



# Peplink Balance and MediaFast User Manual

## Peplink Products:

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

MediaFast 200/500/750

Peplink Balance Firmware 7.1.1

August 2018

## Table of Contents

<b>Introduction and Scope</b>	<b>8</b>
<b>Glossary</b>	<b>9</b>
<b>Product Comparison Chart</b>	<b>11</b>
<b>Product Features</b>	<b>13</b>
Supported Network Features	13
Other Supported Features	16
<b>Advanced Feature Summary</b>	<b>17</b>
Drop-in Mode and LAN Bypass: Transparent Deployment	17
QoS: Clearer VoIP	18
Per-User Bandwidth Control	19
High Availability via VRRP	19
USB Modem and Android Tethering	20
Built-In Remote User VPN Support	21
LACP NIC Bonding	22
<b>Package Contents</b>	<b>23</b>
Peplink Balance One	23
Peplink Balance 20/30/30 LTE/50	23
Peplink Balance 30 LTE/30 Pro	23
Peplink Balance 210/310	23
Peplink Balance 305/380/580/710/1350/2500	23
Peplink MediaFast 200	24
Peplink MediaFast 500	24
<b>Peplink Balance Overview</b>	<b>24</b>
Peplink Balance One	24
Peplink Balance 20	25
Peplink Balance 30 LTE	27
Peplink Balance 30 Pro	28
Peplink Balance 50	29

Peplink Balance 210	31
Peplink Balance 310	32
Peplink Balance 305	33
Peplink Balance 380	35
Peplink Balance 580	36
Peplink Balance 710	37
Peplink Balance 1350	38
Peplink Balance 2500	39
<b>Peplink MediaFast Overview</b>	<b>41</b>
Peplink MediaFast 200	41
Peplink MediaFast 500	42
Peplink MediaFast 750	43
<b>LCD Display Menu</b>	<b>45</b>
<b>Installation</b>	<b>46</b>
Preparation	46
Constructing the Network	46
<b>Basic Configuration</b>	<b>47</b>
Connecting to the Web Admin Interface	47
Configuration with the Setup Wizard	49
<b>Network Tab</b>	<b>53</b>
WAN	53
Health Check Settings	59
Bandwidth Allowance Monitor Settings	63
Additional Public IP Settings	63
Dynamic DNS Settings	64
LAN	66
Network Settings	66
Network Settings (Common Settings)	70
Port Settings	74
VPN	74
SpeedFusion	75
IPsec VPN	81
Outbound Policy	85

Inbound Access	88
Servers	88
Services	89
DNS Settings	92
SOA Records	95
NS Records	96
MX Records	97
CNAME Records	97
A Records	98
PTR Records	99
TXT Records	100
SRV Records	100
Reverse Lookup Zones	101
SOA Record	102
NS Records	103
CNAME Records	103
PTR Records	105
DNS Record Import Wizard	105
NAT Mappings	109
MediaFast	111
Setting Up MediaFast Content Caching	112
Viewing MediaFast Statistics	113
Prefetch Schedule	114
ContentHub	116
MDM Settings	118
Captive Portal	118
QoS	121
User Groups	122
Bandwidth Control	123
Application	123
Prioritization for Custom Application	124
DSL/Cable Optimization	125
Firewall	125
Access Rules	125
Intrusion Detection and DoS Prevention	129



Content Blocking	130
Application Blocking	132
Web Blocking	132
Customized Domains	132
Exempted User Groups	132
Exempted Subnets	133
URL Logging	133
OSPF & RIPv2	133
BGP	135
Remote User Access	138
Misc. Settings	140
High Availability	140
Certificate Manager	143
Service Forwarding	143
SMTP Forwarding	145
Web Proxy Forwarding	145
DNS Forwarding	146
Custom Service Forwarding	146
Service Passthrough	146
<b>AP Tab</b>	<b>147</b>
AP	147
AP Controller	147
Wireless SSID	148
Settings	154
AP Controller Status	158
Info	158
Access Points (Usage)	160
Wireless SSID	162
Wireless Client	163
Nearby Device	164
Event Log	165
Toolbox	166
<b>System Tab</b>	<b>166</b>
System	167

Admin Security	167
Firmware	169
Time	170
Schedule	171
Email Notification	173
Event Log	175
SNMP	175
InControl	178
Configuration	179
Feature Add-ons	180
Reboot	180
Tools	180
Ping	181
Traceroute	181
Wake-on-LAN	182
CLI (Command Line) Support	182
<b>Status Tab</b>	<b>183</b>
Status	183
Device	183
Active Sessions	185
Client List	187
WINS Clients	188
OSPF & RIPv2	188
MediaFast	188
SpeedFusion Status	189
Event Log	193
Device Event Log	194
IPsec Event Log	194
Bandwidth	194
Real-Time	194
Hourly	195
Daily	196
Monthly	198
Harrington Industrial Plastics	206

PLUSS

209

# 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:

- Peplink Balance One
- Peplink Balance 20
- Peplink Balance 30 LTE
- Peplink Balance 30 Pro
- 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.

## 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.

	20/50	30LTE	One	210	310	305	380
WAN Ports	2/5	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

\*Wi-Fi is not available on the Balance One Core

Full product comparison available at:

<http://www.peplink.com/products/balance/model-comparison/>

	580	710	1350	2500	MFA 200	MFA 500	MFA 750
WAN Ports	5	7	13	12	2	5	7
Throughput (Mbps)	1.5G bps	2.5G bps	5Gbp s	8Gbp s	200	800	1.5G bps
<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

#### 4.1.1 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

#### 4.1.2 LAN

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

#### 4.1.3 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

#### **4.1.4 Inbound Traffic Management**

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

#### **4.1.5 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

#### **4.1.6 AP Controller**

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

#### **4.1.7 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

#### **4.1.8 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

#### **4.1.9 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

## 4.2 Other Supported Features

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

## 5 Advanced Feature Summary

### 5.1 Drop-in Mode and LAN Bypass: Transparent Deployment



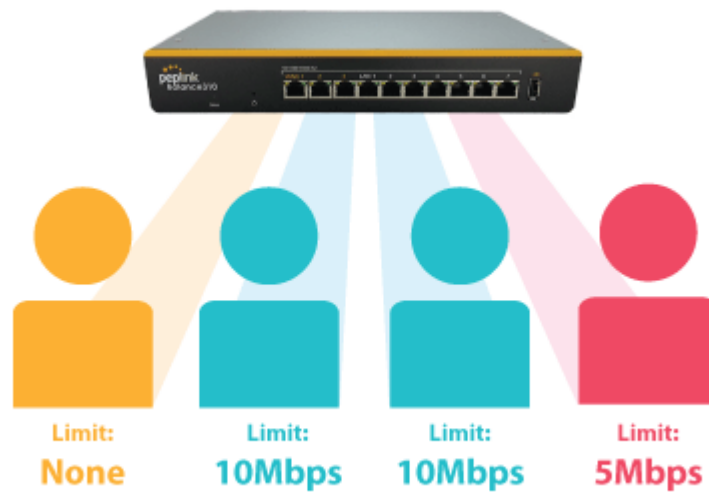
As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass**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

## 5.2 QoS: Clearer VoIP



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

### 5.3 Per-User Bandwidth Control



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

### 5.4 High Availability via VRRP



When your organization has a corporate requirement demanding the highest availability with no single point of failure, you can deploy two Peplink routers in [High Availability mode](#). With High

Availability mode, the second device will take over when needed.

## 5.5 USB Modem and Android Tethering



For increased WAN diversity, plug in a USB LTE modem as backup. Peplink routers are compatible with over [200 modem types](#). You can also tether to smartphones running Android 4.1.X and above.



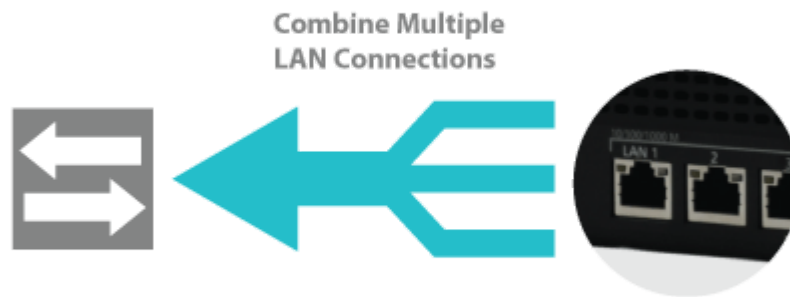
## 5.6 Built-In Remote User VPN Support



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

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

## 5.7 LACP NIC Bonding



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

## 6 Package Contents

The contents of Peplink Balance product packages are as follows:

### 6.1 Peplink Balance One

- Peplink Balance One
- Power adapter
- Information slip

### 6.2 Peplink Balance 20/30/30 LTE/50

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

### 6.3 Peplink Balance 30 LTE/30 Pro

- Peplink Balance 30 LTE/30 Pro
- 4G LTE Antennas
- Wi-Fi Antennas (B30 Pro)
- Power adapter
- Information slip
- Rackmount kit

### 6.4 Peplink Balance 210/310

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

### 6.5 Peplink Balance 305/380/580/710/1350/2500

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

## 6.6 Peplink MediaFast 200

- Peplink MediaFast 200
- Power adapter
- Information slip

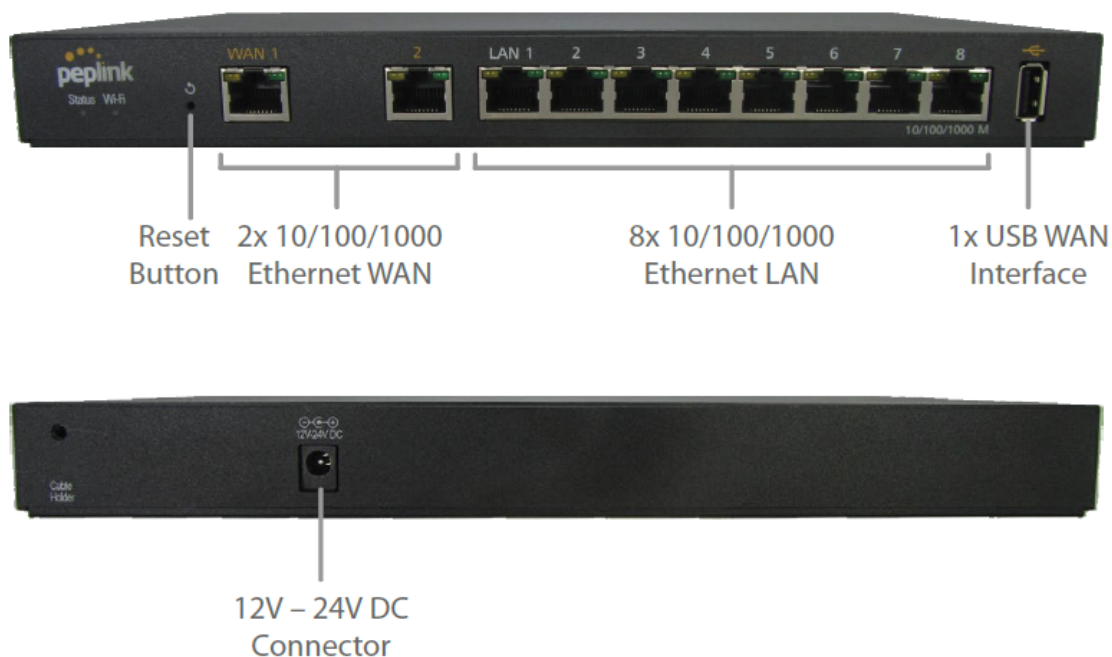
## 6.7 Peplink MediaFast 500

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

# 7 Peplink Balance Overview

## 7.1 Peplink Balance One

### 7.1.1 Panel Appearance



### 7.1.2 LED Indicators

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

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

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

USB Port	
<b>USB Ports</b>	For future functionality

## 7.2 Peplink Balance 20

### 7.2.1 Panel Appearance



### 7.2.2 LED Indicators

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

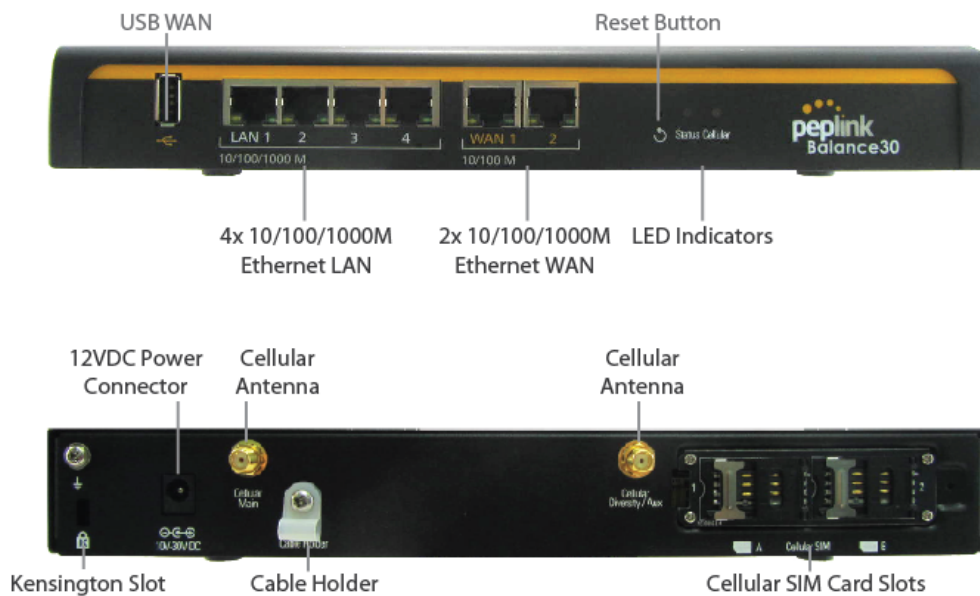
Power and Status Indicators	
<b>Power</b>	OFF – Power off
	Green – Power on
<b>Status</b>	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
<b>USB Ports</b>	For connecting a 4G/3G USB modem

## 7.3 Peplink Balance 30 LTE

### 7.3.1 Panel Appearance



### 7.3.2 LED Indicators

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

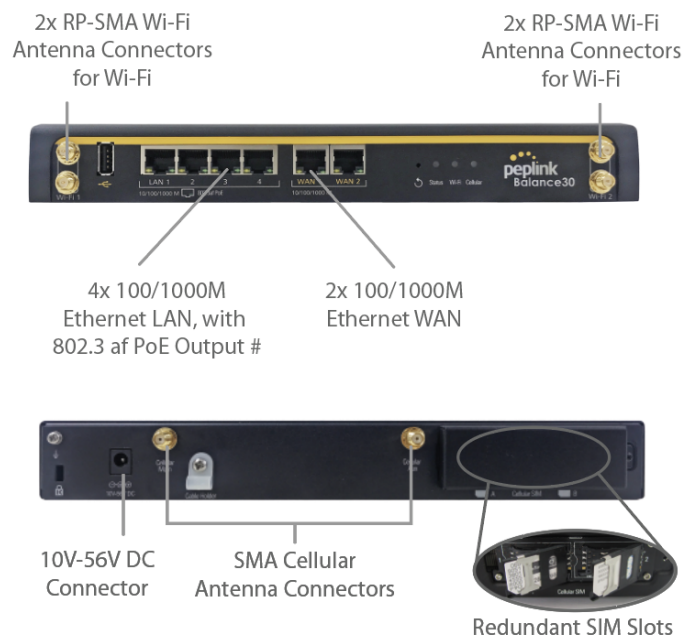
Power and Status Indicators	
<b>Power</b>	OFF – Power off
	Green – Power on
<b>Status</b>	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
<b>USB Ports</b>	For connecting a 4G/3G USB modem

## 7.4 Peplink Balance 30 Pro

### 7.4.1 Panel Appearance





## 7.4.2 LED Indicators

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

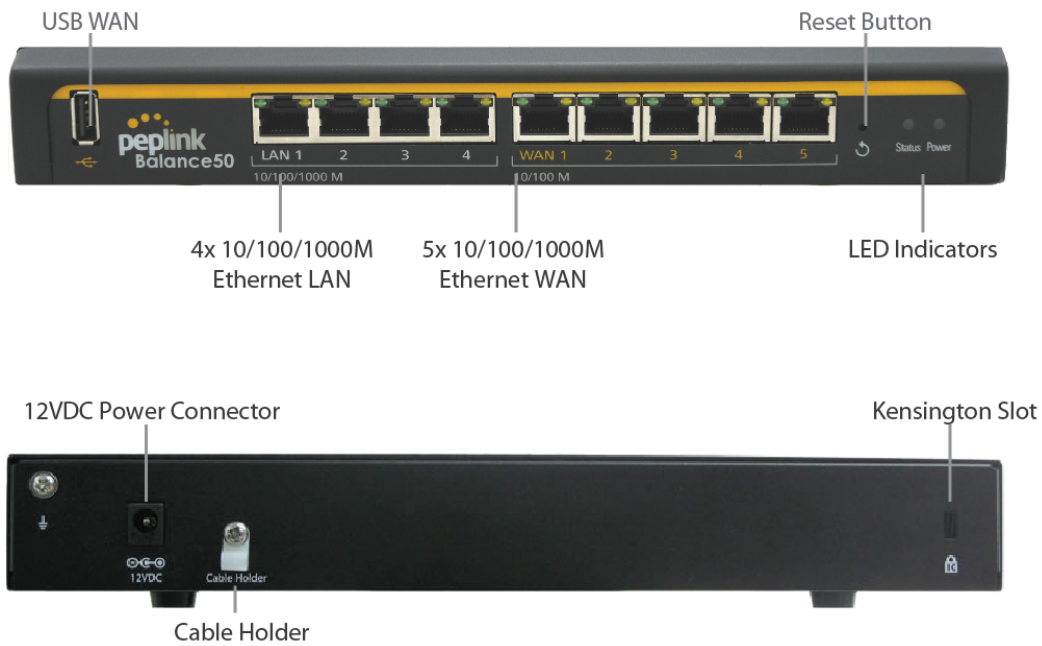
Power and Status Indicators	
<b>Power</b>	OFF – Power off
	Green – Power on
<b>Status</b>	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
<b>USB Ports</b>	For connecting a 4G/3G USB modem

## 7.5 Peplink Balance 50

### 7.5.1 Front Panel Appearance



### 7.5.2 LED Indicators

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

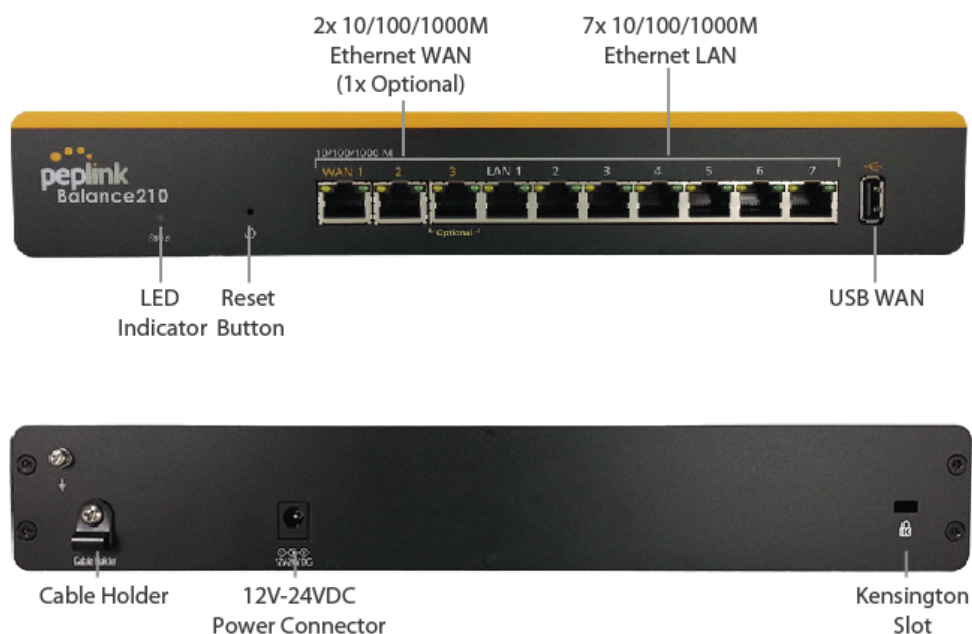
Power and Status Indicators	
<b>Power</b>	OFF – Power off
	Green – Power on
<b>Status</b>	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
<b>USB Ports</b>	For connecting a 4G/3G USB modem

## 7.6 Peplink Balance 210

### 7.6.1 Front Panel Appearance



### 7.6.2 LED Indicators

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

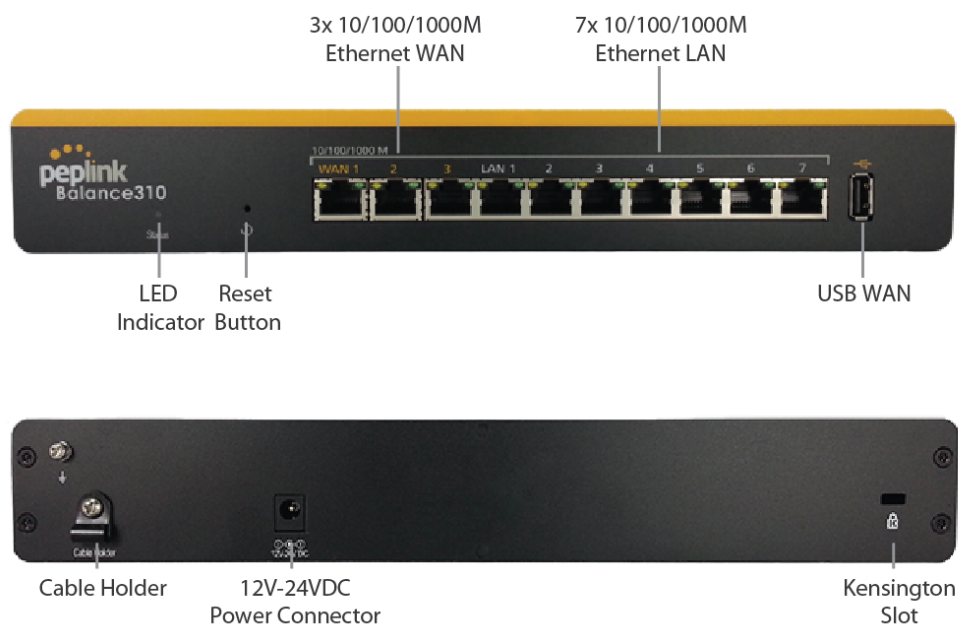
Power and Status Indicators	
<b>Status</b>	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
<b>USB Ports</b>	For connecting a 4G/3G USB modem

## 7.7 Peplink Balance 310

### 7.7.1 Front Panel Appearance



### 7.7.2 LED Indicators

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

Power and Status Indicators	
-----------------------------	--

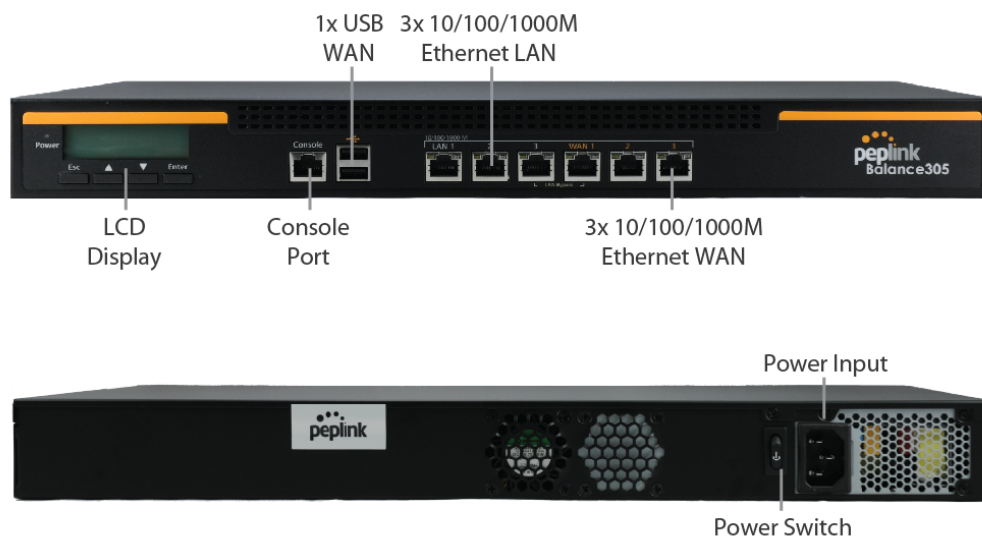
<b>Status</b>	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

USB Port	
<b>USB Ports</b>	For connecting a 4G/3G USB modem

## 7.8 Peplink Balance 305

### 7.8.1 Front Panel Appearance



## 7.8.2 LED Indicators

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

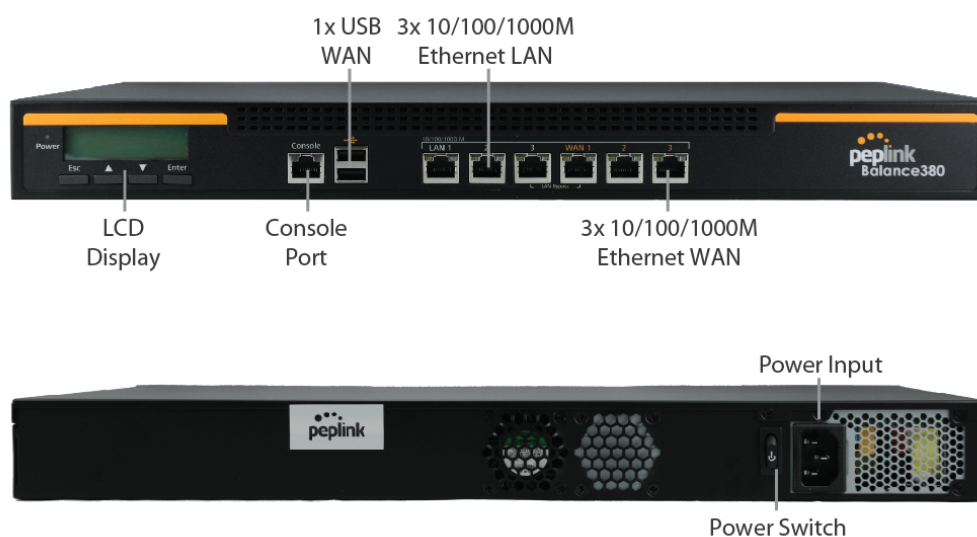
Power and Status Indicators	
<b>Power LED</b>	OFF – Power off
	GREEN – Power on

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

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

## 7.9 Peplink Balance 380

### 7.9.1 Panel Appearance



### 7.9.2 LED Indicators

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

Power and Status Indicators	
<b>Power LED</b>	OFF – Power off
	GREEN – Power on
LAN Port, WAN 1 – 3 Ports	
<b>Right LED</b>	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
<b>Left LED</b>	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected

<b>Port Type</b>	Auto MDI/MDI-X ports
------------------	----------------------

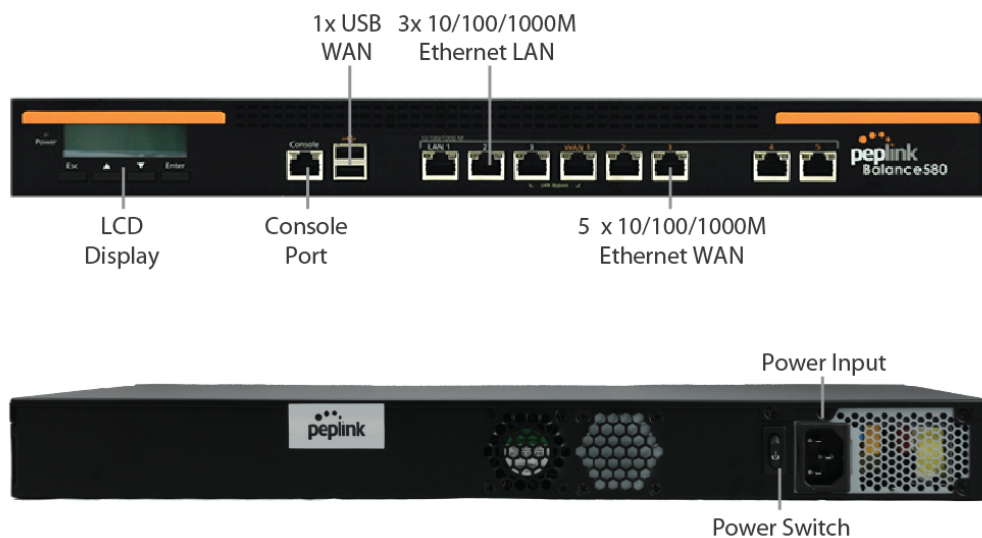
### Console and USB Ports

<b>Console Port</b>	Reserved for engineering use
---------------------	------------------------------

<b>USB Ports</b>	For connecting a 4G/3G USB modem
------------------	----------------------------------

## 7.10 Peplink Balance 580

### 7.10.1 Panel Appearance



### 7.10.2 LED Indicators

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

Power and Status Indicators	
<b>Power LED</b>	OFF – Power off
	GREEN – Power on

### LAN Port, WAN 1 – 5 Ports

<b>Right LED</b>	ORANGE – 1000 Mbps
	GREEN – 100 Mbps

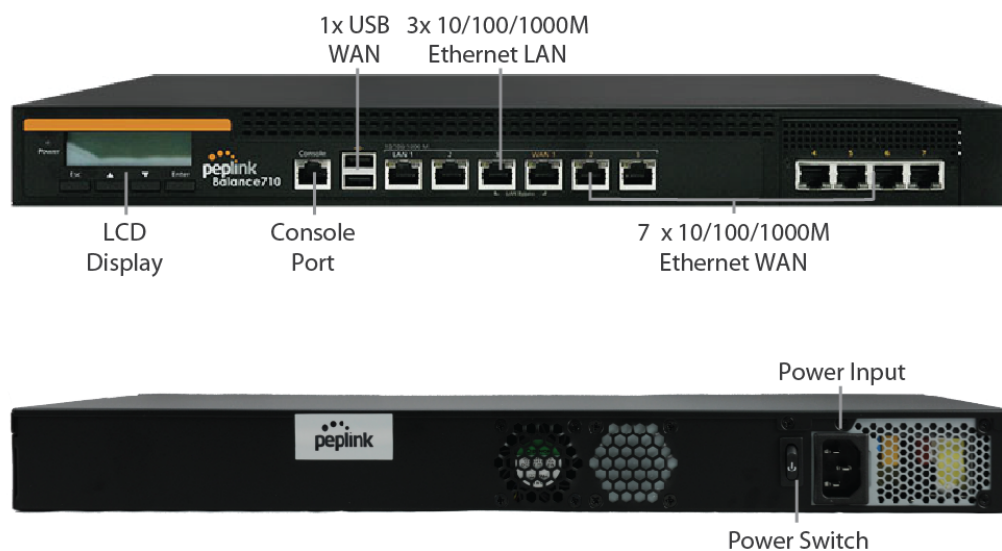


	OFF – 10 Mbps
<b>Left LED</b>	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports

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

## 7.11 Peplink Balance 710

### 7.11.1 Front Panel Appearance



### 7.11.2 LED Indicators

Status indicated in the front panel is as follows:

LED Indicator
---------------

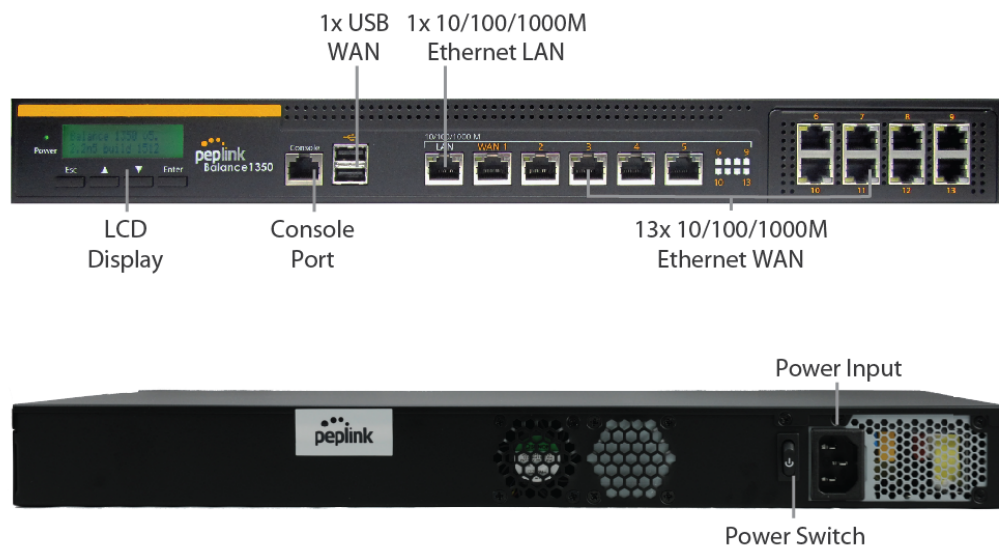
<b>Power LED</b>	OFF – Power off
	GREEN – Power on

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

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

## 7.12 Peplink Balance 1350

### 7.12.1 Panel Appearance



## 7.12.2 LED Indicators

Status indicated in the front panel is as follows:

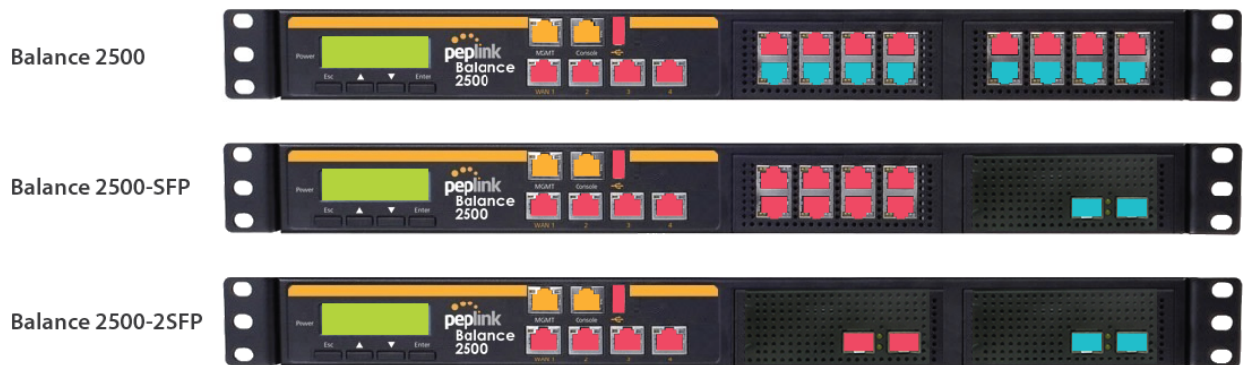
LED Indicator	
<b>Power LED</b>	OFF – Power off
	GREEN – Power on

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

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

## 7.13 Peplink Balance 2500

### 7.13.1 Panel Appearance



- LCD Display
- Console Port
- 10/100/1000M Ethernet WAN
- SFP+ WAN
- USB WAN
- 10/100/1000M Ethernet LAN
- SFP+ LAN



Power Switch      Power Inputs

### 7.13.2 LED Indicators

Status indicated in the front panel is as follows:

LED Indicator	
<b>Power LED</b>	OFF – Power off GREEN – Power on

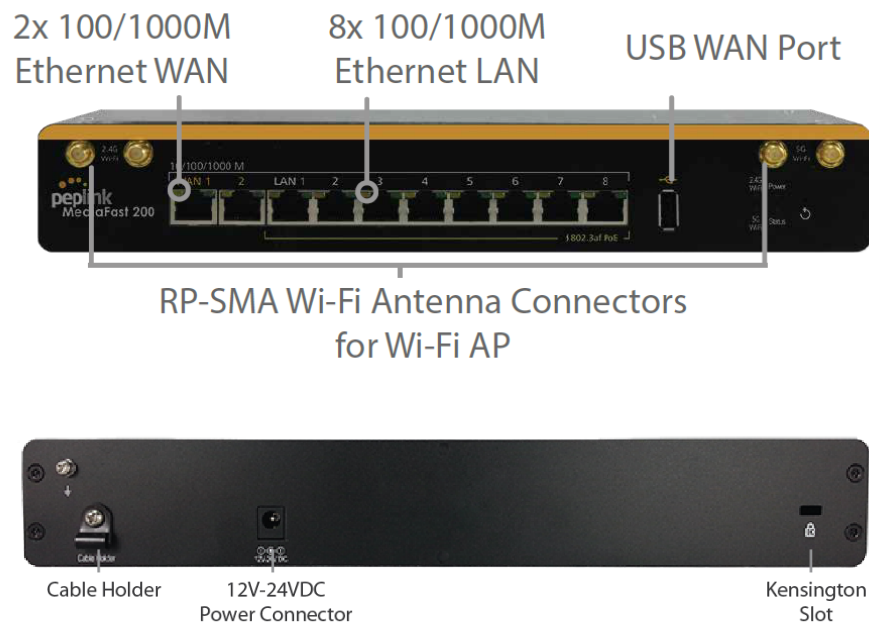
LAN and WAN Ports	
<b>Right LED</b>	ORANGE – 1000 Mbps GREEN – 100 Mbps OFF – 10 Mbps
<b>Left LED</b>	Solid – Port is connected without traffic Blinking – Data is transferring OFF – Port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports

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

## 8 Peplink MediaFast Overview

### 8.1 Peplink MediaFast 200

#### 8.1.1 Panel Appearance



#### 8.1.2 LED Indicators

Status indicated in the front panel is as follows:

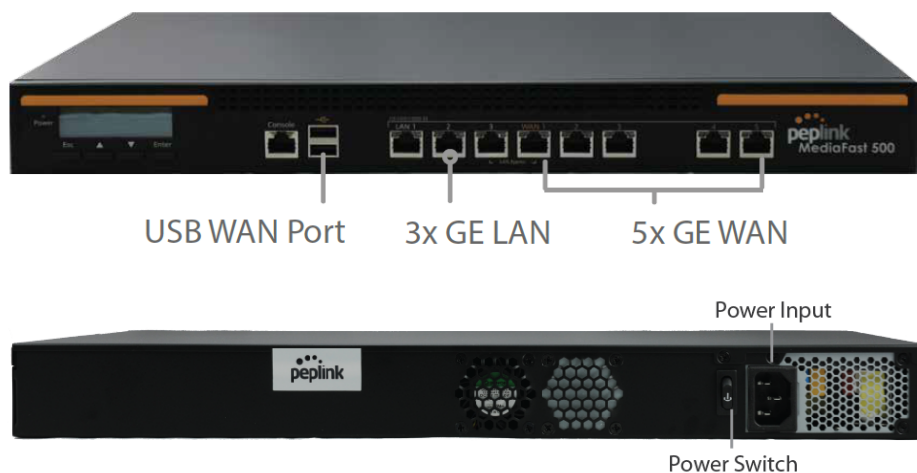
LED Indicator	
<b>Power LED</b>	OFF – Power off
	GREEN – Power on

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

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

## 8.2 Peplink MediaFast 500

### 8.2.1 Panel Appearance



### 8.2.2 LED Indicators

Status indicated in the front panel is as follows:

LED Indicator	
<b>Power LED</b>	OFF – Power off
	GREEN – Power on

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

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

## 8.3 Peplink MediaFast 750

### 8.3.1 Panel Appearance





### 8.3.2 LED Indicators

Status indicated in the front panel is as follows:

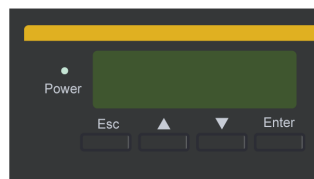
LED Indicator	
<b>Power LED</b>	OFF – Power off
	GREEN – Power on
LAN 1-3 Ports, WAN 1-5 Ports	
<b>Right LED</b>	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
<b>Left LED</b>	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports
Console & USB Ports	
<b>Console Port</b>	Reserved for engineering use
<b>USB Ports</b>	For connecting 4G/3G USB modems



## 9 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*	

\*Layout continues as such for all available WAN ports



## 10 Installation

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

### 10.1 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

### 10.2 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.

## 11 Basic Configuration

### 11.1 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:

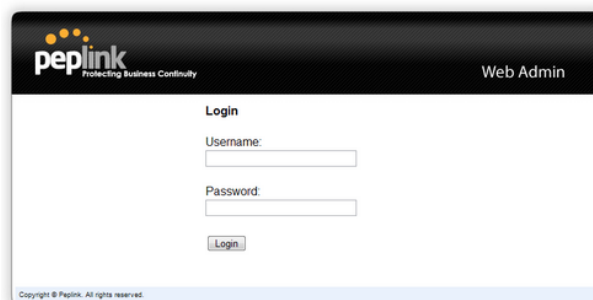
http://192.168.1.1

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



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

<b>1 3G</b>	
IP Address: 17.219.22.1 <a href="#">Details...</a>	Status: <span style="color: green;">●</span> Connected <span style="float: right;">Disconnect</span>
<b>2 Wi-Fi</b>	
IP Address: 18.220.23.1 <a href="#">Details...</a>	Status: <span style="color: green;">●</span> Connected <span style="float: right;">Disconnect</span>
<b>3 FBB</b>	
IP Address: 19.221.24.1 <a href="#">Details...</a>	Status: <span style="color: green;">●</span> Connected <span style="float: right;">Disconnect</span>
<b>4 WAN4</b>	
IP Address: 123.203.209.47 <a href="#">Details...</a>	Status: <span style="color: green;">●</span> Connected <span style="float: right;">Disconnect</span>
<b>5 WAN5</b>	
IP Address: 14.136.11.100 <a href="#">Details...</a>	Status: <span style="color: green;">●</span> Connected <span style="float: right;">Disconnect</span>
<b>6 WAN6</b>	
IP Address: 213.141.82.11 <a href="#">Details...</a>	Status: <span style="color: green;">●</span> Connected <span style="float: right;">Disconnect</span>
<b>USB</b>	
IP Address: (none)	Status: No Device Detected

<b>LAN Interface</b>	
Router IP Address: 192.168.1.1	

<b>PepVPN with SpeedFusion™</b> <span style="float: right;">Status</span>	
SDT	<span style="color: green;">🔒</span> Established
TPTtest	<span style="color: grey;">🔒</span>

<b>AP Controller Information</b> <span style="float: right;">Status</span>	
Access Point: 0 (Online: 0) Connected Clients: 0	

<b>Device Information</b>	
Model:	Peplink Balance 710
Firmware:	6.1.0 build 2863
Uptime:	38 days 22 hours 17 minutes
CPU Load:	<div style="width: 5%; background-color: green; border: 1px solid black;"></div> 5%
Throughput:	<span style="color: green;">↓</span> 0.0 Mbps <span style="color: blue;">↑</span> 0.0 Mbps

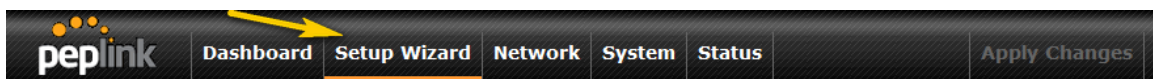
Important Note

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.

## 11.2 Configuration with the Setup Wizard

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

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



Click **Next >>** to begin.

Setup Wizard > WAN Setup > Step 1

Welcome to Setup Wizard!

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

Click *Next* to begin.

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


Setup Wizard > WAN Setup > Step 2

Drop-in Mode	
Do you want to setup drop-in mode?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Which WAN port do you want to enable drop-in mode?	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="font-size: small;">WAN 1 ▼</span>  <span style="background-color: #007bff; color: white; padding: 2px;">WAN 1</span>  <span style="padding: 2px;">WAN 2</span>  <span style="padding: 2px;">WAN 3</span>  <span style="padding: 2px;">WAN 4</span>  <span style="padding: 2px;">WAN 5</span>  <span style="padding: 2px;">WAN 6</span>  <span style="padding: 2px;">WAN 7</span> </div>

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

#### Setup Wizard > WAN Setup > Step 3

Choose the WAN port(s) to be configured.

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

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

#### Setup Wizard > WAN Setup > Step 4


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

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

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

Setup Wizard > WAN Setup > Step 4

Choose a connection method for WAN 1.


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

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

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

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.

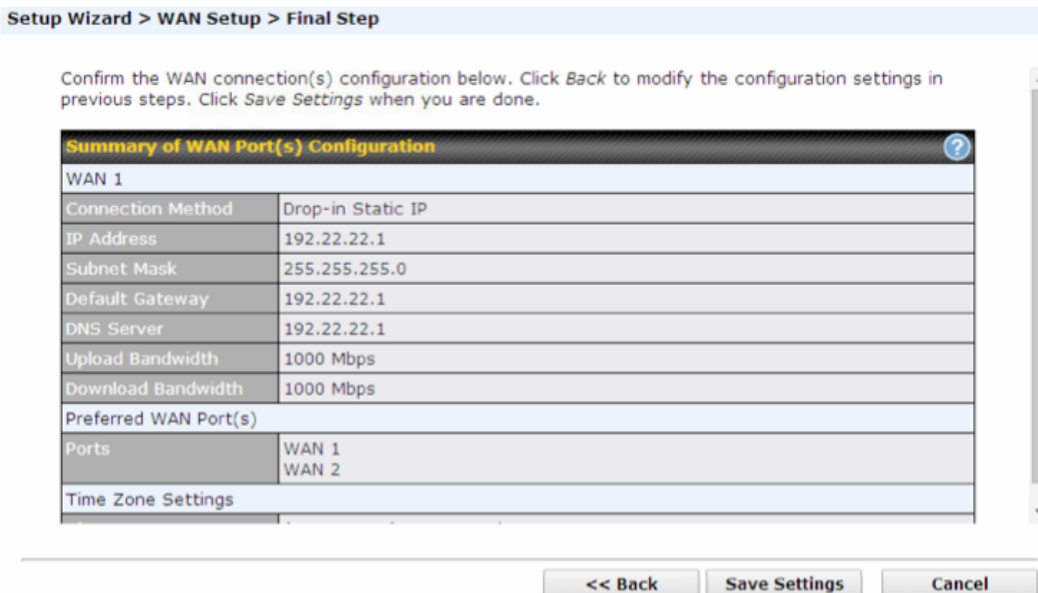
**Setup Wizard > WAN Setup > Step 6**

Choose time zone of your Country / Region.

Time Zone Settings	
Time Zone	<input type="text" value="(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.





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

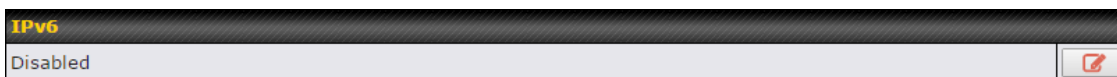
## 12 Network Tab

### 12.1 WAN

From **Network>WAN**, choose a WAN connection by clicking it.

Connection Name	Method	Routing Mode	Type
1. <a href="#">WAN 1</a>	DHCP	NAT	Always-on
2. <a href="#">WAN 2</a>	Not Configured	NAT	Always-on
3. <a href="#">Mobile Internet</a>	PPP	NAT	Backup Group 1

You can also enable IPv6 support in this section



### WAN Connection Settings (Ethernet)

Clicking an Ethernet WAN connection will result in the following screen:

Connection Settings	
WAN Connection Name	WAN 1
Enable	<input checked="" type="checkbox"/> Weekdays Only ▼
Connection Method	? DHCP ▼
Routing Mode	? <input checked="" type="radio"/> NAT
Connection Type	? <input checked="" type="radio"/> Always-on <input type="radio"/> Backup Priority
Independent from Backup WANs	? <input type="checkbox"/>
Reply to ICMP Ping	? <input checked="" type="checkbox"/> Enable
Upload Bandwidth	? 1 Gbps ▼
Download Bandwidth	? 1 Gbps ▼

WAN Connection Settings	
<b>WAN Connection Name</b>	Enter a name to represent this WAN connection.
<b>Enable</b>	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.
<b>Connection Method</b>	<p>There are three possible connection methods for Ethernet WAN:</p> <ul style="list-style-type: none"> <li>• DHCP</li> <li>• Static IP</li> <li>• PPPoE</li> </ul> <p>The connection method and details are determined by, and can be obtained from, the ISP. See the following sections for details on each connection method. DNS server settings can be configured in the corresponding menu for each connection method.</p>
<b>Routing Mode</b>	This field shows that <b>NAT</b> (network address translation) will be applied to the traffic routed over this WAN connection. <b>IP Forwarding</b> is available when you click the link in the help text.
<b>DNS Servers</b>	Select a DNS server for this port to use. This port can either be automatically selected or manually designated.
<b>Independent from Backup WANs</b>	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
<b>Standby State</b>	This setting specifies the standby state of the WAN connection. The available options are <b>Remain connected</b> and <b>Disconnect</b> . The default state is <b>Remain Connected</b> .
<b>Reply to ICMP</b>	If No is selected, this option is disabled and the system will not reply to any ICMP ping echo

<b>PING</b>	requests to the WAN IP addresses of this WAN connection. Default: Yes
<b>Upload Bandwidth</b>	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.
<b>Download Bandwidth</b>	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

### WAN Connection Settings (Cellular)

Clicking an Ethernet WAN connection will result in the following screens:


Connection Settings	
WAN Connection Name	Cellular
Enable	<input type="checkbox"/>
Routing Mode	<input checked="" type="radio"/> NAT
Connection Type	<input type="radio"/> Always-on <input checked="" type="radio"/> Backup Priority <span>Group 1 (Highest) ▼</span>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Idle Disconnect	<input type="checkbox"/>
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"/>

Connection Settings	
<b>WAN Connection Name</b>	Indicate a name you wish to give this WAN connection
<b>Enable</b>	Click the checkbox to toggle the on and off state of this connection.
<b>Routing Mode</b>	<p>This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding.</p> <p>In the case if you need to choose IP Forwarding for your scenario. Click the  button to enable IP Forwarding.</p>
<b>Connection</b>	This option allows you to configure the WAN connection whether for normal daily usage or as

<b>Type</b>	<p>a backup connection only.</p> <p>If Always-on is chosen, the WAN connection will be kept on continuously and is used for load balancing.</p> <p>If Backup Priority is chosen, the WAN connection will not be used unless none of the Always-on connection(s) is available.</p>
<b>Standby State</b>	<p>This option allows you to choose whether to remain the connection connected or disconnect it when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, upon bringing up this WAN connection to active, it will be immediately available for use. If this WAN connection is charged by connection time, you may want to set this option to Disconnect so that connection will be made only when needed.</p>
<b>Idle Disconnect</b>	<p>If checked, you can define the number of minutes of idle time has passed before a network gets disconnected.</p>
<b>DNS Servers</b>	<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>

Cellular Settings <span style="float: right;">?</span>		
SIM Card	<input checked="" type="radio"/> Both SIMs <input type="radio"/> SIM A Only <input type="radio"/> SIM B Only	
Preferred SIM Card	<input checked="" type="radio"/> No Preference <input type="radio"/> SIM A <input type="radio"/> SIM B	
	SIM Card A	SIM Card B
Network Selection <span>?</span>	<input checked="" type="radio"/> Auto	<input checked="" type="radio"/> Auto
LTE/3G <span>?</span>	Auto ▾	Auto ▾
Authentication	Auto ▾	Auto ▾
Data Roaming	<input type="checkbox"/>	<input type="checkbox"/>
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	<input type="text"/>	<input type="text"/>
Username	<input type="text"/>	<input type="text"/>
Password	<input type="text"/>	<input type="text"/>
Confirm Password	<input type="text"/>	<input type="text"/>
SIM PIN (Optional) <span>?</span>	<input type="text"/> <input type="text"/> (Confirm)	<input type="text"/> <input type="text"/> (Confirm)
Bandwidth Allowance Monitor <span>?</span>	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable

## Cellular Settings

<b>SIM Card</b>	Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards.
<b>Preferred SIM Card</b>	If both cards were enabled on the above field, then you can designate the priority of the SIM card slots here.
<b>3G/2G</b>	This drop-down menu allows restricting cellular to particular band. Click the  button to enable the selection of specific bands.
<b>Authentication</b>	Choose from <b>PAP Only</b> or <b>CHAP Only</b> to use those authentication methods exclusively. Select <b>Auto</b> to automatically choose an authentication method.
<b>Data Roaming</b>	This checkbox enables data roaming on this particular SIM card. Please check your service provider's data roaming policy before proceeding.
<b>Operator Settings</b>	This setting applies to 3G/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems. This allows you to configure the APN settings of your connection. If <b>Auto</b> is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select <b>Custom</b> to enter your carrier's <b>APN</b> , <b>Login</b> , <b>Password</b> , and <b>Dial Number</b> settings manually. The correct values can be obtained from your carrier. The default and recommended setting is <b>Auto</b> .
<b>APN / Login / Password / SIM PIN</b>	When <b>Auto</b> is selected, the information in these fields will be filled automatically. Select <b>Custom</b> to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
<b>Bandwidth Allowance Monitor</b>	Check the box <b>Enable</b> to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
<b>Action</b>	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If <b>Disconnect when usage hits 100% of monthly allowance</b> 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.
<b>Start Day</b>	This option allows you to define which day of the month each billing cycle begins.
<b>Monthly Allowance</b>	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

### WAN Connection Settings (Common)

The remaining WAN-related settings are common to both Ethernet and cellular WAN

Physical Interface Settings	
Port Speed	<input type="text" value="Auto"/>
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: <input type="text" value="1440"/> <input type="button" value="Default"/>
MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom Value: <input type="text"/>
MAC Address Clone	<input type="text" value="00"/> : <input type="text" value="1A"/> : <input type="text" value="1A"/> : <input type="text" value="1A"/> : <input type="text" value="1A"/> : <input type="text" value="1A"/> <input type="button" value="Default"/>
VLAN	<input type="checkbox"/>

Physical Interface Settings	
<b>Port Speed</b>	<p>This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems.</p> <p>When a static speed is set, you may choose whether to advertise its speed to the peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device.</p> <p>Default: Auto</p>
<b>MTU</b>	<p>This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value.</p>
<b>MSS</b>	<p>This field is for specifying the Maximum Segment Size of the WAN connection.</p> <p>When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections.</p> <p>Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections.</p> <p>Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size.</p> <p>Default: Auto</p>
<b>MAC Address Clone</b>	<p>Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.</p>
<b>VLAN</b>	<p>Check the box to assign a VLAN to the interface.</p>

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	
<b>Hostname (Optional)</b>	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.
<b>DNS Servers</b>	<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 <b>Obtain DNS server address automatically</b> 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 <b>Use the following DNS server address(es)</b> is selected, you may enter custom DNS server addresses for this WAN connection into the <b>DNS server 1</b> and <b>DNS server 2</b> fields.</p>

## Health Check Settings

To ensure traffic is routed to healthy WAN connections only, the Peplink Balance can periodically check the health of each WAN connection.

Health Check settings for each WAN connection can be independently configured via **Network>Interfaces>WAN>\*Connection name\*>Health Check Settings**.

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

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

Health Check Settings	
<b>Method</b>	This setting specifies the health check method for the WAN connection. This value can be configured as <b>Disabled</b> , <b>PING</b> , <b>DNS Lookup</b> , or <b>HTTP</b> . The default method is <b>DNS</b>

**Lookup.** For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

### Health Check Disabled

Health Check Settings	
Health Check Method	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="float: right;">?</span> <span style="float: right;">Disabled ▾</span> </div> <small style="color: red;">Health Check disabled. Network problem cannot be detected.</small>

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

### Health Check Method: PING

Health Check Method	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="float: right;">?</span> <span style="float: right;">PING ▾</span> </div>
PING Hosts	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="float: right;">?</span> <div style="display: flex; gap: 5px;"> <input style="width: 100px;" type="text"/> <input style="width: 100px;" type="text"/> </div> <div style="display: flex; gap: 5px;"> <input style="width: 100px;" type="text"/> <input style="width: 100px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts                 </div> </div>

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

#### PING Hosts

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

### Health Check Method: DNS Lookup

Health Check Method	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="float: right;">?</span> <span style="float: right;">DNS Lookup ▾</span> </div>
Health Check DNS Servers	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="float: right;">?</span> <div style="display: flex; gap: 5px;"> <input style="width: 100px;" type="text"/> <input style="width: 100px;" type="text"/> </div> <div style="display: flex; gap: 5px;"> <input style="width: 100px;" type="text"/> <input style="width: 100px;" type="text"/> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers  <input type="checkbox"/> Include public DNS servers                 </div> </div>

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.

<b>URL1</b>	<p><b>WAN Settings&gt;WAN Edit&gt;Health Check Settings&gt;URL1</b></p> <p>The URL will be retrieved when performing an HTTP health check. When <b>String to Match</b> 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 <b>String to Match</b> 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.</p>
<b>URL 2</b>	<p><b>WAN Settings&gt;WAN Edit&gt;Health Check Settings&gt;URL2</b></p> <p>If <b>URL2</b> is also provided, a health check will pass if either one of the tests passed.</p>

### 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.**

## Bandwidth Allowance Monitor Settings

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 <a href="#">Email Notification</a> . <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	
<b>Action</b>	If <b>Email Notification</b> is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If <b>Disconnect when usage hits 100% of monthly allowance</b> 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.
<b>Start Day</b>	This option allows you to define which day of the month each billing cycle begins.
<b>Monthly Allowance</b>	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

**Disclaimer**

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

## Additional Public IP Settings

Additional Public IP Settings											
IP Address List	<table border="1"> <tr> <td>IP Address</td> <td>210.10.10.0</td> </tr> <tr> <td>Subnet Mask</td> <td>255.255.255.255 (/32)</td> </tr> <tr> <td colspan="2" style="text-align: center;">↓</td> </tr> <tr> <td colspan="2">                     210.10.10.1                      210.10.10.2                      210.10.10.3                      210.10.10.4                      210.10.10.5                 </td> </tr> <tr> <td colspan="2" style="text-align: right;">✖</td> </tr> </table> <p>Those settings will not be saved until the save button below has been pressed.</p>	IP Address	210.10.10.0	Subnet Mask	255.255.255.255 (/32)	↓		210.10.10.1 210.10.10.2 210.10.10.3 210.10.10.4 210.10.10.5		✖	
IP Address	210.10.10.0										
Subnet Mask	255.255.255.255 (/32)										
↓											
210.10.10.1 210.10.10.2 210.10.10.3 210.10.10.4 210.10.10.5											
✖											

**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**.

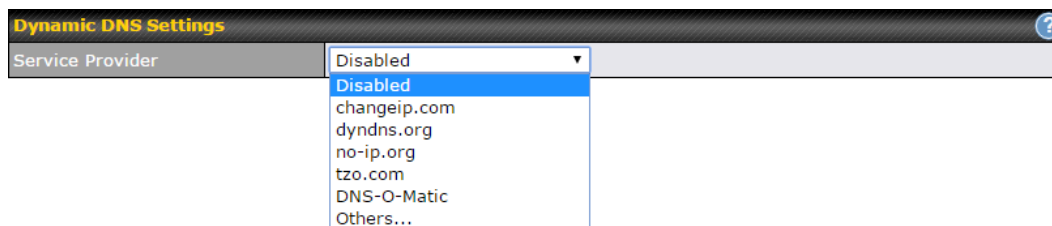
## Dynamic DNS Settings

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

Dynamic DNS Settings	
<b>Service Provider</b>	<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"> <li>• changeip.com</li> <li>• dyndns.org</li> <li>• no-ip.org</li> <li>• tzo.com</li> <li>• DNS-O-Matic</li> <li>• Others...                             <p style="margin-left: 20px;">support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.</p> </li> </ul> <p>Select <b>Disabled</b> to disable this feature.</p>
<b>User ID / User / Email</b>	This setting specifies the registered user name for the dynamic DNS service.
<b>Password / Pass / TZO Key</b>	This setting specifies the password for the dynamic DNS service.
<b>Update All Hosts</b>	Check this box to automatically update all hosts.
<b>Hosts / Domain</b>	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

### Important Note

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

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

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

a WAN's IP address did not change.

## 12.2 LAN



### 12.2.1 Network Settings

LAN	VLAN	Network	
Untagged LAN	None	192.168.1.1/24	?
New LAN			

Click the LAN or VLAN you wish to edit or click **New LAN** to create a new VLAN. When you do so, the following configuration menus will appear:

IP Settings			?
IP Address	192.168.1.1	255.255.255.0 (/24)	

IP Settings	
<b>IP Address &amp; Subnet Mask</b>	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"/>	

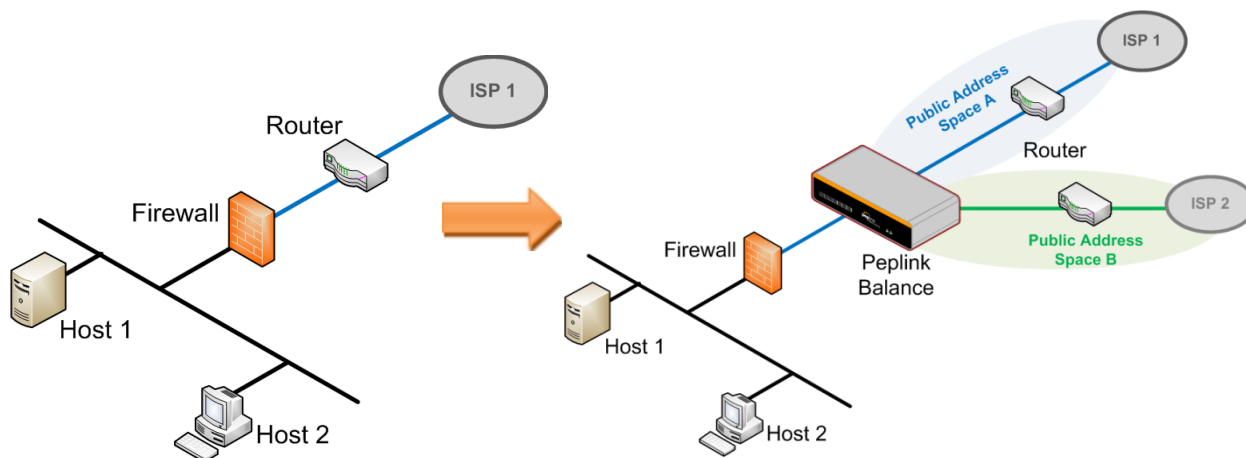
Network Settings	
<b>Name</b>	Enter a name for the LAN.

<b>VLAN ID</b>	Enter a VLAN ID for your LAN.
<b>Inter-VLAN routing</b>	Check this box to enable routing between virtual LANs.
<b>Captive Portal</b>	Check this box to turn on captive portals.

## 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.

Please note the Drop-In Mode is mutually exclusive with VLAN.

**Drop-In Mode Settings** ?

Enable	<input checked="" type="checkbox"/>
WAN for Drop-In Mode <span>?</span>	WAN 1 with LAN bypass ▾
WAN Default Gateway <span>?</span>	<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"/> <div style="text-align: center;">↓</div> <div style="border: 1px solid gray; height: 40px; width: 100%;"></div> <div style="text-align: right;">Delete</div>
WAN DNS Servers <span>?</span>	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>

NOTE: The DHCP Server Settings will be overwritten.


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

The PPTP Server will be disabled.  
High Availability will be disabled.




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

Drop-in Mode Settings	
<b>Enable</b>	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 <b>Section 12, Drop-in Mode</b> for details.
<b>WAN for Drop-In Mode</b>	Select the WAN port to be used for drop-in mode. If <b>WAN 1 with LAN Bypass</b> is selected, the high availability feature will be disabled automatically.
<b>Shared Drop-In IP<sup>A</sup></b>	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Balance will listen for this IP address when WAN hosts access services provided by the Balance (web admin access from the WAN, DNS server requests, etc.).  To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The Balance will listen for this IP address when LAN hosts access services provided by the Balance (web admin access from the WAN, DNS proxy, etc.).
<b>Shared IP Address<sup>A</sup></b>	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.)



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

<sup>A</sup> - 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 <sup>A</sup>	
<b>PepVPN Profiles to Bridge<sup>A</sup></b>	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.
<b>Remote Network Isolation<sup>A</sup></b>	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.
<b>Spanning Tree Protocol<sup>A</sup></b>	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.
<b>Override IP Address when bridge is connected<sup>A</sup></b>	<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>

<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner of the **Network Settings** menu to activate.

### 12.2.2 Network Settings (Common Settings)

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:	
		WINS Server 2:	
BOOTP	<input checked="" type="checkbox"/>	Server IP Address:	
		Boot File:	
		Server Name:	(Optional)
Extended DHCP Option		Option	Value
		No Extended DHCP Option	
		Add	
DHCP Reservation	<input checked="" type="checkbox"/>	Name	MAC Address
			00:00:00:00:00:00
		Static IP	
			+

For VLAN-enabled configurations, DHCP Server settings are accessible by clicking individual VLAN

DHCP Server Settings	
<b>DHCP Server</b>	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.
<b>DHCP Server Logging</b>	Check this box to log DHCP server activity.
<b>IP Range &amp; Subnet Mask</b>	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Peplink Balance’s DHCP server.
<b>Lease Time</b>	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of <b>Lease Time</b> , the assigned IP address will no longer be valid and the IP address assignment must be renewed.
<b>DNS Servers</b>	This option allows you to input the DNS server addresses to be offered to DHCP clients. If <b>Assign DNS server automatically</b> is selected, the Peplink Balance’s built-in DNS server address (i.e., LAN IP address) will be offered.
<b>WINS Server</b>	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>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 <b>DHCP WINS Servers</b> 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 <b>Status&gt;WINS Clients</b>.</p>
<b>BOOTP</b>	<p>Check this box to enable BOOTP on older networks that still require it.</p>
<b>Extended DHCP Option</b>	<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 <b>Add</b> 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>
<b>DHCP Reservation</b>	<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><b>Name</b> (an optional field) allows you to specify a name to represent the device. MAC addresses should be in <b>00:AA:BB:CC:DD:EE</b> format. Press  to create a new record. Press  to remove a record. Reserved clients information can be imported from the <b>Client List</b>, located at <b>Status&gt;Client List</b>. For more details, please refer to <b>Section 27.3</b>.</p>

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	
<b>DHCP Relay</b>	Enter the address of the DHCP server here. DHCP requests will be relayed to it.
<b>DHCP Server IP Address</b>	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 <b>DHCP Server 1</b> and <b>DHCP Server 2</b> fields.
<b>DHCP Option</b>	This feature includes device information as relay agent for the attached client when

<b>82</b>	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.
<b>DHCP Relay Logging</b>	Check this box to log DHCP relay activity.

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

### Static Route Settings

**Static Route**

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

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

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

### WINS Server Settings

**Enable**

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

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

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

Preferred connections are shown with

DNS Proxy Settings	
<b>Enable</b>	<p>To enable the DNS proxy feature, check this box, and then set up the feature at <b>Network&gt;LAN&gt;DNS Proxy Settings</b>.</p> <p>A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the <b>DNS servers/resolvers</b> defined for each WAN connection.</p>
<b>DNS Caching</b>	<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, <b>DNS Caching</b> is disabled.</p>
<b>Include Google Public DNS Servers</b>	<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>
<b>Local DNS Records</b>	<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>
<b>Domain Lookup Policy</b>	<p>DNS proxy will look up the domain names defined here using only the specified connections.</p>
<b>DNS</b>	<p>Check the box to enable the WINS server. A list of WINS clients will be displayed at <b>Network&gt;LAN&gt;DNS Proxy Settings&gt;DNS Resolvers</b>.</p>

**Resolvers<sup>A</sup>** This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

<sup>A</sup> - 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	
<b>Enable</b>	Check this box to turn on Bonjour forwarding.
<b>Bonjour Service</b>	Choose <b>Service</b> and <b>Client</b> networks from the drop-down menus, and then click  to add the networks. To delete an existing Bonjour listing, click .

### 12.2.3 Port Settings

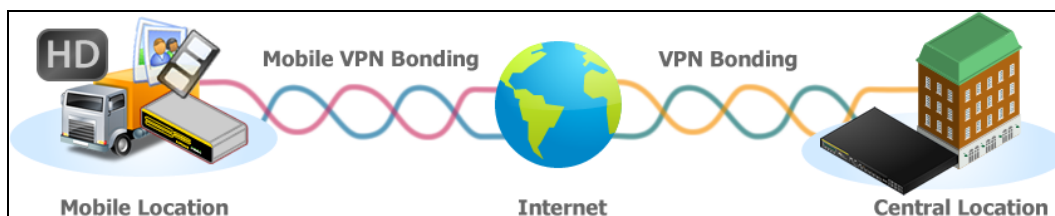
To configure port settings, navigate to **Network > Port Settings**

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

On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

## 12.3 VPN

### 12.3.1 SpeedFusion



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.

To begin, navigate to **Network > VPN > SpeedFusion** and enter a Local ID and click save.

PepVPN	
Local ID	<input type="text" value="Balance-DDCD"/>
<small>Please define a local ID before using the PepVPN. Remote units can identify this unit by this "Local ID", in addition to the serial number.</small>	
<input type="button" value="Save"/>	

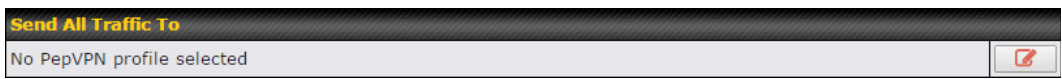
This device will be identified by other SpeedFusion Peers by this local ID. The following menus will appear:

Profile	Remote ID	Remote Address(es)	
No VPN Connection Defined			
<input type="button" value="New Profile"/>			

### SpeedFusion Profiles

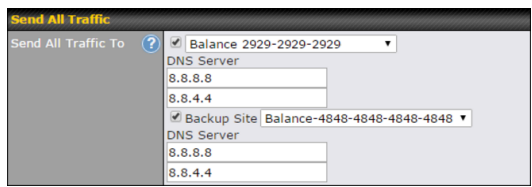
This table displays all defined profiles. Click the **New Profile** button to create a new profile for making a VPN connection to a remote unit via available WAN connections. Each pair of VPN connection requires its own profile.

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 will be able to route to local subnets.

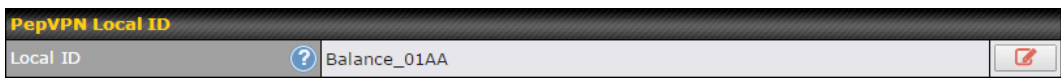


### Send All Traffic To

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

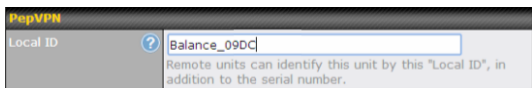


You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main PepVPN connection fail.



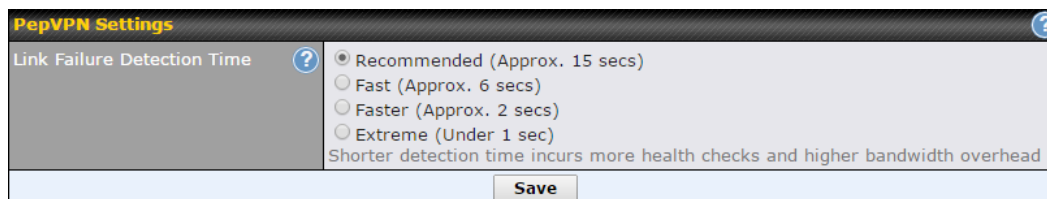
### PepVPN Local ID

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



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





**PepVPN Settings**

Link Failure Detection Time ?

- Recommended (Approx. 15 secs)
- Fast (Approx. 6 secs)
- Faster (Approx. 2 secs)
- Extreme (Under 1 sec)

Shorter detection time incurs more health checks and higher bandwidth overhead

Save

## Link Failure Detection

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

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

### Link Failure Detection Time

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

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

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

## Important Note

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



### SpeedFusion: Profile Configuration

Click the **New Profile** button, or click one of the existing profiles, and the following menus will appear:

PepVPN Profile <span style="float: right;">?</span>					
Name	<input type="text" value="Balance 2929-2929-2929"/>				
Active	<input checked="" type="checkbox"/>				
SpeedFusion	Supported				
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF				
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key <input type="radio"/> X.509				
Remote ID / Pre-shared Key	<table border="1" style="width: 100%;"> <tr> <th>Remote ID</th> <th>Pre-shared Key</th> </tr> <tr> <td>Balance 9898-9898-9898</td> <td>.....</td> </tr> </table>	Remote ID	Pre-shared Key	Balance 9898-9898-9898	.....
Remote ID	Pre-shared Key				
Balance 9898-9898-9898	.....				
NAT Mode	<input type="checkbox"/> Untagged LAN ▾				
Remote IP Address / Host Names (Optional)	<input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small>				
Data Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>				
Bandwidth Limit	<input type="checkbox"/>				
Cost	<input type="text" value="10"/>				
WAN Smoothing	<input type="text" value="Off"/>				
Use IP ToS	<input type="checkbox"/>				

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

PepVPN Profile Settings	
<b>Name</b>	<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 <b>PepVPN Profile</b> title bar to use the IP ToS field of your data packet on PepVPN WAN traffic.</p>
<b>Active</b>	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
<b>Encryption</b>	By default, VPN traffic is encrypted with <b>256-bit AES</b> . If <b>Off</b> is selected on both sides of a VPN connection, no encryption will be applied.
<b>Authentication</b>	Select from <b>By Remote ID Only</b> , <b>Preshared Key</b> , or <b>X.509</b> to specify the method the Peplink Balance will use to authenticate peers. When selecting <b>By Remote ID Only</b> , be sure to enter a unique peer ID number in the <b>Remote ID</b> field.

<b>Remote ID / Pre-shared Key</b>	<p>This optional field becomes available when <b>Remote ID / Pre-shared Key</b> is selected as the Peplink Balance's VPN <b>Authentication</b> method, as explained above. <b>Pre-shared Key</b> 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>
<b>Remote ID/Remote Certificate</b>	<p>These optional fields become available when <b>X.509</b> 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 <b>Show Details</b> link below the field.</p>
<b>Allow Shared Remote ID</b>	<p>When this option is enabled, the router will allow multiple peers to run using the same remote ID.</p>
<b>NAT Mode</b>	<p>Check this box to allow the local DHCP server to assign an IP address to the remote peer. When <b>NAT Mode</b> is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.</p>
<b>Remote IP Address / Host Names (Optional)</b>	<p>If <b>NAT Mode</b> is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.</p> <p>This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.</p> <p>Click the  icon to customize the handshake port (TCP)</p>
<b>Data Port</b>	<p>This field is used to specify a UDP port number for transporting outgoing VPN data. If <b>Default</b> 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 <b>Custom</b> is selected, enter an outgoing port number from 1 to 65535.</p>
<b>Bandwidth Limit</b>	<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>
<b>Cost</b>	<p>Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10</p>
<b>WAN Smoothing<sup>A</sup></b>	<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</p>

WAN's available bandwidth.

Off - Disable WAN Smoothing.

Normal - The total bandwidth consumption will be at most 2x of the original data traffic.

Medium - The total bandwidth consumption will be at most 3x of the original data traffic.

High - The total bandwidth consumption depends on the number of connected active tunnels.

<sup>A</sup> - 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\***

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

### WAN Connection Priority

#### WAN Connection Priority

If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used.

To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the button.

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.



### 12.3.2 IPsec VPN

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**.


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

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.

Name	Profile 1											
Active	<input checked="" type="checkbox"/>											
Connect Upon Disconnection of	<input checked="" type="checkbox"/>	WAN 2										
Remote Gateway IP Address / Host Name	<input type="text"/>	12.12.12.12										
Local Networks	<p>Propose the following networks to remote gateway:</p> <p><input type="checkbox"/> 172.16.1.1/24</p> <p><input type="checkbox"/> 172.16.2.1/24</p> <p><input type="checkbox"/> 172.16.3.1/24</p> <p><input checked="" type="checkbox"/> 10.10.0.1/32</p> <p><input checked="" type="checkbox"/> 192.168.10.0/24</p> <p><input checked="" type="checkbox"/> 192.168.11.0/24</p> <p><input type="checkbox"/> <input type="text"/></p> <p>Apply the following NAT policies:</p> <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"/></td> <td><input type="text"/></td> <td><input type="button" value="+"/></td> </tr> <tr> <td>192.167.11.193</td> <td>255.255.255.0 (/24)</td> <td></td> </tr> </tbody> </table>	Network	Subnet Mask		<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>	192.167.11.193	255.255.255.0 (/24)			
Network	Subnet Mask											
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>										
192.167.11.193	255.255.255.0 (/24)											
Authentication	<input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate											
Mode	<input checked="" type="radio"/> Main Mode (All WANs need to have Static IP)											
	<input type="radio"/> Aggressive Mode											
Force UDP Encapsulation	<input type="checkbox"/>											
Preshared Key	<input type="text"/> <p><input checked="" type="checkbox"/> Hide Characters</p>											
Local ID	<input type="text"/>											
Remote ID	<input type="text"/>											
Phase 1 (IKE) Proposal	<p>1 <input type="text"/></p> <p>2 <input type="text"/></p>											
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"/>	seconds	<input type="button" value="Default"/>									
Phase 2 (ESP) Proposal	<p>1 <input type="text"/></p> <p>2 <input type="text"/></p>											
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"/>	seconds	<input type="button" value="Default"/>									

IPsec VPN Settings	
<b>Name</b>	This field is for specifying a local name to represent this connection profile.
<b>Active</b>	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
<b>Connect Upon Disconnection of</b>	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.
<b>Remote Gateway IP Address / Host Name</b>	Enter the remote peer's public IP address. For <b>Aggressive Mode</b> , this is optional.
<b>Local Networks</b>	<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><b>One-to-One NAT policy:</b> if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 &gt; 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too.</p> <p><b>Many-to-One NAT policy:</b> if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 &gt; 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.</p>
<b>Remote Networks</b>	Enter the LAN and subnets that are located at the remote site here.
<b>Authentication</b>	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the <b>Preshared Key</b> and <b>X.509 Certificate</b> methods of authentication.
<b>Mode</b>	Choose <b>Main Mode</b> if both IPsec peers use static IP addresses. Choose <b>Aggressive Mode</b> if one of the IPsec peers uses dynamic IP addresses.
<b>Force UDP</b>	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.

Encapsulation	
<b>Pre-shared Key</b>	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
<b>Remote Certificate (pem encoded)</b>	Available only when <b>X.509 Certificate</b> is chosen as the <b>Authentication</b> method, this field allows you to paste a valid X.509 certificate.
<b>Local ID</b>	In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
<b>Remote ID</b>	In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
<b>Phase 1 (IKE) Proposal</b>	In <b>Main Mode</b> , this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In <b>Aggressive Mode</b> , only one selection is permitted.
<b>Phase 1 DH Group</b>	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. <b>Group 2: 1024-bit</b> is the default value. <b>Group 5: 1536-bit</b> is the alternative option.
<b>Phase 1 SA Lifetime</b>	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at <b>3600</b> seconds.
<b>Phase 2 (ESP) Proposal</b>	In <b>Main Mode</b> , 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 <b>Aggressive Mode</b> , only one selection is permitted.
<b>Phase 2 PFS Group</b>	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. <b>None</b> - 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. <b>Group 2:</b> 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. <b>Group 5:</b> 1536-bit is the third option.
<b>Phase 2 SA Lifetime</b>	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at <b>28800</b> seconds.

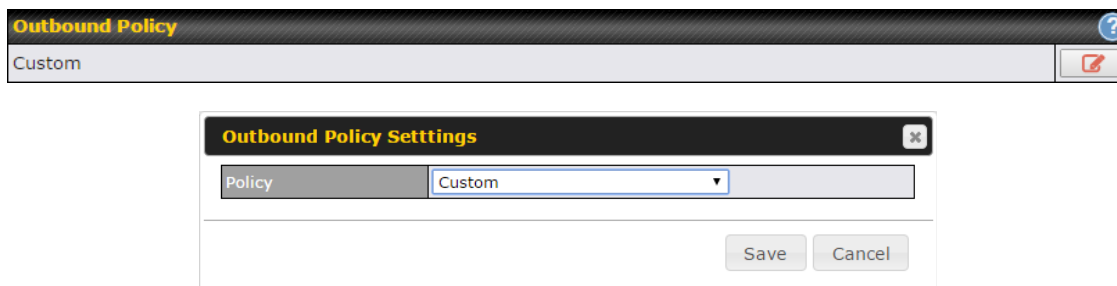
**IPsec Status** shows the current connection status of each connection profile and is displayed at **Status>IPsec VPN**.



## 12.4 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at

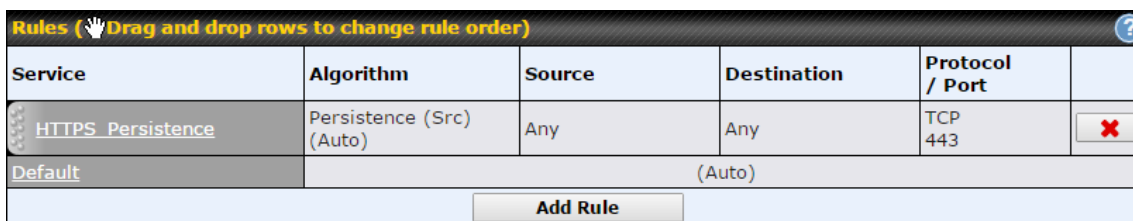
**Network>Outbound Policy**. Click the  button beside the **Outbound Policy** box:



A selection menu will appear, giving you the choice between three different Outbound Policy Settings:

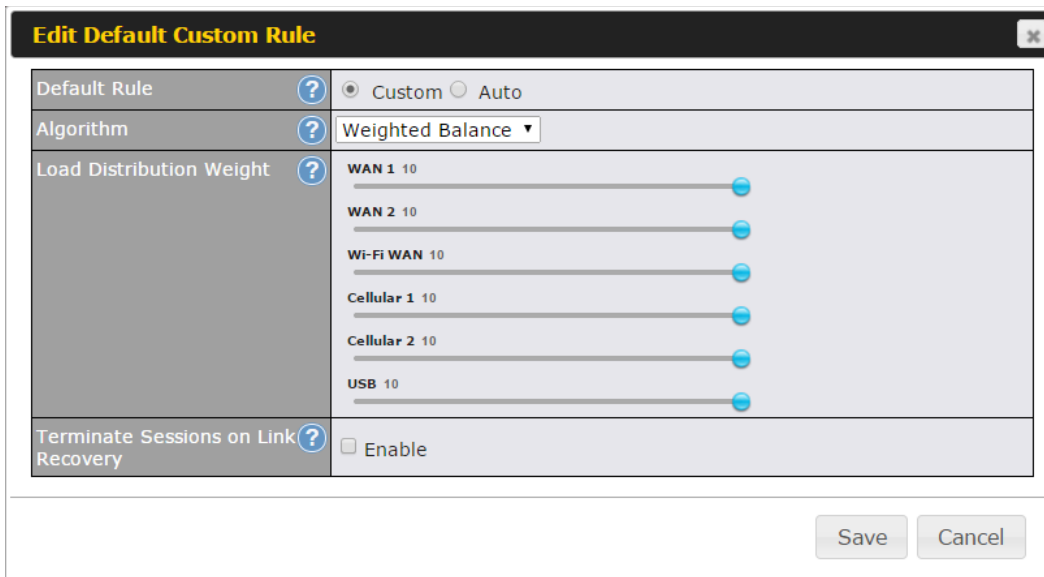
Outbound Policy Settings	
<b>High Application Compatibility</b>	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the highest application compatibility.
<b>Normal Application Compatibility</b>	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.
<b>Custom</b>	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 menu underneath enables you to define Outbound policy rules:



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

Save Cancel

By default, **Auto** is selected 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. Note that some Pepwave routers display this button at **Advanced>PepVPN>PepVPN Outbound Custom Rules**.



	<p>not supported. NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.</p>
<b>Protocol and Port</b>	This setting specifies the IP protocol and port of traffic that matches this rule.
<b>Algorithm</b>	<p>This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected (note that some Pepwave routers provide only some of these options):</p> <ul style="list-style-type: none"> <li>• Weighted Balance</li> <li>• Persistence</li> <li>• Enforced</li> <li>• Priority</li> <li>• Overflow</li> <li>• Least Used</li> <li>• Lowest Latency</li> </ul> <p>For a full explanation of each Algorithmn, please see the following article: <a href="https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithmns-work/8059">https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithmns-work/8059</a></p>
<b>Terminate Sessions on Link Recovery</b>	<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 <b>Weighted</b>, <b>Persistence</b>, and <b>Priority</b> algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.</p>

## 12.5 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.

#### 12.5.1 Servers

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		
<input type="button" value="Add Server"/>		

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

**Inbound Server** ✕

Server Name	<input type="text" value="myserver"/>
IP Address	<input type="text" value="192.168.1.123"/>

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	✕
<input type="button" value="Add Server"/>		

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

### 12.5.2 Services

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

Service	IP Address(es)	Server	Protocol
No Services Defined			
<input type="button" value="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 :: <input type="button" value="▼"/>																				
Port	Single Port <input type="button" value="▼"/> Service Port: 80																				
Inbound IP Address(es) (Require at least one IP address)	<table border="1"> <thead> <tr> <th colspan="2">Connection / IP Address(es)</th> <th>All</th> <th>Clear</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> WAN 1</td> <td><input checked="" type="checkbox"/> 10.88.3.184 (Interface IP)</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 3</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Mobile Internet</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Connection / IP Address(es)		All	Clear	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.184 (Interface IP)			<input type="checkbox"/> WAN 2				<input type="checkbox"/> WAN 3				<input type="checkbox"/> Mobile Internet			
Connection / IP Address(es)		All	Clear																		
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.184 (Interface IP)																				
<input type="checkbox"/> WAN 2																					
<input type="checkbox"/> WAN 3																					
<input type="checkbox"/> Mobile Internet																					
Included Server(s) (Require at least one IP address)	<table border="1"> <thead> <tr> <th colspan="2">Server</th> <th>Weight</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> myserver (192.168.1.123)</td> <td></td> <td>10 <input type="range" value="10"/></td> </tr> </tbody> </table>	Server		Weight	<input checked="" type="checkbox"/> myserver (192.168.1.123)		10 <input type="range" value="10"/>														
Server		Weight																			
<input checked="" type="checkbox"/> myserver (192.168.1.123)		10 <input type="range" value="10"/>																			

Services Settings	
<b>Enable</b>	<p>This setting specifies whether the inbound service rule takes effect.</p> <p>When <b>Yes</b> 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.</p> <p>When <b>No</b> is selected, the inbound service rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.</p>
<b>Service Name</b>	<p>This setting identifies the service to the system administrator. Only alphanumeric and the underscore “_” characters are valid.</p>
<b>IP Protocol</b>	<p>The <b>IP Protocol</b> setting, along with the <b>Port</b> setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Inbound traffic that matches the specified <b>IP Protocol</b> and <b>Port(s)</b> will be forwarded to the LAN hosts specified by the <b>Servers</b> setting.</p> <p>Upon choosing a protocol, the <b>Protocol Selection Tool</b> drop-down menu can be used to automatically the port information of common Internet services (e.g. HTTP, HTTPS, etc.).</p> <p>After selecting an item from the <b>Protocol Selection Tool</b> drop-down menu, the protocol and the port number will remain manually modifiable.</p>
<b>Port</b>	<p>The <b>Port</b> setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p> <p><b>Any Port, Single Port, Port Range, Port Map, and Range Mapping</b></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Port <input type="button" value="?"/> Any Port <input type="button" value="▼"/></p> </div> <p><b>Any Port:</b> all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the <b>Servers</b> setting.</p> <p>For example, if <b>IP Protocol</b> is set to <b>TCP</b> and <b>Port</b> is set to <b>Any Port</b>, then all TCP traffic will be forwarded to the configured servers.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Port <input type="button" value="?"/> Single Port <input type="button" value="▼"/> Service Port: 80</p> </div> <p><b>Single Port:</b> 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 <b>Servers</b> setting.</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.

**Port Range:** traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting.

For example, if **IP Protocol** is set to **TCP**, **Port** is set to **Port Range**, and **Service Port** set to 80-88, then TCP traffic received on ports 80 through 88 will be forwarded to the configured servers via the respective ports.

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

For example, if **IP Protocol** is set to **TCP**, **Port** is set to **Port Mapping**, **Service Port** is set to 80, and **Map to Port** is set to 88, then TCP traffic on port 80 is forwarded to the configured servers via port 88.

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

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

**Inbound IP Address(es)**

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

**Included Server(s)**

This setting specifies the LAN servers that handle requests for the service, and the relative weight values. The amount of traffic that is distributed to a server is proportional to the weight value assigned to the server relative to the total weight.

Example:

With the following weight settings on a Peplink Balance:

- demo\_server\_1: 10
- demo\_server\_2: 5

The total weight is 15 = (10 + 5)

Matching traffic distributed to demo\_server\_1: 67% = (10 / 15) x 100%

Matching traffic distributed to demo\_server\_2: 33% = (5 / 15) x 100%

**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
<input type="button" value="Save"/>	

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**.

### 12.5.3 DNS Settings

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.

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

<b>DNS Server</b>	Disabled	
<b>Zone Transfer</b>	Disabled	
<b>Default SOA / NS</b>	Undefined	
<b>Default Connection Priority</b>	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	
<b>Domain Names</b>	Domain Name <i>These is currently no DNS domains.</i> <input type="button" value="New Domain Name"/>	
<b>Reverse Lookup Zones</b>	Zone Name <i>There is currently no Reverse Lookup Zones.</i> <input type="button" value="New Reverse Lookup Zone"/>	

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



DNS Settings	
<b>DNS Servers</b>	<p>This setting specifies the WAN IP addresses on which the DNS server of the Peplink Balance should listen.</p> <p>If no addresses are selected, the inbound link load balancing feature will be disabled and the Peplink Balance will not respond to DNS requests.</p> <p>To specify and/or modify the IP addresses on which the DNS server should listen, click the button that corresponds to <b>DNS Server</b>, and a selection screen will be displayed:</p> <p>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.)</p> <p>Click <b>Save</b> to save the settings when configuration is complete.</p>
<b>Zone Transfer</b>	<p>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.</p> <p>The zone transfer server of the Peplink Balance listens on TCP port 53.</p> <p>The Peplink Balance serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing its LAN interface.</p>
<b>Routing Control by Subnet Database</b>	<p>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.</p>
<b>Default SOA / NS</b>	<p>Click the button to define a default SOA / NS record for all domain names.</p> <p>When defining a default SOA record, <b>Name Server IP Address</b> is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain.</p> <p>For defining default NS records, the host <i>[domain]</i> 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 <b>Host</b> field left empty. When the entered name server is a fully qualified domain name (FQDN), the <b>IP Address</b> field will be disabled.</p>
<b>Default Connection Priority</b>	<p><b>Default Connection Priority</b> defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the <b>Connection Priority</b> set to <b>Default</b>. Please refer to <b>Section 17.3.9</b> for details.</p> <p>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.</p> <p>To specify the primary and backup connections, click the button that corresponds to <b>Default Connection Priority</b>. A selection screen will appear.</p> <p>Each WAN connection is associated with a priority number. Click <b>Save</b> to save the settings when configuration is complete.</p>
<b>Domain name</b>	<p>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 <b>New Domain Name</b> button. Click on a domain name to edit. Press the red X to remove a domain name.</p>

### New Domain Name

Upon clicking the New Domain Name button, and the following screen will appear:

SOA Record						
Use Default SOA and NS Records						

NS Records			
Host	Name Server	TTL (sec)	
<i>There is currently no NS records.</i>			
<input type="button" value="New NS Records"/>			

MX Records			
Host	Priority	Mail Server	TTL (sec)
<i>There is currently no MX records.</i>			
<input type="button" value="New MX Records"/>			

CNAME Records		
Host	Points To	TTL (sec)
<i>There is currently no CNAME records.</i>		
<input type="button" value="New CNAME Record"/>		

A Records		
Host	Included IP Address(es)	TTL (sec)
<i>There is currently no A records.</i>		
<input type="button" value="New A Record"/>		

TXT Records		
Host	TXT Value	TTL (sec)
<i>There is currently no default TXT records.</i>		
<input type="button" value="New TXT Record"/>		


SRV Records					
Service	Priority	Weight	Target	Port	TTL (sec)
<i>There is currently no SRV records</i>					
<input type="button" value="New SRV Record"/>					

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.

## 12.5.3.1 SOA Records

**Default / Custom SOA Record**
✕

<b>Policy</b>	<input checked="" type="radio"/> Use Default SOA and NS Records <input type="radio"/> Customize SOA Record for this domain
---------------	---

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 <span style="float: right;">?</span>	<input type="text" value="ns1"/>
Name Server IP Address <span style="float: right;">?</span>	<input type="text"/>
Email <span style="float: right;">?</span>	<input type="text" value="webmaster"/>
Refresh (sec) <span style="float: right;">?</span>	<input type="text" value="14400"/>
Retry (sec) <span style="float: right;">?</span>	<input type="text" value="900"/>
Expire (sec) <span style="float: right;">?</span>	<input type="text" value="1209600"/>
Min Time (sec) <span style="float: right;">?</span>	<input type="text" value="3600"/>
TTL (sec) <span style="float: right;">?</span>	<input type="text" value="3600"/>

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

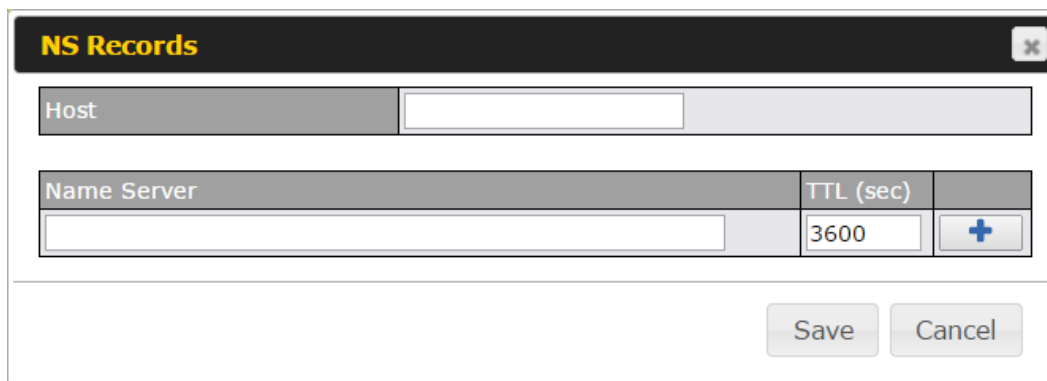
entry in this field is optional. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically. 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.

### 12.5.3.2 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:



Name Server	TTL (sec)	
<input type="text"/>	3600	<input data-bbox="1209 1465 1258 1518" type="button" value="+"/>

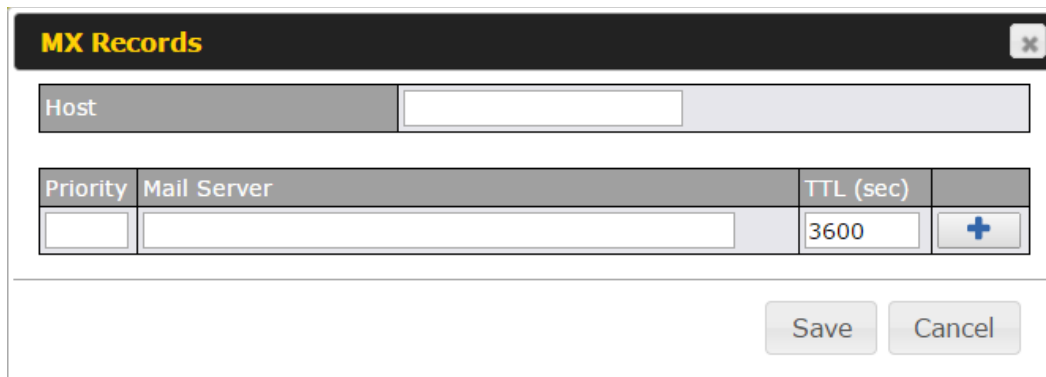
When creating an NS record for the domain itself (not a sub-domain), the **Host** field should be left blank.

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.

### 12.5.3.3 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 screenshot shows a dialog box titled "MX Records" with a close button (X) in the top right corner. It contains a form with the following fields:

- Host**: A text input field.
- Priority**: A text input field.
- Mail Server**: A text input field.
- TTL (sec)**: A text input field containing the value "3600".
- +**: A button with a plus sign to add a new record.

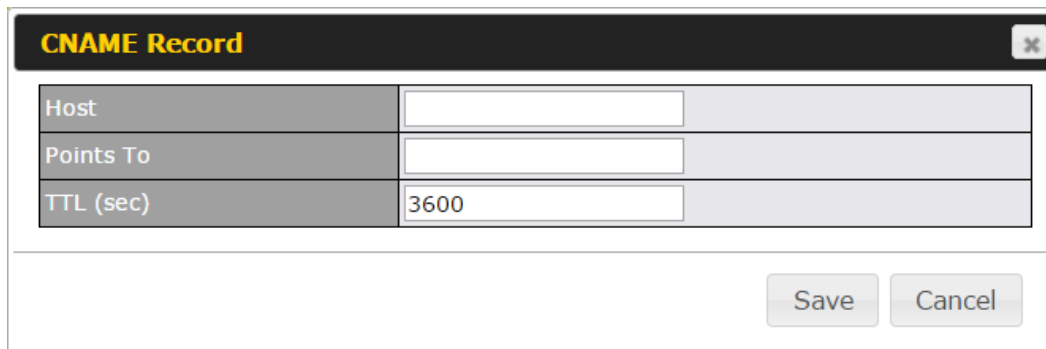
At the bottom of the dialog are two buttons: "Save" and "Cancel".

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.

### 12.5.3.4 CNAME Records

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 screenshot shows a dialog box titled "CNAME Record" with a close button (X) in the top right corner. It contains a form with the following fields:

- Host**: A text input field.
- Points To**: A text input field.
- TTL (sec)**: A text input field containing the value "3600".

At the bottom of the dialog are two buttons: "Save" and "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.

### 12.5.3.5 A Records

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

<b>Host Name</b>	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.
<b>TTL</b>	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.
<b>Priority</b>	This option specifies the priority of different connections. Select the <b>Default</b> option to apply the <b>Default Connection Priority</b> (refer to the table shown on the main DNS settings page) to an A record. To customize priorities, choose the <b>Custom</b> option and a priority selection table will be shown at the bottom.
<b>Included IP Address(es)</b>	<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 <b>Host Name</b>.</p> <p>The IP addresses listed in each box as <b>default</b> 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 <b>Custom IP</b> 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 <b>Custom IP Address</b> field will always be returned.</p> <p>If the <b>Connection Priority</b> field is set to <b>Custom</b>, 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, <b>Connection Priority</b> is set to <b>Default</b>.</p>

### 12.5.3.6 PTR Records

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

### 12.5.3.7 TXT Records

This table shows the TXT record of the domain name.

**TXT Record**
✕

Host	<input style="width: 90%;" type="text"/>
TXT Value	<input style="width: 90%; height: 40px;" type="text"/>
TTL (sec)	<input style="width: 90%;" 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.

### 12.5.3.8 SRV Records

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

**SRV Records**
✕

Service

Priority	Weight	Target	Port	TTL (sec)	
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	3600	<input style="background-color: #007bff; color: #fff; border: none; border-radius: 50%;" 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.

## Reverse Lookup Zones

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



The screenshot shows a dialog box titled "New Reverse Lookup Zone". It contains a text input field labeled "Zone Name" with the text ".in-addr.arpa" entered. Below the input field are two buttons: "Save" and "Cancel".

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!			
<input type="button" value="New NS Records"/>			

**CNAME Records**
?

Host	Points To	TTL (sec)	
There is currently no CNAME records.			
<input type="button" value="New CNAME Record"/>			

**PTR Records**
?

Host IP Number	Points To	TTL (sec)	
There is currently no PTR records.			
<input type="button" value="New PTR Record"/>			

## 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	?	<input type="text"/>
Email	?	<input type="text" value="webmaster"/>
Refresh (sec)	?	<input type="text" value="14400"/>
Retry (sec)	?	<input type="text" value="900"/>
Expire (sec)	?	<input type="text" value="1209600"/>
Min Time (sec)	?	<input type="text" value="3600"/>
TTL (sec)	?	<input type="text" value="3600"/>

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

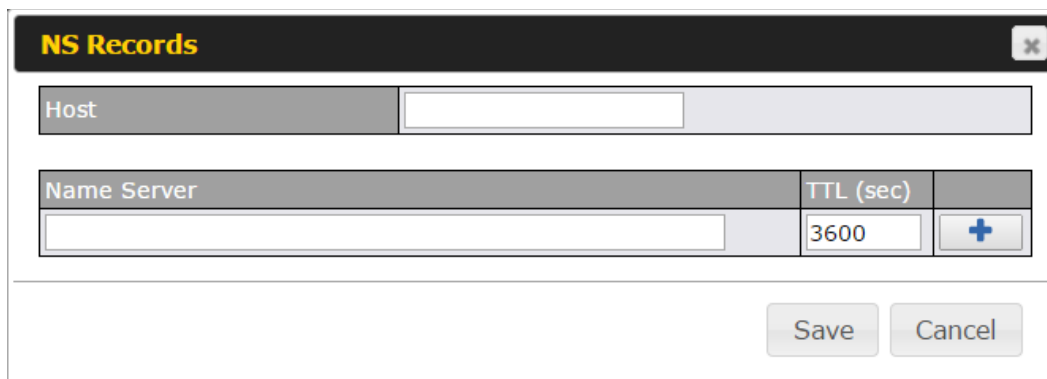
For example:

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

"ns2.mydomain.com."

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

## NS Records

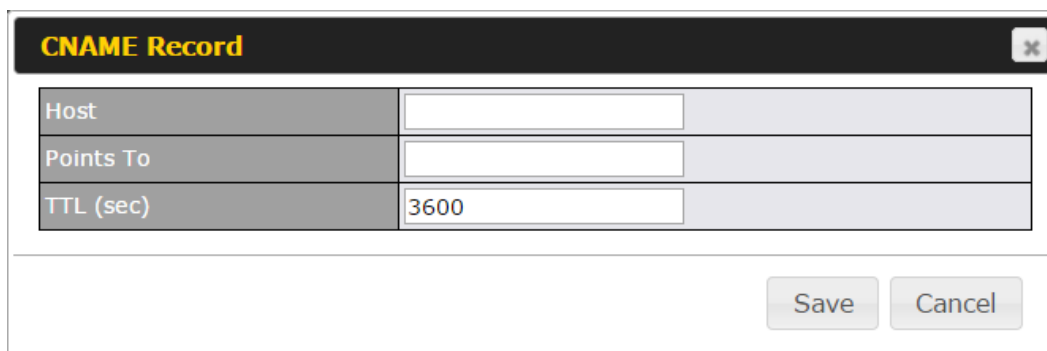


NS Records		
Host	<input type="text"/>	
Name Server	TTL (sec)	
<input type="text"/>	3600	+
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

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.

## CNAME Records



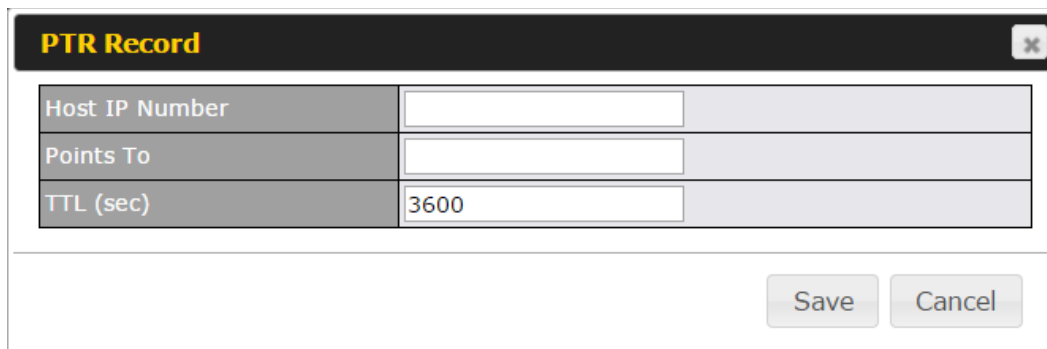
CNAME Record	
Host	<input type="text"/>
Points To	<input type="text"/>
TTL (sec)	3600
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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."



## PTR Records



The dialog box titled "PTR Record" contains a table with three rows and two columns. The first row is "Host IP Number" with an empty text input field. The second row is "Points To" with an empty text input field. The third row is "TTL (sec)" with a text input field containing the value "3600". Below the table are two buttons: "Save" and "Cancel".

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

Save Cancel

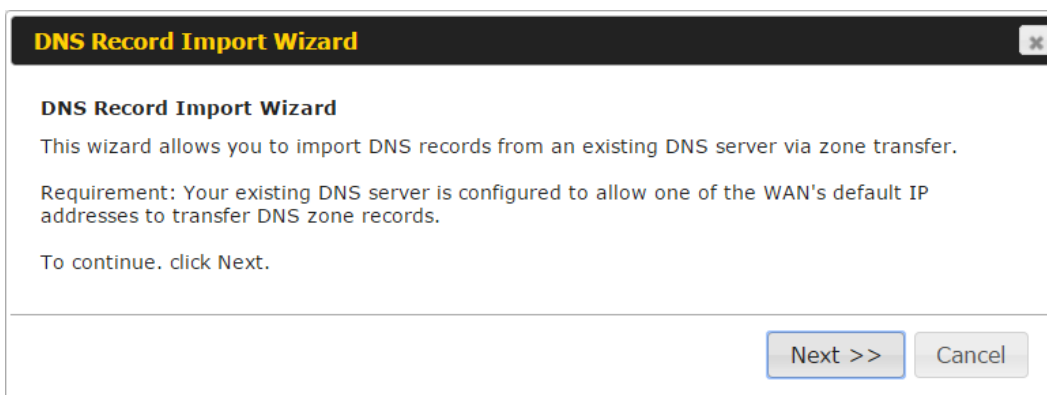
To create a new PTR record, click the **New PTR Record** button.

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

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

## 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.



The dialog box titled "DNS Record Import Wizard" contains the following text:

**DNS Record Import Wizard**

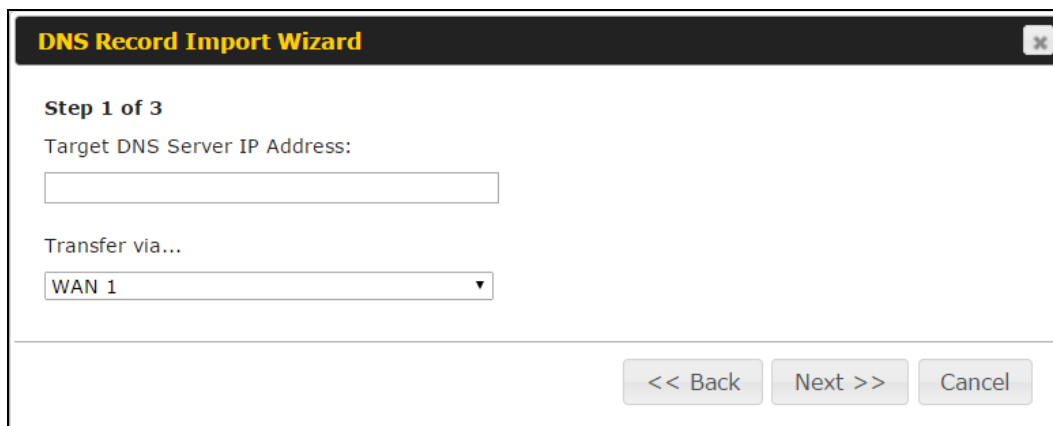
This wizard allows you to import DNS records from an existing DNS server via zone transfer.

Requirement: Your existing DNS server is configured to allow one of the WAN's default IP addresses to transfer DNS zone records.

To continue, click Next.

Next >> Cancel

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



**DNS Record Import Wizard**

**Step 1 of 3**

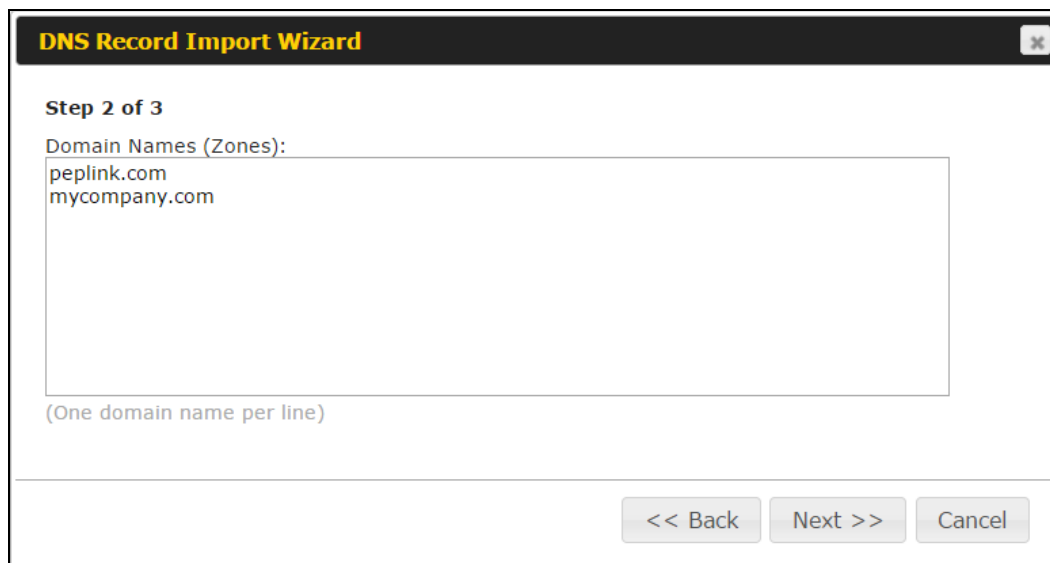
Target DNS Server IP Address:

Transfer via...

WAN 1

<< Back   Next >>   Cancel

- 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

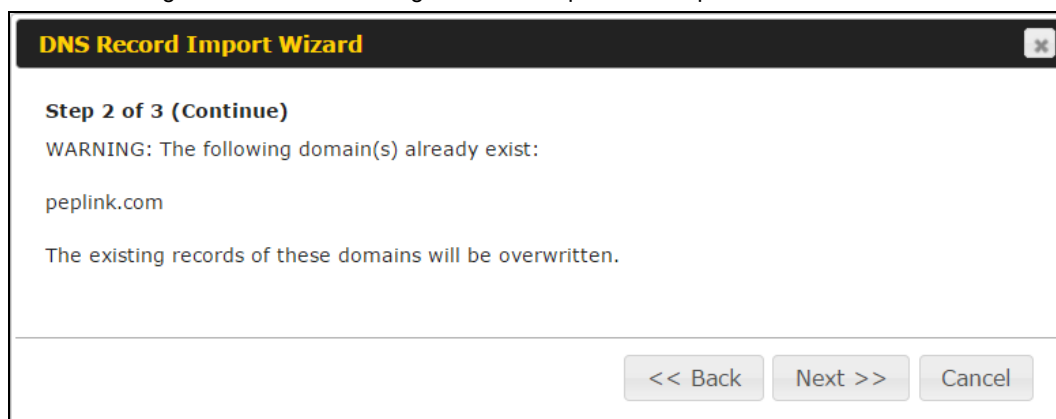
(One domain name per line)

<< 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**

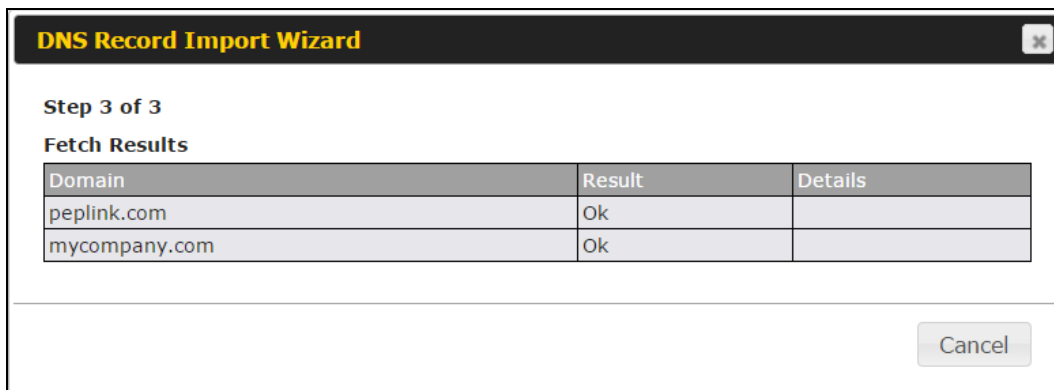
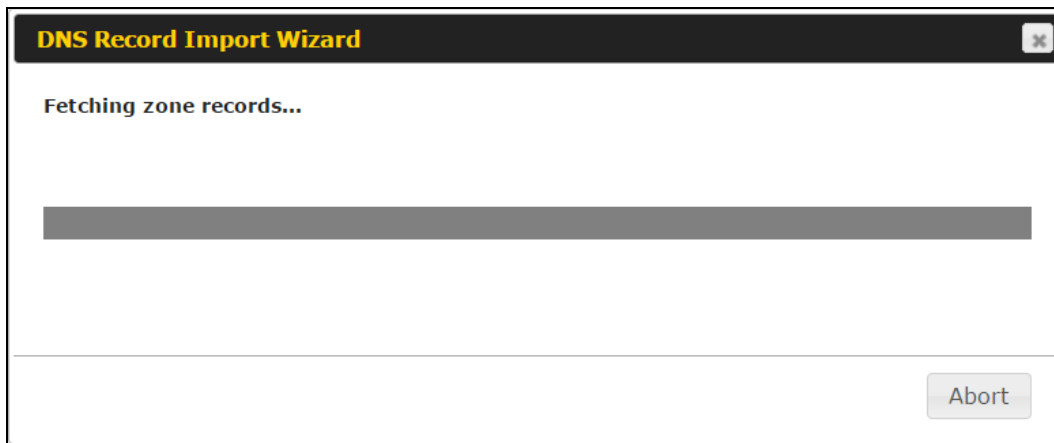
**Step 2 of 3 (Continue)**

WARNING: The following domain(s) already exist:

peplink.com

The existing records of these domains will be overwritten.

<< Back   Next >>   Cancel





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

## 12.6 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	
<a href="#">Add NAT Rule</a>			

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 ?	<b>Connection / Inbound IP Address(es)</b>
	<input checked="" type="checkbox"/> WAN 1 <span style="float: right;"><input checked="" type="checkbox"/> 10.91.137.1 (Interface IP)</span>
	<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
Outbound Mappings ?	<b>Connection / Outbound IP Address</b>
	WAN 1 <span style="float: right;">10.91.137.1 (Interface IP) ▼</span>
	WAN 2 <span style="float: right;">10.91.138.1 (Interface IP) ▼</span>
	WAN 3 <span style="float: right;">10.91.139.1 (Interface IP) ▼</span>
	WAN 4 <span style="float: right;">Interface IP ▼</span>
	WAN 5 <span style="float: right;">Interface IP ▼</span>
	WAN 6 <span style="float: right;">Interface IP ▼</span>
	WAN 7 <span style="float: right;">Interface IP ▼</span>
	WAN 8 <span style="float: right;">Interface IP ▼</span>
	WAN 9 <span style="float: right;">Interface IP ▼</span>
	WAN 10 <span style="float: right;">Interface IP ▼</span>
	WAN 11 <span style="float: right;">Interface IP ▼</span>
	WAN 12 <span style="float: right;">Interface IP ▼</span>
	Mobile Internet <span style="float: right;">Interface IP ▼</span>

<b>NAT Mapping Settings</b>	
<b>LAN Client(s)</b>	NAT Mapping rules can be defined for a single LAN <b>IP Address</b> , an <b>IP Range</b> , or an <b>IP Network</b> .

<b>Address</b>	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 <b>IP Address</b> is selected.
<b>Range</b>	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 <b>IP Range</b> is selected.
<b>Network</b>	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 <b>IP Network</b> is selected.
<b>Inbound Mappings</b>	<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 <b>IP Address</b> is selected in the <b>LAN Client(s)</b> 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>
<b>Outbound Mappings</b>	<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 <b>Outbound Policy</b> 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

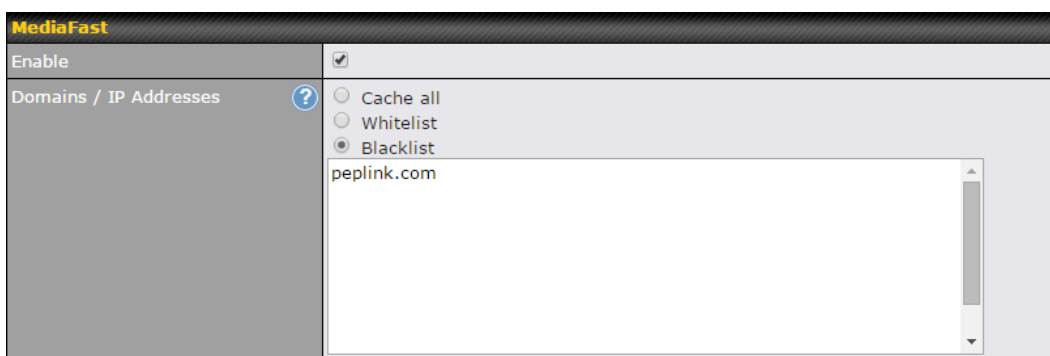
Inbound firewall rules override inbound mapping settings.

## 12.7 MediaFast

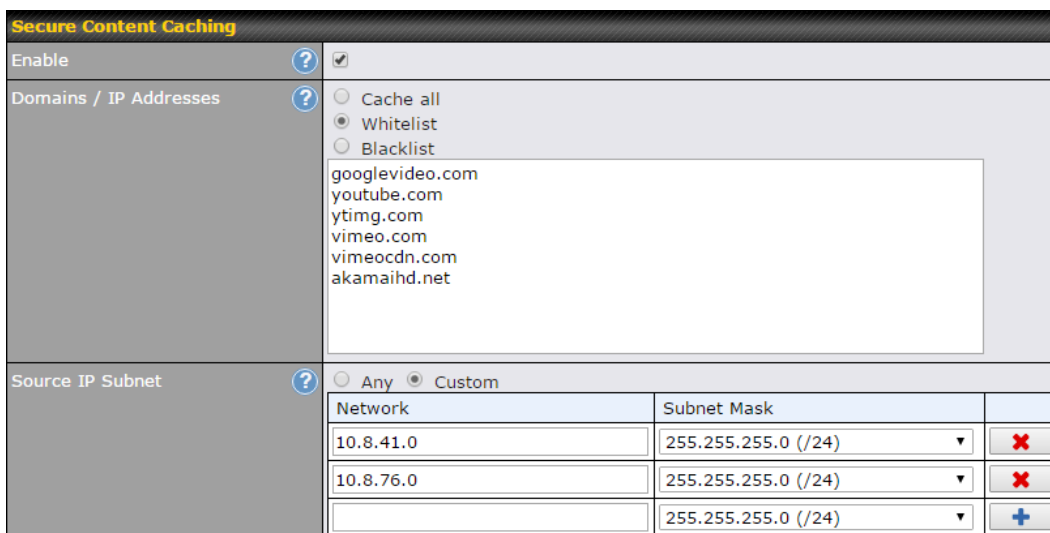
MediaFast settings can be configured by navigating to **Network > MediaFast**.

## Setting Up MediaFast Content Caching

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



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



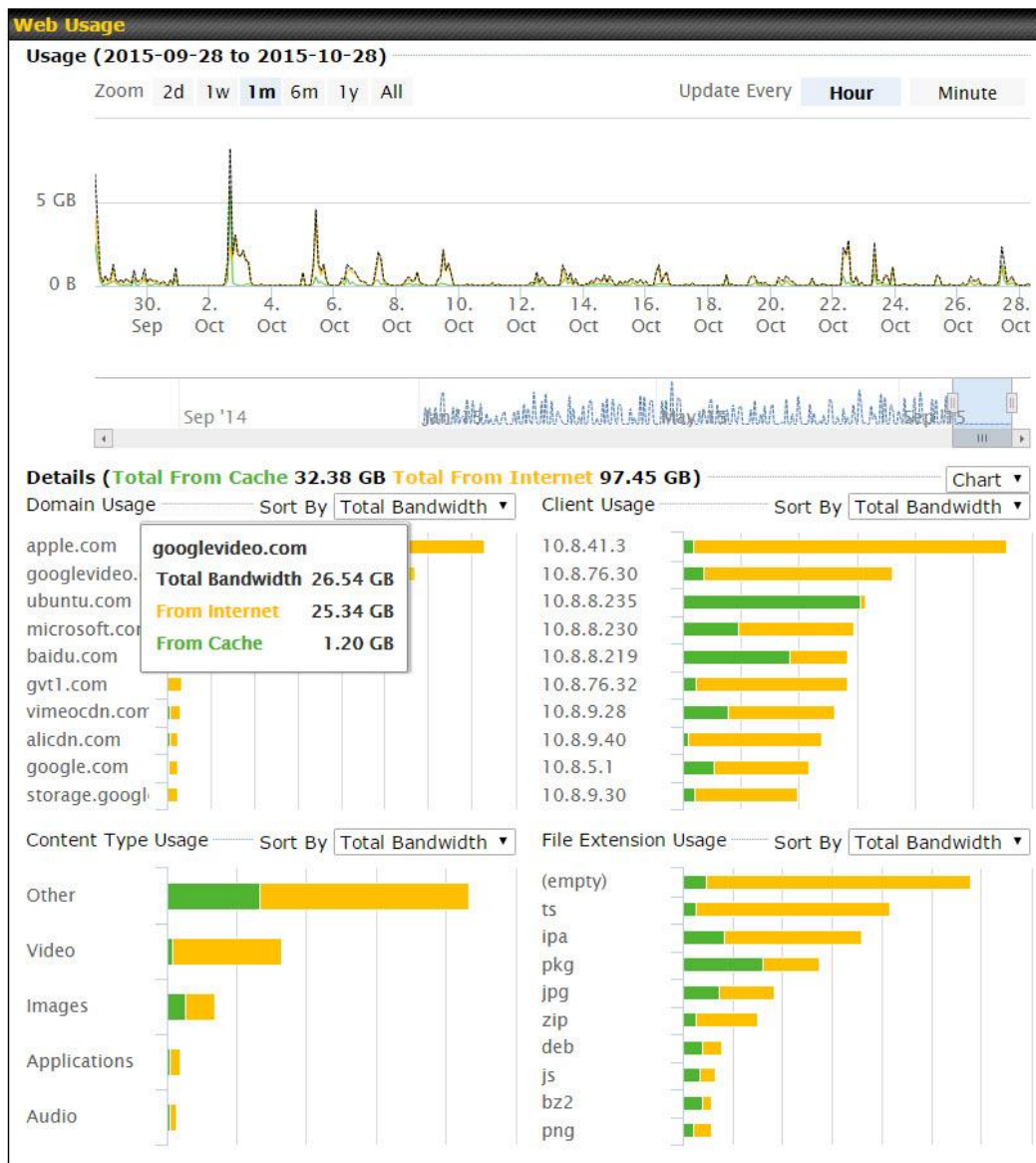
The **Secure Content Caching** menu operates identically to the **MediaFast** menu, except it is for secure contenting accessible through <https://>.

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

Cache Control	
<b>Content Type</b>	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
<b>Cache Lifetime Settings</b>	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.

## Viewing MediaFast Statistics

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



### 12.7.1 Prefetch Schedule

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	
<b>Name</b>	This field displays the name given to the scheduled download.
<b>Status</b>	Check the status of your scheduled download here.
<b>Next Run Time/Last Run Time</b>	These fields display the date and time of the next and most recent occurrences of the scheduled download.
<b>Last Duration</b>	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.
<b>Result</b>	This field indicates whether downloads are in progress (  ) or complete (  ).
<b>Last Download</b>	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.
<b>Actions</b>	<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>
<b>New Schedule</b>	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	www.peplink.com	✖
	www.peplink.com/knowledgebase	+
Depth	2 levels <b>Default</b>	
Time Period	From 00:00 to 01:00	
Repeat	Everyday	

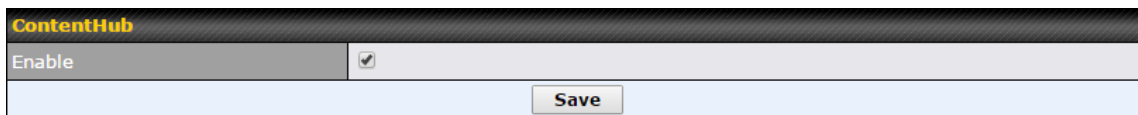
Simply provide the requested information to create your schedule.

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

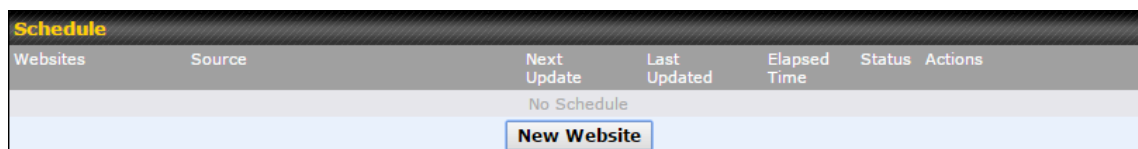
**Clear Statistics**      Click to clear all prefetch and status page statistics.

## 12.8 ContentHub

Integrated into MediaFast-enabled routers, ContentHub allows you to deliver webpages and applications using the cache. To access ContentHub, navigate to **Network > ContentHub**:



Check the **Enable** box.



Click **New Website**, and the following configuration options will appear:



Active	<input checked="" type="checkbox"/>
Type	<input checked="" type="radio"/> Website <input type="radio"/> Application

The Active checkbox toggles the activation of the website/application. This will be useful when there are multiple applications being delivered. For type, you can select either Website or Application:

Selecting Website:

Domain/Path	<input type="text" value="http://"/>
Source	ftp:// <input type="text"/> Username: <input type="text"/> Password: <input type="text"/>
Period	Everyday <input type="text"/> From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="01"/> : <input type="text" value="00"/>
Bandwidth Limit	<input type="text" value="0"/> Gbps (0: Unlimited)

<b>Domain/Path</b>	Both domain and path must be specified for website type.
<b>Source</b>	Enter the FTP server you will be downloading the content from. Enter your credentials under <b>Username</b> and <b>Password</b> .
<b>Period</b>	This field determines how often the Router will search for updates to the source content.
<b>Bandwidth Limit</b>	This field determines the amount of bandwidth dedicated to this website.

Selecting Application:

Domain	<input type="text" value="http://"/>
Method	<input type="radio"/> Sync <input checked="" type="radio"/> File Upload
Bandwidth Limit	<input type="text" value="0"/> Gbps (0: Unlimited)

<b>Domain</b>	Enter the domain your application is hosted at
---------------	--

<b>Method</b>	Enter the FTP server you will be downloading the content from. Enter your credentials under <b>Username</b> and <b>Password</b> .
<b>Bandwidth Limit</b>	This field determines the amount of bandwidth dedicated to this application.

## 12.9 MDM Settings

In addition to performing content caching, MediaFast-enabled routers can also serve as an MDM, administrating to client devices. To access MDM Settings, navigate to **Network > MDM Settings**:

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





MDM Settings	
<b>Enable</b>	Click this checkbox to enable MDM on your router.
<b>Account Settings</b>	Click <b>Follow Web Admin Account</b> to allow client devices to use the built-in administrator account when performing MDM. Set <b>Custom</b> to specify a username and password your router will use to log into your client devices.

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

Captive Portal Settings															
<b>Enable</b>	Check <b>Enable</b> and then, optionally, select the LANs/VLANs that will use the captive portal.														
<b>Hostname</b>	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 <b>Default</b> .														
<b>Access Mode</b>	Click <b>Open Access</b> to allow clients to freely access your router. Click <b>User Authentication</b> to force your clients to authenticate before accessing your router.														
<b>RADIUS Server</b>	<p>This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:</p> <table border="1"> <tbody> <tr> <td>Authentication</td> <td>RADIUS Server</td> </tr> <tr> <td>Auth Server</td> <td><input type="text"/> Port <input type="text" value="1812"/> <a href="#">Default</a></td> </tr> <tr> <td>Auth Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>CoA-DM</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Accounting Server</td> <td><input type="text"/> Port <input type="text" value="1813"/> <a href="#">Default</a></td> </tr> <tr> <td>Accounting Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Accounting Interim Interval</td> <td><input type="text"/> seconds</td> </tr> </tbody> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	RADIUS Server	Auth Server	<input type="text"/> Port <input type="text" value="1812"/> <a href="#">Default</a>	Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	CoA-DM	<input type="checkbox"/>	Accounting Server	<input type="text"/> Port <input type="text" value="1813"/> <a href="#">Default</a>	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 <input type="text" value="1812"/> <a href="#">Default</a>														
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters														
CoA-DM	<input type="checkbox"/>														
Accounting Server	<input type="text"/> Port <input type="text" value="1813"/> <a href="#">Default</a>														
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters														
Accounting Interim Interval	<input type="text"/> seconds														
<b>LDAP Server</b>	<p>This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:</p> <table border="1"> <tbody> <tr> <td>Authentication</td> <td>LDAP Server</td> </tr> <tr> <td>LDAP Server</td> <td><input type="text"/> Port <input type="text" value="389"/> <a href="#">Default</a></td> </tr> <tr> <td></td> <td><input type="checkbox"/> Use DN/Password to bind to LDAP Server</td> </tr> <tr> <td>Base DN</td> <td><input type="text"/></td> </tr> <tr> <td>Base Filter</td> <td><input type="text"/></td> </tr> </tbody> </table>	Authentication	LDAP Server	LDAP Server	<input type="text"/> Port <input type="text" value="389"/> <a href="#">Default</a>		<input type="checkbox"/> Use DN/Password to bind to LDAP Server	Base DN	<input type="text"/>	Base Filter	<input type="text"/>				
Authentication	LDAP Server														
LDAP Server	<input type="text"/> Port <input type="text" value="389"/> <a href="#">Default</a>														
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server														
Base DN	<input type="text"/>														
Base Filter	<input type="text"/>														

	Fill in the necessary information to complete your connection to the server and enable authentication.
<b>Access Quota</b>	Set a time and data cap to each user's Internet usage.
<b>Quota Reset Time</b>	This menu determines how your usage quota resets. Setting it to <b>Daily</b> will reset it at a specified time every day. Setting a number of <b>minutes after quota reached</b> establish a timer for each user that begins after the quota has been reached.
<b>Allowed Networks</b>	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.
<b>Allowed Clients</b>	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.
<b>Splash Page</b>	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 style="border: 1px solid #ccc; height: 100px;"></div>
Terms & Conditions	<div style="border: 1px solid #ccc; height: 100px; text-align: center;">[Use default Terms &amp; Conditions]</div>
Custom Landing Page	<input checked="" type="checkbox"/> <input type="text" value="http://"/>

Portal Customization	
<b>Logo Image</b>	Click the <b>Choose File</b> button to select an logo to use for the built-in portal.
<b>Message</b>	If you have any additional messages for your users, enter them in this field.
<b>Terms &amp; Conditions</b>	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.
<b>Custom Landing Page</b>	Fill in this field to redirect clients to an external URL.

## 12.11 QoS

### 12.11.1 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	
<b>Subnet / IP Address</b>	From the drop-down menu, choose whether you are going to define the client(s) by an <b>IP Address</b> or a <b>Subnet</b> . If <b>IP Address</b> is selected, enter a name defined in DHCP reservation table or a LAN client's IP address. If <b>Subnet</b> is selected, enter a subnet address and specify its subnet mask.
<b>Group</b>	This field is to define which <b>User Group</b> 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.

### 12.11.2 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%
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	
Staff:	20	Mbps	10 Mbps (0: unlimited)
Guest:	500	Mbps	100 Mbps (0: unlimited)

### 12.11.3 Application

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


Application Prioritization	
<input type="radio"/>	Apply same settings to all users
<input checked="" type="radio"/>	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			?
	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				

### 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** ✘

Type	<input checked="" type="radio"/> Supported Applications <input type="radio"/> Custom Applications
Category	Miscellaneous
Application	All Supported Miscellaneous Protocols All Supported Miscellaneous Protocols HTTP NTP SNMP STUN USENET

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

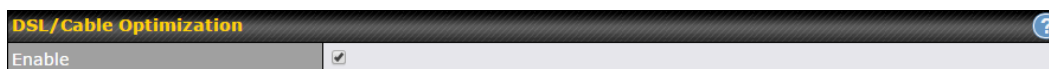


## DSL/Cable Optimization

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.



## 12.12 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)

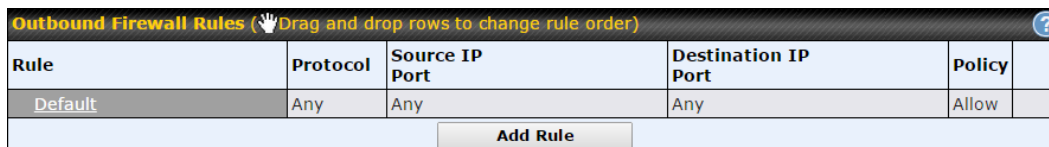
The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion™ enabled, the firewall rules also apply to VPN tunneled traffic. The Firewall function can be found at **Network>Firewall**

### 12.12.1 Access Rules

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



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

**Add a New Outbound Firewall Rule** ✕

---

**New Firewall Rule**

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

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

Inbound Firewall Rules <span style="float: right;">? (Drag and drop rows to change rule order)</span>						
Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy	
Default	Any	Any	Any	Any	Allow	
<input type="button" value="Add Rule"/>						

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

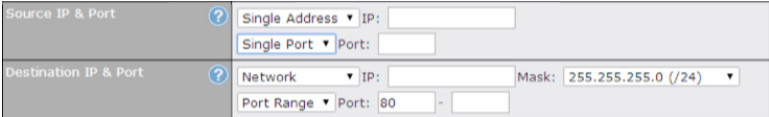
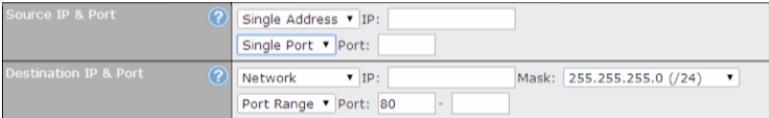
**Add a New Inbound Firewall Rule** ✕

---

**New Firewall Rule**

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

Inbound / Outbound Firewall Settings	
<b>Rule Name</b>	This setting specifies a name for the firewall rule.

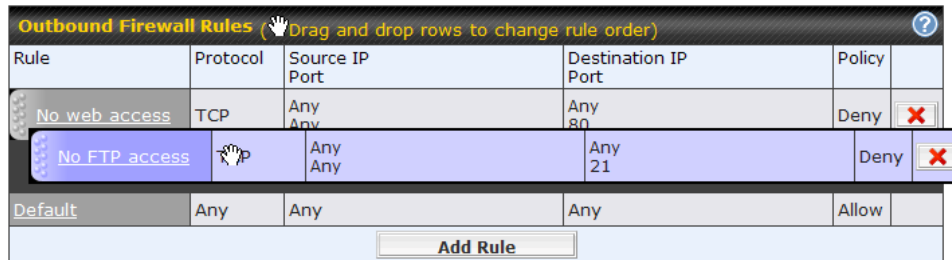
<p><b>Enable</b></p>	<p>This setting specifies whether the firewall rule should take effect.</p> <p>If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule.</p> <p>If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>
<p><b>WAN Connection (Inbound)</b></p>	<p>Select the WAN connection that this firewall rule should apply to.</p>
<p><b>Protocol</b></p>	<p>This setting specifies the protocol to be matched.</p> <p>Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• IP</li> </ul> <p>Alternatively, the <b>Protocol Selection Tool</b> 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 <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remains manually modifiable.</p>
<p><b>Source IP &amp; Port</b></p>	<p>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 <b>Source IP &amp; Port</b> setting, as indicated with the following screenshots:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Source IP &amp; Port</b> settings.</p>
<p><b>Destination IP &amp; Port</b></p>	<p>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 <b>Destination IP &amp; Port</b> setting, as indicated with the following screenshots:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Destination IP &amp; Port</b> settings.</p>

<b>Action</b>	<p>This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:</p> <ul style="list-style-type: none"><li>• Source IP &amp; port</li><li>• Destination IP &amp; port</li></ul> <p>With the value of <b>Allow</b> for the <b>Action</b> setting, the matching traffic passes through the router (to be routed to the destination). If the value of the <b>Action</b> setting is set to <b>Deny</b>, the matching traffic does not pass through the router (and is discarded).</p>
<b>Event Logging</b>	<p>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page <b>Status&gt;Event Log</b>. A sample message is as follows:</p> <p>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</p> <ul style="list-style-type: none"><li>• <b>CONN:</b> The connection where the log entry refers to</li><li>• <b>SRC:</b> Source IP address</li><li>• <b>DST:</b> Destination IP address</li><li>• <b>LEN:</b> Packet length</li><li>• <b>PROTO:</b> Protocol</li><li>• <b>SPT:</b> Source port</li><li>• <b>DPT:</b> Destination port</li></ul>

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.

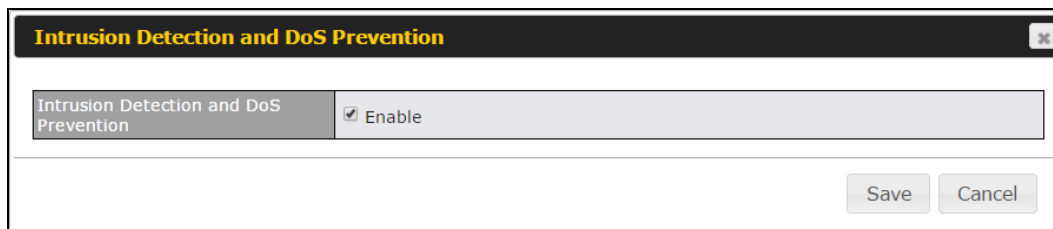
Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default** rule will be applied.


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.

## 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

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

### **12.12.2 Content Blocking**

**Application Blocking** ?

Please Select Application... +

**Web Blocking** ?

Preset Category

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

Customized Domains

<input type="text" value="cbs.com"/>	✖
<input type="text"/>	+

Exempted Domains from Web Blocking

<input type="text"/>	+
----------------------	---

**Exempted User Groups** ?

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

**Exempted Subnets** ?

Network	Subnet Mask
<input type="text"/>	255.255.255.0 (/24) <span style="float: right;">+</span>

**URL Logging**

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

## 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.

## 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.

## Customized Domains

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

You may enter the wild card ".\*" at the end of a domain name to block any web site with a host name having the domain name in the middle. For example, If you enter "foobar.\*", then "www.foobar.com," "www.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.

## Exempted User Groups

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



## Exempted Subnets

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

## URL Logging

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

## 12.13 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	LAN IP Address	
Area	Interfaces	
0.0.0.0	PepVPN	
<input type="button" value="Add"/>		

PepVPN OSPF Area	
0.0.0.0	


RIPv2	
No RIPv2 Defined.	

OSPF	
<b>Router ID</b>	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 <b>Custom</b> field.
<b>Area</b>	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 <b>Add</b> . To delete an existing area, click  .

**OSPF settings**
✕

<b>Area ID</b>	<input type="text" value="0.0.0.0"/>
<b>Link Type</b>	<input checked="" type="radio"/> Broadcast <input type="radio"/> Point-to-Point
<b>Authentication</b>	None ▾
<b>Interfaces</b>	<div style="display: flex; align-items: flex-start;"> <div style="width: 20px; text-align: center; font-size: 0.8em; color: #007bff; margin-right: 5px;">?</div> <ul style="list-style-type: none"> <li><input type="checkbox"/> Untagged LAN</li> <li><input type="checkbox"/> V167 (192.168.167.1/24)</li> <li><input type="checkbox"/> WAN 1</li> <li><input type="checkbox"/> WAN 2</li> <li><input type="checkbox"/> WAN 3</li> <li><input type="checkbox"/> WAN 4</li> <li><input type="checkbox"/> WAN 5</li> <li><input checked="" type="checkbox"/> PepVPN</li> </ul> </div>

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

To access RIPv2 settings, click  .

**RIPv2 settings** ✕

Authentication	None ▾
Interfaces	<input type="checkbox"/> Untagged LAN <input type="checkbox"/> V167 (192.168.167.1/24) <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

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

**OSPF & RIPv2 Route Advertisement**

PepVPN Route Isolation <span style="float: right;">?</span>	<input type="checkbox"/> Enable							
Network Advertising <span style="float: right;">?</span>	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span style="font-size: 0.8em;">---</span> <span style="margin-left: 10px;">▾</span> <span style="margin-left: 10px;">+</span> </div> <small>All LAN/VLAN networks will be advertised when no network advertising is chosen.</small>							
Static Route Advertising <span style="float: right;">?</span>	<input checked="" type="checkbox"/> Enable							
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="font-size: 0.8em;">Excluded Networks</th> <th style="font-size: 0.8em;">Subnet Mask</th> <th style="font-size: 0.8em;"></th> </tr> </thead> <tbody> <tr> <td style="border: 1px solid #ccc; height: 15px;"></td> <td style="border: 1px solid #ccc; font-size: 0.8em;">255.255.255.0 (/24) ▾</td> <td style="border: 1px solid #ccc; text-align: center; font-size: 0.8em;">+</td> </tr> </tbody> </table>	Excluded Networks	Subnet Mask			255.255.255.0 (/24) ▾	+	
Excluded Networks	Subnet Mask							
	255.255.255.0 (/24) ▾	+						

OSPF & RIPv2 Route Advertisement	
<b>PepVPN Route Isolation</b>	Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption..
<b>Network Advertising</b>	Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.
<b>Static Route Advertising</b>	Enable this option to advertise LAN static routes over OSPF & RIPv2. Static routes that match the Excluded Networks table will not be advertised.

## 12.14 BGP

Click the Network tab from the top bar, and then click the **BGP** item on the sidebar to configure BGP.

BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	
<input type="button" value="Add"/>			

Click "x" to delete a BGP profile

Click "Add" to add a new BGP profile

BGP Profile						
Profile Name	<input type="text"/>					
Enable	<input checked="" type="checkbox"/>					
Interface	WAN 1					
Router ID	<input type="radio"/> LAN IP Address <input type="radio"/> Custom: <input type="text"/>					
Autonomous System	<input type="text"/>					
Neighbor	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
	<input type="text"/>	<input type="text"/>	disable	<input type="text"/>	<input type="text"/>	
Hold Time		<input type="text" value="240"/>				

BGP	
<b>Name</b>	This field is for specifying a name to represent this profile.
<b>Enable</b>	When this box is checked, this BGP profile will be enabled. Otherwise, it will be disabled.
<b>Interface</b>	The interface where BGP neighbor is located
<b>Autonomous System</b>	The Autonomous System Number (ASN) of this profile
<b>Neighbor</b>	BGP Neighbor's details
<b>IP address</b>	Neighbor's IP address
<b>Autonomous</b>	Neighbor's ASN

System	
<b>Multihop/TTL</b>	Time-to-live (TTL) of BGP packet. Leave it blank if BGP neighbor is directly connected, otherwise you must specify a TTL value. Accurately, this option should be used if the configured neighbor IP address does not match the selected Interface's network subnets. TTL value must be between 2 to 255.
<b>Password</b>	Optional password for MD5 authentication of BGP sessions.
<b>AS-Path Prepending:</b>	AS path to be prepended to the routes received from this neighbor. The value must be a comma separated ASN. For example "64530,64531" will prepend "64530, 64531" to received routes.
<b>Hold Time</b>	Time in seconds to wait for a keepalive message from the neighbor before considering the BGP connection is staled. This value must be either 0 (infinite hold time) or between 3 and 65535 inclusively.

Route Advertisement			
Network Advertising		---	
Static Route Advertising		<input checked="" type="checkbox"/> Enable	
		Excluded Networks	Subnet Mask
			255.255.255.0 (/24)
Advertise OSPF Route		<input type="checkbox"/>	

<b>Network Advertising</b>	Networks to be advertised to BGP neighbor.
<b>Static Route Advertising</b>	Enable this option to advertise LAN static routes. Static routes that match the Excluded Networks table will not be advertised.
<b>Advertise OSPF Route</b>	When this box is checked, all learnt OSPF routes will be advertised.

Route Import			
Filter Mode		Accept ▼	
Restricted Networks	Network	Subnet Mask	Exact Match
		255.255.255.0 (/24) ▼	<input type="checkbox"/>

<b>Filter Mode</b>	<p>This option selects the route import filter mode.</p> <p><b>None:</b> all BGP routes will be accepted.</p> <p><b>Accept:</b> Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p><b>Reject:</b> Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.</p>
<b>Restricted Networks</b>	<p>This specifies the network in the "route import" entry</p> <p><b>Exact Match:</b> When this box is checked, only routes with the same Networks and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnet will be filtered.</p>

Route Export	
Export to other BGP Profile	<input type="checkbox"/>
Export to OSPF	<input type="checkbox"/>

<b>Export to other BGP Profile</b>	When this box is checked, routes learnt from this BGP profile will export to other BGP profiles.
<b>Export to OSPF</b>	When this box is checked, routes learnt from this BGP profile will export to the OSPF routing protocol.

## 12.15 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	<b>Connection / IP Address(es)</b>		
	<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	Username	Password	
	admin	.....	<input type="button" value="X"/>
	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>

Remote User Access Settings	
<b>Enable</b>	Click the checkbox to enable Remote User Access.
<b>VPN Type</b>	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.
<b>Preshared Key</b>	Enter your preshared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
<b>Listen On</b>	This setting is for specifying the WAN IP addresses where the PPTP server of the router should listen on.
<b>User Accounts</b>	<p>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.</p> <p>Click the  button to switch to enters user accounts by pasting the information in.CSV</p>

format.

## 12.16 Misc. Settings

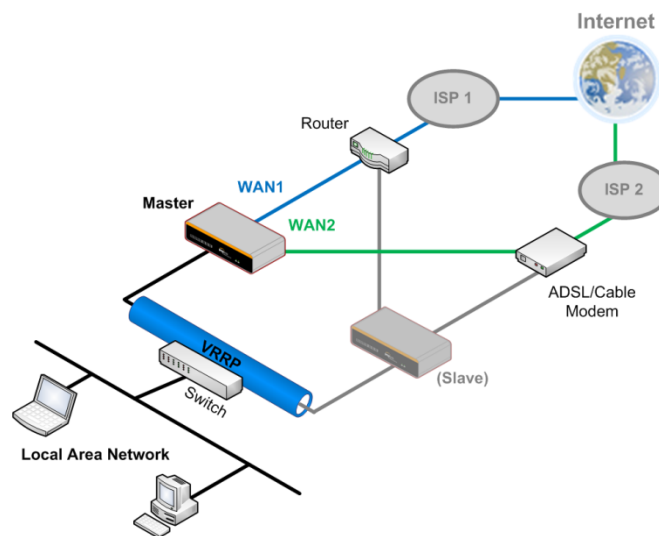
### 12.16.1 High Availability

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	
Enable	<input checked="" type="checkbox"/>
Group Number	5
Preferred Role	<input checked="" type="radio"/> Master <input type="radio"/> Slave
Resume Master Role Upon Recovery	<input checked="" type="checkbox"/>
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

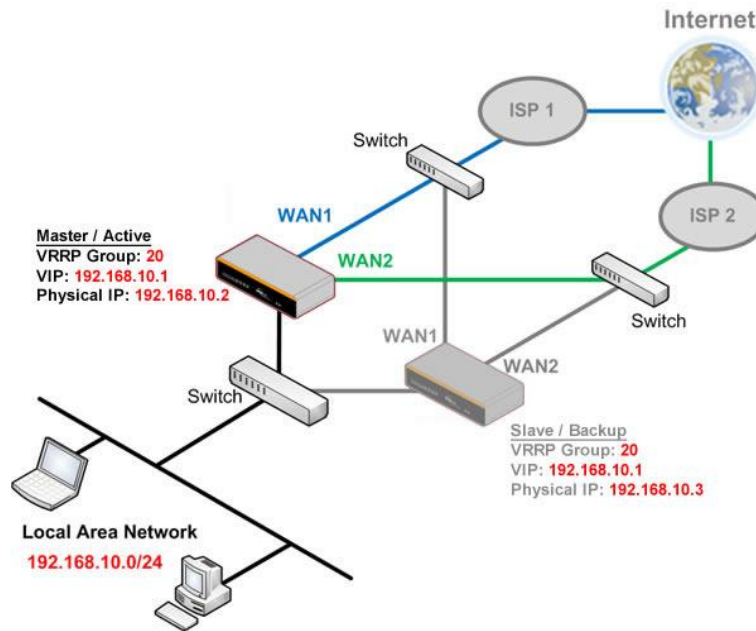
High Availability	
Enable	<input checked="" type="checkbox"/>
Group Number	5
Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/> Slave
Configuration Sync.	<input type="checkbox"/> Master Serial Number: 5454- 5454 - 5454
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

High Availability	
<b>Enable</b>	Checking this box specifies that the Peplink Balance unit is part of a high availability configuration.
<b>Group Number</b>	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 <b>Group Number</b> value.
<b>Preferred Role</b>	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.
<b>Resume Master Role Upon Recovery</b>	This option is displayed when <b>Master</b> mode is selected in <b>Preferred Role</b> . If this option is enabled, once the device has recovered from an outage, it will take over and resume its <b>Master</b> role from the slave unit.
<b>Configuration Sync.</b>	This option is displayed when <b>Slave</b> mode is selected in <b>Preferred Role</b> . If this option is enabled and the <b>Master Serial Number</b> entered matches with the actual master unit's, the master unit will automatically transfer the configuration to this unit. Please make sure the <b>LAN IP Address</b> and the <b>Subnet Mask</b> fields are set correctly in the LAN settings page. You can refer to the <b>Event Log</b> for the configuration synchronization status.
<b>Master Serial Number</b>	If <b>Configuration Sync.</b> is checked, the serial number of the master unit is required here for the feature to work properly.
<b>Virtual IP</b>	The HA pair must share the same <b>Virtual IP</b> . The <b>Virtual IP</b> and the <b>LAN Administration IP</b> must be under the same network.

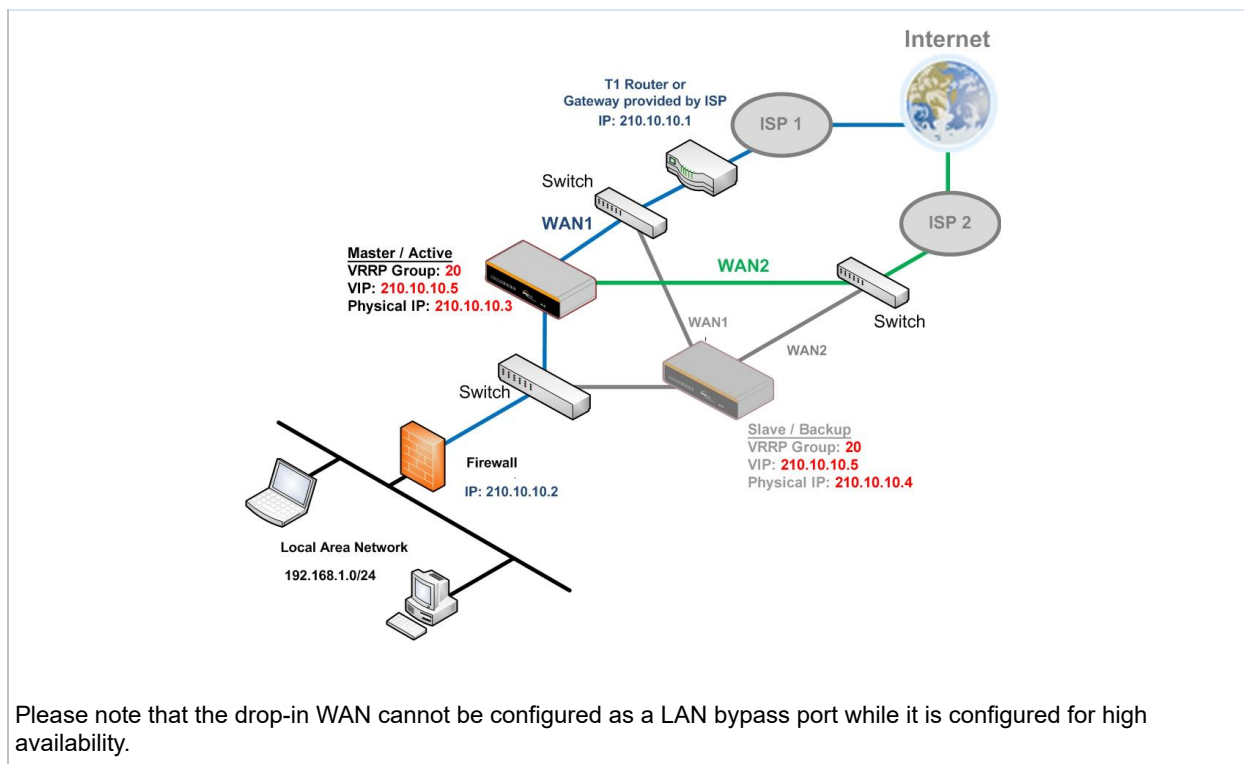
<b>LAN Administration IP</b>	This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN.
<b>Subnet Mask</b>	This setting specifies the subnet mask of the LAN.

### 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.



### 12.16.2 Certificate Manager

Certificate Manager		
VPN Certificate	No Certificate	<a href="#">Assign</a>
Web Admin SSL Certificate	No Certificate	<a href="#">Assign</a>
Captive Portal SSL Certificate	No Certificate	<a href="#">Assign</a>

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.

### 12.16.3 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	
<b>SMTP Forwarding</b>	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 <b>Enable</b> .
<b>Web Proxy Forwarding</b>	When this option is enabled, all outgoing connections destined for the proxy server specified in <b>Web Proxy Interception Settings</b> 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 <b>Enable</b> .
<b>DNS Forwarding</b>	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.
<b>Custom Service Forwarding</b>	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.

## 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 16.1**).

## 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"/>
<small>(Current settings in users' browser)</small>			
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.

### 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.

### 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.

## 12.16.4 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	
<b>SIP</b>	<p>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 correctly in NAT mode. Such passthrough support is always enabled and there are two modes for selection: <b>Standard Mode</b> and <b>Compatibility Mode</b>.</p> <p>If your SIP server's signal port number is non-standard, you can check the box <b>Define custom signal ports</b> and input the port numbers to the text boxes.</p>
<b>H.323</b>	<p>With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and passthrough the Balance.</p>
<b>FTP</b>	<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 <b>Define custom control ports</b> and enter the port numbers in the text boxes.</p>
<b>TFTP</b>	<p>The Peplink Balance monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select <b>Enable</b> if you want to enable TFTP passthrough support.</p>
<b>IPsec NAT-T</b>	<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 <b>Define custom ports</b>. If the VPN contains IPsec site-to-site VPN traffic, check <b>Route IPsec Site-to-Site VPN</b> and choose the WAN connection to route the traffic to.</p>

## 13 AP Tab

### 13.1 AP

#### 13.1.1 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 gray; height: 100px; width: 100%;"></div> <p>(One serial number per line)</p>

AP Controller	
<b>AP Management</b>	<p>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, <b>CAPWAP Access Controller addresses</b> (field 138), will be added to the DHCP server. A local DNS record, <b>AP Controller</b>, will be added to the local DNS proxy.</p>
<b>Support Remote AP</b>	<p>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.</p> <p>The DHCP server and/or local DNS server of the remote AP's network should be configured in the <b>DNS Proxy Settings</b> menu under <b>Network&gt;LAN</b>. The procedure is as follows:</p> <ol style="list-style-type: none"> <li>1. Define an extended DHCP option, <b>CAPWAP Access Controller addresses</b> (field 138), in the DHCP server, where the values are the AP controller's public IP addresses; and/or</li> <li>2. Create a local DNS record for the AP controller with a value corresponding to the AP controller's public IP address.</li> </ol>
<b>Permitted AP</b>	<p>Access points to manage can be specified here. If <b>Any</b> is selected, the AP controller will manage any AP that reports to it. If <b>Approved List</b> is selected, only APs with serial numbers listed in the provided text box will be managed.</p>

### 13.1.2 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	
<a href="#">New SSID</a>		


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

SSID Settings	
SSID	PEPLINK_DDCCD
Enable	Always on ▾
VLAN ID	Untagged LAN ▾
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Multicast Filter	<input type="checkbox"/>
Multicast Rate	MCS0/6M ▾
IGMP Snooping	<input type="checkbox"/>
Layer 2 Isolation	<input type="checkbox"/>
Maximum number of clients	2.4 GHz: <input type="text" value="0"/> 5 GHz: <input type="text" value="0"/> (0: Unlimited)
Band Steering	Disable ▾

SSID Settings	
<b>SSID</b>	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
<b>Enable</b>	Choose an operating schedule for this SSID. Define schedules under <b>System &gt; Schedule</b>
<b>VLAN ID</b>	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 <b>0</b> , which means VLAN tagging is disabled (instead of tagged with zero).
<b>Broadcast SSID</b>	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. <b>Broadcast SSID</b> is enabled by default.
<b>Data Rate <sup>A</sup></b>	Select <b>Auto</b> to allow the Peplink Balance to set the data rate automatically, or select <b>Fixed</b> and choose a rate from the displayed drop-down menu.
<b>Multicast Filter<sup>A</sup></b>	This setting enables the filtering of multicast network traffic to the wireless SSID.
<b>Multicast Rate<sup>A</sup></b>	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected <b>Protocol</b> and <b>Channel Bonding</b> settings will affect the rate options and values available here.

<b>IGMP Snooping</b> <sup>A</sup>	To allow the Peplink Balance to listen to internet group management protocol (IGMP) network traffic, select this option.
<b>DHCP Option 82</b> <sup>A</sup>	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.
<b>Network Priority (QoS)</b> <sup>A</sup>	Select from <b>Gold</b> , <b>Silver</b> , and <b>Bronze</b> to control the QoS priority of this wireless network's traffic.
<b>Layer 2 Isolation</b> <sup>A</sup>	<b>Layer 2</b> 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.
<b>Maximum Number of Clients</b>	Enter the maximum number of clients on the 2.4Ghz channel and on the 5Ghz channel.
<b>Band Steering</b> <sup>A</sup>	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 <b>Enforce</b> . To cause the Peplink Balance to preferentially choose steering, select <b>Prefer</b> . The default for this setting is <b>Disable</b> .

<sup>A</sup> - 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"/> 
	<input checked="" type="checkbox"/> Hide Characters

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

Access Control	
Restricted Mode	None

Access Control	
<b>Restricted Mode</b>	The settings allow administrator to control access using Mac address filtering. Available options are <b>None</b> , <b>Deny all except listed</b> , <b>Accept all except listed</b> , and <b>RADIUS MAC Authentication</b> .

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

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	
<b>Block All Private IP</b>	Check this box to deny all connection attempts by private IP addresses.
<b>Custom Subnet</b>	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"/> .
<b>Block Exception</b>	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"/> .
<b>Block PepVPN</b>	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	
<b>Upstream Limit</b>	Enter a value in kbps to limit the wireless network's upstream bandwidth. Enter <b>0</b> to allow unlimited upstream bandwidth.
<b>Downstream Limit</b>	Enter a value in kbps to limit the wireless network's downstream bandwidth. Enter <b>0</b> to allow unlimited downstream bandwidth.

<b>Client Upstream Limit</b>	Enter a value in kpbs to limit connected clients' upstream bandwidth. Enter <b>0</b> to allow unlimited upstream bandwidth.
<b>Client Downstream Limit</b>	Enter a value in kpbs to limit connected clients' downstream bandwidth. Enter <b>0</b> to allow unlimited downstream bandwidth.
<b>Max Number of Clients</b>	Enter the maximum number of clients that can simultaneously connect to the wireless network or enter <b>0</b> to allow an unlimited number of connections.

Firewall Settings	
<b>Firewall Mode</b>	Choose Flexible – <b>Allow all except...</b> or <b>Lockdown – Block all except...</b> to turn on the firewall. Once you save changes, the <b>New Rule</b> 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 <b>X</b> button. To turn off the firewall, select <b>Disable</b> .

Firewall Rule	
<b>Name</b>	Enter a descriptive name for the firewall rule in this field.
<b>Type</b>	Choose <b>Port</b> , <b>Domain</b> , <b>IP Address</b> , or <b>MAC Address</b> to allow or deny traffic from any of those identifiers. Depending on the option chosen, the following fields will vary.
<b>Protocol / Port</b>	Choose <b>TCP</b> or <b>UDP</b> from the <b>Protocol</b> drop-down menu to allow or deny traffic using either of those protocols. From the <b>Port</b> drop-down menu, choose <b>Any Port</b> to allow or deny TCP or UDP traffic on any port. Choose <b>Single Port</b> 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 <b>Port Range</b> and enter a range of ports in the provided fields to allow or deny TCP or UDP traffic from the specified port range.
<b>IP Address / Subnet Mask</b>	If you have chosen <b>IP Address</b> as your firewall rule type, enter the IP address and subnet mask identifying the subnet to allow or deny.
<b>MAC Address</b>	If you have chosen <b>MAC Address</b> as your firewall rule type, enter the MAC address identifying the machine to allow or deny.

### 13.1.3 Settings

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


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

**Important Note**

Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.

	2.4 GHz	5 GHz
Protocol	802.11ng	802.11n/ac
Channel Width	20 MHz	Auto
Channel	Auto <input type="button" value="Edit"/> Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto <input type="button" value="Edit"/> Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Auto Channel Update	Daily at 03:00 <input checked="" type="checkbox"/> Wait until no active client associated	Daily at 03:00 <input checked="" type="checkbox"/> Wait until no active client associated
Output Power	Fixed: Max <input type="checkbox"/> Boost	Fixed: Max <input type="checkbox"/> Boost
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)	0 (0: Unlimited)

AP Settings (part 2)	
<b>Protocol</b>	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are <b>802.11ng</b> and <b>802.11na</b> . By default, <b>802.11ng</b> is selected.
<b>Channel Width</b>	Available options are <b>20 MHz</b> , <b>40 MHz</b> , and <b>Auto (20/40 MHz)</b> . Default is <b>Auto (20/40 MHz)</b> , which allows both widths to be used simultaneously.
<b>Channel</b>	This option allows you to select which 802.11 RF channel will be utilized. <b>Channel 1 (2.412 GHz)</b> is selected by default.
<b>Auto Channel Update</b>	Indicate the time of day at which update automatic channel selection.
<b>Output Power</b>	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – <b>Max</b> , <b>High</b> , <b>Mid</b> , and <b>Low</b> . The actual output power will be bound by the regulatory limits of the selected country.
<b>Client Signal Strength Threshold</b>	This setting determines the maximum strength at which the Wi-Fi AP can broadcast
<b>Maximum number of clients</b>	This setting determines the maximum number of clients that can connect to this Wi-Fi frequency.

Advanced Wi-Fi AP settings can be displayed by clicking the  on the top right-hand corner of the **Wi-Fi AP Settings** section, which can be found at **AP>Settings**. Other models will display a separate section called **Wi-Fi AP Advanced Settings**, which can be found at **Advanced>Wi-Fi Settings**.

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

Advanced AP Settings	
<b>Management VLAN ID</b>	<p>This field specifies the VLAN ID to tag to management traffic, such as communication traffic between the AP and the AP Controller. The value is zero by default, which means that no VLAN tagging will be applied.</p> <p>NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller.</p>
<b>Operating Schedule</b>	<p>Choose from the schedules that you have defined in System&gt;Schedule. Select the schedule for the integrated AP to follow from the drop-down menu.</p>
<b>Beacon Rate</b> <sup>A</sup>	<p>This option is for setting the transmit bit rate for sending a beacon. By default, <b>1Mbps</b> is selected.</p>
<b>Beacon Interval</b> <sup>A</sup>	<p>This option is for setting the time interval between each beacon. By default, <b>100ms</b> is selected.</p>
<b>DTIM</b> <sup>A</sup>	<p>This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to <b>1 ms</b>.</p>
<b>RTS Threshold</b> <sup>A</sup>	<p>The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500.</p>
<b>Fragmentation Threshold</b> <sup>A</sup>	<p>This setting determines the maximum size of a packet before it gets fragmented into multiple pieces.</p>
<b>Distance / Time Converter</b>	<p>Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout.</p>
<b>Slot Time</b> <sup>A</sup>	<p>This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to <b>9 µs</b>.</p>



<b>ACK Timeout</b> <sup>A</sup>	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to <b>48 μs</b> .
---------------------------------	--

<b>Frame Aggregation</b> <sup>A</sup>	This option allows you to enable frame aggregation to increase transmission throughput.
---------------------------------------	---

<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner to activate.

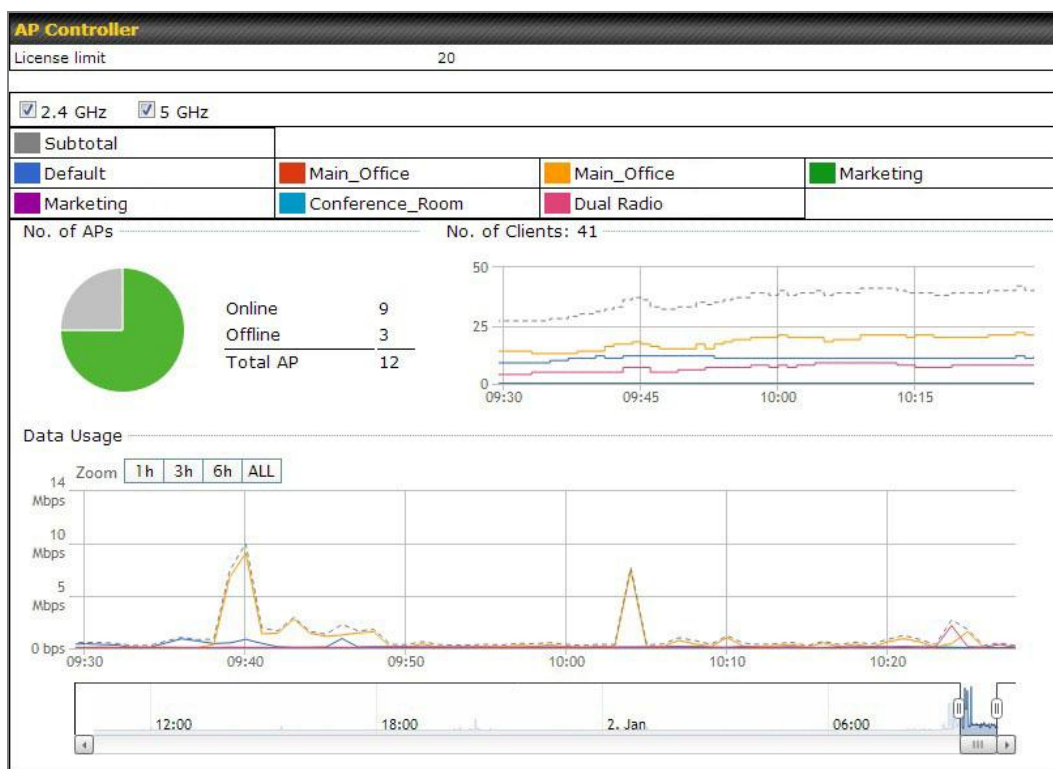
Web Administration Settings (on External AP)	
Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	<input type="text" value="443"/>
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username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

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

## 13.2 AP Controller Status

### 13.2.1 Info

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



AP Controller	
<b>License Limit</b>	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.
<b>Frequency</b>	Underneath, there are two check boxes labeled <b>2.4 Ghz</b> and <b>5 Ghz</b> . 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.
<b>SSID</b>	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.
<b>No. of APs</b>	This pie chart and table indicates how many APs are online and how many are offline.
<b>No. of Clients</b>	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.
<b>Data Usage</b>	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 <b>Zoom</b> to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

### 13.2.2 Access Points (Usage)

A detailed breakdown of data usage for each AP is available at **AP> Access Point**.

**Search Filter**

AP Name / Serial Number / SSID	All <input type="text"/>
	<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"/> JEDD-ANIP-8000	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2 None	✓ -

Usage

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

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


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

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

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

**Client List** Close


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:fac: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

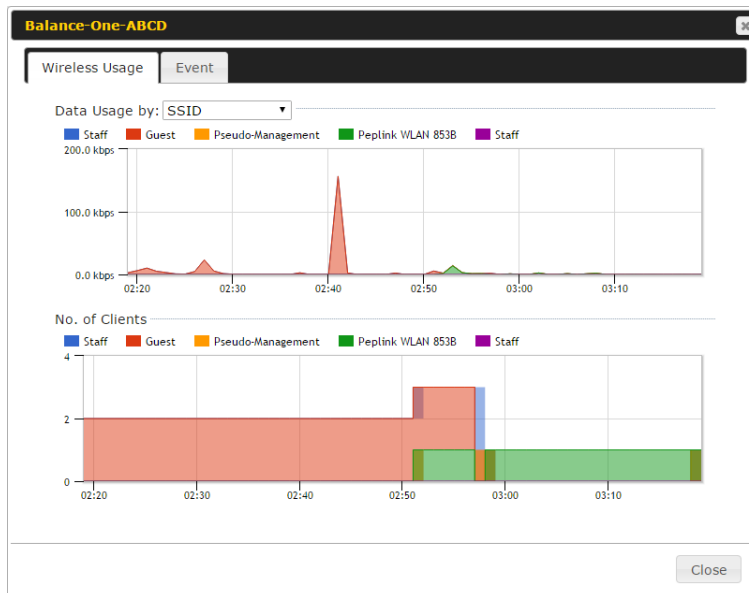
Click the  icon to configure each client

**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 ▼

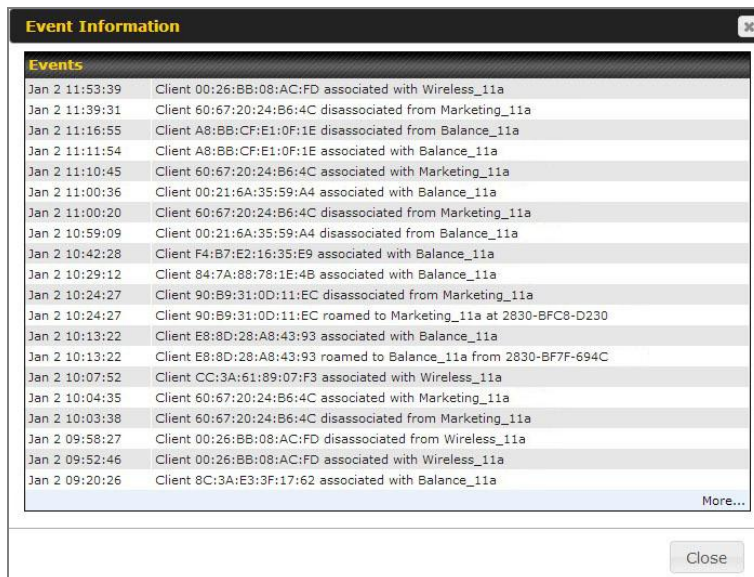
For easier network management, you can give each client a name and designate its location. You can also designate which firmware pack (if any) this client will follow, as well as the channels on which the client will broadcast.

Click the  icon to see a graph displaying usage:



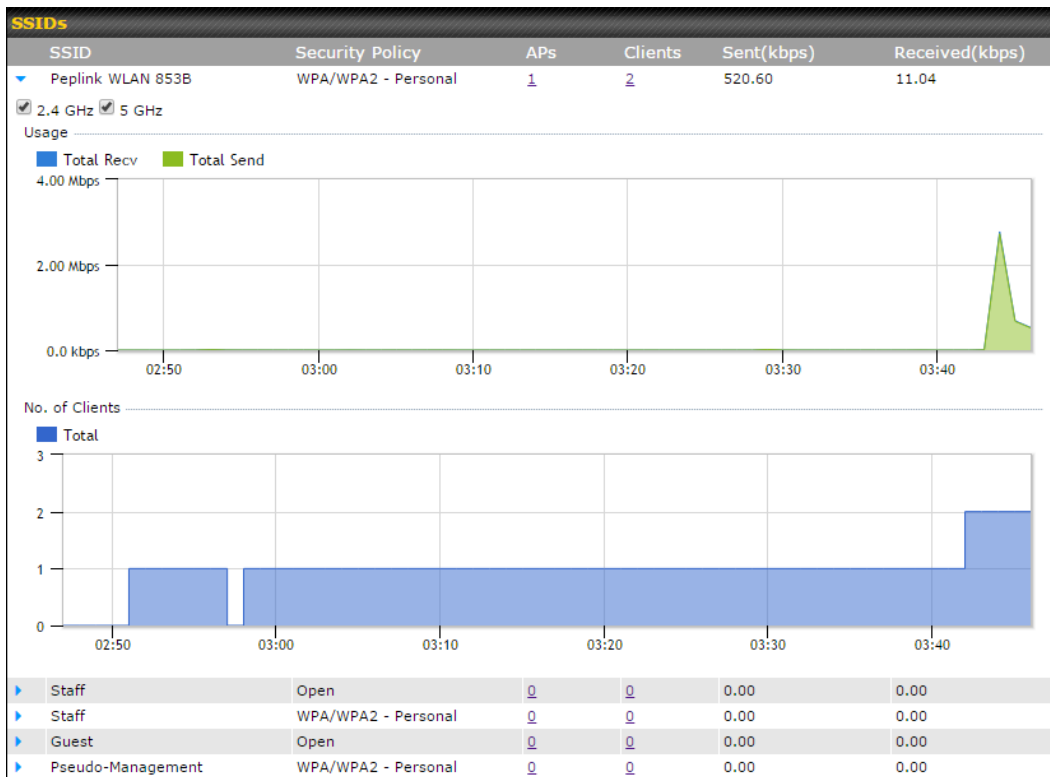
Click any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can

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:



### 13.2.3 Wireless 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.

### 13.2.4 Wireless Client

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

**Search Filter**

Client MAC / SSID / AP Serial Number

Maximum Result (1-256)

Search Result

---

**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:

**Client C0:EE:FB:20:13:36**
✕

**Information**

Status	Associated
Access Point	1111-2222-3333
SSID	Peplink WLAN 853B
IP Address	192.168.1.34
Duration	00:27:31
Usage (Upload / Download)	141.28 MB / 4.35 MB
RSSI	-48
Rate (Upload / Download)	150M / 48M
Type	802.11na

■ Download
 ■ Upload

SSID	AP	From	To	Upload	Download
Peplink WLAN 853B	192C-1835-642F	Nov 23 03:43:04	-	141.28 MB	4.35 MB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:58:36	Nov 23 03:47:52	173.7 KB	94.2 KB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:52:15	Nov 23 02:58:15	105.9 KB	62.5 KB

Close

### 13.2.5 Nearby Device

A listing of near devices can be accessed by navigating to **AP > Controller Status > Nearby Device**.



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	

### Nearby 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.

### 13.2.6 Event Log

You can access the AP Controller Event log by navigating to **AP > Controller Status > Event Log**.

Filter	
Search key	<input type="text" value="Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name"/>
Time	From <input type="text" value=""/> hh:mm to <input type="text" value=""/> hh:mm
Alerts only	<input type="checkbox"/>
<input type="button" value="Search"/>	

Events		<a href="#">View Alerts</a>
Jan 2 11:01:11	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:11:6A:35:79:A4 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 60:67:20:24:06:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:11:6A:35:79:A4 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:2D:3C:48:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3C:48:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 22:BF:48:89:78:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:25:2B:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 9C:24:0B:10:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	

[More...](#)

**Events**

This event log displays all activity on your AP network, down to the client level. Use to filter box to search by MAC address, SSID, AP Serial Number, or AP Profile name. Click **View Alerts** to see only alerts, and click the **More...** link for additional records.

### 13.3 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 **Check for Updates** to download new packs or you can press **Manual Upload** to manually upload a firmware pack. Press **Default...** to define which firmware pack is default.

# 14 System Tab

## 14.1 System

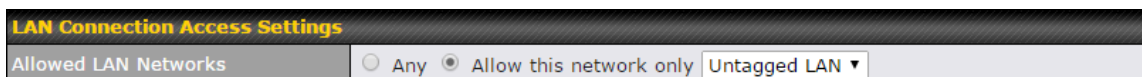
### 14.1.1 Admin Security

Admin Settings	
Router Name	1818-1818-1818 <small>hostname: 1818-1818-1818</small>
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	<input type="text"/> Port <input type="text"/> <b>Default</b>
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Auth Timeout	3 seconds
Accounting Server	<input type="text"/> Port <input type="text"/> <b>Default</b>
Accounting Server Secret	<input type="text"/> <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 <b>Default</b>
CLI SSH Access	LAN/WAN
Security	HTTP
Web Admin Port	80 <b>Default</b>
Web Admin Access	LAN/WAN

Admin Settings	
<b>Router Name</b>	This field allows you to define a name for this Peplink Balance unit. By default, <b>Router Name</b> is set as <b>Balance_XXXX</b> , where XXXX refers to the last 4 digits of the serial number of that balance unit.
<b>Admin User</b>	<b>Admin User Name</b> is set as <b>admin</b> by default, but can be changed, if desired.

<b>Name</b>	
<b>Admin Password</b>	This field allows you to specify a new administrator password.
<b>Confirm Admin Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Read-only User Name</b>	Read-only User Name is set as <b>user</b> by default, but can be changed, if desired.
<b>User Password</b>	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
<b>Confirm User Password</b>	This field allows you to verify and confirm the new user password.
<b>Front Panel Passcode</b>	To require a 4-digit passcode to access front panel controls, check this box and then select the code from the drop-down menus.
<b>Web Session Timeout</b>	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 <b>4 hours</b> .
<b>Authentication by RADIUS</b>	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.
<b>Auth Protocol</b>	This specifies the authentication protocol used. Available options are <b>MS-CHAP v2</b> and <b>PAP</b> .
<b>Auth Server</b>	This specifies the access address and port of the external RADIUS server.
<b>Auth Server Secret</b>	This field is for entering the secret key for accessing the RADIUS server.
<b>Auth Timeout</b>	This option specifies the time value for authentication timeout.
<b>Accounting Server</b>	This specifies the access address and port of the external accounting server.
<b>Accounting Server Secret</b>	This field is for entering the secret key for accessing the accounting server.
<b>Network Connection</b>	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.

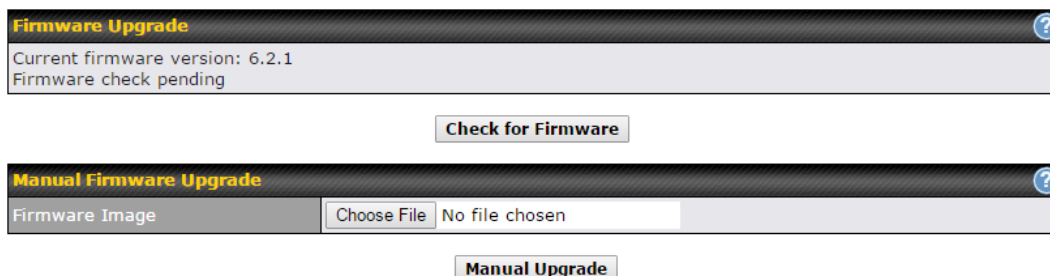
<b>Restricted Admin Access</b>	Check this box to restrict management to administrators connected to the management port.
<b>CLI SSH &amp; Console</b>	The CLI (command line interface) can be accessed via SSH. It can also be accessed from the serial console port on some Peplink Balance models. This field enables CLI support. For additional information regarding CLI, please refer to <b>Section 22.5</b> .
<b>CLI SSH Port</b>	This field determines the port on which clients can access CLI SSH.
<b>CLI SSH Access</b>	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
<b>Security</b>	<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"> <li>• HTTP</li> <li>• HTTPS</li> <li>• HTTP/HTTPS</li> </ul>
<b>Web Admin Port</b>	This field is for specifying the port number on which the web admin interface can be accessed.
<b>Web Admin Access</b>	<p>This option is for specifying the network interfaces through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> <li>• LAN only</li> <li>• LAN/WAN</li> </ul> <p>If LAN/WAN is chosen, the <b>WAN Connection Access Settings</b> form will be displayed.</p>



LAN Connection Access Settings	
<b>Allowed LAN Networks</b>	This field allows you to permit only specific networks or VLANs to access the Web UI.

### 14.1.2 Firmware

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



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

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

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

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

### Firmware Upgrade Status

- Status LED Information during firmware upgrade:
- OFF – Firmware upgrade in progress (DO NOT disconnect power.)
  - Red – Unit is rebooting
  - Green – Firmware upgrade successfully completed

### Important Note

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

#### 14.1.3 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"/>

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

#### 14.1.4 Schedule

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

Schedule			
Enabled			<input type="button" value="✎"/>
Name	Time	Used by	
Weekdays Only	Weekdays only	-	<input type="button" value="✕"/>
<input type="button" value="New Schedule"/>			

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

**Edit schedule profile**
✕

**Schedule Settings**

<b>Enable</b>	<input checked="" type="checkbox"/> <small>The schedule function of those associated features will be lost if profile is disabled.</small>
<b>Name</b>	<input type="text" value="Weekdays Only"/>
<b>Schedule</b>	<input type="text" value="Weekdays only"/>
<b>Used by</b>	<small>You may go to supported feature settings page and set this profile as scheduler.</small>

**Schedule Map**

	Midnight				4am				8am				Noon				4pm				8pm							
Sunday	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Monday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Thursday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Saturday	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x



Edit Schedule Profile	
<b>Enabling</b>	Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.
<b>Name</b>	Enter your desired name for this particular schedule profile.
<b>Schedule</b>	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.
<b>Schedule Map</b>	Click on the desired times to enable features at that time period. You can hold your mouse for faster entry.

### 14.1.5 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 <span style="border: 1px solid #ccc; padding: 2px;">Default</span>
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

Test Email Notification
Save

Email Notification Settings	
<b>Email Notification</b>	This setting specifies whether or not to enable email notification. If <b>Enable</b> is checked, the Peplink Balance will send email messages to system administrators when the WAN status changes or when new firmware is available. If <b>Enable</b> is not checked, email notification is disabled and the Peplink Balance will not send email messages.
<b>SMTP Server</b>	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check <b>Require authentication</b> .

<b>SSL Encryption</b>	Check the box to enable SMTPS. When the box is checked, <b>SMTP Port</b> will be changed to <b>465</b> automatically.
<b>SMTP Port</b>	This field is for specifying the SMTP port number. By default, this is set to <b>25</b> ; when <b>SSL Encryption</b> is checked, the default port number will be set to <b>465</b> . You may customize the port number by editing this field. Click <b>Default</b> to restore the number to its default setting.
<b>SMTP User Name / Password</b>	This setting specifies the SMTP username and password while sending email. These options are shown only if <b>Require authentication</b> is checked in the <b>SMTP Server</b> setting.
<b>Confirm SMTP Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Sender's Email Address</b>	This setting specifies the email address which the Peplink Balance will use to send its reports.
<b>Recipient's Email Address</b>	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

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
```

### 14.1.6 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	
<b>Remote Syslog</b>	This setting specifies whether or not to log events at the specified remote syslog server.
<b>Remote Syslog Host</b>	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.
<b>Push Events</b>	For more information on the Router Utility, go to: <a href="http://www.peplink.com/products/router-utility">www.peplink.com/products/router-utility</a>

### 14.1.7 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_0D84
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	
<b>SNMP Device Name</b>	This field shows the router name defined at <b>System&gt;Admin Security</b> .
<b>SNMP Port</b>	This option specifies the port which SNMP will use. The default port is <b>161</b> .
<b>SNMPv1</b>	This option allows you to enable SNMP version 1.
<b>SNMPv2</b>	This option allows you to enable SNMP version 2.
<b>SNMPv3</b>	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)". There are "Save" and "Cancel" buttons at the bottom right.

SNMP Community Settings	
<b>Community Name</b>	This setting specifies the SNMP community name.
<b>Allowed Source Subnet Address</b>	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 text field with "password", and "Privacy" with a dropdown menu set to "DES" and a text field with "privacypassword". There are "Save" and "Cancel" buttons at the bottom right.

SNMPv3 User Settings	
<b>User Name</b>	This setting specifies a user name to be used in SNMPv3.
<b>Authentication Protocol</b>	This setting specifies via a drop-down menu one of the following valid authentication protocols: <ul style="list-style-type: none"> <li>• NONE</li> </ul>

	<ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA</li> </ul> <p>When MD5 or SHA is selected, an entry field will appear for the password.</p>
<b>Privacy Protocol</b>	<p>This setting specifies via a drop-down menu one of the following valid privacy protocols:</p> <ul style="list-style-type: none"> <li>• NONE</li> <li>• DES</li> </ul> <p>When DES is selected, an entry field will appear for the password.</p>

### 14.1.8 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.

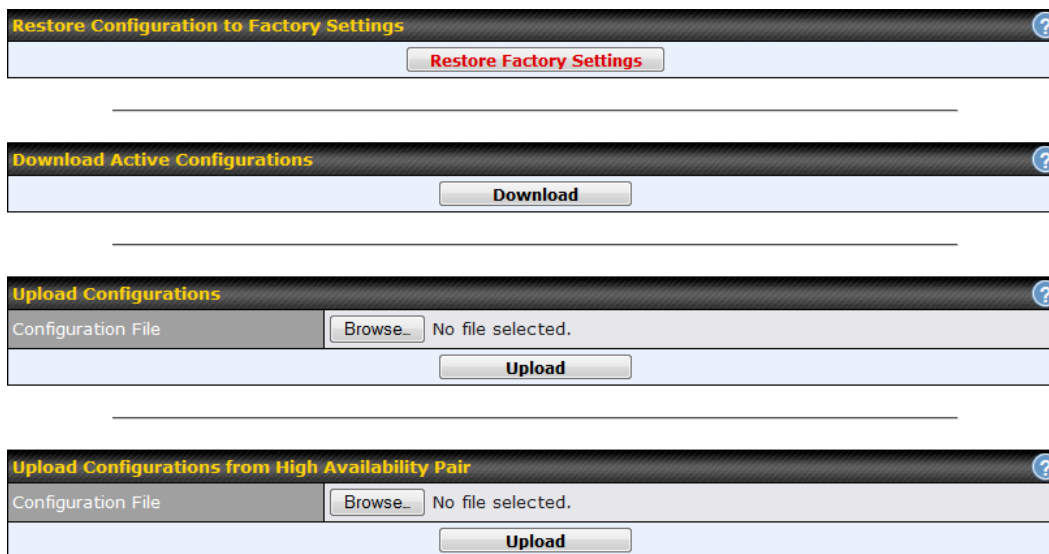
When this check box is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

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.

### 14.1.9 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**.



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

**Availability Pair** counterpart.

### 14.1.10 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**.

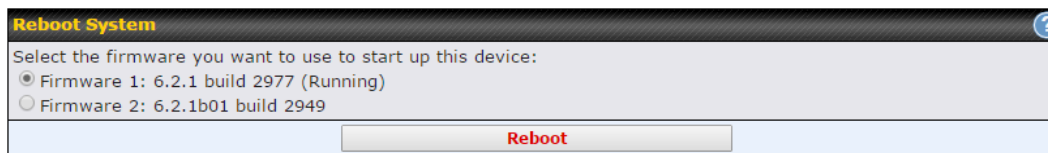


The screenshot shows a form titled "Feature Activation". It contains a single input field labeled "Activation Key" which is currently empty.

### 14.1.11 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 screenshot shows a form titled "Reboot System" with a help icon in the top right corner. The form contains the following text and options:

Select the firmware you want to use to start up this device:

- Firmware 1: 6.2.1 build 2977 (Running)
- Firmware 2: 6.2.1b01 build 2949

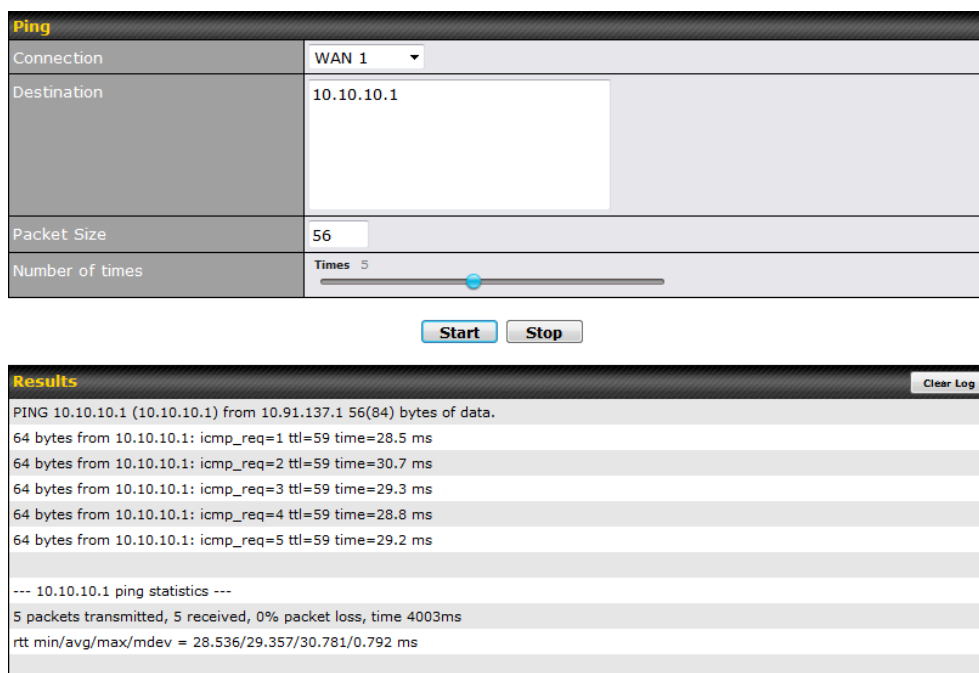
At the bottom of the form is a button labeled "Reboot".



## 14.2 Tools

### 14.3 Ping

The ping test tool sends pings through a specific 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		Clear Log
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.

### 14.4 Traceroute

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

---

**Results**

```

1 10.0.0.0/24 (10.0.0.0) 0.000 ms
2 10.0.0.1 (10.0.0.1) 0.000 ms
3 10.0.0.2 (10.0.0.2) 0.000 ms
4 10.0.0.3 (10.0.0.3) 0.000 ms
5 10.0.0.4 (10.0.0.4) 0.000 ms
6 10.0.0.5 (10.0.0.5) 0.000 ms
7 10.0.0.6 (10.0.0.6) 0.000 ms
8 10.0.0.7 (10.0.0.7) 0.000 ms
9 10.0.0.8 (10.0.0.8) 0.000 ms
10 10.0.0.9 (10.0.0.9) 0.000 ms
11 10.0.0.10 (10.0.0.10) 0.000 ms
12 10.0.0.11 (10.0.0.11) 0.000 ms
13 10.0.0.12 (10.0.0.12) 0.000 ms
14 10.0.0.13 (10.0.0.13) 0.000 ms
15 10.0.0.14 (10.0.0.14) 0.000 ms
16 10.0.0.15 (10.0.0.15) 0.000 ms
17 10.0.0.16 (10.0.0.16) 0.000 ms
18 10.0.0.17 (10.0.0.17) 0.000 ms
19 10.0.0.18 (10.0.0.18) 0.000 ms
20 10.0.0.19 (10.0.0.19) 0.000 ms
21 10.0.0.20 (10.0.0.20) 0.000 ms
22 10.0.0.21 (10.0.0.21) 0.000 ms
23 10.0.0.22 (10.0.0.22) 0.000 ms
24 10.0.0.23 (10.0.0.23) 0.000 ms
25 10.0.0.24 (10.0.0.24) 0.000 ms
26 10.0.0.25 (10.0.0.25) 0.000 ms
27 10.0.0.26 (10.0.0.26) 0.000 ms
28 10.0.0.27 (10.0.0.27) 0.000 ms
29 10.0.0.28 (10.0.0.28) 0.000 ms
30 10.0.0.29 (10.0.0.29) 0.000 ms
31 10.0.0.30 (10.0.0.30) 0.000 ms
32 10.0.0.31 (10.0.0.31) 0.000 ms
33 10.0.0.32 (10.0.0.32) 0.000 ms
34 10.0.0.33 (10.0.0.33) 0.000 ms
35 10.0.0.34 (10.0.0.34) 0.000 ms
36 10.0.0.35 (10.0.0.35) 0.000 ms
37 10.0.0.36 (10.0.0.36) 0.000 ms
38 10.0.0.37 (10.0.0.37) 0.000 ms
39 10.0.0.38 (10.0.0.38) 0.000 ms
40 10.0.0.39 (10.0.0.39) 0.000 ms
41 10.0.0.40 (10.0.0.40) 0.000 ms
42 10.0.0.41 (10.0.0.41) 0.000 ms
43 10.0.0.42 (10.0.0.42) 0.000 ms
44 10.0.0.43 (10.0.0.43) 0.000 ms
45 10.0.0.44 (10.0.0.44) 0.000 ms
46 10.0.0.45 (10.0.0.45) 0.000 ms
47 10.0.0.46 (10.0.0.46) 0.000 ms
48 10.0.0.47 (10.0.0.47) 0.000 ms
49 10.0.0.48 (10.0.0.48) 0.000 ms
50 10.0.0.49 (10.0.0.49) 0.000 ms
51 10.0.0.50 (10.0.0.50) 0.000 ms
52 10.0.0.51 (10.0.0.51) 0.000 ms
53 10.0.0.52 (10.0.0.52) 0.000 ms
54 10.0.0.53 (10.0.0.53) 0.000 ms
55 10.0.0.54 (10.0.0.54) 0.000 ms
56 10.0.0.55 (10.0.0.55) 0.000 ms
57 10.0.0.56 (10.0.0.56) 0.000 ms
58 10.0.0.57 (10.0.0.57) 0.000 ms
59 10.0.0.58 (10.0.0.58) 0.000 ms
60 10.0.0.59 (10.0.0.59) 0.000 ms
61 10.0.0.60 (10.0.0.60) 0.000 ms
62 10.0.0.61 (10.0.0.61) 0.000 ms
63 10.0.0.62 (10.0.0.62) 0.000 ms
64 10.0.0.63 (10.0.0.63) 0.000 ms
65 10.0.0.64 (10.0.0.64) 0.000 ms
66 10.0.0.65 (10.0.0.65) 0.000 ms
67 10.0.0.66 (10.0.0.66) 0.000 ms
68 10.0.0.67 (10.0.0.67) 0.000 ms
69 10.0.0.68 (10.0.0.68) 0.000 ms
70 10.0.0.69 (10.0.0.69) 0.000 ms
71 10.0.0.70 (10.0.0.70) 0.000 ms
72 10.0.0.71 (10.0.0.71) 0.000 ms
73 10.0.0.72 (10.0.0.72) 0.000 ms
74 10.0.0.73 (10.0.0.73) 0.000 ms
75 10.0.0.74 (10.0.0.74) 0.000 ms
76 10.0.0.75 (10.0.0.75) 0.000 ms
77 10.0.0.76 (10.0.0.76) 0.000 ms
78 10.0.0.77 (10.0.0.77) 0.000 ms
79 10.0.0.78 (10.0.0.78) 0.000 ms
80 10.0.0.79 (10.0.0.79) 0.000 ms
81 10.0.0.80 (10.0.0.80) 0.000 ms
82 10.0.0.81 (10.0.0.81) 0.000 ms
83 10.0.0.82 (10.0.0.82) 0.000 ms
84 10.0.0.83 (10.0.0.83) 0.000 ms
85 10.0.0.84 (10.0.0.84) 0.000 ms
86 10.0.0.85 (10.0.0.85) 0.000 ms
87 10.0.0.86 (10.0.0.86) 0.000 ms
88 10.0.0.87 (10.0.0.87) 0.000 ms
89 10.0.0.88 (10.0.0.88) 0.000 ms
90 10.0.0.89 (10.0.0.89) 0.000 ms
91 10.0.0.90 (10.0.0.90) 0.000 ms
92 10.0.0.91 (10.0.0.91) 0.000 ms
93 10.0.0.92 (10.0.0.92) 0.000 ms
94 10.0.0.93 (10.0.0.93) 0.000 ms
95 10.0.0.94 (10.0.0.94) 0.000 ms
96 10.0.0.95 (10.0.0.95) 0.000 ms
97 10.0.0.96 (10.0.0.96) 0.000 ms
98 10.0.0.97 (10.0.0.97) 0.000 ms
99 10.0.0.98 (10.0.0.98) 0.000 ms
100 10.0.0.99 (10.0.0.99) 0.000 ms
101 10.0.0.100 (10.0.0.100) 0.000 ms
    
```

**Tip**

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

### 14.5 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**

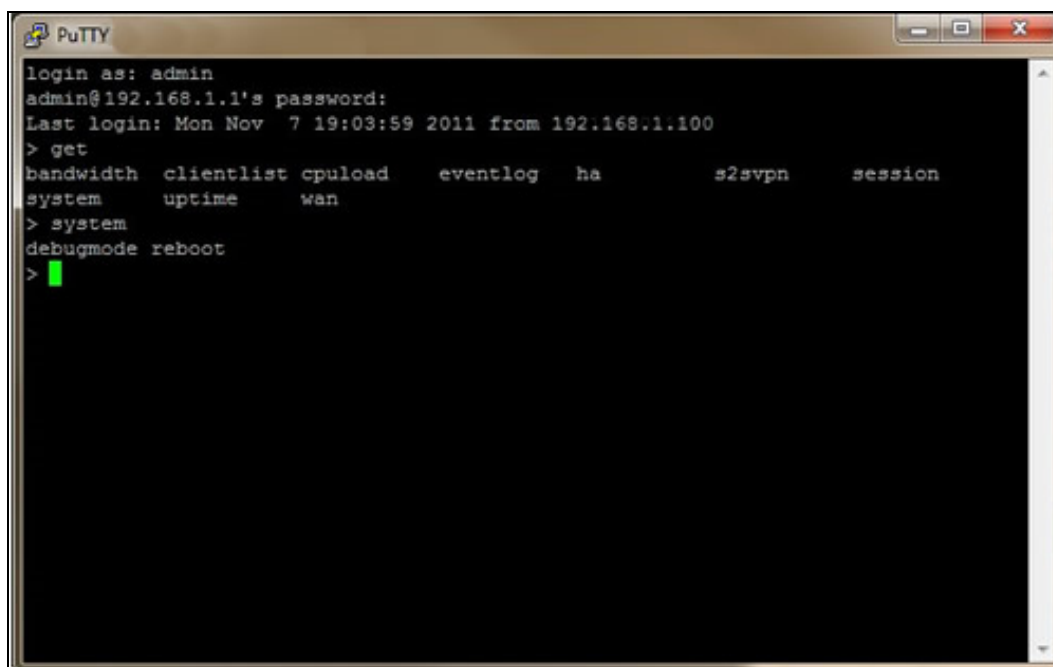
Wake-on-LAN Target	Surf_SOHO (00:90:90:90:90:90)	<input type="button" value="Send"/>
--------------------	-------------------------------	-------------------------------------

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

### 14.6 CLI (Command Line) 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*.



```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist  cpuload    eventlog  ha        s2svpn    session
system    uptime    wan
> system
debugmode  reboot
> █
```

## 15 Status Tab

### 15.1 Status

#### 15.1.1 Device

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

System Information	
Router Name	1818-1818-1818
Model	Peplink Balance 30
Hardware Revision	2
Serial Number	1818-1818-1818
Firmware	6.2.1 build 2977
PepVPN Version	4.0.0
Modem Support Version	1018 ( <a href="#">Modem Support List</a> )
Host Name	1818-1818-1818
Uptime	8 days 1 hour 12 minutes
System Time	Sun Jun 21 07:51:07 WET 2015
Diagnostic Report	<a href="#">Download</a>
Remote Assistance	<a href="#">Turn on</a>

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

System Information	
<b>Router Name</b>	This is the name specified in the <b>Router Name</b> field located at <b>System&gt;Admin Security</b> .
<b>Model</b>	This shows the model name and number of this device.
<b>Hardware Revision</b>	This shows the hardware version of this device.
<b>Serial Number</b>	This shows the serial number of this device.
<b>Firmware</b>	This shows the firmware version this device is currently running.
<b>Uptime</b>	This shows the length of time since the device has been rebooted.
<b>System Time</b>	This shows the current system time.
<b>Diagnostic Report</b>	The <b>Download</b> link is for exporting a diagnostic report file required for system investigation.
<b>Remote Assistance</b>	Click <b>Turn on</b> 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 ( <a href="http://www.peplink.com/contact/">http://www.peplink.com/contact/</a> ), 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 <b>System&gt;Reboot</b> .

### 15.1.2 Active Sessions

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

Service	Inbound Sessions	Outbound Sessions
<a href="#">AIM/ICQ</a>	0	1
<a href="#">Bittorrent</a>	0	32
<a href="#">DNS</a>	0	51
<a href="#">Flash</a>	0	1
<a href="#">HTTPS</a>	0	76
<a href="#">Jabber</a>	0	5
<a href="#">MSN</a>	0	11
<a href="#">NTP</a>	0	4
<a href="#">QQ</a>	0	1
<a href="#">Remote Desktop</a>	0	3
<a href="#">SSH</a>	0	12
<a href="#">SSL</a>	0	64
<a href="#">XMPP</a>	0	4
<a href="#">Yahoo</a>	0	1

Interface	Inbound Sessions	Outbound Sessions
<a href="#">WAN1</a>	0	219
<a href="#">WAN2</a>	0	0
<a href="#">WAN3</a>	0	0
<a href="#">Mobile Internet</a>	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 <input type="text"/> / 255.255.255.255 (/32) <input type="text"/>
Port	Source or Destination <input type="text"/>
Protocol / Service	SSL <input type="text"/>
Interface	<input type="checkbox"/> 1 WAN 1 <input type="checkbox"/> 2 WAN 2 <input type="checkbox"/> 3 WAN 3 <input type="checkbox"/> 4 WAN 4 <input type="checkbox"/> 5 WAN 5 <input type="checkbox"/> 6 WAN 6 <input type="checkbox"/> 7 WAN 7 <input type="checkbox"/> 8 WAN 8 <input type="checkbox"/> 9 WAN 9 <input type="checkbox"/> 10 WAN 10 <input type="checkbox"/> 11 WAN 11 <input type="checkbox"/> 12 WAN 12 <input type="checkbox"/> Mobile Internet <input type="checkbox"/> VPN

**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.

### 15.1.3 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	10:58:58:58:58:58	
192.168.167.11	U64-2-1	0	0	00:50:58:58:58:1A	
192.168.167.12	U64-2-2	0	0	10:58:58:58:58:75	

If the PPTP server SpeedFusion™, or AP controller is enabled, you may see the corresponding connection name listed in the **Name** field.

### 15.1.4 WINS Clients

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. 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.

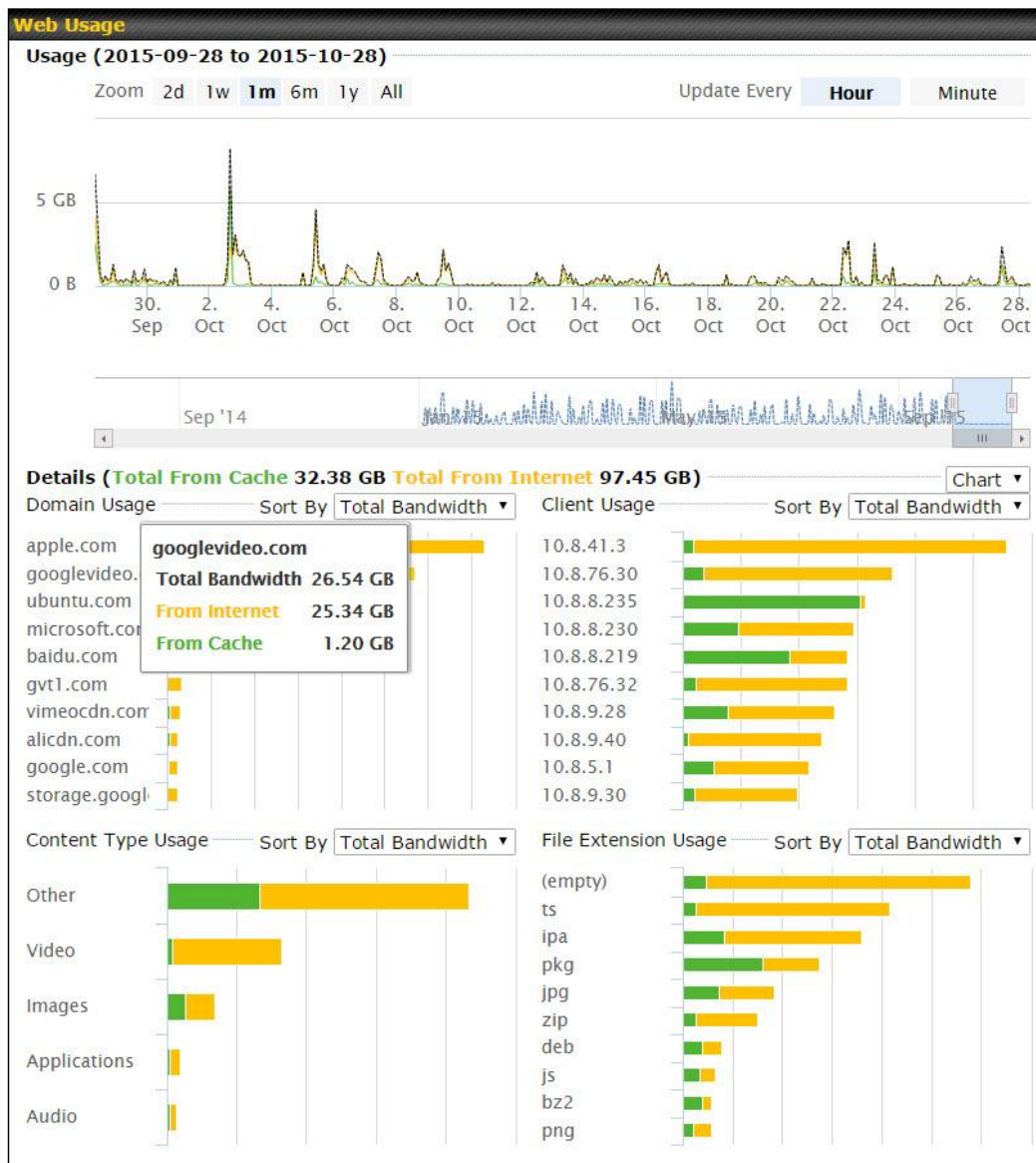
### 15.1.5 OSPF & RIPv2

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

### 15.1.6 MediaFast

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





### 15.1.7 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** Show disconnected profiles

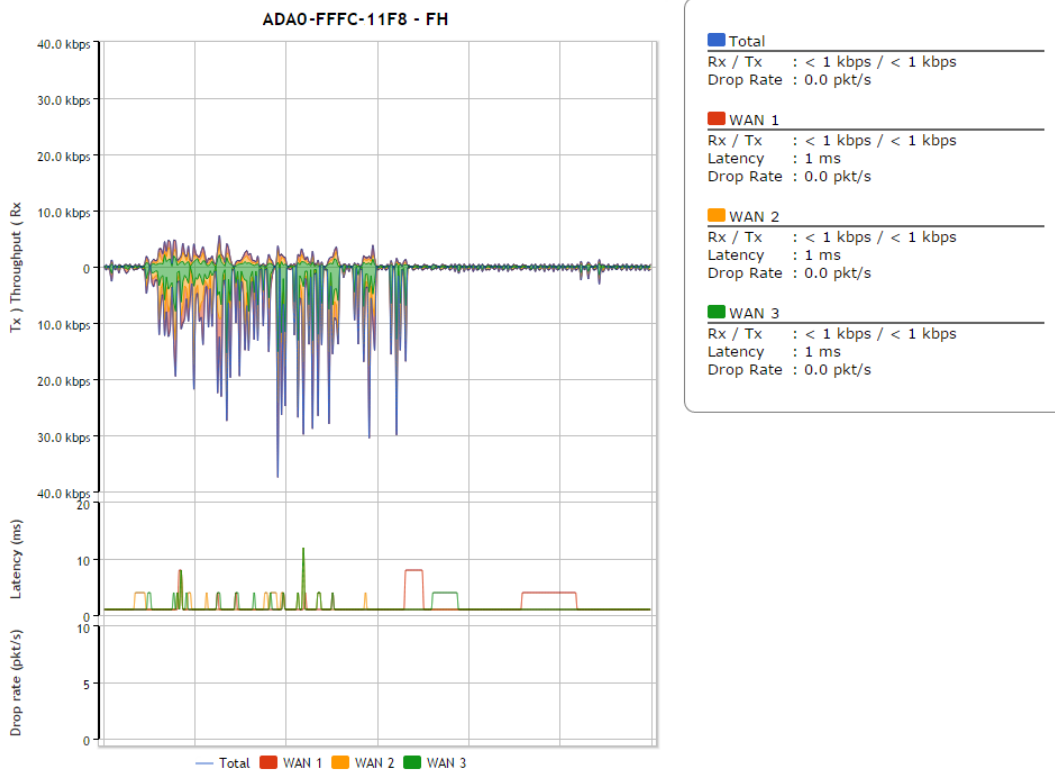
Search


Remote Peer	Profile	Information		
FFFC-FFFC-FFFC	FH	192.168.77.0/24		
3ED2-3ED2-3ED2	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		
FFFC-FFFC-FFFC	FH	192.168.77.0/24		
<ul style="list-style-type: none"> <li>WAN 1</li> <li>WAN 2</li> <li>WAN 3</li> <li>Total</li> </ul>	<ul style="list-style-type: none"> <li>Rx: &lt; 1 kbps</li> <li>Tx: &lt; 1 kbps</li> <li>Rx: &lt; 1 kbps</li> <li>Tx: &lt; 1 kbps</li> <li>Rx: &lt; 1 kbps</li> <li>Tx: &lt; 1 kbps</li> <li>Rx: &lt; 1 kbps</li> <li>Tx: 1.1 kbps</li> </ul>	<ul style="list-style-type: none"> <li>Drop rate: 0.0 pkt/s</li> <li>Latency: 1 ms</li> <li>Drop rate: 0.0 pkt/s</li> <li>Latency: 1 ms</li> <li>Drop rate: 0.0 pkt/s</li> <li>Latency: 1 ms</li> <li>Drop rate: 0.0 pkt/s</li> </ul>		
3ED2-3ED2-3ED2	380-5 - NO NAT	192.168.3.0/24		
<ul style="list-style-type: none"> <li>WAN 1</li> <li>WAN 2</li> <li>WAN 3</li> <li>Total</li> </ul>	<ul style="list-style-type: none"> <li>Rx: &lt; 1 kbps</li> <li>Tx: &lt; 1 kbps</li> <li>Rx: &lt; 1 kbps</li> <li>Tx: &lt; 1 kbps</li> <li>Rx: &lt; 1 kbps</li> <li>Tx: &lt; 1 kbps</li> <li>Rx: 1.6 kbps</li> <li>Tx: &lt; 1 kbps</li> </ul>	<ul style="list-style-type: none"> <li>Drop rate: 0.0 pkt/s</li> <li>Latency: 4 ms</li> <li>Drop rate: 0.0 pkt/s</li> <li>Latency: 4 ms</li> <li>Drop rate: 0.0 pkt/s</li> <li>Latency: 4 ms</li> <li>Drop rate: 0.0 pkt/s</li> </ul>		

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




When pressing the  button, the following menu will appear:

**PepVPN performance analysis - 9B0A-A29B-2931** ✕



**PepVPN Test:**  
Check the general TCP/UDP throughput.



**PepVPN Analyzer:**  
Check the uplink performance of each tunnel.

Warning: PepVPN Analyzer will temporarily interrupt VPN connectivity and will restore after test.

Close



**PepVPN Test:**  
Check the general TCP/UDP throughput.

After clicking the icon, the following menu appears:

**Configuration** ?

<b>Type</b>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<span style="border: 1px solid gray; padding: 5px 10px;"><b>Start</b></span>
<b>Direction</b>	<input checked="" type="radio"/> Upload <input type="radio"/> Download	
<b>Duration</b>	<input type="text" value="10"/> seconds (5 - 600)	

**WAN Statistics**

<span style="color: green;">●</span> WAN 1	Rx: 2.5 kbps	Tx: 5.3 kbps	Drop rate: 0.0 pkt/s	Latency: 186 ms
<span style="color: red;">●</span> WAN 3	Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a
<span style="color: red;">●</span> WAN 4	Rx: n/a	Tx: n/a	Drop rate: n/a	Latency: n/a
<b>Total</b>	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 <span style="float: right;">?</span>							
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)
O				5.87	16.95	0.76	420.51
	O			20.72	26.39	1.59	29.89
		O		30.10	43.69	2.24	29.61
			O	45.01	55.93	2.16	28.24
O	O			24.87	33.56	0.86	49.86
O		O		19.30	31.28	0.01	49.78
	O	O		18.59	30.41	2.08	39.78
O	O	O		20.56	34.60	0.00	38.11
O			O	36.70	59.16	2.64	42.06
	O		O	19.98	30.40	4.40	38.01
O	O		O	31.63	42.99	0.72	37.99
		O	O	36.88	55.78	2.60	33.89
O		O	O	38.30	47.89	0.01	29.98
	O	O	O	33.21	55.23	2.69	30.48
O	O	O	O	30.02	46.66	3.77	28.68

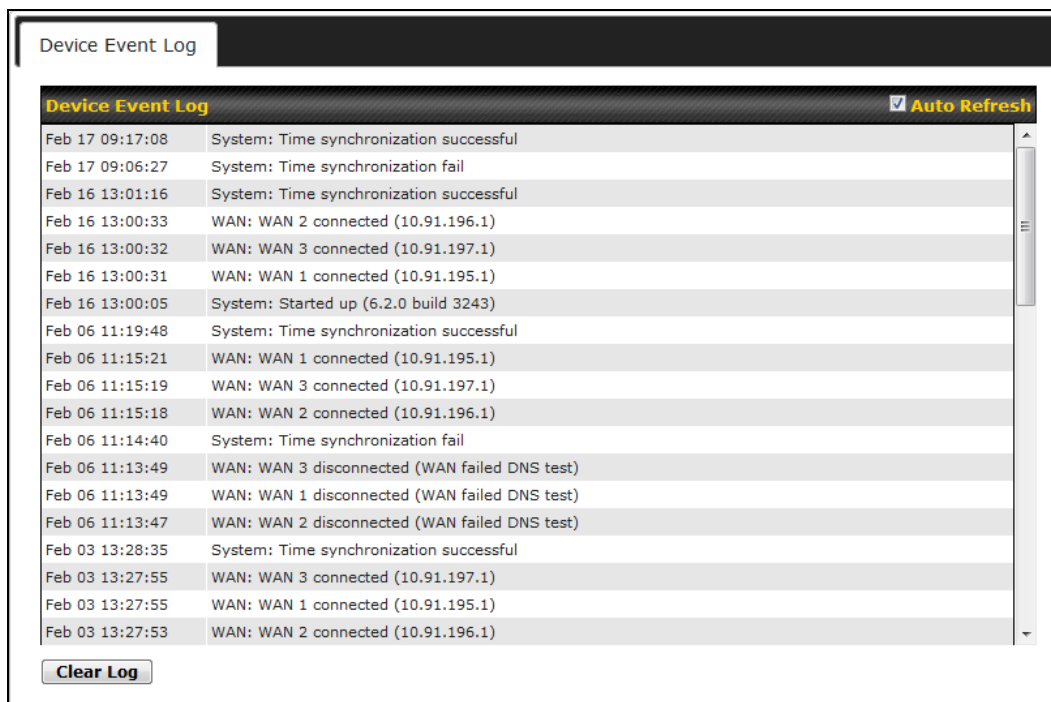
"O" indicates that specific WAN / Tunnel is active for that particular test.

"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.

### 15.1.8 Event Log

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

## Device Event Log

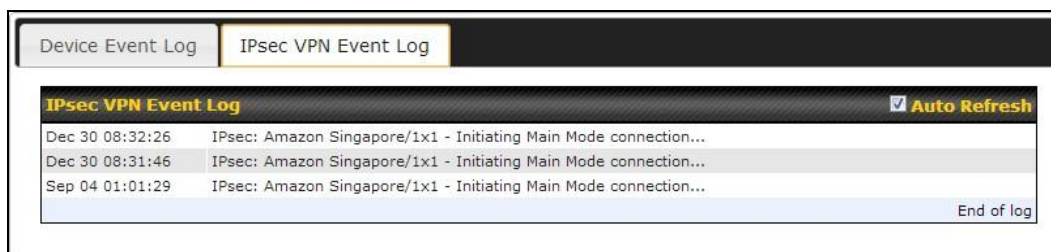


Device Event Log		<input checked="" type="checkbox"/> Auto Refresh
Feb 17 09:17:08	System: Time synchronization successful	
Feb 17 09:06:27	System: Time synchronization fail	
Feb 16 13:01:16	System: Time synchronization successful	
Feb 16 13:00:33	WAN: WAN 2 connected (10.91.196.1)	
Feb 16 13:00:32	WAN: 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.

## IPsec Event Log



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**.

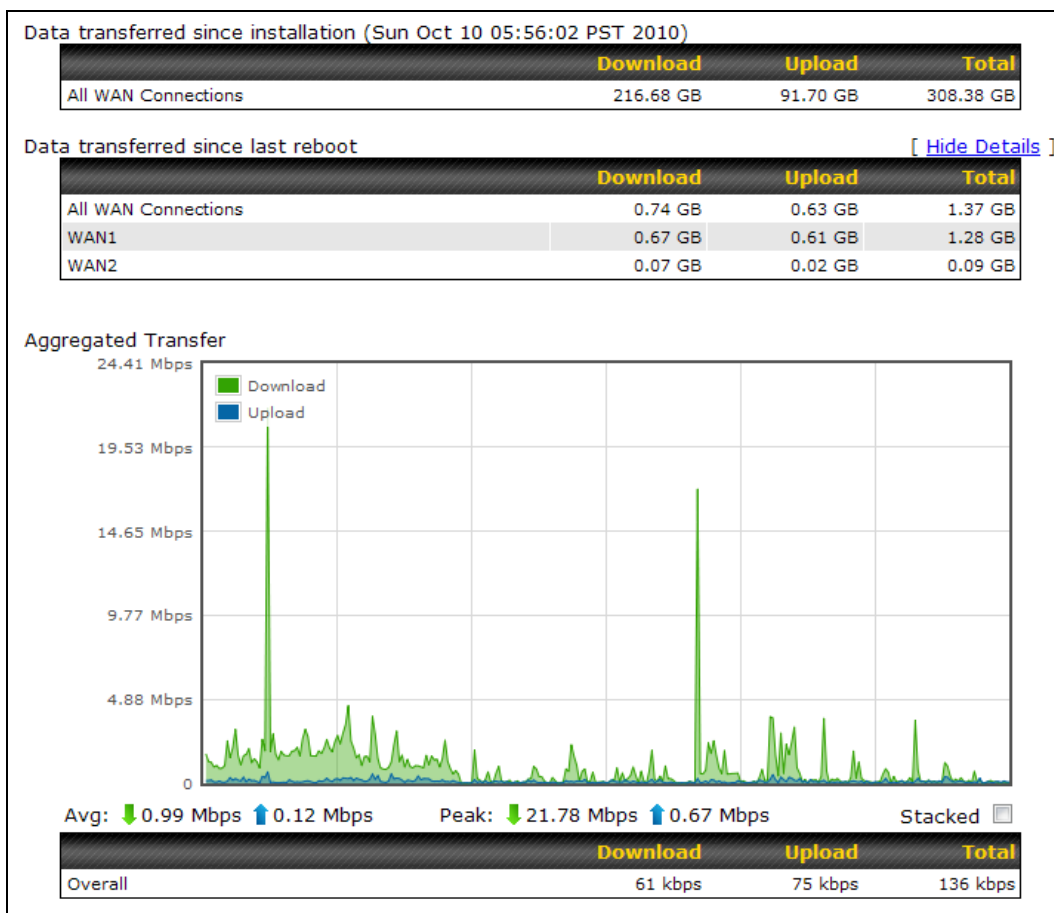
## 15.2 Bandwidth

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.

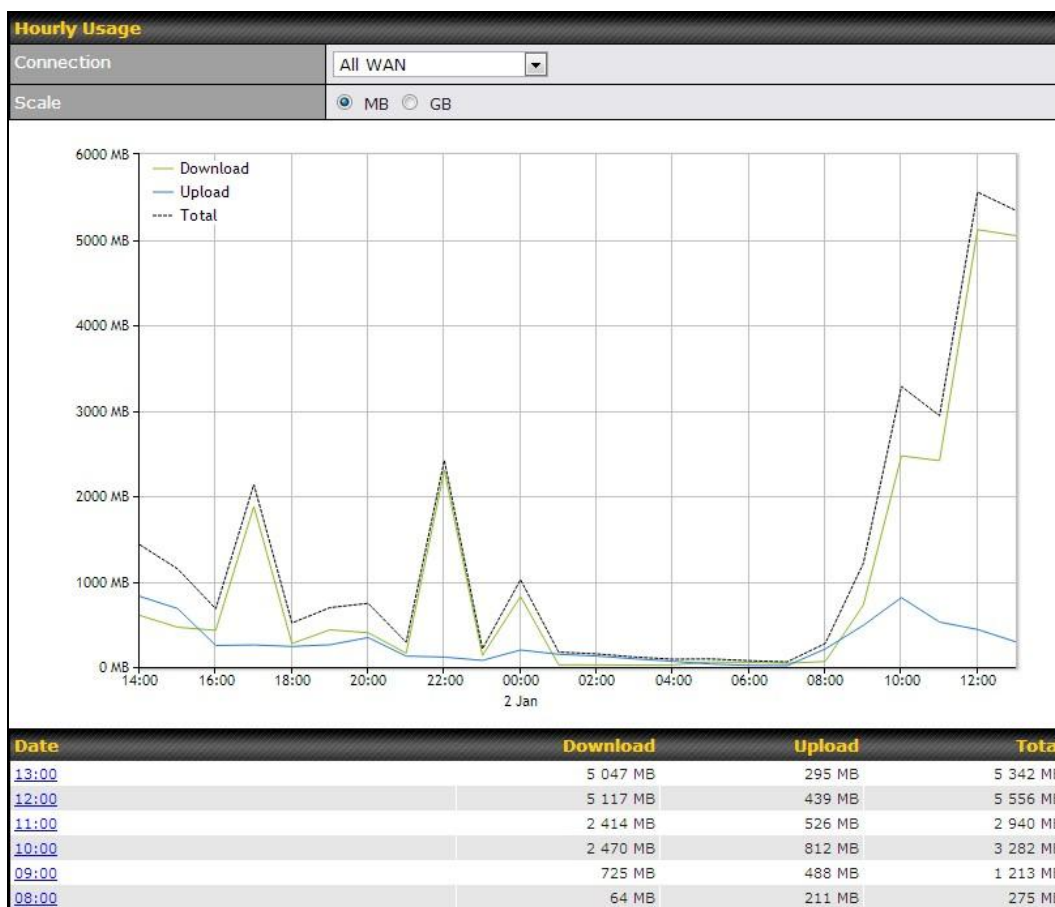
### 15.2.1 Real-Time

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.



### 15.2.2 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.



### 15.2.3 Daily

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

Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature as shown in **Section 13.4**, the **Current Billing Cycle** table for that WAN connection will be displayed.

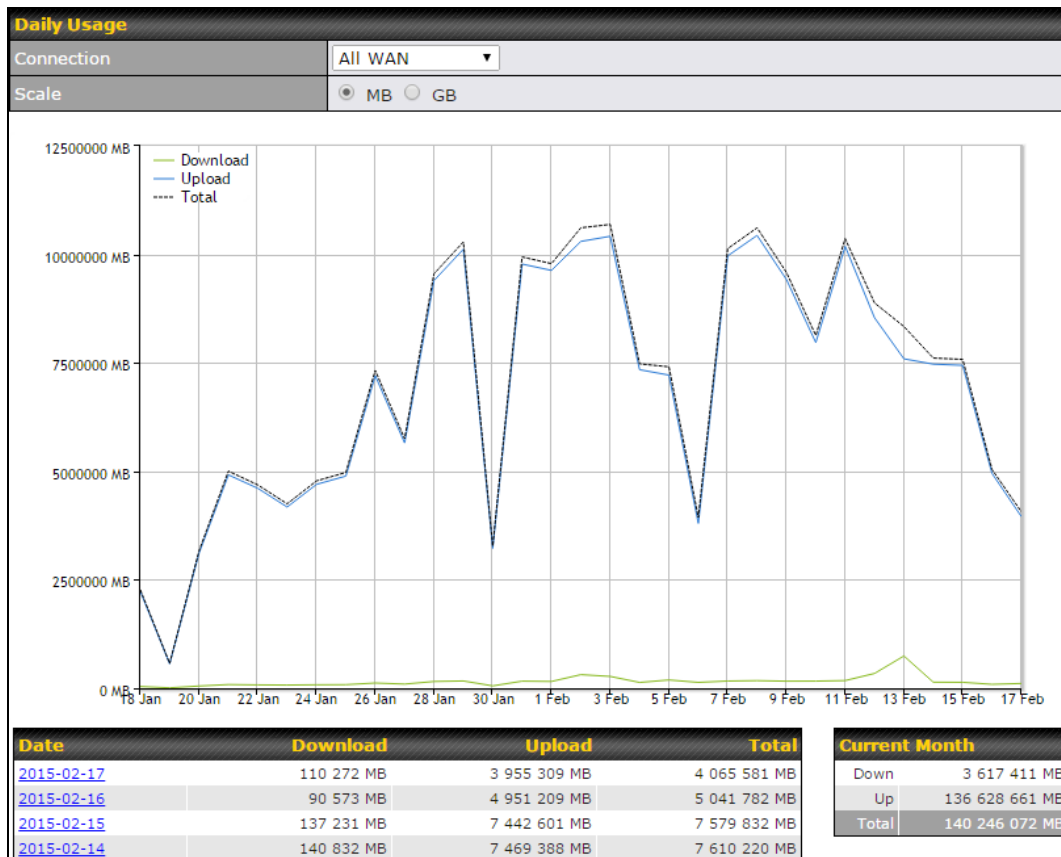
Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes



(GB).



Status



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

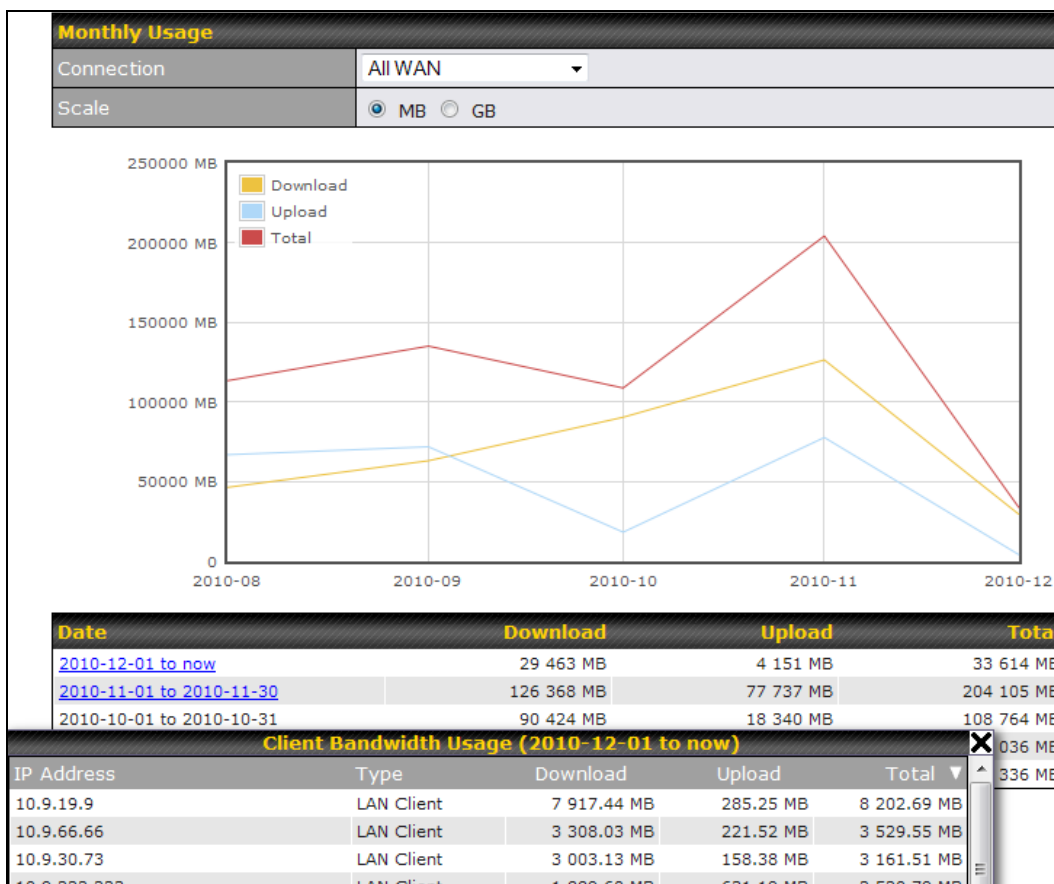
**Client Bandwidth Usage (2015-02-15)**

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

### 15.2.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection. If you have enabled **Bandwidth Monitoring** feature as shown in **Section 13.4**, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

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



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

## Appendix A. Restoration of Factory Defaults

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

### For Balance models with a reset button:

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

### For Balance/MediaFast models with an LCD menu:

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

Afterwards, the factory default settings will be restored.

### Important Note

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

## Appendix B. Routing under DHCP, Static IP, and PPPoE

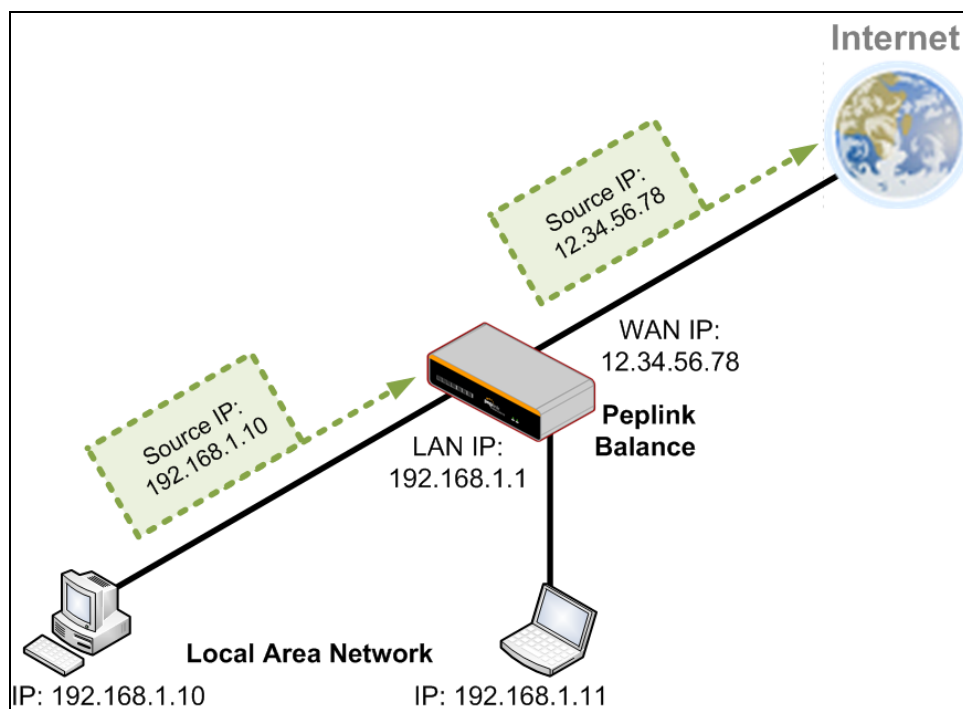
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

### B.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.

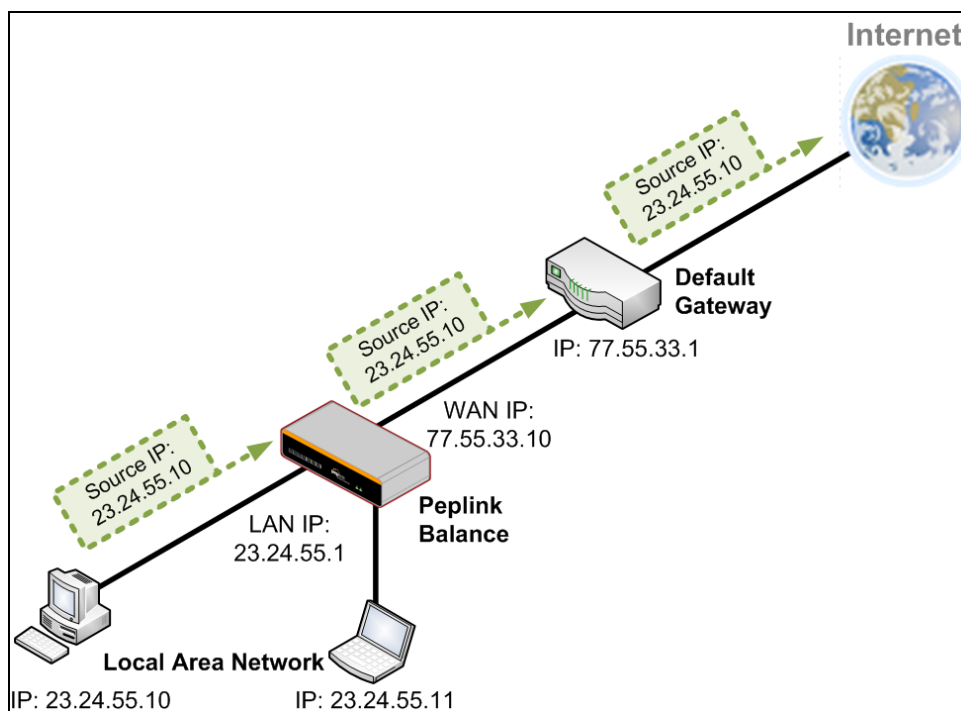
The following figure shows the packet flow in NAT mode:



## B.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 C. Case Studies

### 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.

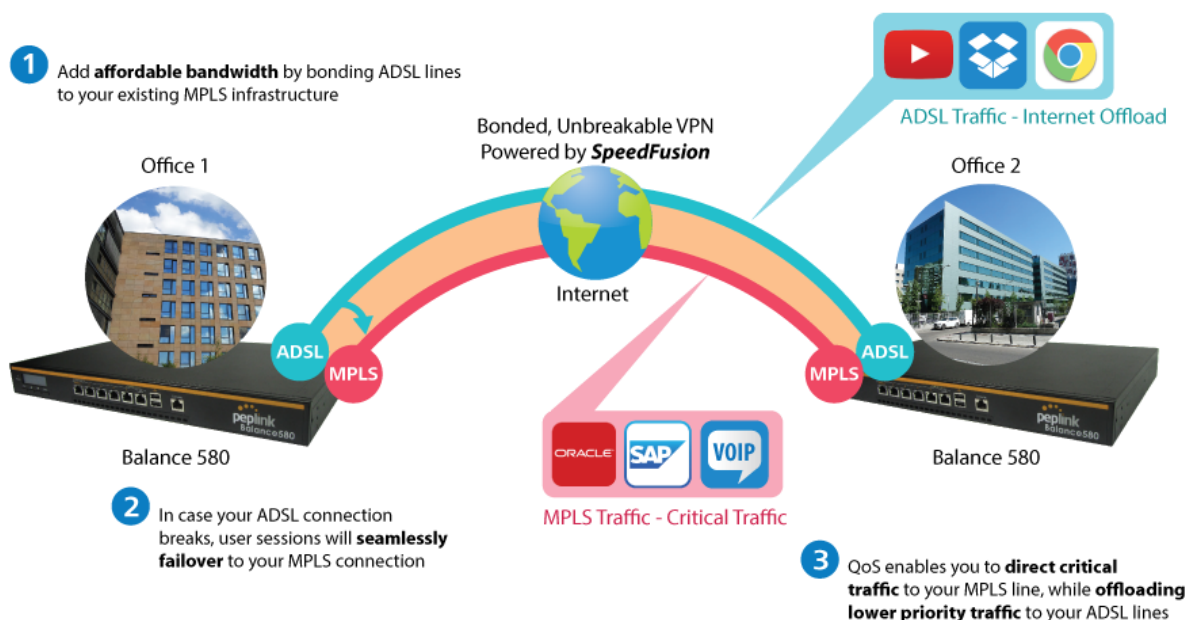
Special features of Balance 580: have high availability capability

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.

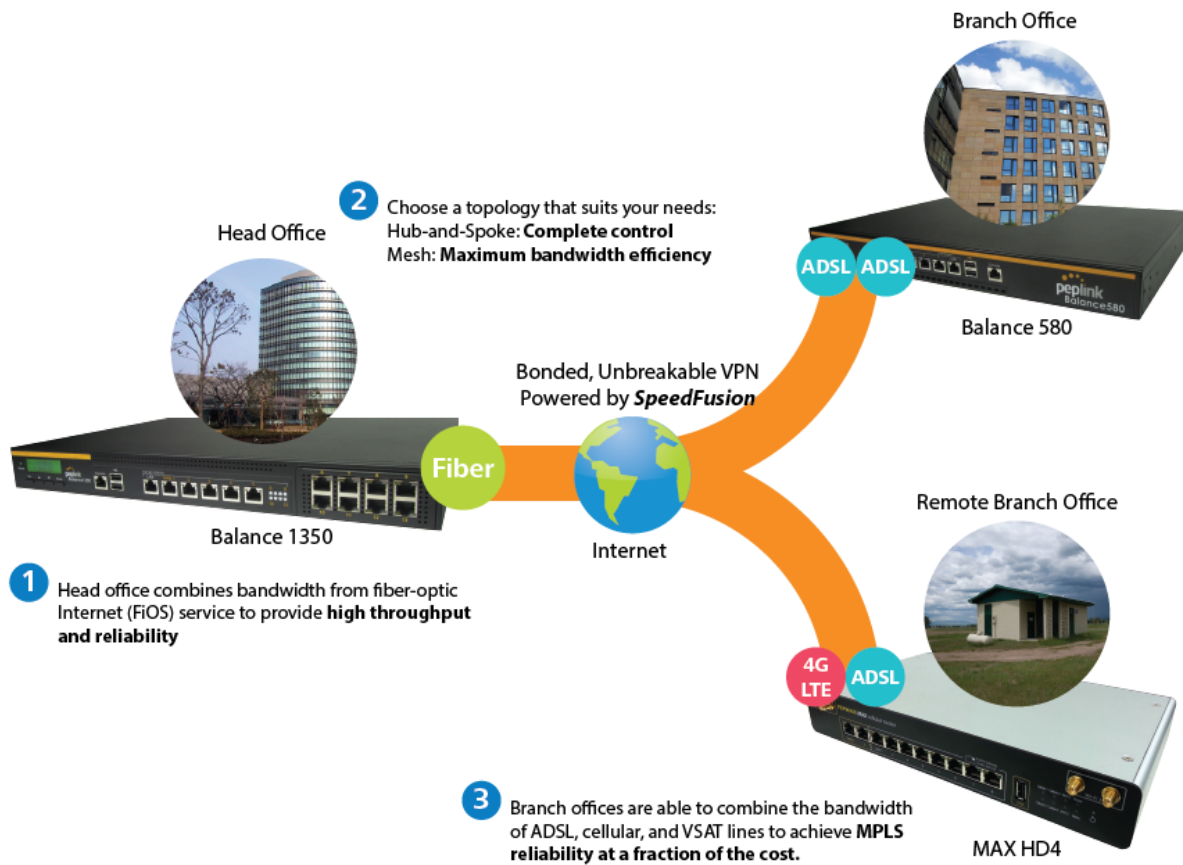
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

## 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.

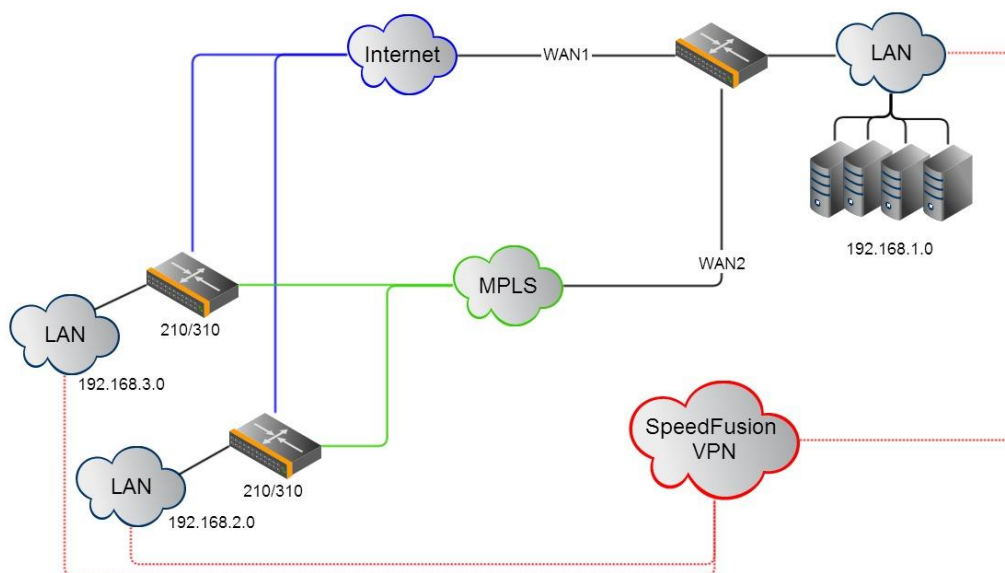
## Option 2: MPLS Alternative



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 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**

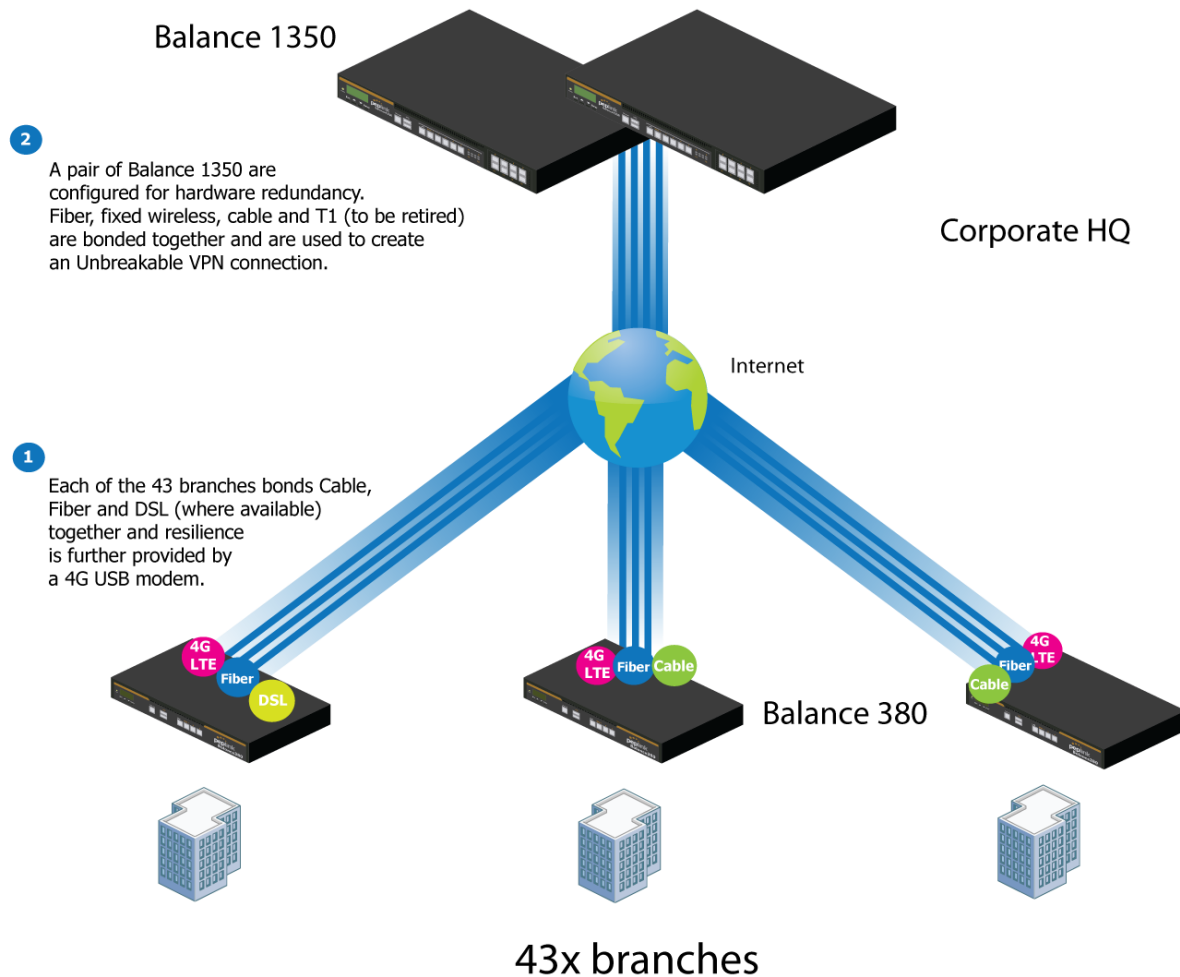
- Extreme savings of \$100,000 per year
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

### **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.

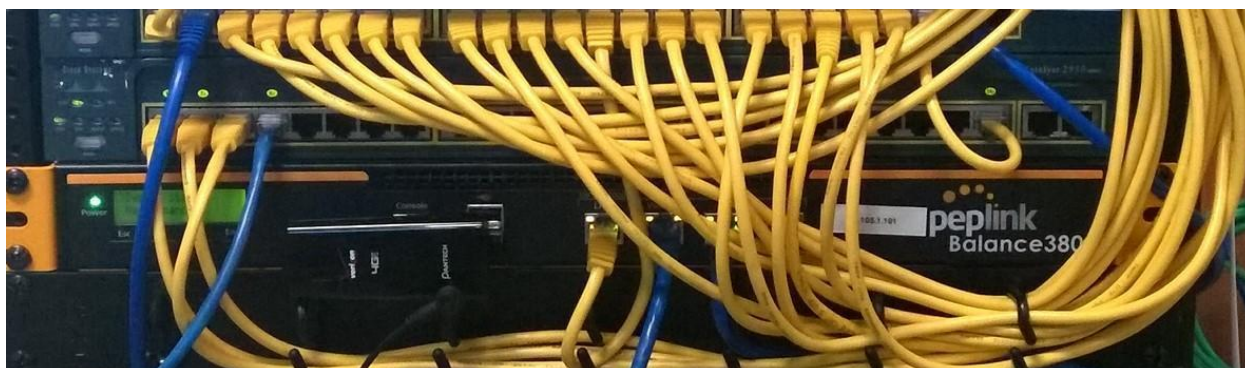
### **Quick Deployment and Unbreakable Connectivity**

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

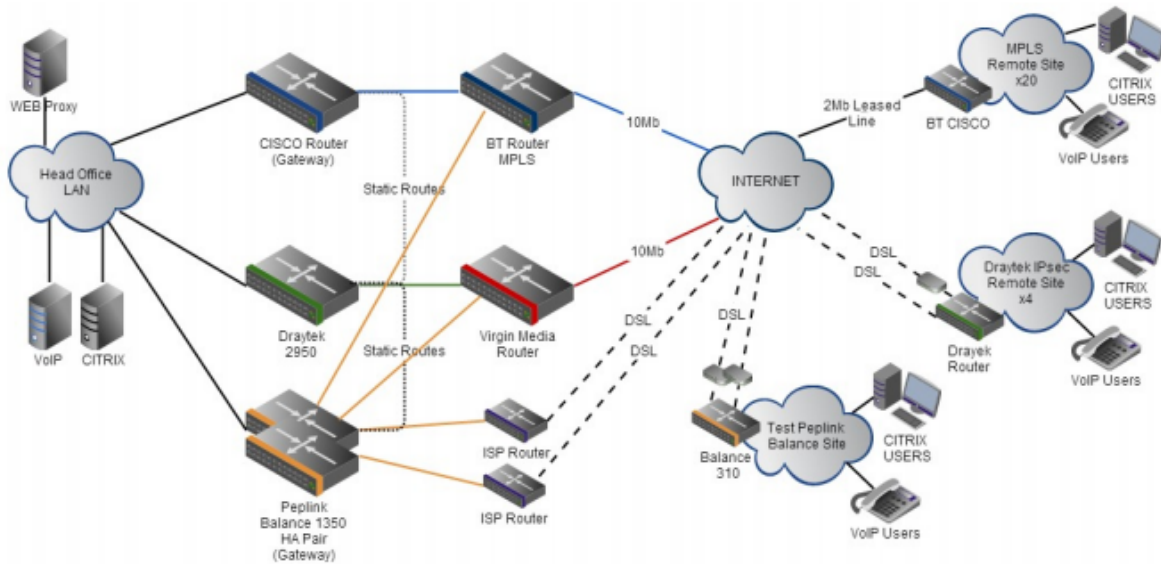


A Peplink customer since 2006, Pluss is a social enterprise that each year makes gainful employment a reality for more than 5000 disabled and disadvantaged UK citizens. With 37 locations and 300+ active users, Pluss makes heavy use of its WAN infrastructure, which until recently was built on managed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



## 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

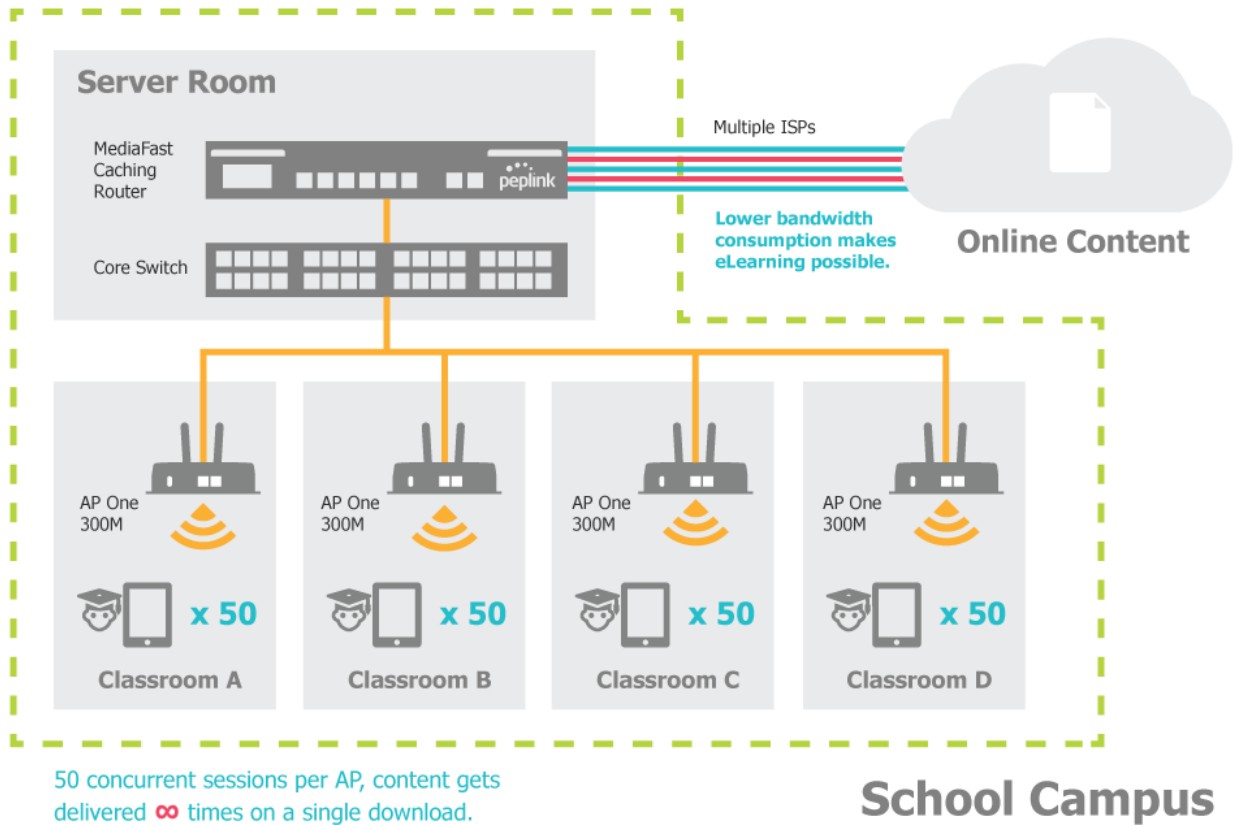
#### Solution

- 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





## Performance Optimization

### 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).

### 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.

## Maintaining the Same IP Address Throughout a Session

### 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.

### 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.

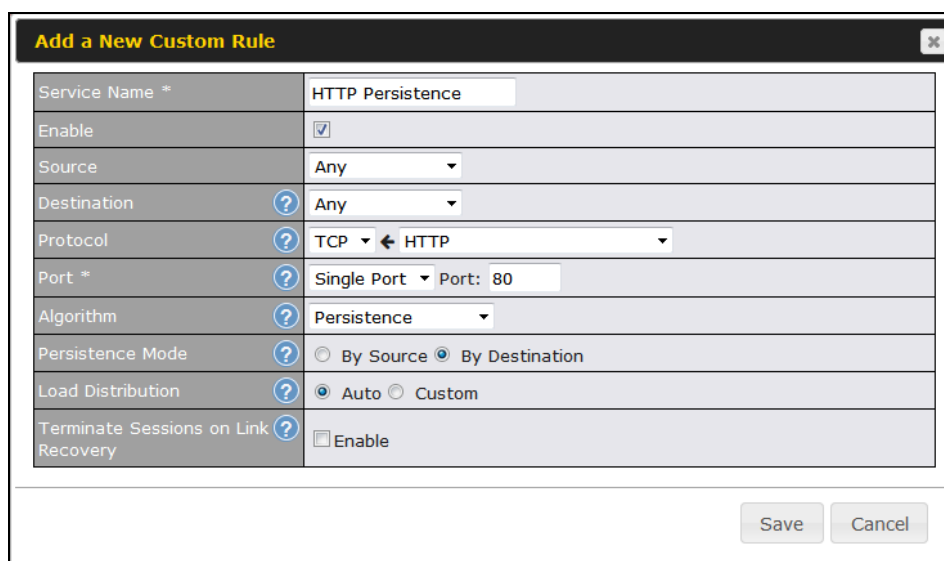
With persistence configured and the option **By Source** is selected, the Peplink Balance uses a consistent WAN connection for same-source IP addresses. This option offers

higher application compatibility but may inhibit the load balancing function unless there are many clients using the Internet.

## 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 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.

## Bypassing the Firewall to Access Hosts on LAN

### 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.

### 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 ?	<b>Connection / Inbound IP Address(es)</b>
	<input checked="" type="checkbox"/> WAN 1 <span style="float: right;"><input checked="" type="checkbox"/> 10.90.0.75 (Interface IP)</span>
	<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 ?	<b>Connection / Outbound IP Address</b>
	WAN 1 <span style="float: right;">10.90.0.75 (Interface IP) ▾</span>
	WAN 2 <span style="float: right;">10.90.0.76 (Interface IP) ▾</span>
	WAN 3 <span style="float: right;">Interface IP ▾</span>
	WAN 4 <span style="float: right;">Interface IP ▾</span>
	WAN 5 <span style="float: right;">Interface IP ▾</span>
	WAN 6 <span style="float: right;">Interface IP ▾</span>
	WAN 7 <span style="float: right;">Interface IP ▾</span>
Mobile Internet <span style="float: right;">Interface IP ▾</span>	

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

## Inbound Access Restriction

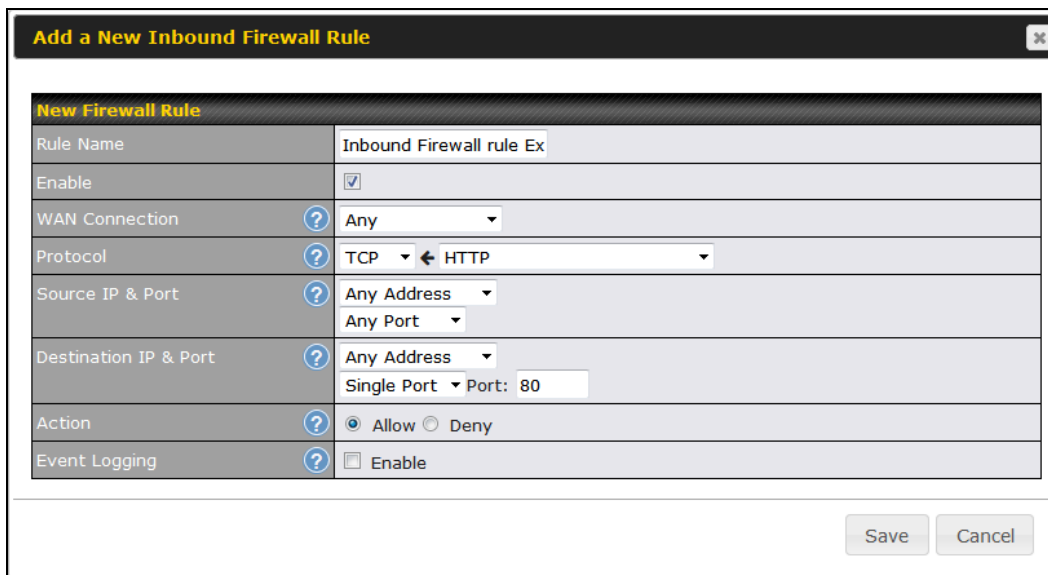
### Scenario

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

### 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

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.

## Outbound Access Restriction

### 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.

### Solution

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

### Add a New Outbound Firewall Rule ✕

---

#### New Firewall Rule

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

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 D. 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](http://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 Community Forums: <https://forum.peplink.com/>

## Appendix E. Declaration

### **CAUTION:**

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

### **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.

### **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.