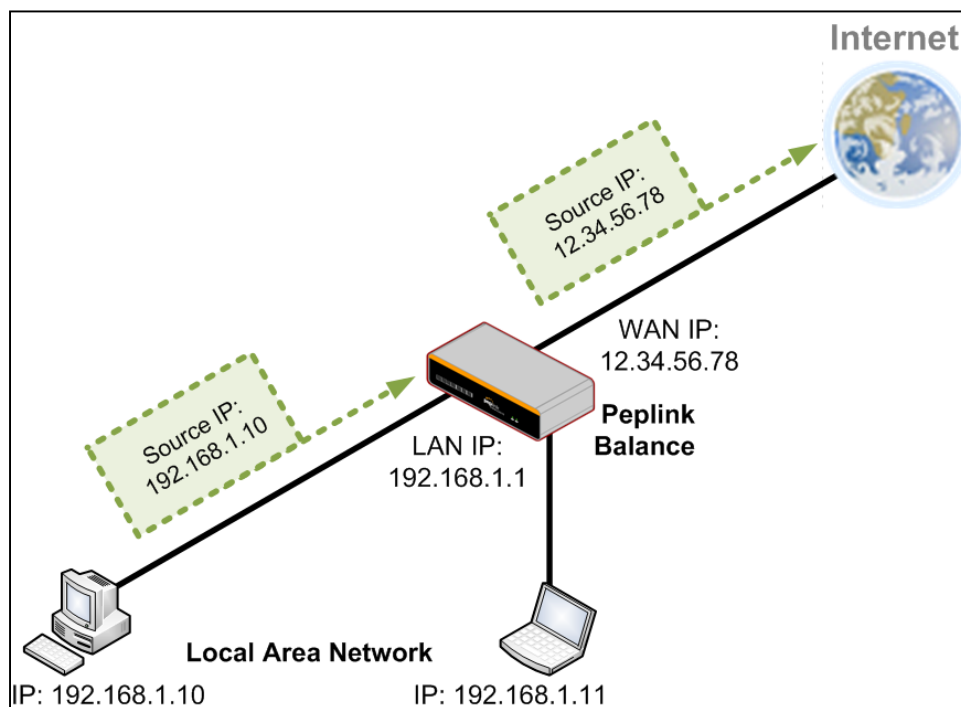
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

C.1 Routing Via Network Address Translation (NAT)

When the Peplink Balance is operating under NAT mode, the source IP addresses of outgoing IP packets are translated to the WAN IP address of the Peplink Balance. With NAT, all LAN devices share the same WAN IP address to access the Internet (i.e., the WAN IP address of the Peplink Balance).

Operating the Peplink Balance in NAT mode requires only one WAN (Internet) IP address. In addition, operating in NAT mode also has security advantages because LAN devices are hidden behind the Peplink Balance. They are not directly accessible from the Internet and hence less vulnerable to attacks.

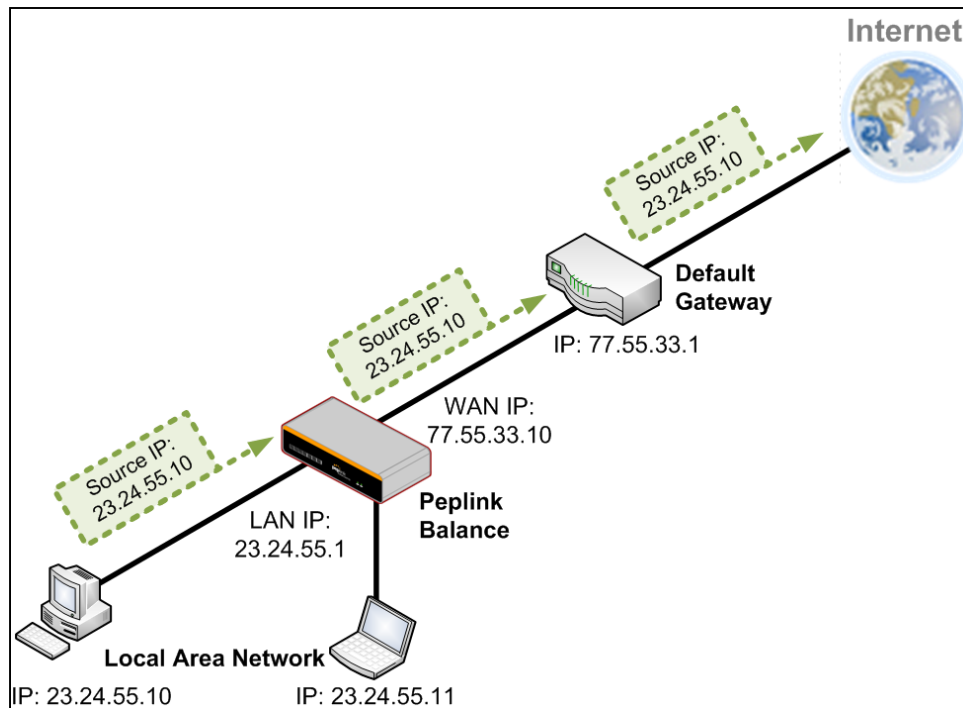
The following figure shows the packet flow in NAT mode:



C.2 Routing Via IP Forwarding

When the Peplink Balance is operating under IP forwarding mode, the IP addresses of IP packets are unchanged; the Peplink Balance forwards both inbound and outbound IP packets without changing their IP addresses.

The following figure shows the packet flow in IP forwarding mode:



Appendix D. Case Studies

D.1 MPLS Alternative

Our SpeedFusion enabled routers can be used to bond multiple low-cost/commodity Internet connections to replace an expensive managed business Internet connection, private leased line, MPLS, and frame relay without sacrificing reliability and availability.

Belows are typical deployment for using our Balance routers to replace expensive MPLS connection with commodity connections, such as ADSL, 3G, and 4G LTE links.

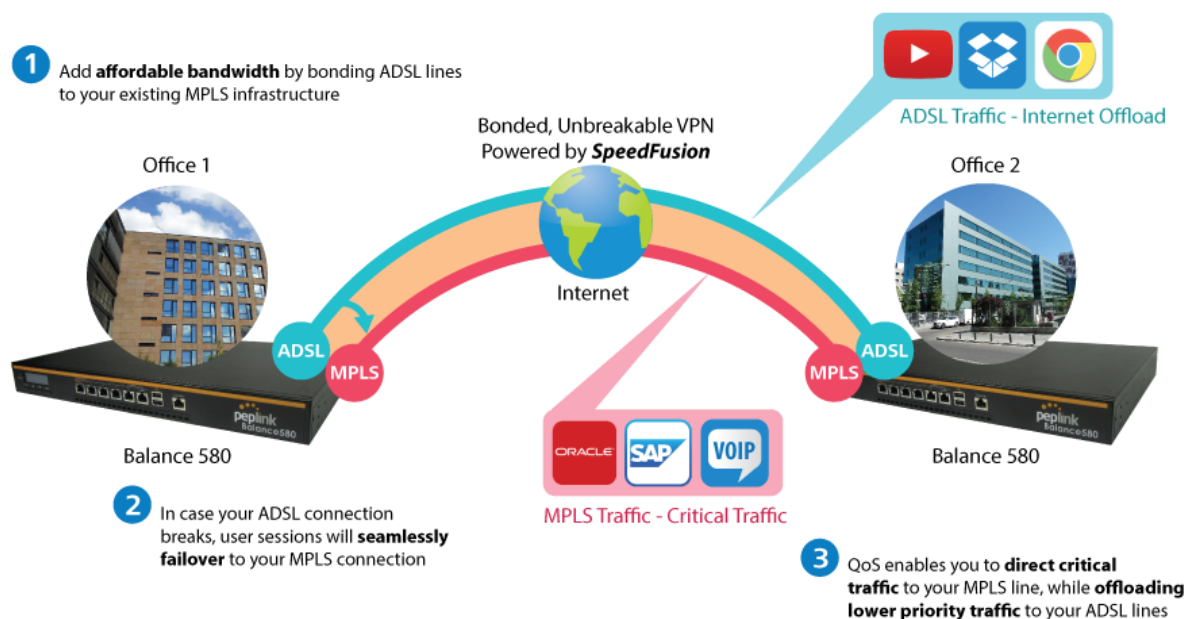
Special features of Balance 580: have high availability capability

Special features of Balance 2500: have high availability capability and capable of connecting to optical fiber based LAN through SFP+ connector

Our WAN-bonding routers which comprise our Balance series and MediaFast series are capable of connecting multiple devices, and end users' networks to the Internet through multiple Internet connections.

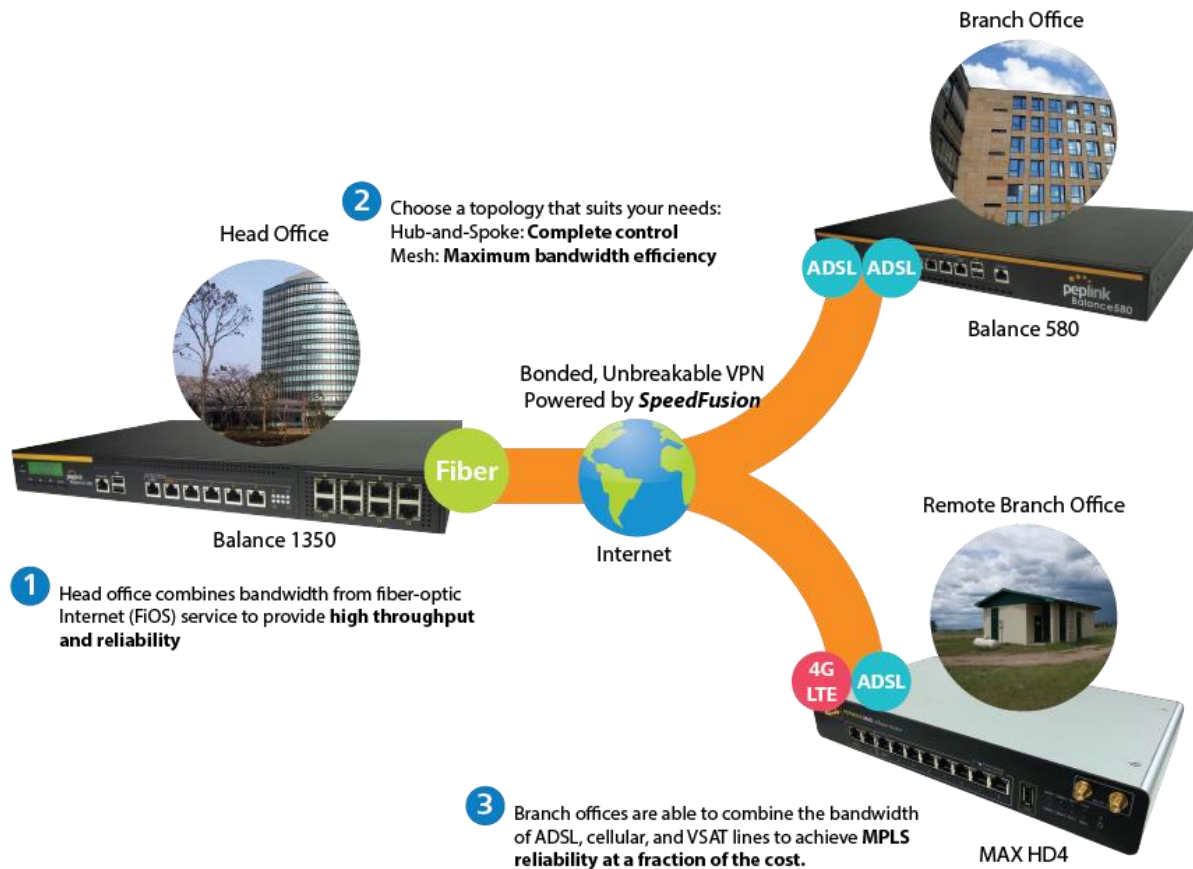
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement



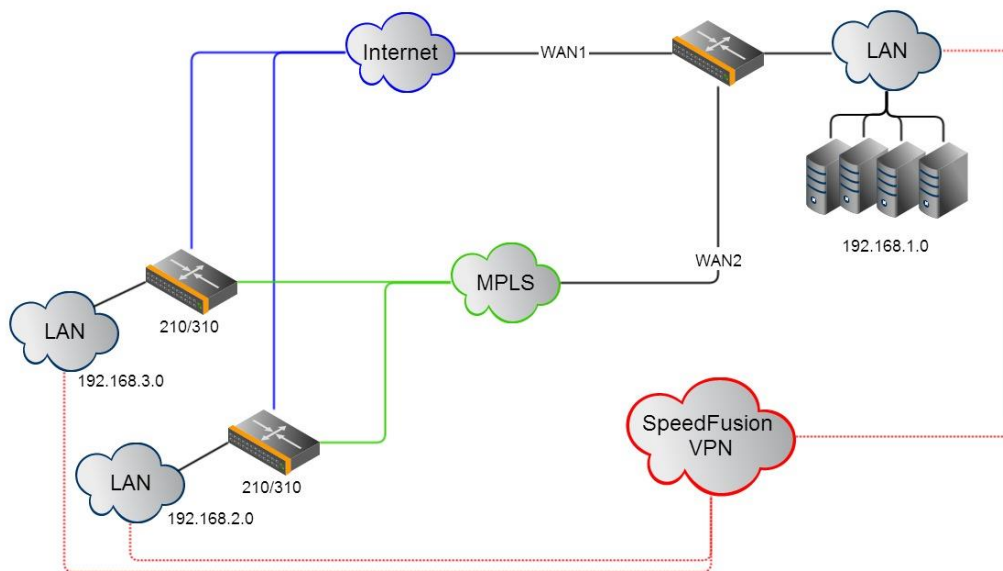
Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your network.

Option 2: MPLS Alternative



Achieve faster speeds and greater reliability while paying only 20% of MPLS costs by connecting multiple ADSL, 3G, and 4G LTE links. Choose a topology that suits your requirements: a hub-and-spoke topology maximizes control over your network, while a meshed topology can reduce your bandwidth overhead by enabling your devices to form Unbreakable VPN connections directly with each other.

Here is an example of to supplement of existing Multi-Office MPLS network with DSL bonding through SpeedFusion using a Balance 580 at the headquarters and Balance 210/310 at branch offices.



Environment:

- This organization has one head office with and two branch offices, with most of the crucial information stored in a server room at the head office.
- They are connecting the offices together using a managed MPLS Solution. However, the MPLS Network is operating at capacity and upgrading the links is cost prohibitive.
- As the organization grows, it needs a cost-efficient way to to add more bandwidth to its wide area network.
- Internet access at the remote sites is sent via a web proxy at head office for corporate web filtering compliance.

Requirement:

- User sessions need to remain uninterrupted
- More bandwidth is required at the head office location for direct internet access.

Recommended Solution:

- Form a SpeedFusion tunnel between the branch offices and head office to bond the MPLS and additional DSL lines.
- SpeedFusion allows for hot failover, maintaining a persistent session while switching connections.
- The DSLs at head office can be used for direct internet access providing lots of cheap internet bandwidth.
- Head office can use outbound policies to send internet traffic out over the DSLs and only use the MPLS connection for speedfusion, freeing up bandwidth.

Devices Deployed: Balance 210, Balance 310, Balance 580

Harrington Industrial Plastics



Overview

Harrington Plastics, the US's largest industrial plastics distributor, was looking to upgrade its network equipment. Harrington's team came across Peplink and started thinking about MPLS alternatives. By choosing Peplink, they saved a fortune on upgrades and ended up with yearly savings of up to \$100,000.

Requirements

- Zero network outages
- Flexible resilience options
- Cost-effective solution

Solution

- Peplink Balance 1350
- Peplink Balance 380
- Unbreakable VPN

Benefits

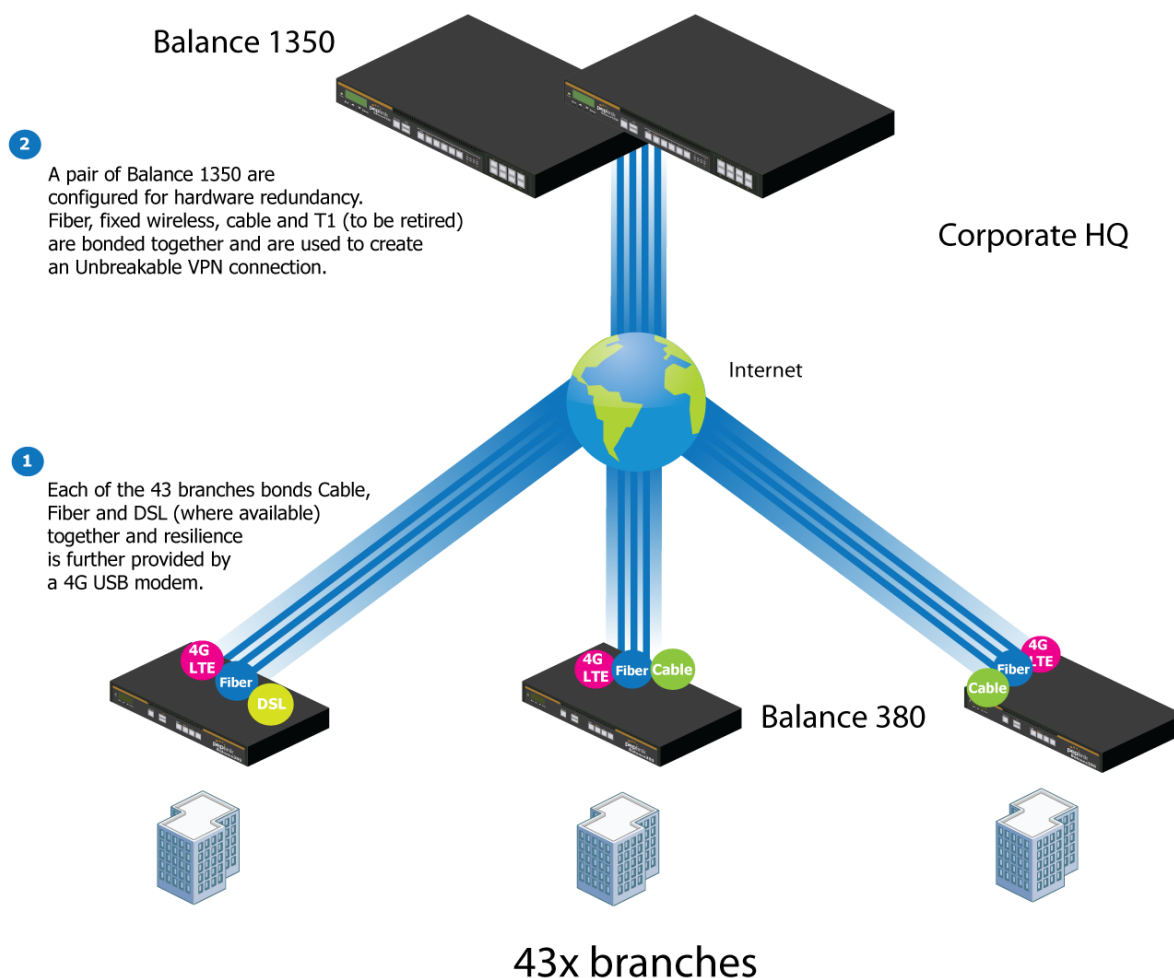
- Extreme savings of \$100,000 per year
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

Time For An Upgrade

Harrington Industrial Plastics decided it was time to upgrade its network equipment. Its existing solution used redundant MPLS for site-to-site traffic and broadband connections for Internet access. Harrington is the US's largest distributor of industrial plastics piping, serving all industries with corrosive and high-purity applications. It requires peak performance at all times in order to serve its large customer base and 43 busy branches.

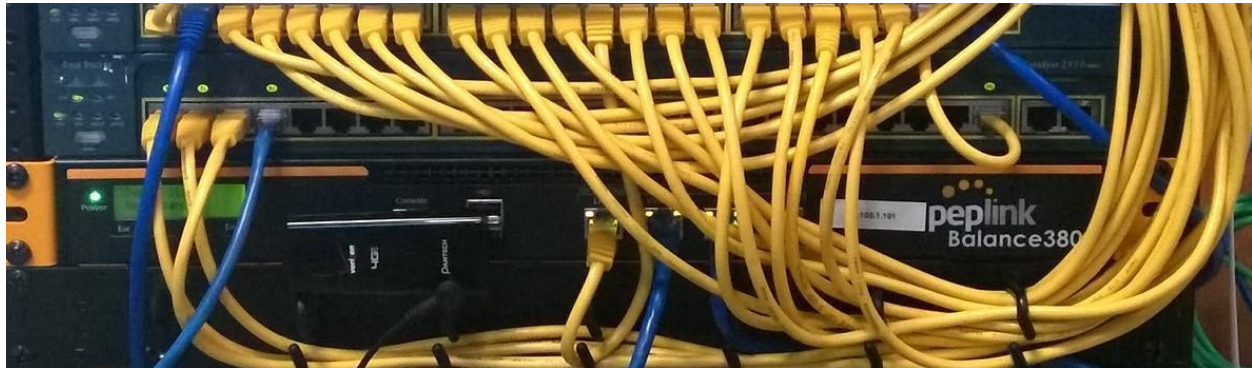
Quick Deployment and Unbreakable Connectivity

In evaluating an upgrade to its network infrastructure, it was only natural that Harrington settled on the best in the industry — Peplink. Peplink partner Frontier Computer Corporation was chosen to help design and deploy the solution. Since Peplink gear is so easy to configure and install, Harrington was able to design, prototype and roll out the entire solution to the corporate headquarters and all 43 branches within just one year.



The corporate office houses a pair of redundant Balance 1350s for hardware resilience. Served by 4 separate links from multiple service providers, the network's chance of an outage is practically zero. All 43 branches are now equipped with a fleet of Balance 380s, bonding a combination of DSL, cable and fiber-optic links together with an additional 4G USB modem for added resilience. These work together to create an Unbreakable VPN connection to the Balance 1350s at the corporate office, connecting the final dot.

Dependable, Resilient Networking that's also Very Budget-friendly



Harrington Industrial Plastics couldn't be happier. They now benefit from an extremely reliable and cost-effective network. Supplying additional resilience is as easy as plugging in a 4G USB modem. Where the MPLS 768kb deployed previously had cost them \$192000 a year for all 40 sites, their new solution is now only costing them \$92000. Their total bandwidth has been bumped from 36 Mbps to 138 Mbps.

PLUSS

Peplink + Citrix + VoIP Adds Up to Fast, Cost-Effective WAN for Pluss

Adding to **Life**
pluss

400
USERS

VoIP 290
EndPoints

30+
SITES

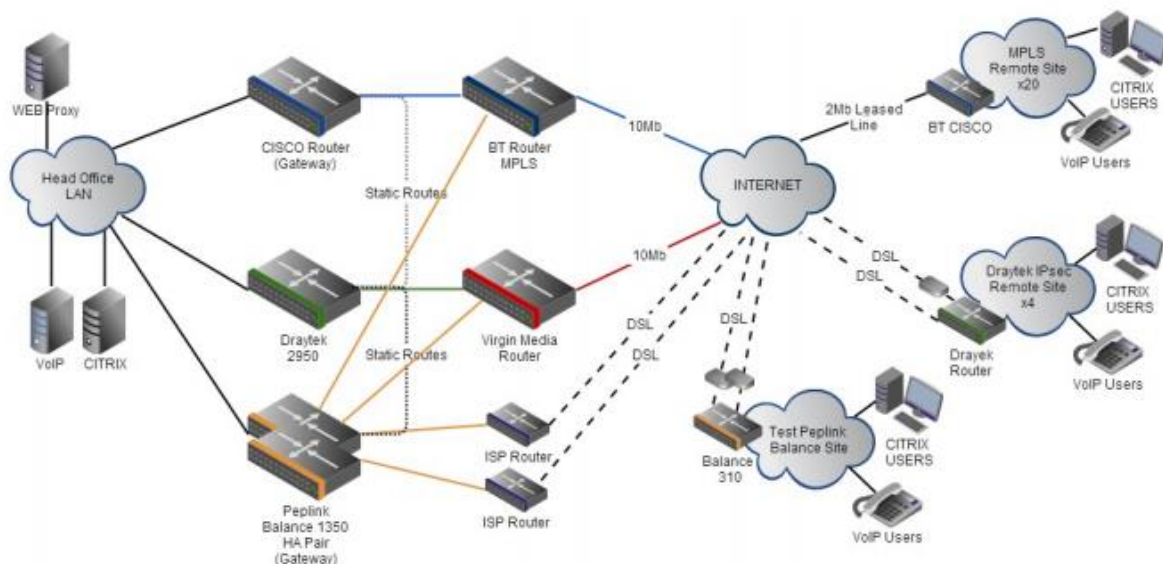
"It saves us money, is easy to manage and grows with us effortlessly."

Steve Taylor - Pluss

A Peplink customer since 2006, Pluss is a social enterprise that each year makes gainful employment a reality for more than 5000 disabled and disadvantaged UK citizens. With 37 locations and 300+ active users, Pluss makes heavy use of its WAN infrastructure, which until recently was built on managed MPLS lines.

Hoping to cut expenses and, if possible, boost performance at the same time, Steve Taylor, IT Manager at Pluss, set out to find a solution that would allow Pluss to replace costly MPLS service with a commodity alternative, such as DSL or EFM.

Steve found the solution Pluss needed in Peplink products, especially the Balance series of high-performance enterprise routers and SpeedFusion bonding technology. Pluss now powers its entire WAN infrastructure with simple-to-install, highly reliable, and cost-effective Peplink gear, which allows it to aggregate DSL and other commodity connections and replace expensive leased lines.



D.2 Colégio Next - Enabling eLearning



Colégio Next, a recognized Apple Distinguished School - deploys over 500 iPads to its 600 students as a teaching and learning tool.

Despite being equipped with iPads, teachers and students alike were not making use of them. The reason for this was because of the slow network access speeds. Apps would not download and course contents were inaccessible. Often, having more than a couple students connected to the same Wi-Fi access point was enough to bring it to its knees.

Colégio Next needed a unique solution, so they contacted Peplink.

Requirements

- Solve network congestion problem caused by 600 students over rural Internet connections
- Wi-Fi that can handle 50+ users per classroom
- An affordable network infrastructure that can provide simultaneous access to media-rich educational content

Solution

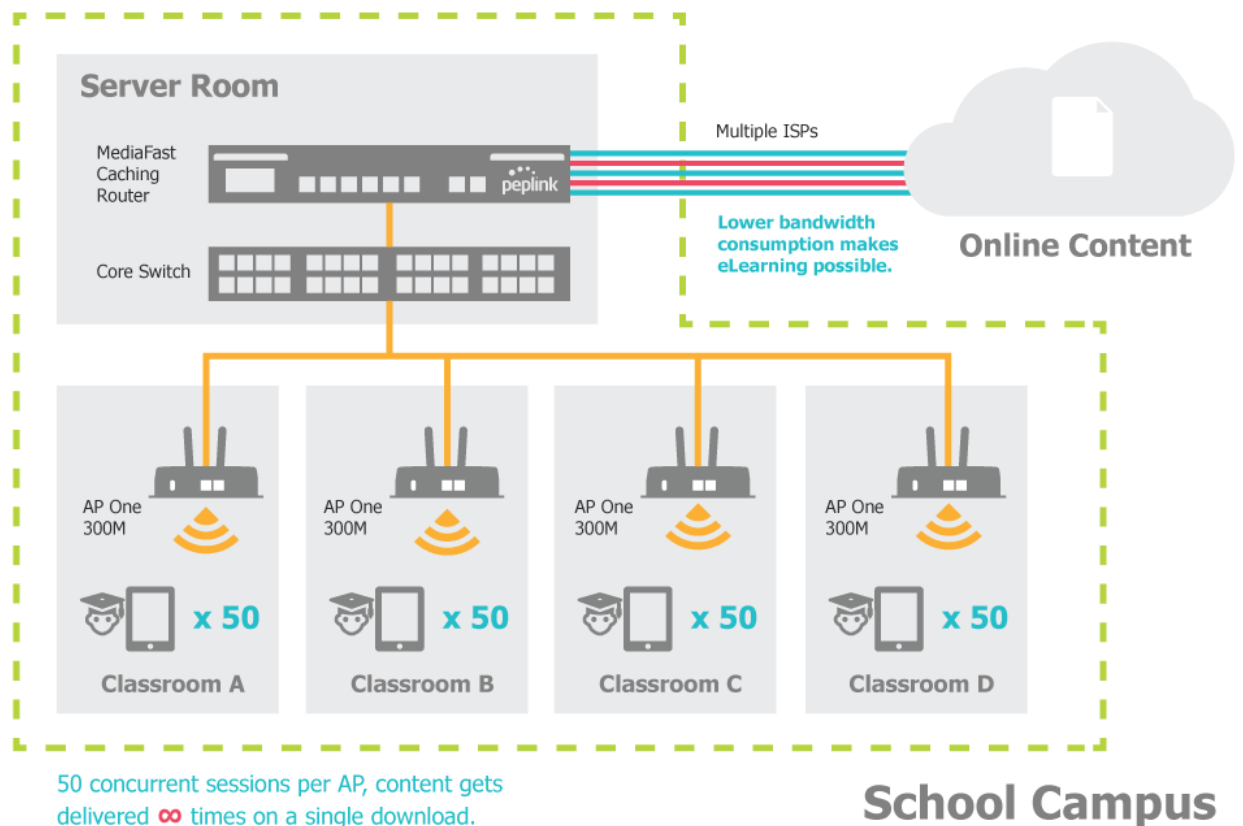
- Peplink MediaFast
- Multi-WAN Content-caching router, tailor-made for Education networking.
- AP One 300M
- Enterprise grade AP, 5GHz Wi-Fi, up to 60 concurrent users.

Benefits

- Instant, simultaneous access to media-rich educational content for 500+ iPads
- Wi-Fi connection stability for 50+ users per classroom, not achievable by other tested

equipment

- Teachers, students and guests can be assigned access priority to available bandwidth, further preventing congestion
- iOS updates (often 2GB size) no longer congest the network as they are downloaded only once, cached on the MediaFast and then distributed to all iOS devices
- AP Controller makes MAC Address Filtering easy. Students are assigned to designated APs by their devices' MAC Address in order to prevent saturating any single AP.
- Flawless iPad AirPlay mirroring at all times
- iPads are used all day, reaching their full potential with a fast and stable network all the time
- Students are far more engaged and teachers rely on their iPads all day



D.3 Performance Optimization

D.3.1 Scenario

In this scenario, email and web browsing are the two main Internet services used by LAN users.

The mail server is external to the network. The connections are ADSL (WAN1, with slow uplink and fast downlink) and Metro Ethernet (WAN2, symmetric).

D.3.2 Solution

For optimal performance with this configuration, individually set the WAN load balance according to the characteristics of each service.

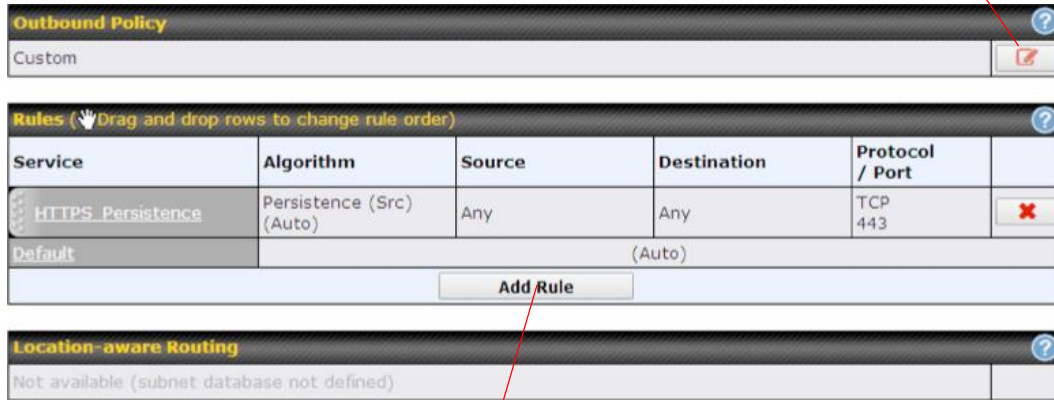
- Web browsing mainly downloads data; sending e-mails mainly consumes upload bandwidth.
- Both connections offer good download speeds; WAN2 offers good upload speeds.
- Define WAN1 and WAN2's inbound and outbound bandwidths to be 3M/512k and 4M/4M, respectively. This will ensure that outbound traffic is more likely to be routed through WAN2.
- For HTTP, set the weight to 3:4.
- For SMTP, set the weight to 1:8, such that users will have a greater chance to be routed via WAN2 when sending e-mail.

D.3.3 Settings

1. Add a new outbound traffic rule for HTTP.
2. Add a new outbound traffic rule for SMTP.

In general, to add a new outbound traffic rule, navigate to **Advanced>Outbound Policy**.

Click here and select **Managed by Custom Rules**



Click **Add Rule** to add a new load distribution rule.

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

Settings for HTTP:

Add a New Custom Rule

Service Name *	SMTP
Enable	<input checked="" type="checkbox"/>
Source	Any
Destination	Any
Protocol	TCP HTTP
Port *	Single Port Port: 80
Algorithm	Weighted Balance
Load Distribution Weight	<div><div>WAN 1 3</div><div>WAN 2 4</div><div>WAN 3 0</div><div>WAN 4 0</div><div>WAN 5 0</div><div>WAN 6 0</div><div>WAN 7 0</div><div>Mobile Internet 0</div></div>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

Set the weight of WAN1 and WAN2 for HTTP to 3 and 4, respectively.

Save Cancel

Settings for SMTP:

Add a New Custom Rule

Service Name *	SMTP
Enable	<input checked="" type="checkbox"/>
Source	Any
Destination	Any
Protocol	TCP SMTP
Port *	Single Port Port: 25
Algorithm	Weighted Balance
Load Distribution Weight	<div><div>WAN 1 1</div><div>WAN 2 8</div><div>WAN 3 10</div><div>WAN 4 10</div><div>WAN 5 10</div><div>WAN 6 10</div><div>WAN 7 10</div><div>Mobile Internet 10</div></div>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

Save Cancel

Set the weight of WAN1 and WAN2 for SMTP to 1 and 8, respectively.

D.4 Maintaining the Same IP Address Throughout a Session

D.4.1 Scenario

Some IP address-sensitive websites (for example, Internet banking) use both client IP address and cookie matching for session identification. Since load balancing uses different IP addresses, the session is dropped when a mismatched IP is detected, resulting in frequent interruptions while visiting such sites.

D.4.2 Solution

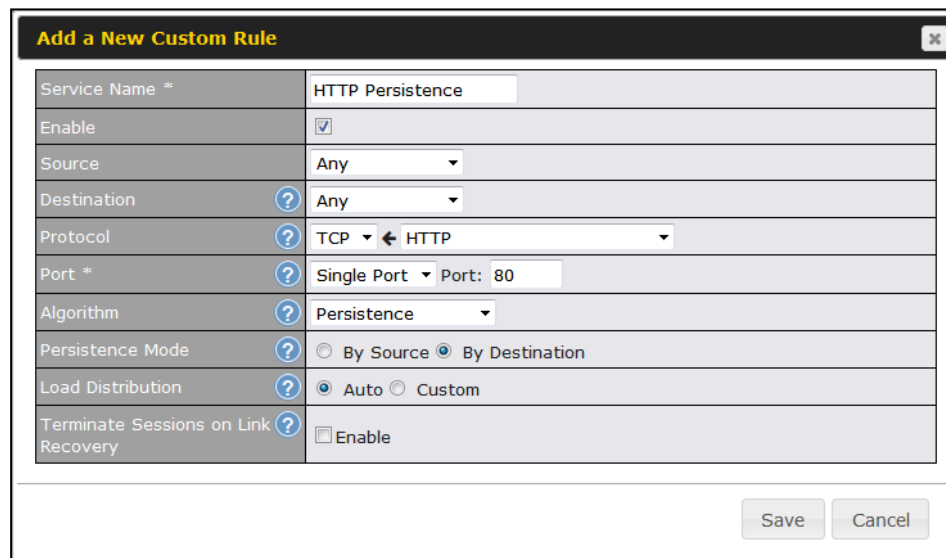
Make use of the persistence functionality of the Peplink Balance. With persistence configured and the **By Destination** option selected, the Peplink Balance will use a consistent WAN connection for source-destination pairs of IP addresses, preventing sessions from being dropped.

With persistence configured and the option **By Source** is selected, the Peplink Balance uses a consistent WAN connection for same-source IP addresses. This option offers higher application compatibility but may inhibit the load balancing function unless there are many clients using the Internet.

D.4.3 Settings

Set persistence in at **Advanced>Outbound Policy**.

Click **Add Rule**, select **HTTP** (TCP port 80) for web service, and select **Persistence**. Click **Save** and then **Apply Changes**, located at the top right corner, to complete the process.



Add a New Custom Rule	
Service Name *	HTTP Persistence
Enable	<input checked="" type="checkbox"/>
Source	Any
Destination	Any
Protocol	TCP HTTP
Port *	Single Port Port: 80
Algorithm	Persistence
Persistence Mode	<input type="radio"/> By Source <input checked="" type="radio"/> By Destination
Load Distribution	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
Terminate Sessions on Link Recovery	<input checked="" type="checkbox"/> Enable

Save Cancel

Tip

A network administrator can use the traceroute utility to manually analyze the connection path of a particular WAN connection.

D.5 Bypassing the Firewall to Access Hosts on LAN

D.5.1 Scenario

There are times when remote access to computers on the LAN is desirable; for example, when hosting web sites, online businesses, FTP download and upload areas, etc. In such cases, it may be appropriate to create an inbound NAT mapping for the network to allow some hosts on the LAN to be accessible from outside of the firewall.

D.5.2 Solution

The web admin interface can be used to add an inbound NAT mapping to a host and to bind the host to the WAN connection(s) of your choice. To begin, navigate to **Network>NAT Mappings**.

In this example, the host with an IP address of 192.168.1.102 is bound to 10.90.0.75 of WAN1:

LAN Client(s)	IP Address ▼																
Address	192.168.1.102																
Inbound Mappings	<div> Connection / Inbound IP Address(es) <table border="1"> <tr> <td><input checked="" type="checkbox"/> WAN 1</td> <td><input checked="" type="checkbox"/> 10.90.0.75 (Interface IP)</td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 3</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 4</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 5</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 6</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 7</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Mobile Internet</td> <td></td> </tr> </table> </div>	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.90.0.75 (Interface IP)	<input 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 checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.90.0.75 (Interface IP)																
<input 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																	
Outbound Mappings	<div> Connection / Outbound IP Address <table border="1"> <tr> <td>WAN 1</td> <td>10.90.0.75 (Interface IP) ▼</td> </tr> <tr> <td>WAN 2</td> <td>10.90.0.76 (Interface IP) ▼</td> </tr> <tr> <td>WAN 3</td> <td>Interface IP ▼</td> </tr> <tr> <td>WAN 4</td> <td>Interface IP ▼</td> </tr> <tr> <td>WAN 5</td> <td>Interface IP ▼</td> </tr> <tr> <td>WAN 6</td> <td>Interface IP ▼</td> </tr> <tr> <td>WAN 7</td> <td>Interface IP ▼</td> </tr> <tr> <td>Mobile Internet</td> <td>Interface IP ▼</td> </tr> </table> </div>	WAN 1	10.90.0.75 (Interface IP) ▼	WAN 2	10.90.0.76 (Interface IP) ▼	WAN 3	Interface IP ▼	WAN 4	Interface IP ▼	WAN 5	Interface IP ▼	WAN 6	Interface IP ▼	WAN 7	Interface IP ▼	Mobile Internet	Interface IP ▼
WAN 1	10.90.0.75 (Interface IP) ▼																
WAN 2	10.90.0.76 (Interface IP) ▼																
WAN 3	Interface IP ▼																
WAN 4	Interface IP ▼																
WAN 5	Interface IP ▼																
WAN 6	Interface IP ▼																
WAN 7	Interface IP ▼																
Mobile Internet	Interface IP ▼																

Click **Save** and then **Apply Changes**, located at the top right corner, to complete the process.

D.6 Inbound Access Restriction

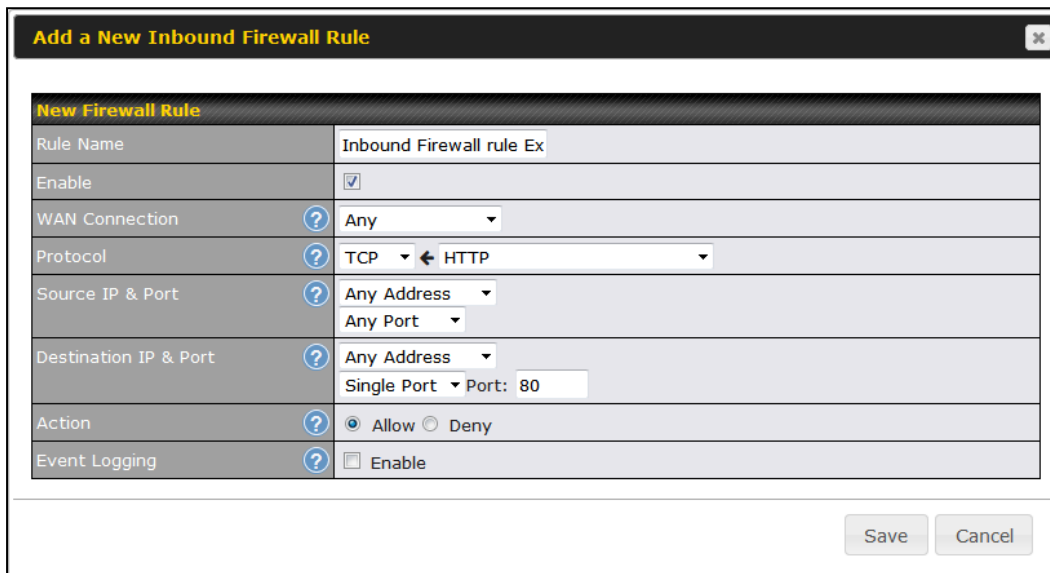
D.6.1 Scenario

A firewall is required in order to protect the network from potential hacker attacks and other Internet security threats.

D.6.2 Solution

Firewall functionality is built into the Peplink Balance. By default, inbound access is unrestricted. Enabling a basic level of protection involves setting up firewall rules.

For example, in order to protect your private network from external access, you can set up a firewall rule between the Internet and your private network. To do so, navigate to **Advanced>Firewall>Access Rules**. Then click the **Add Rule** button in the **Inbound Firewall Rules** table and change the settings according to the following screenshot:



New Firewall Rule	
Rule Name	Inbound Firewall rule Ex
Enable	<input checked="" type="checkbox"/>
WAN Connection	Any
Protocol	TCP HTTP
Source IP & Port	Any Address Any Port
Destination IP & Port	Any Address Single Port Port: 80
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save Cancel

After the fields have been entered as in the screenshot, click **Save** to add the rule. Afterwards, change the default inbound rule to **Deny** by clicking the **default** rule in the **Inbound Firewall Rules** table. Click **Apply Changes** on the top right corner to complete the process.

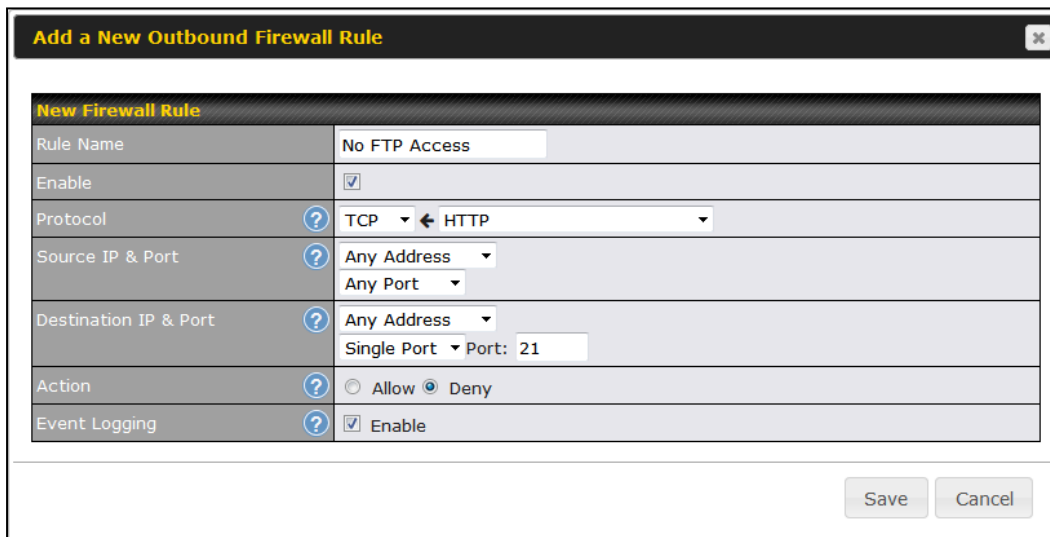
D.7 Outbound Access Restriction

D.7.1 Scenario

For security reasons, it may be appropriate to restrict outbound access. For example, you may want to prevent LAN users from using ftp to transfer files to and from the Internet. This can easily be achieved by setting up an outbound firewall rule with the Peplink Balance.

D.7.2 Solution

To setup a firewall between Internet and private network for outbound access, navigate to **Advanced>Firewall>Access Rules**. Click the **Add Rule** button in the **Outbound Firewall Rules** table, and then adjust settings according the screenshot:



New Firewall Rule	
Rule Name	No FTP Access
Enable	<input checked="" type="checkbox"/>
Protocol	TCP <input type="button" value="←"/> HTTP
Source IP & Port	Any Address Any Port
Destination IP & Port	Any Address Single Port Port: 21
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

Save Cancel

After the fields have been entered as in the screenshot, click **Save** to add the rule. Click **Apply Changes** on the top right corner to complete the process.

Appendix E. Troubleshooting

Problem 1

Outbound load is only distributed over one WAN connection.

Solution

Outbound load balancing can only be distribute traffic evenly between available WAN connections if many outbound connections are made. If there is only one user on the LAN and only one download session is made from his/her browser, the WAN connections cannot be fully utilized.

For a single user, download management applications are recommended. The applications can split a file into pieces and download the pieces simultaneously. Examples include: DownThemAll (Firefox Extension), iGetter (Mac), etc.

If the outbound traffic is going across the SpeedFusion™ tunnel, (i.e., transferring a file to a VPN peer) the bandwidth of all WAN connections will be bonded. In this case, all bandwidth will be utilized and a file will be transferred across all available WAN connections.

For additional details, please refer to this FAQ:

<http://www.peplink.com/knowledgebase/maximizing-your-wan-connections-without-speedfusion/>

Problem 2

I am using a download manager program (e.g., Download Accelerator Plus, DownThemAll, etc.). Why is the download speed still only that of a single link?

Solution

First, check whether all WAN connections are up. Second, ensure your download manager application has split the file into 3 parts or more. It is also possible that all of 2 or even 3 download sessions were being distributed to the same link by chance.

Problem 3

I am using some websites to look up my public IP address, e.g., www.whatismyip.com. When I press the browser's Refresh button, the server almost always returns the same address. Isn't the IP address supposed to be changing for every refresh?

Solution

The web server has enabled the **Keep Alive** function, which ensures that you use the same TCP session to query the server. Try to test with a website that does not enable **Keep Alive**.

For example, try <http://private.dnsstuff.com/tools/aboutyou.ch>. (This third-party web site is provided only for reference. Peplink has no association with the site and does not guarantee the site's validity or availability.)

Problem 4

What can I do if I suspect a problem on my LAN connection?

Solution

You can test the LAN connection using ping. For example, if you are using DOS/Windows, at the command prompt, type *ping 192.168.1.1*. This pings the Peplink Balance device (provided that Peplink Balance's IP is 192.168.1.1) to test whether the connection to the Peplink Balance is OK.

Problem 5

What can I do if I suspect a problem on my Internet/WAN connection?

Solution

You can test the WAN connection using ping, as in the solution to Problem 4. As we want to isolate the problems from the LAN, ping will be performed from the Peplink Balance. By using **Ping/Traceroute** under the **Status** tab of the Peplink Balance, you may be able to find the source of problem.

Problem 6

When I upload files to a server via FTP, the transfer stalls after a few kilobytes of data are sent. What should I do?

Solution

The maximum transmission unit (MTU) or MSS setting may need to be adjusted. By default, the MTU is set at 1440. Choose **Auto** for all of your WAN connections. If that does not solve the problem, you can try the MTU 1492 if a connection is DSL. If problem still persists, change the size to progressive smaller values until your problem is resolved (e.g., 1462, 1440, 1420, 1400, etc).

Additional troubleshooting resources:

Peplink Knowledgebase: <http://www.peplink.com/knowledgebase/>

Peplink Community Forums: <https://forum.peplink.com/>

Appendix F. Declaration

1. CAUTION:

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

2. Federal Communication Commission Interference Statement

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

3. Radiation Exposure Statement (for Balance One):

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

Note: The country code selection is for non-US models only and is not available to all US models. Per FCC regulation, all WiFi products marketed in US must fixed to US operation channels only.

Appendix G: Product Datasheets



Peplink Balance multi-WAN router

Load Balancing. Unbreakable VPN. Bandwidth Bonding.



Peplink Balance Multi-WAN Router

The Peplink Balance multi-WAN router delivers Unbreakable VPN, SpeedFusion™ bandwidth bonding, and a host of other innovative technologies that let you take control of your WAN and improve Internet connectivity, all with one easy-to-manage device.

Connect Up to 13 Links from Multiple Providers

Connect any combination of DSL, cable, 4G LTE, and 3G links – up to 13 of them, from any ISP for anytime, anywhere connectivity. Whatever mix of connections you choose, the Balance intelligently distributes network traffic over all links connected anywhere on the network. You can also customize traffic flow and service availability with outbound policies and inbound load balancing settings, so you're always in control. And with the Balance's instant, automatic failover between links, you're always online, too.

Reduce MPLS Costs up to 90%

With the Balance and SpeedFusion, you can bond multiple links connected anywhere on your network for VPNs that can add speed and reliability to expensive MPLS deployments or replace them entirely. Because you can combine a variety of affordable DSL, MPLS, cellular, and other WAN links into one secure, high-bandwidth tunnel, you get unprecedented reliability and performance while saving big on connectivity costs.

SpeedFusion-powered Unbreakable VPN

The Balance can bond affordable DSL, cable, cellular, and other WAN links into a single secure and fast VPN tunnel using SpeedFusion technology. Packet-level failover across WANs within VPN tunnels is instant and seamless, so your voice calls and RDP sessions won't be interrupted when the Balance automatically switches between connections.

Monitor AP Usage Report and Create Guest Hotspot Easily from Your Balance

Our AP Controller makes it easy to manage your wireless network from a convenient, intuitive user interface built right into your Balance. You can easily manage your AP with graphical usage reports, and detailed event logs. Setting up a guest hotspot? The Balance's included captive portal and splash screen help you provide a secure, fast, and customized Internet experience for everyone.

Try out the Balance Web Admin Demo Now!
peplink.com/demo

Break Internet Bandwidth Limits. Higher Speed. Extreme Reliability.

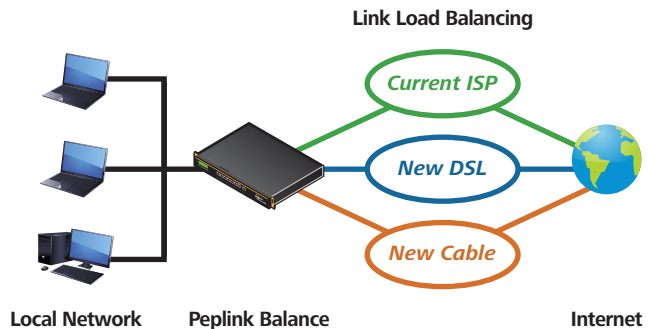
Internet Load Balancing

Boost network data rates, reliability, and flexibility while slashing connectivity costs with Peplink Internet Load Balancing technology. The Peplink Balance can distribute the traffic of up to 13 Internet links and route data using seven intelligent algorithms. It all adds up to high speeds and rock-solid dependability at a savings of up to 90% compared to solutions built on leased lines and other expensive links.

With the Peplink Balance, all your cable, DSL, leased line, cellular, and other links will work together to handle even the most demanding traffic, without lags or downtime. When you need more speed, add more connections.

Prioritize and Balance Traffic by Type or Application

The Peplink Balance incorporates 7 advanced link load balancing algorithms and customizable rules that put you in complete control of network data priorities. Just set your traffic priorities, including VoIP and custom application traffic, with a few clicks and let



Peplink take care of the load balancing and optimization details – day in, day out.

Count on 100% Uptime with Automatic Failover

Automatic Failover keeps your network up and running by continually checking the health of all connected links and routing traffic around inactive or intermittent connections. You can even customize Automatic Failover's behavior, specifying conditional or dedicated backup links that dynamically respond to network status.



Balance 380



Balance 1350

Replace MPLS with a Bonded VPN. SpeedFusion Shifts VPN Traffic into High Gear.

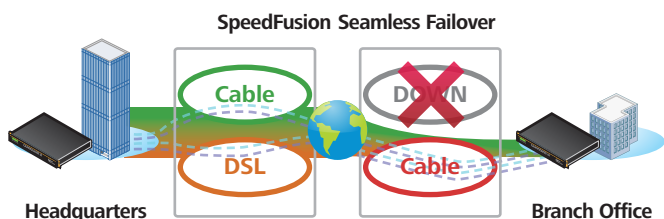
VPN for Branch Networking

Shift WAN data transfer, video delivery, VPNs, and more into overdrive with Peplink SpeedFusion. Peplink's patent-pending SpeedFusion true bandwidth bonding technology combines the bandwidth of up to 13 cable, DSL, 4G LTE/3G, and other links to drive high-speed, high-reliability, and high-security networking – all at a lower cost, with fewer maintenance headaches. Whether you're transferring a single file or sharing dozens of documents, video feeds, and VoIP conversations, SpeedFusion teams up all your links to make it happen faster and more dependably.

optimization. With SpeedFusion, your network stays up and running smoothly, without micromanagement, even when network traffic's at its heaviest.

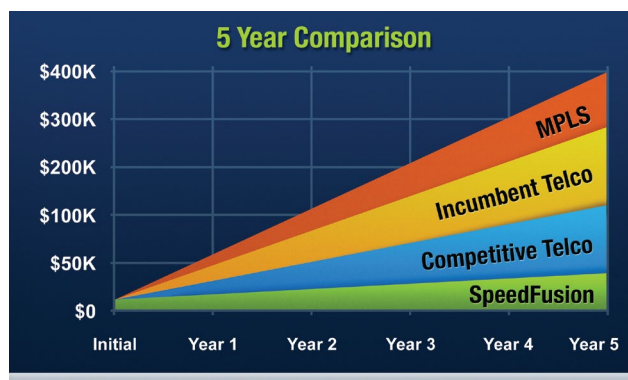
Ditch Expensive MPLS.

Looking for an alternative to expensive leased lines? SpeedFusion bonds the bandwidth of up to 13 cable/DSL, 4G LTE/3G, WiMAX, and other Internet connections from multiple providers, boosting transfer speeds and reliability while saving you money compared to single-line MPLS.



Maximum Performance. Minimum Hassle.

SpeedFusion increases performance across the board with intelligent bonding algorithms, advanced QoS, and video stream



Mobile Bandwidth Bonding. Turbocharge Mobile VPNs.

4G LTE/3G Bandwidth Bonding

SpeedFusion, the technology at the heart of every Balance Multi-WAN and MAX Mobile router, bonds the bandwidth from multiple cellular connections. You get faster and more reliable mobile VPNs in every application. Plus, all your data is secured by military-grade encryption, and data volume is monitored and controlled to keep you under your usage cap and within budget.



Get the Speed You Need on the Road.

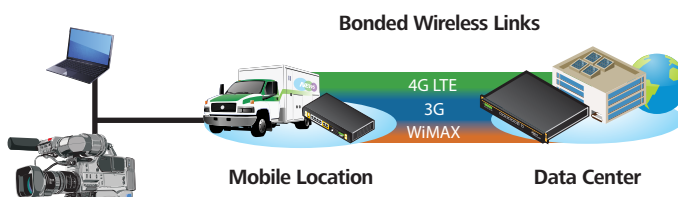
SpeedFusion Bandwidth Bonding automatically aggregates all connected 4G LTE/3G/WiMAX links to give you fast data transfers, smooth HD video, and blazing performance wherever you go. Need more speed? Just add cellular connections and let SpeedFusion take care of the details.

Enjoy Wired Reliability without the Wires.

SpeedFusion bonds cellular connections from multiple providers, continuously monitoring link connectivity and automatically switching to healthy connections in the event of link failure. Your network stays up and running, and you stay open for business.

Do More on the Road with SpeedFusion.

The speed, reliability, and security delivered by SpeedFusion open up a wide range of new mobile VPN applications in demanding, mission-critical fields, such as newscasting and public safety. In addition, transferring large files, such as those generated by digital production, photography, and POS activities, becomes practical and profitable wherever your mobile workforce roams.



MAX



AP One

All-in-One AP Controller Solution. Manage hundreds of APs. Built-in Captive Portal.

AP Controller Solution

Peplink's AP Controller solution combines an enterprise-grade wireless access point and centralized access point management in one easy-to-use and affordable package. Now you can manage wireless LAN networks of up to 1,500 Peplink AP One devices using a single Peplink Balance. With Peplink's AP Controller solution, all your mobile devices, including iPhones, iPads, and Android devices, get the same reliable Internet connection that you've come to expect from Peplink – without the wires!

Built-in AP Controller

Simplify your network management by controlling your AP One access points using a centralized admin interface built into the Peplink Balance. Just connect an AP One to the network and it will be discovered by the Balance automatically, allowing you manage and set-up your access point instantly!

Easy Wi-Fi Portal

Peplink's AP Controller solution features a built-in captive portal, which allows you to provide Wi-Fi hotspot service to your customers or Wi-Fi access to your guests in a corporate environment. From showing a splash screen for free users to accept service terms to creating a user login for your paid customers, you can easily customize your Wi-Fi portal in just a few clicks.

Unified Network Management

With our AP Controller solution, you can manage all network connections, local client access, and user bandwidth policy using one single package. Administrators can monitor and generate reports on AP activity and bandwidth consumption, giving you complete and easy control over your network.



Specifications



	20/30/50	30 LTE	One	210/310	305	380	580	710	1350	2500
Designed For	Power User & Home Office		Small Business		Mid-Size Business			Large Enterprise/Campus		
Ethernet WAN Ports	2/3/5	2	2 (GbE)	2+3 (GbE)	3 (GbE)	3 (GbE)	5 (GbE)	7 (GbE)	13 (GbE)	12 (GbE)
LAN Ports	4 (GbE)	4 (GbE)	8 (GbE)	7 (GbE)	3 (GbE)	3 (GbE)	3 (GbE)	3 (GbE)	3 (GbE)	8(GbE) /2(10G SFP+)^
USB WAN Modem Port ¹	1	1	1	1	1	1	1	1	1	1
Embedded LTE Modem	○	1	○	○	○	○	○	○	○	○
Wi-Fi Interface	○	○	802.11a/b/g/n AP ⁵	○	○	○	○	○	○	○
Recommended Users ²	1-60	1-60	1-60	25-150	50-500	50-500	300-1000	500-2000	1000-5000	5000-20000+
Router Throughput	150Mbps	150Mbps	600Mbps	200Mbps	1Gbps	1Gbps	1.5Gbps	2.5Gbps	5Gbps	8Gbps
Load Balancing/Failover	●	●	●	●	●	●	●	●	●	●
Drop-In Mode	○	○	○	●	●	●	●	●	●	●
Inbound Load Balancing	○	○	○	●	●	●	●	●	●	●
SpeedFusion Bandwidth Bonding	○	○	● [#]	●	● [#]	●	●	●	●	●
Number of SpeedFusion Peers ³	○	○	2	2	2/20 [%]	20	50	300	800	4000
SpeedFusion Throughput	○	○	30Mbps	50Mbps	150Mbps	150Mbps	200Mbps	400Mbps	800Mbps	2Gbps
PPTP VPN Server	●	●	●	●	●	●	●	●	●	●
IPsec VPN (Network-to-Network)	●	●	●	●	●	●	●	●	●	●
Manage Pepwave AP Series	●	●	●	●	●	●	●	●	●	●
Maximum Number of AP Supported	10	10	10	10	50	50	100	250	500	2000
Manage Remote AP & Multiple Config Profiles	○	○	○	○	● [°]	● [°]	● [°]	● [°]	● [°]	● [°]
Bandwidth Usage Monitor	●	●	●	●	●	●	●	●	●	●
QoS for VoIP and E-commerce	●	●	●	●	●	●	●	●	●	●
User Groups Bandwidth Control	●	●	●	●	●	●	●	●	●	●
Web Blocking	●	●	●	●	●	●	●	●	●	●
1U Rackmount	○	○	○	●	●	●	●	●	●	●
High Availability	○	○	○	●	●	●	●	●	●	●
LAN Bypass	○	○	○	○	●	●	●	●	●	●
Dual Hot Swap Power Supply	○	○	○	○	○	○	○	○	○	●

¹ For a list of supported modems, please refer to: <http://www.peplink.com/modem> ² Recommendation for sizing purposes only. No software restrictions applied. ³ Number of peer Peplink or Pepwave devices you can connect using SpeedFusion. [°]The Balance 210 has 2 WAN ports activated by default. The third WAN port can be activated by an optional license key. [°]Available in BPL-ONE. [#] SpeedFusion is available as an optional feature. [%]Balance 305 supports 2 PepVPN peers. With purchase of SpeedFusion License, the Balance 305 supports up to 20 SpeedFusion peers. [°]Balance 20/30/30 LTE/50/One/210/310 comes with AP Controller Standard, which supports one configuration profile with multiple SSIDs, meaning that all APs will share the same configuration, and you can only manage APs on the local physical LAN. Balance 305/380/580/710/1350/2500 comes with AP Controller Pro, which supports multiple configuration profiles with multiple SSIDs, and you can manage remote APs outside the local physical LAN. [^] Balance 2500 is available in two configurations with different LAN interfaces.

Ordering Information

Balance One

Product Code	Description
BPL-ONE	Advanced Dual-WAN Router. 8x GbE LAN Ports. Built-in simultaneous dual-band 802.11a/b/g/n Wi-Fi AP with embedded antennas.
BPL-ONE-CORE	Advanced Dual-WAN Router. 8x GbE LAN Ports.

Balance 30 LTE

Product Code	Carrier	Description
BPL-031-LTE-US-T	Verizon/AT&T/T-Mobile	4G LTE: B2/1900, B4/AWS (XLTE), B5/850, B13/700, B17/700, B25/190
BPL-031-LTE-E-T	Europe/International	4G LTE: B1/2100, B3/1800, B7/2600, B8/900, B20/800

Balance 2500

Product Code	Description
BPL-2500	12x GbE WAN ports and 8x GbE LAN ports. Supports LACP (802.3ad) NIC bonding.
BPL-2500-SFP	12x GbE WAN ports and 2x 10G SFP+ LAN ports.

Features

- WAN**

 - Support for PPPoE, Static IP, DHCP
 - WAN Link Health Check
 - Bandwidth Allowance Monitor
 - IPv6 Support
 - USB 4G LTE/3G Modem Support
 - Support for Dynamic DNS Services
 - WAN Port Convertible into LAN Port
- LAN**

 - DHCP Server for LAN Clients
 - Extended DHCP Options
 - DHCP Reservation
 - DNS Proxy for LAN Clients
 - VLAN on LAN Support
- DNS**

 - Built-in Authoritative DNS, Support for A, CNAME, NS, MX, PTR, SOA, SRV, TXT Records

- Load Balancing**

 - Intelligent Failover
 - Session Persistence
 - Per-Service Load Distribution
 - Multiple Algorithms
- Complete VPN Solution**

 - PepVPN/SpeedFusion
 - Site-to-Site VPN
 - Bandwidth Aggregation
 - Intelligent Failover
 - 256-bit AES Encryption
 - Pre-shared Key Authentication
 - Dynamic Routing
 - X.509 Certificate Support
 - PPTP VPN Server
 - RADIUS, LDAP Authentication
 - IPsec VPN (Network-to-Network)
 - X.509 Certificate Support

- Advanced QoS**

 - User Groups
 - Bandwidth Reservation
 - Individual Bandwidth Limit
 - Application Prioritization
 - By User Groups
 - SIP, HTTPS, VPN QoS
 - Custom Application QoS
- Networking**

 - NAT and IP Forwarding
 - Static Routes
 - Port Forwarding
 - Many to One, One to One NAT
 - NAT Pool
 - SIP ALG, H.323 ALG
 - UPnP, NAT-PMP
 - WINS Server
 - OSPFv2 and RIPv2

- AP Controller**

 - Support for Pepwave AP Series
 - Auto AP Discovery
 - Auto AP Firmware Management
 - AP Profile Configuration
 - Wi-Fi usage statistics
- Captive Portal**

 - Support for Wired and Wireless LAN Clients
 - Support RADIUS Authentication
 - Support LDAP Authentication
 - Time and Usage Quotas on Open Access Mode
 - Built-in Customizable Splash Page
- Security**

 - DoS Prevention
 - Stateful Firewall
 - Web Blocking Support
 - Web Filtering Blacklists

Specifications vary across different Balance models. For the most updated specifications, please refer to our website: <http://www.peplink.com/balance/>



Peplink MediaFast

Lightning Fast Content Delivery. And So Much More.



Works with:



iTunes U



iOS Updates



TED.com

and more...



MediaFast 500

MediaFast is our supercharged content caching solution. Designed with education and entertainment in mind, it downloads and accelerate video, iTunes U, iOS updates, app download, and other content for uninterrupted learning and fun anytime.

Prefetch. Off-Peak Downloads. Anytime, Anywhere Playback.

Schedule one-time or recurring content downloads during off-peak hours, and then playback downloaded content anytime. Need HD video and other content in places with spotty or congested Internet connections? Download whenever and wherever the connection is best. Then pack up and take the MediaFast anywhere you need seamless content delivery.

Cache. Download x1. Playback x ∞ .

Cache iTunes/iTunes U and other content automatically by domain and file type. With MediaFast, you can download once and play back over and over again, cutting loading time, bandwidth usage and cost. Keep content as long as you like or purge it automatically by file type and age.

Reporting. Insight. On-Demand.

Check bandwidth usage and savings. Track popular URLs and file types. You can also monitor client IP addresses, find your heaviest users, and more, all from a single intuitive interface.

iOS and App Caching.

Managing hundreds of iPads at your campus? The MediaFast can cache iOS updates and app downloads. Download the updates once, and apply to all iPads without consuming extra bandwidth or stressing the network.

SpeedFusion. Bonded Bandwidth. 24/7 Connectivity.

Take advantage of all available connections with SpeedFusion bandwidth bonding and load balancing. Automatic failover keeps your learners learning and teachers teaching, even when a link fails.

InControl 2 and AP Controller. Your Network. At Your Fingertips.

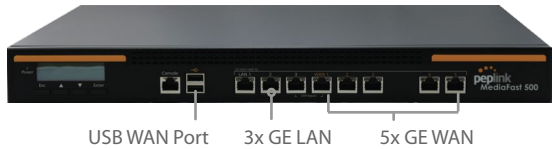
Monitor and manage routers, access points, and other connected devices with InControl 2 and AP Controller. Wi-Fi networks are easy to set up, and you get complete control over your entire wireless and wired network from any compatible web browser.

Specifications

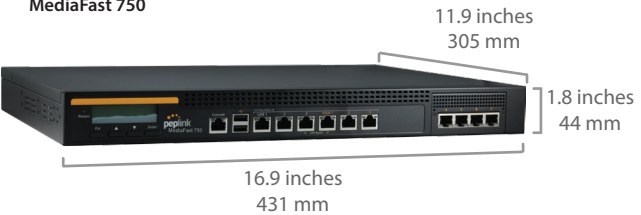
	Branch Office/Hotspot	School/Campus	
	MediaFast 200	MediaFast 500	MediaFast 750
Product Code	MFA-200-W	MFA-500-B	MFA-750-B
Cache Throughput	200Mbps	1.5Gbps	2.5Gbps
Router Throughput	200Mbps	800Mbps	1.5Gbps
Cache Storage	120GB SSD	500GB SSD	1TB SSD
Recommended Users	25-150	300-1000	500-2000
WAN Interface	2x GE 1x USB Interface	5x GE 1x USB Interface	7x GE 1x USB Interface
Wi-Fi Interface	Simultaneous Dual-Band 802.11a/b/g/n AP	○	○
LAN Interface	8 (GbE) 802.3af PoE Output*	3 (GbE)	3 (GbE)
Video and Content Caching	●	●	●
Multi-WAN Load Balancing	●	●	●
PepVPN	●	●	●
Web Filtering Blacklist	Light	Full	Full
SpeedFusion Hot Failover	●#	●	●
SpeedFusion WAN Smoothing	●#	●	●
SpeedFusion Bandwidth Bonding	●#	●	●
Number of PepVPN/ SpeedFusion Peers	2	50	300
InControl Cloud Management	●	●	●
AP Controller	●	●	●
Maximum No. of AP Supported	50	100	250
Manage Remote AP & Multiple Config Profiles	○	●	●
Operating Temperature	32° – 104°F (0° – 40°C)		

*PoE Kit is available separately. # Available as optional features.

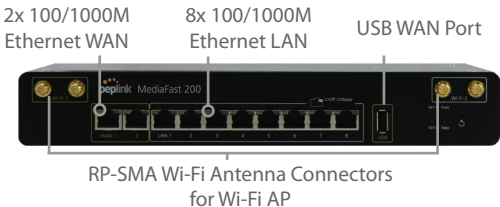
MediaFast 500



MediaFast 750



MediaFast 200



Features

- WAN**

 - Support for PPPoE, Static IP, DHCP
 - WAN Link Health Check
 - Bandwidth Allowance Monitor
 - USB 4G LTE/3G Modem Support
 - Support for Dynamic DNS Services
 - IPv6 Support
- LAN**

 - DHCP Server for LAN Clients
 - Extended DHCP Options
 - DHCP Reservation
 - DNS Proxy for LAN Clients
- DNS***

 - Built-in Authoritative DNS
 - Support for A, CNAME, NS, MX, PTR, SOA, SRV, TXT Records
- Advanced QoS**

 - User Groups
 - Bandwidth Reservation*
 - Individual Bandwidth Limit
 - Application Prioritization
 - By User Groups
 - SIP, HTTPS, VPN QoS
 - Custom Application QoS
- Caching**

 - Video Caching
 - iTunes
 - iTunes U
 - TED.com
 - Content Caching
 - HTML
 - JavaScript
 - Image
 - Flash Applications
- Networking**

 - NAT and IP Forwarding
 - Static Routes
 - Port Forwarding
 - Many to One, One to One NAT
 - NAT Pool
 - SIP ALG, H.323 ALG
 - UPnP, NAT-PMP
 - WINS Server
 - OSPF and RIPv2 support*
- AP Controller**

 - Support for Pepwave AP Series
 - Auto AP Discovery
 - Auto AP Firmware Management
 - AP Profile Configuration
 - Wi-Fi usage statistics
- Load Balancing**

 - Intelligent Failover
 - Session Persistence
 - Per-Service Load Distribution
 - Multiple Algorithms
- Complete VPN Solution**

 - PepVPN/SpeedFusion
 - Site-to-Site VPN
 - Bandwidth Aggregation
 - Intelligent Failover
 - 256-bit AES Encryption
 - Pre-shared Key Authentication
 - Dynamic Routing
 - PPTP VPN Server
 - RADIUS, LDAP Authentication
 - IPsec VPN (Network-to-Network)
- Device Management**

 - Web Administrative Interface
 - Command Line Interface
 - InControl Cloud Management
 - Router Utility Mobile App
 - Email Notification
 - Active Client & Session Lists
 - Bandwidth Usage Statistics
 - Syslog Service
 - SNMP v1, v2c and v3
- Security**

 - Stateful Firewall
 - DoS Prevention
 - Web Filtering Blacklist

*Specifications vary across different models. For the most updated specifications, please refer to our website.



United States
T: +1 (650) 450 9668
E: sales@peplink.com

www.peplink.com

Peplink Balance One

Advanced Dual-WAN Router for Branch Networking.



Works With



And 250+ USB Modem from Worldwide Carriers



One Huge Leap Forward for SMB, and Branch Networking.

The Balance One router with dual-WAN load balancing delivers big-business uptime and speed in an affordable package designed just for SMBs, branch offices, and power users. Featuring:



600Mbps Throughput. Dual WAN Support.

Drives data at 600Mbps and keeps connections dependable and fast with automatic balancing and failover between links.



Built-in AP Controller and InControl 2.

Built in AP Controller or InControl 2 cloud management puts you in charge of all connected access points, create and manage custom captive portals.



Simultaneous Dual-Band Wi-Fi. (Balance One Only)

Balance One (BPL-ONE) gives you two independent networks that also work together, so all your devices can connect without clashing. Recommended Concurrent Users Per Radio is 60.



Remote User VPN



QoS: Assign Priority



Enterprise Features.

Connect remote clients to your private network using L2TP with IPsec, monitor Bandwidth Usage, allocate bandwidth for user groups, and more.

Eight GbE LAN Ports.

Connect all your devices at high speeds, without complicated setup, compromises, or external switches to buy and maintain.

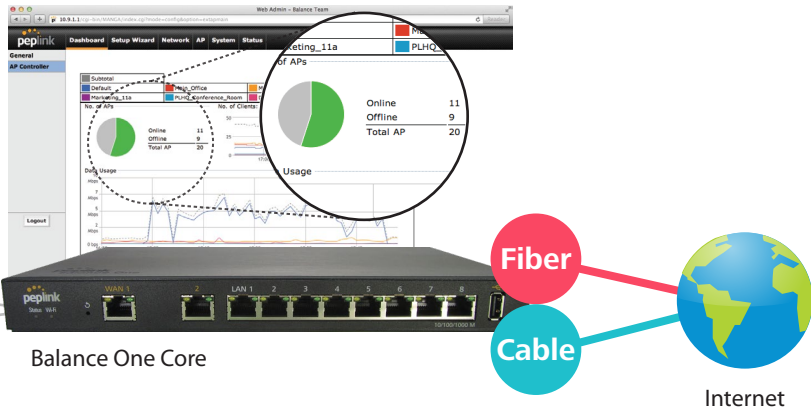


Unparalleled Modem Support.

The Balance One's USB port supports more than 250 4G LTE/3G modems used by a variety of carriers worldwide.

Setup, Manage, and Monitor Office Wi-Fi from Your Balance One

- 1 Provision AP One access points with the Balance One's built-in AP Controller
- 2 Web blocking keeps your staff out of unwanted websites and help them stay productive
- 3 Get detailed access point usage reports anytime, right from your Balance One



The AP One is available in a variety of configurations. Visit peplink.com/ap for details.

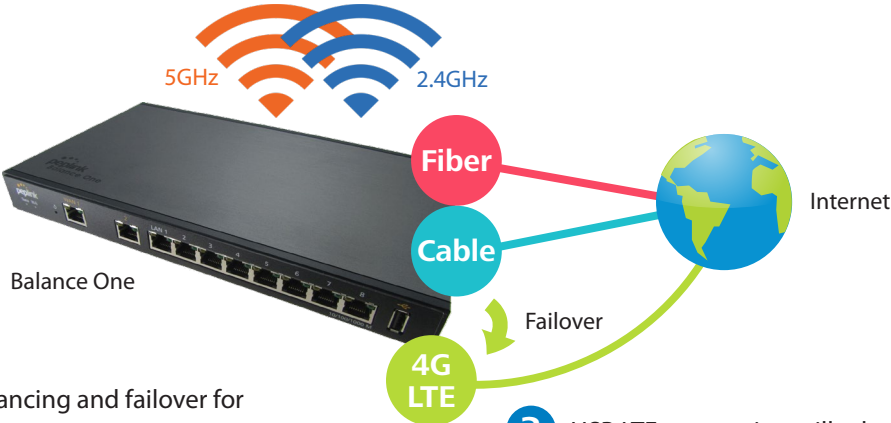


Connect Your Home Office with LTE Backup for 100% Uptime

- 4 The Balance One has simultaneous dual-band 11n Wi-Fi for your wireless devices



- 1 600Mbps capacity for your blazing fast fiber Internet



- 2 Dual-WAN load balancing and failover for unparalleled uptime

- 3 USB LTE connection will take place when Ethernet connections are down

Specifications

Balance One / Balance One Core	
WAN Interface	2x 10/100/1000M Ethernet Ports 1x USB Interface
LAN Interface	8x 10/100/1000M Ethernet Ports
Wi-Fi Interface	Simultaneous Dual-Band 802.11a/b/g/n Access Point*
Wi-Fi AP Operating Frequency	2412 – 2472 and 5180 - 5825 MHz*
Router Throughput	600Mbps
Recommended Users	1-60
Number of VPN/SpeedFusion Peers	2
PepVPN/SpeedFusion Throughput	30Mbps
Power Input	Device: 12V – 24V DC AC Adapter: AC Input 100V – 240V, DC Output 12V
Power Consumption	15W (max.)
Dimension	1.2 x 10.7 x 6.3 inches 30 x 271 x 160 mm (H x W x D)
Weight	1.3 pound 570 grams
Operating Temperature	-40° – 149°F -40° – 65°C
Humidity	15% – 95% (non-condensing)
Certifications	FCC, CE, RoHS
Warranty	1-Year Limited Warranty

*Wi-Fi is available on Balance One(BPL-ONE) only.



Product Ordering Information

Product Code	802.11a/b/g/n AP	Dual-WAN	PepVPN	SpeedFusion Hot Failover/ SpeedFusion Bandwidth Bonding
BPL-ONE-CORE	○	●	●	Feature Add-On (BPL-ONE-LC-SF)
BPL-ONE	●	●	●	Feature Add-On (BPL-ONE-LC-SF)

Feature Add-On		
Product Code	Applicable to	Description
BPL-ONE-LC-SF	BPL-ONE/BPL-ONE-CORE	SpeedFusion bonding license

Features

WAN USB 4G/3G Modem Support Support for PPPoE, Static IP, DHCP Support for Dynamic DNS services WAN Link Health Check Intelligent Failover Bandwidth Allowance Monitor	AP Controller AP Controller Support Wi-Fi Usage Statistics Complete VPN Solution PepVPN/SpeedFusion ^ Site-to-Site VPN Bandwidth Aggregation ^ Hot Failover ^ 256-bit AES Encryption Pre-shared Key Authentication Dynamic Routing L2TP with IPsec VPN Server PPTP VPN Server RADIUS, LDAP Authentication IPsec VPN (Network-to-Network)	Load Balancing Intelligent Failover Session Persistence Per-Service Load Distribution Multiple Algorithms Networking NAT and IP Forwarding Static Routes Port Forwarding Many to One, One to One NAT NAT Pool SIP ALG, H.323 ALG UPnP, NAT-PMP WINS Server	Advanced QoS User Groups Bandwidth Reservation Individual Bandwidth Limit Application Prioritization By User Groups SIP, HTTPS, VPN QoS Custom Application QoS Web Blocking Blacklist Captive Portal Support Support for Wired and Wireless LAN Clients Support RADIUS Authentication Time and Usage Quotas on Open Access Mode Built-in Customizable Splash Page	Device Management Web Administrative Interface Command Line Interface InControl Cloud Management Email Notification Active Client & Session Lists Bandwidth Usage Statistics Syslog Service SNMP v1, v2c and v3 Package Content Balance One/Balance One Core 12V Power Supply
---	--	---	--	--

^ SpeedFusion is available as an optional add-on



Contact Us:

Sales

<http://www.peplink.com/contact/sales/>

Support

<http://www.peplink.com/contact/>

Certified Peplink Partner

<http://www.peplink.com/partners/channel-partner-program/>