Peplink Balance and MediaFast User Manual

Peplink Products:
One/One Core/Two/20/30 LTE/30 Pro/210/305/380/580/710/1350/2500/EPX/SDX/
MediaFast 200/500/750

Peplink Balance Firmware 8.0.1
November 2019

Table of Contents

Introduction and Scope

Peplink Balance routers provide link aggregation and load balancing across multiple WAN connections. We develop products and technologies that can help you build SD-WAN networks with unbreakable connection resilience, unmatched deployment flexibility, and intuitive ease of use.

Our product and technology focus has always been on WAN virtualization and the intelligent use of multiple WAN links at the same time to increase reliability and bandwidth whilst reducing costs. We have two key WAN virtualization technologies, Intelligent load balancing for Internet access and SpeedFusion VPN Bonding for secure branch to branch connectivity.

The Peplink MediaFast series are a range of routers capable of content caching. Designed with education and entertainment in mind, Mediafast downloads and accelerates video, iTunes iOS updates, app downloads, and other content for uninterrupted learning and fun anytime. The MediaFast can prefetch content during off-peak hours, saving connectivity costs and reducing network burden during busy times.

This manual applies to the following Peplink Balance products:

- Peplink Balance One
- Peplink Balance Two
- Peplink Balance 20
- Peplink Balance 30 LTE/Pro
- Peplink Balance 210
- Peplink Balance 380
- Peplink Balance 580
- Peplink Balance 710
- Peplink Balance 1350
- Peplink Balance 2500
- Peplink MediaFast 200/500/750
- Peplink EPX
- Peplink SDX

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.

1 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
VRF	Virtual Routing and Forwarding
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

2 Product Comparison Charts

2.1 Balance Routers

	Balance One	Balance Two	Balance 20	Balance 30 LTEA	Balance 30 Pro	Balance 210	Balance 305	Balance 380	Balance 580	Balance 710	Balance 1350	
WAN Interface	2x GE	2 x GE	2x GE	2x GE	2 x GE	2x GE	3x GE	3x GE	5x GE	7x GE	13x GE	12x GE
Wi-Fi Interface	Yes	-	-	-	Yes	-	-	-	-	-	-	-
Embedded 3G/4G LTE	-	-	-	1 (LTEA)	1 (LTEA)	-	-	-	-	-	-	-
USB WAN Modem	1	1	1	1	1	1	1	1	1	1	1	1
LAN Interface	8x GE	4 x GE	4x GE	4x GE	4 x GE PoE	7x GE	3x GE	3x GE	3x GE	3x GE	3x GE	2x 10G SFP+
Recommended Users	1-60	25-150	1-60	1-60	1-60	25-150	50-500	50-500	300-1000	500-2000	1000-5000	5000-20000+
Router Throughput	600Mbps	1 Gbps	150Mbps	200Mbps	400 Mbps	350Mbps	1Gbps	1Gbps	1.5Gbps	2.5Gbps	5Gbps	8Gbps
Disk Drive	-	-	-	-	-	-	-	-	-	-	-	-
Load Balancing & Failover	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PepVPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SpeedFusion Hot Failover	Optional Feature	Optional Feature	-	-	Yes	Yes	Optional Feature	Yes	Yes	Yes	Yes	Yes
SpeedFusion WAN Smoothing	Optional Feature	-	-	-	Optional Feature	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SpeedFusion Bandwidth Bonding	Optional Feature	Optional Feature	Optional Feature	Optional Feature	Optional Feature	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of PepVPN/SpeedFusion Peers	2	2	2	2	2	2	2	30	50	300	800	4000

PepVPN/ SpeedFusion Throughput	30Mbps	150 Mbps	30Mbps	55Mbps	55Mbps	80Mbps	150Mbps	150Mbps	200Mbps	400Mbps	800Mbps	2Gbps
Built-in AP Controller	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maximum Number of AP Support	10		10	30	30	30	50	50	100	250	500	1500
Dimensions	271 x 160 x 30 mm	175 x 188 x 42 mm	260 x 133 x 35 mm	260 x 133 x 35 mm	260 x 143 x 40	293 x 273 x 44 mm	426 x 278 x 44 mm	426 x 278 x 44 mm	426 x 278 x 44 mm	426 x 365 x 44 mm	426 x 395 x 44 mm	426 x 550 x 44 mm
Gross Weight	1 kg	0.45 kg	1.6 kg	1.6 kg		2 kg	6.4 kg	6.4 kg	6.4 kg	6.4 kg	6.6 kg	16.4 kg

A full product comparison for Balance routers is available at:
http://www.peplink.com/products/balance/model-comparison/

2.2 MediaFast Routers

-	MediaFast 200	MediaFast 500	MediaFast 750
Product Code	MFA-200-W	MFA-500-B	MFA-750-B
WAN Interface	2x GE (Only WAN 1 is activated.)	5x GE	7x GE
Wi-Fi Interface	Simultaneous Dual-Band 802.11a/b/g/n Access Point	-	-
Embedded 3G/4G LTE	-	-	-
USB WAN Modem	1	1	1
LAN Interface	8x GE; 802.3af PoE Output	3x GE	3x GE
Recommended Users	25-150	300-1000	500-2000
Router Throughput	200Mbps	800Mbps	1.5Gbps
Disk Drive	120GB SSD	500GB SSD	1TB SSD
Load Balancing & Failover	Yes	Yes	Yes
PepVPN	Yes	Yes	Yes
SpeedFusion Hot Failover	Optional Feature	Yes	Yes
SpeedFusion WAN Smoothing	Optional Feature	Yes	Yes

SpeedFusion Bandwidth Bonding	Optional Feature	Yes	Yes
Number of PepVPN/SpeedFusion Peers	2	50	300
PepVPN/ SpeedFusion Throughput	50Mbps	200Mbps	400Mbps
Built-in AP Controller	Yes	Yes	Yes
Maximum Number of AP Support	50	100	250
PoE Input	-	-	-
PoE Output	8x 802.3af (optional feature)	-	-
Dimensions	292 x 177 x 44 mm	431 x 305 x 44 mm	426 x 365 x 44 mm
Gross Weight	2.8 kg	6.6 kg	5.5 kgs

A full product comparison for MediaFast routers is available at:
https://www.peplink.com/products/mediafast-specifications/

3 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:

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
- WAN throughput and consistency diagnosis
- WAN to WAN speed test

LAN

- DHCP server on LAN
- Extended DHCP option support
- Static routing rules
- Local DNS proxy server
- 802.1q VLANs
- Port-based VLANs
- Virtual Network Mapping

VPN

- Secure SpeedFusionTM
- SpeedFusion performance analyzer
- X.509 certificate support
- 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
- SpeedFusionTM throughput, ping, and traceroute tests
- Built-in L2TP / PPTP / OpenVPN VPN server
- Authenticate L2TP / PPTP clients using RADIUS and LDAP servers
- Multi-Site PepVPN Profile
- IPsec VPN for network-to-network connections
- L2TP / PPTP and IPsec passthrough
- Simultaneous L2 & L3 VPN tunnel between the same pair of devices

Inbound Traffic Management

- TCP/UDP traffic redirection to dedicated LAN server(s)

- Inbound link load balancing by means of DNS

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

AP Controller

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

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

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

Captive Portal

- Social Wi-Fi Hotspot Support
- Splash screen of open networks, login page for secure networks
- Customizable built-in captive portal

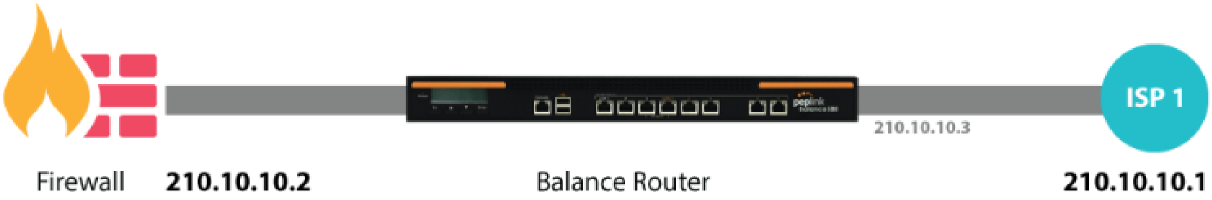
- Supports linking to outside page for captive portal

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
- Event log is persistent across reboots
- IPv6 support
- Support for USB tethering on Android phones

4 Advanced Feature Summary

4.1 Drop-in Mode and LAN Bypass: Transparent Deployment

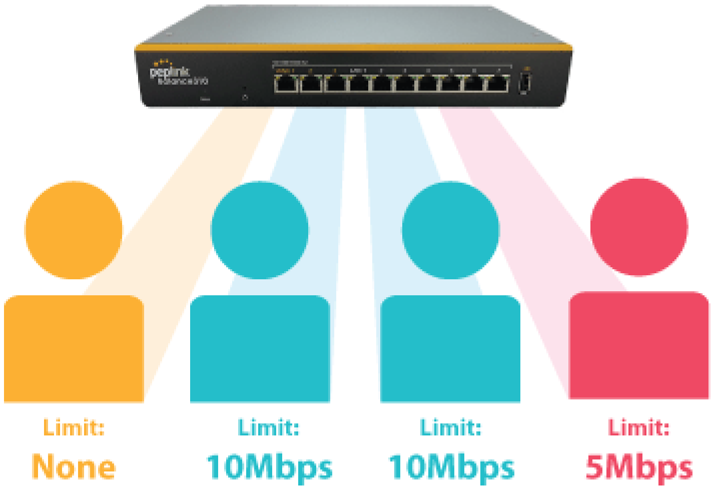


As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass**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

4.2 QoS: Clearer VoIP

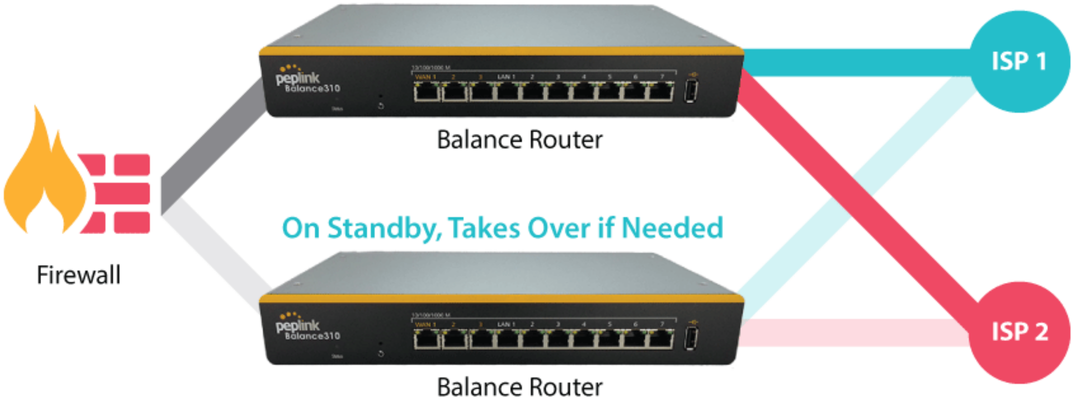
VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.

4.3 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.

4.4 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.

4.5 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.

4.6 Built-In Remote User VPN Support

Use OpenVPN or 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 the full instructions on setting up L2TP with IPsec.
Click here for the full instructions on setting up OpenVPN connections

4.7 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.

5 Package Contents

The contents of Peplink Balance product packages are as follows:

5.1 Peplink Balance One/Two

- Peplink Balance One/Two
- Power adapter
- Information slip

5.2 Peplink Balance 20/30/30 LTE/50

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

5.3 Peplink Balance 210/310

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

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

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

5.5 Peplink MediaFast 200

- Peplink MediaFast 200
- Power adapter
- Information slip

5.6 Peplink MediaFast 500

- Peplink MediaFast 500
- Power cord
- Information slip

- Rackmount kit

5.7 Peplink EPX

- Wireless SD-WAN Powerhouse
- EPX Chassis with LCD
- Optional x LTE-A modules
- Optional x Copper ETH module
- Optional x Fiber ETH module
- Rack mounting kit with brackets and slide

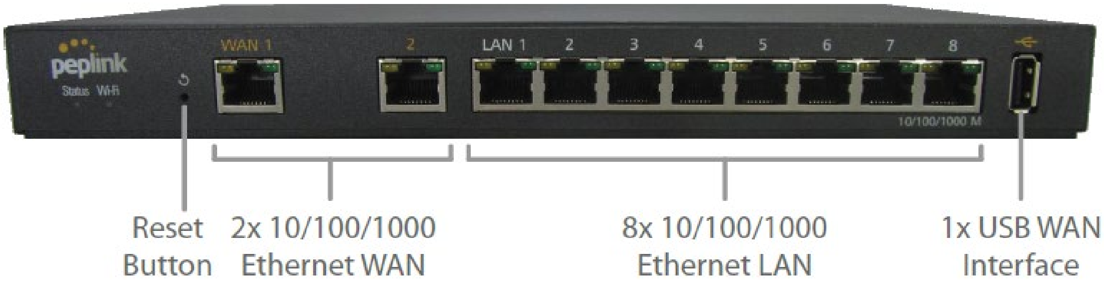
5.8 Peplink SDX

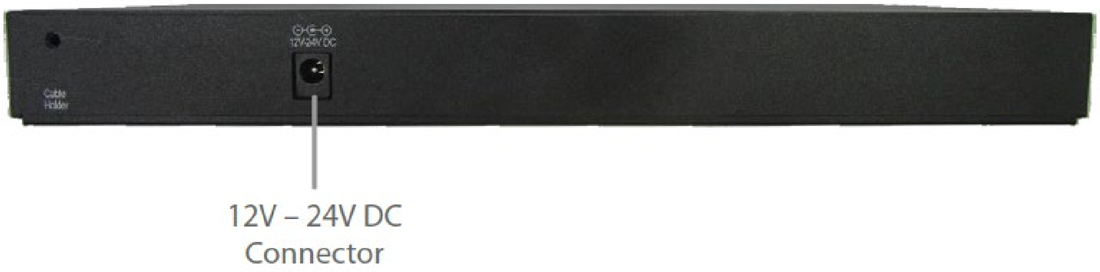
- SDX Base Chassis
- 1U 19″ Rackmount Chassis

6 Peplink Balance Overview

6.1 Peplink Balance One

6.1.1 Panel Appearance





6.1.2 LED Indicators

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

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

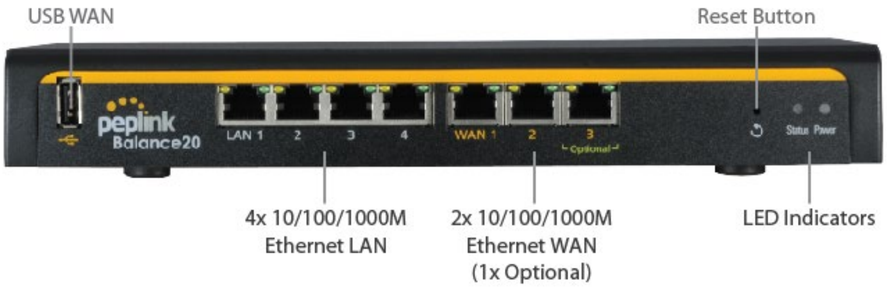
LAN and WAN Ports	
Green LED	ON – 10 / 100 / 1000 Mbps
	Blinking – Data is transferring

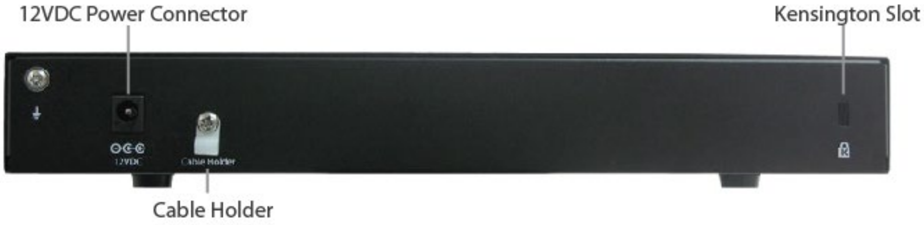
Orange LED	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

USB Port	
USB Ports	For future functionality

6.2 Peplink Balance 20

6.2.1 Panel Appearance





6.2.2 LED Indicators

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

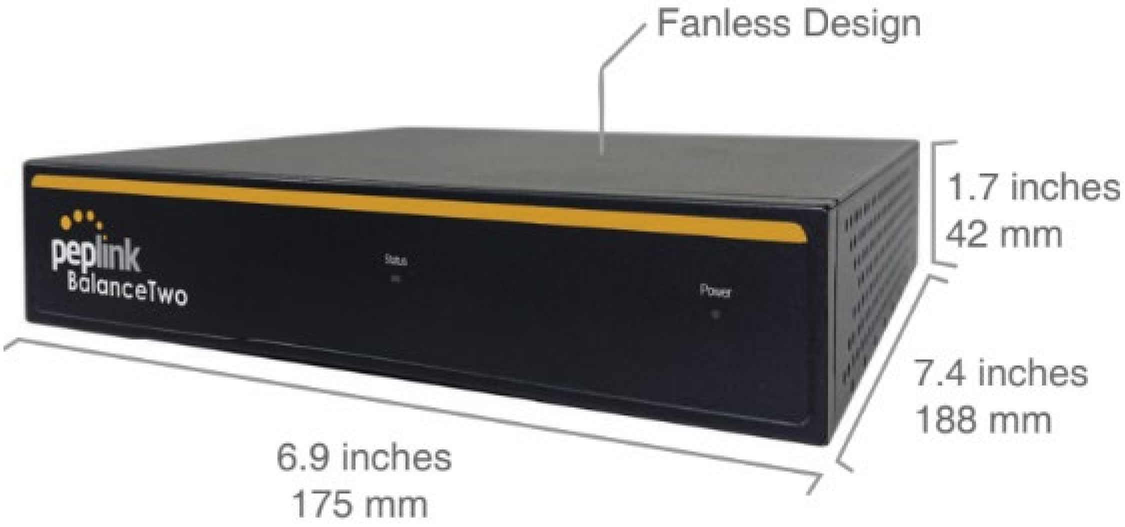
Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

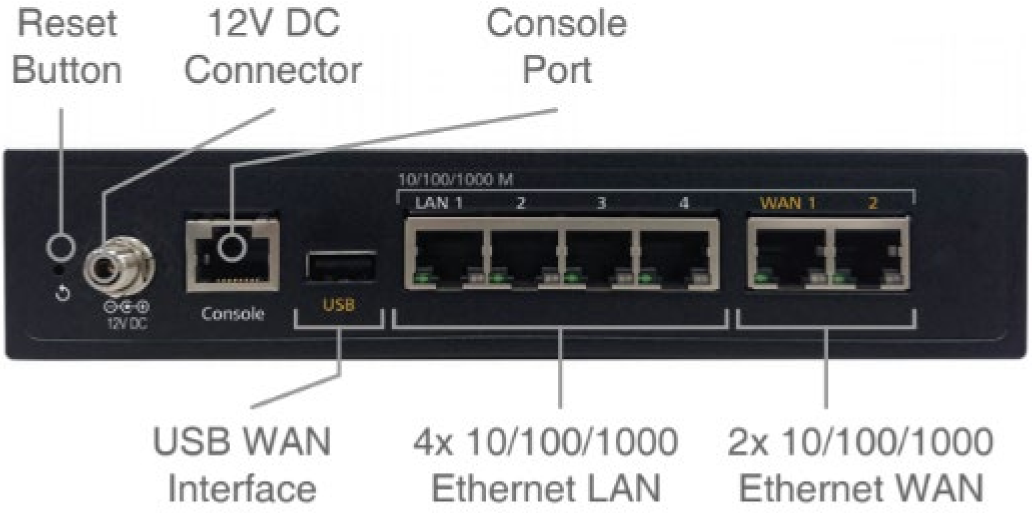
LAN and WAN Ports	
Green LED	ON – 10 / 100 / 1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.3 Peplink Balance Two

6.3.1 Panel Appearance





6.3.2 LED Indicators

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

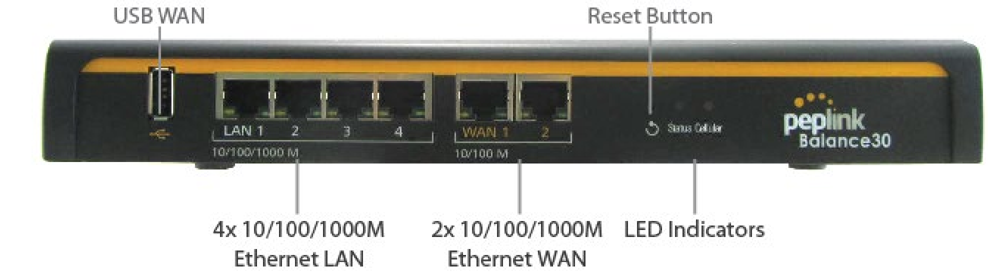
Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

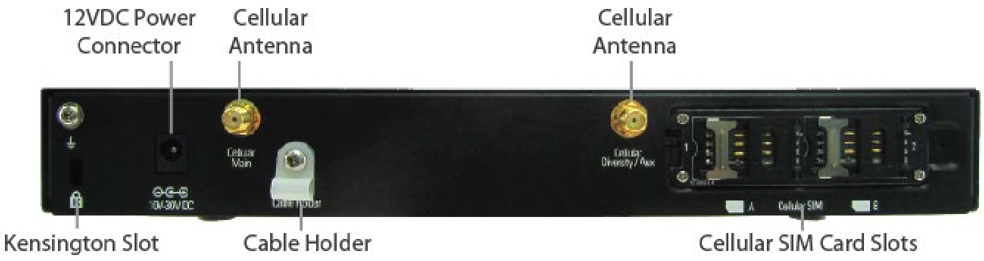
LAN and WAN Ports	
Green LED	ON – 10 / 100 /1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.4 Peplink Balance 30 LTE

6.4.1 Panel Appearance





6.4.2 LED Indicators

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

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

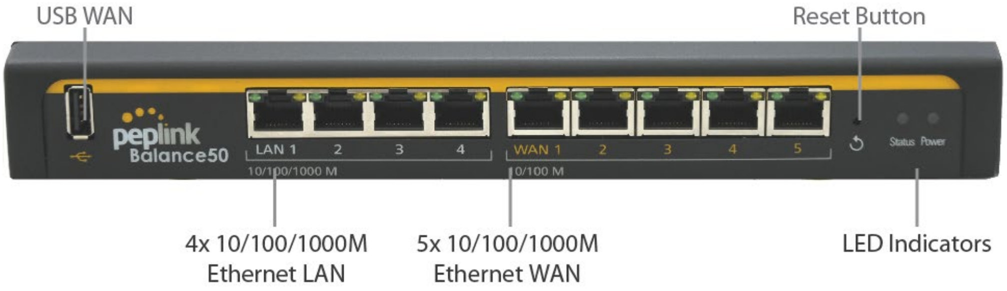
LAN and WAN Ports

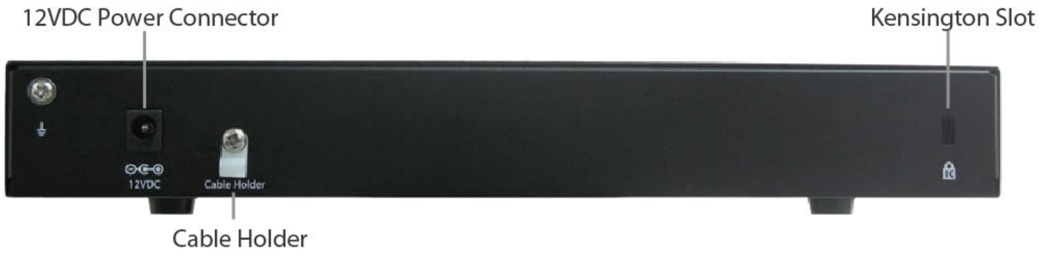
Green LED	ON – 10 / 100 /1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.5 Peplink Balance 50

6.5.1 Front Panel Appearance





6.5.2 LED Indicators

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

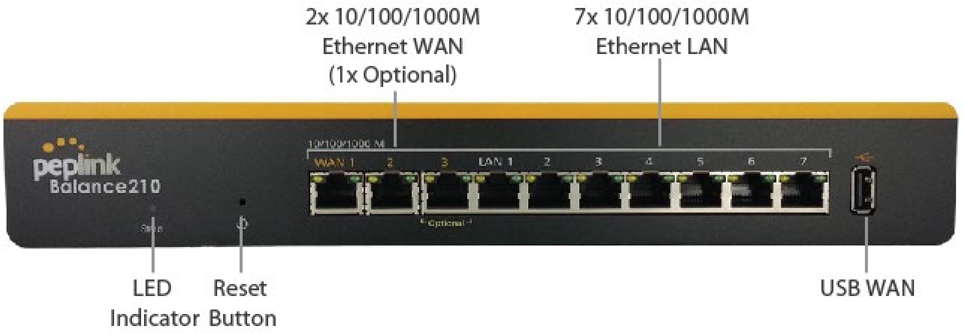
Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

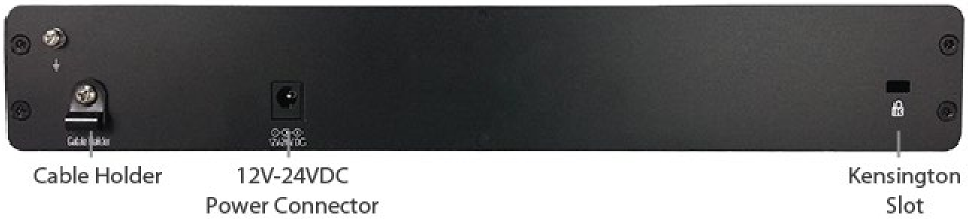
LAN and WAN Ports	
Green LED	ON – 10 / 100 /1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.6 Peplink Balance 210

6.6.1 Front Panel Appearance





6.6.2 LED Indicators

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

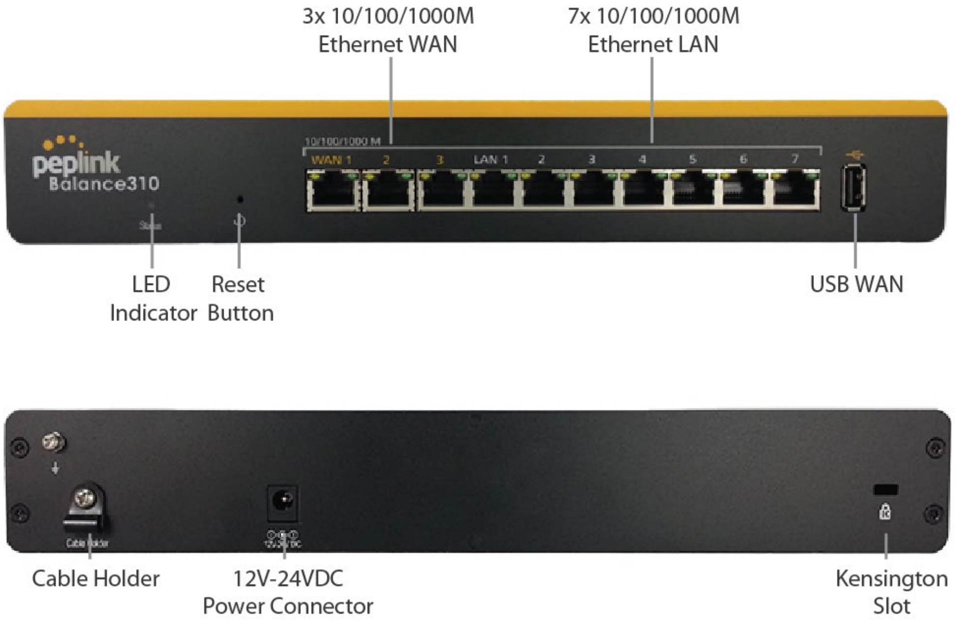
Power and Status Indicators	
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

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

6.7 Peplink Balance 310

6.7.1 Front Panel Appearance



6.7.2 LED Indicators

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

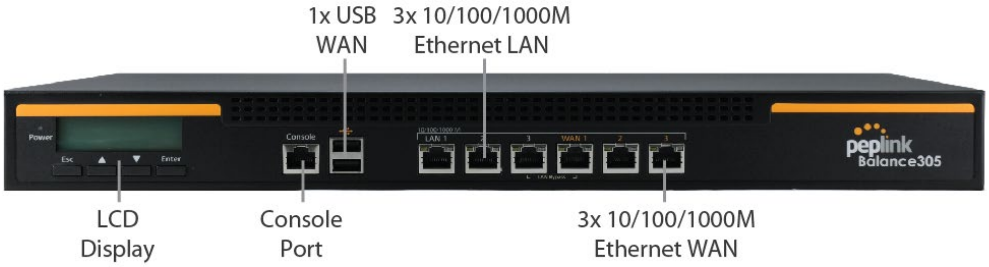
Power and Status Indicators	
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

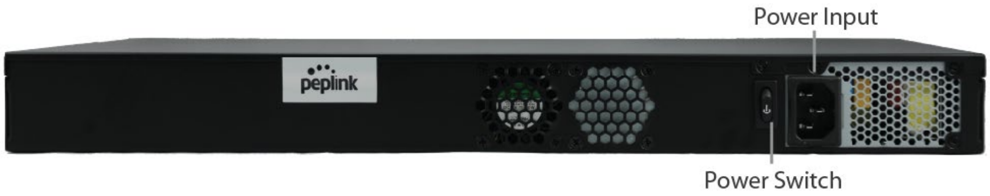
LAN and WAN Ports	
Green LED	ON – 10 / 100 / 1000 Mbps
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.8 Peplink Balance 305

6.8.1 Front Panel Appearance





6.8.2 LED Indicators

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

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

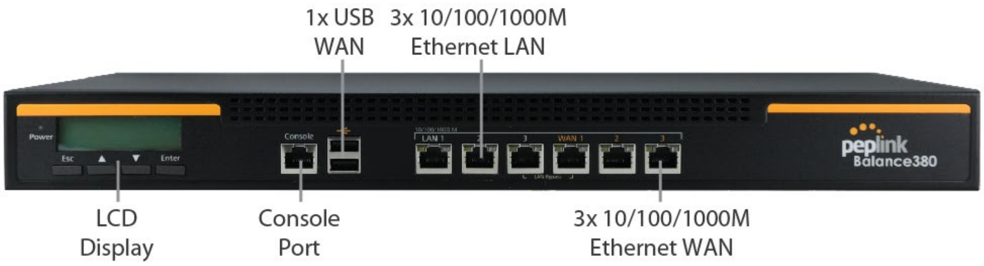
LAN Port, WAN 1 – 3 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring

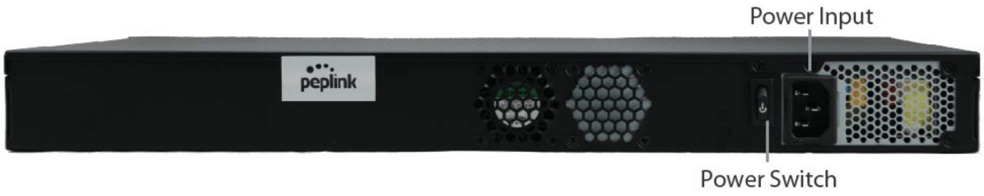
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.9 Peplink Balance 380

6.9.1 Panel Appearance





6.9.2 LED Indicators

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

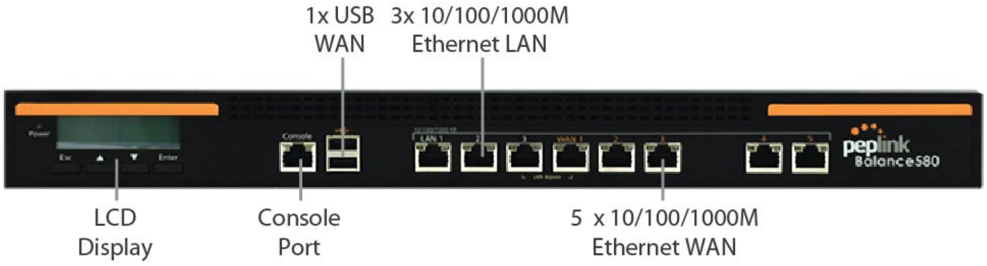
Power and Status Indicators	
Power LED	OFF – Power off
	GREEN – Power on

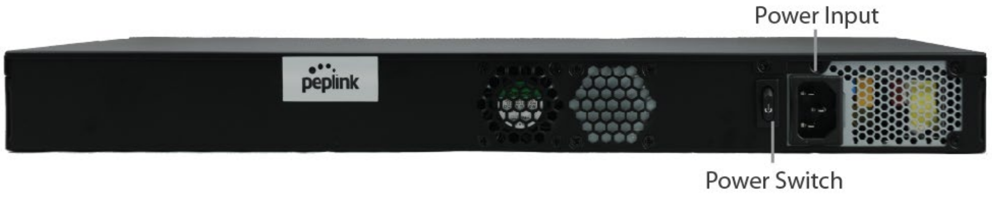
LAN Port, WAN 1 – 3 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.10 Peplink Balance 580

6.10.1 Panel Appearance





6.10.2 LED Indicators

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

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

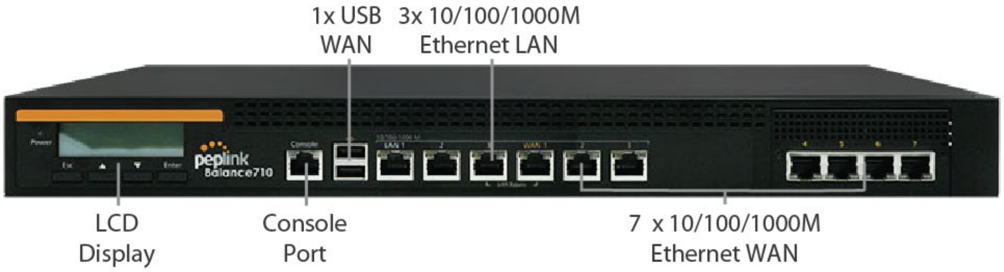
LAN Port, WAN 1 – 5 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

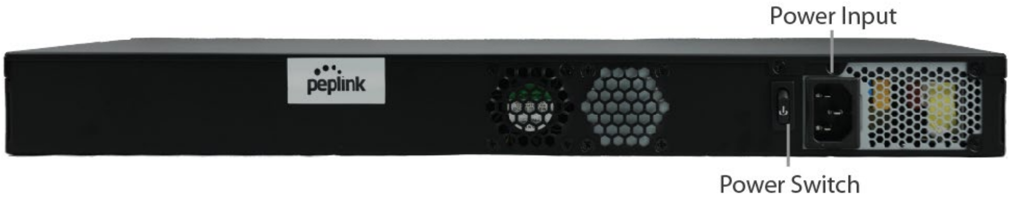
Console and USB Ports

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

6.11 Peplink Balance 710

6.11.1 Front Panel Appearance





6.11.2 LED Indicators

Status indicated in the front panel is as follows:

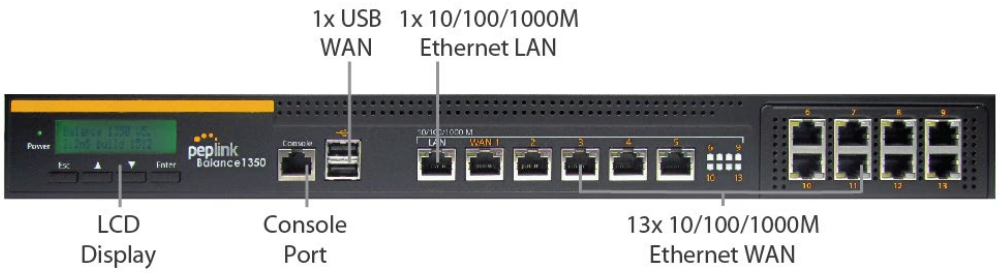
LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

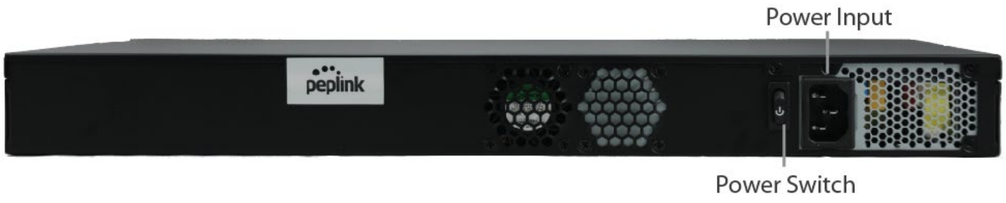
LAN Port, WAN 1 – 7 Ports	
Green LED	ON – 1000 Mbps
	OFF – 100/10 Mbps
Orange LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.12 Peplink Balance 1350

6.12.1 Panel Appearance





6.12.2 LED Indicators

Status indicated in the front panel is as follows:

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

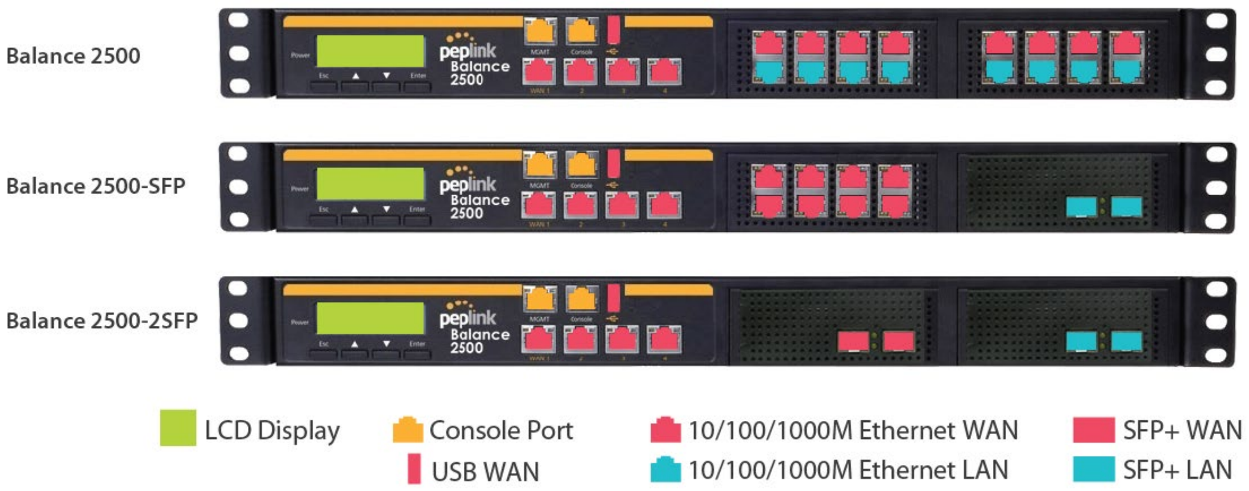
LAN Port, WAN 1 – 13 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring

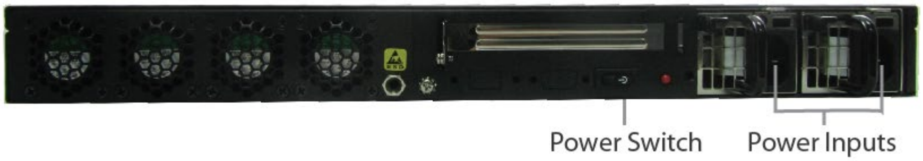
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

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

6.13 Peplink Balance 2500

6.13.1 Panel Appearance





6.13.2 LED Indicators

Status indicated in the front panel is as follows:

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

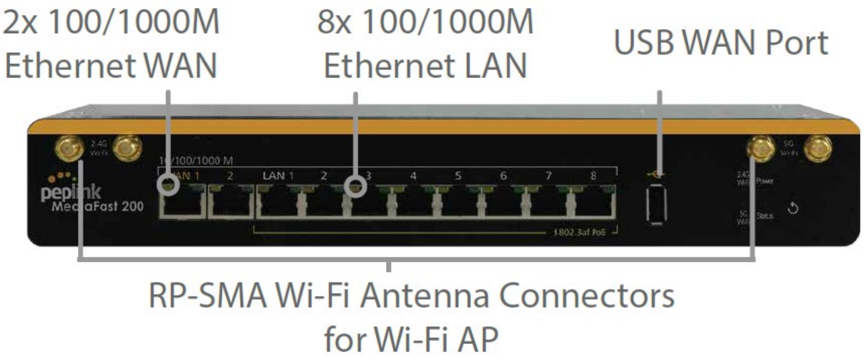
LAN and WAN Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

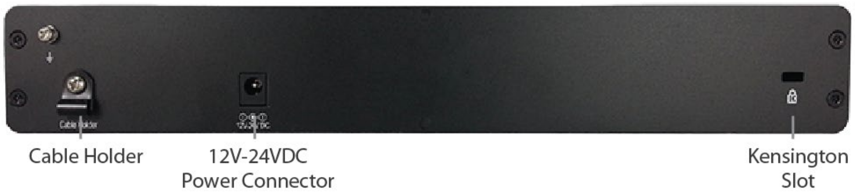
Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

7 Peplink MediaFast Overview

7.1 Peplink MediaFast 200

7.1.1 Panel Appearance


2x 100/1000M Ethernet WAN
8x 100/1000M Ethernet LAN
USB WAN Port
RP-SMA Wi-Fi Antenna Connectors for Wi-Fi AP
peplink
MediaFast 200



7.1.2 LED Indicators

Status indicated in the front panel is as follows:

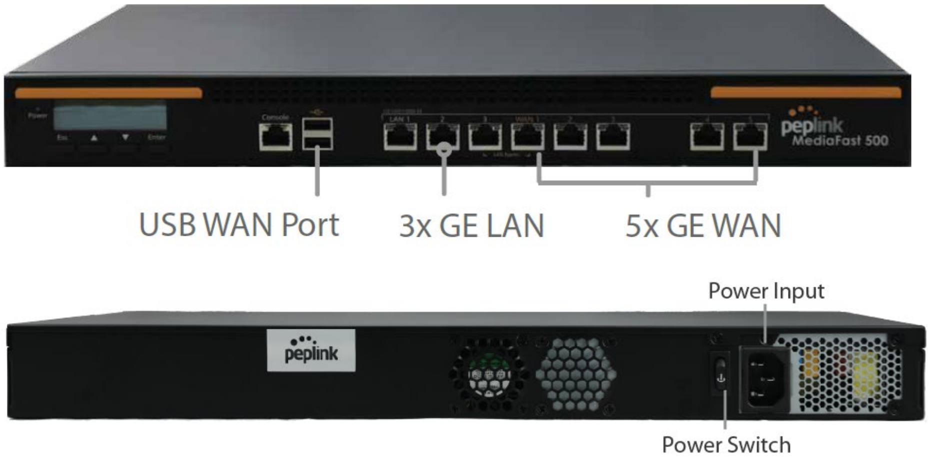
LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

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

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

7.2 Peplink MediaFast 500

7.2.1 Panel Appearance



7.2.2 LED Indicators

Status indicated in the front panel is as follows:

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

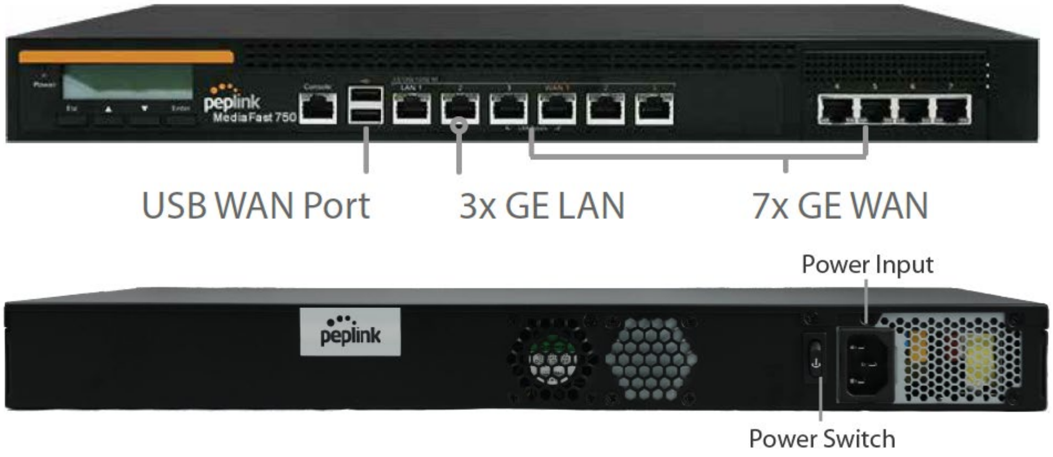
LAN 1-3 Ports, WAN 1-5 Ports	
Right LED	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected

Port Type	Auto MDI/MDI-X ports

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

7.3 Peplink MediaFast 750

7.3.1 Panel Appearance



7.3.2 LED Indicators

Status indicated in the front panel is as follows:

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

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

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

8 Peplink Flex-Module Supported Models

8.1 Peplink EPX

The EPX is a rapidly deployable, powerful, and versatile SD-WAN router that connects a wide range of WAN options from LTE-A, satellite modems, to fixed line networks which can be used simultaneously to allow bonding using our SpeedFusion technology.

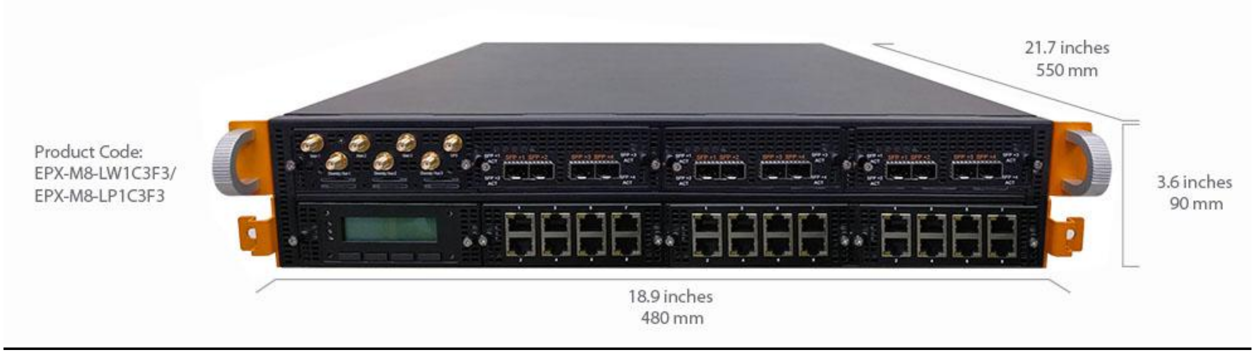
With its modular construction, the EPX is suitable for any deployment.

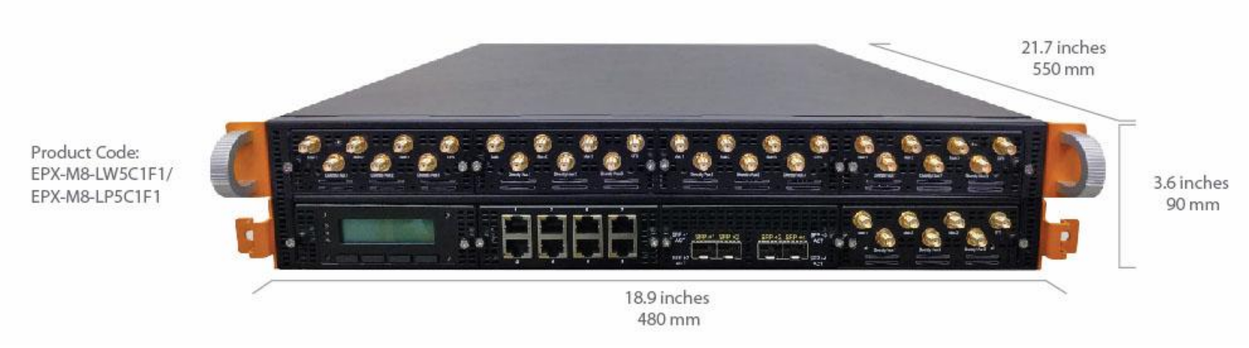
8.1.1 Main Chassis

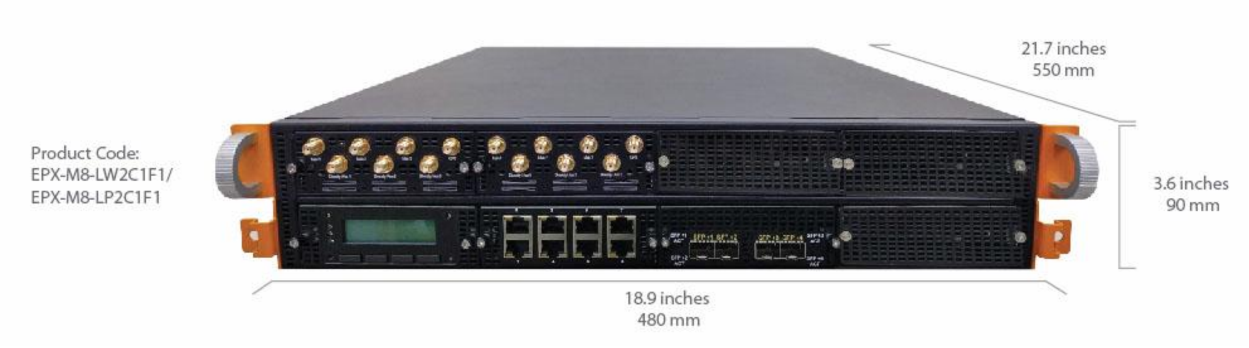
EPX Main Chassis	
Power Input	AC Input 100V - 240V
Power Consumption (Main Chassis only)	215W
Throughput	30Gbps
PepVPN/SpeedFusion Throughput (256-bit AES)	2Gbps
Dimensions	18.9 x 21.7 x 3.6 inches - 480 x 550 x 90 mm
Weight (No Modules)	31.3 pounds - 14.2 kilograms
Operating Temperature	32° – 113°F (0° – 45°C)
Humidity	5% – 90% (non-condensing)
Certifications	FCC, IC, CE-RED EN 50155: Railway Applications EN 61373:1999 IEC 61373:1999 : Shock and Vibration Resistance EN 50121: Rolling Stock EMC, Signalling and Telecom Apparatus

Warranty	1-Year Limited Warranty

8.1.2 Panel Appearance







8.1.3 LED Indicators

Status indicated in the LAN/WAN port module is as follows:
Note: some EPX configurations are not shipped with this module

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

LAN Port, WAN Ports	
Right LED	ORANGE – Enabled as WAN port
	GREEN – PoE enabled
	OFF – Port is not connected
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

Console & USB Ports	
Console Port	CLI Console connection
USB Ports	For connecting a 4G/3G USB modem

8.2 Peplink SDX

The SDX is a Modular Enterprise Grade Router. In addition to popular features such as SpeedFusion SD-WAN and InControl centralized management, the SDX has an expandable module that you can change according to your needs.

The SDX includes two integrated SFP+ WAN Ports, as well as eight PoE-enabled LAN Ports. These ports are available no matter which module you use.

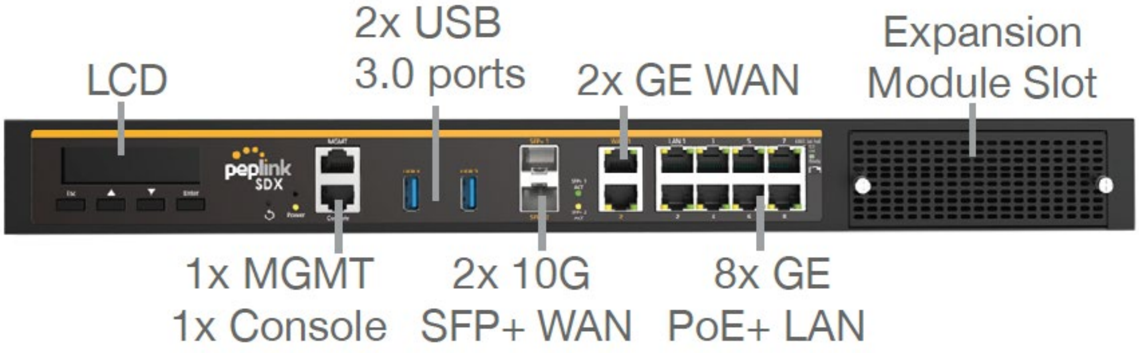
8.2.1 Main Chassis

SDX Main Chassis	
Power Input	AC Input 100V - 240V
Power Consumption	80W System* , 330W PoE+ Power Budget
Throughput	12 Gbps
PepVPN/SpeedFusion Throughput	No Encryption: 1 Gbps 256-bit AES: 600 Mbps
Dimensions	17.2 x 13.3 x 1.7 inches - 438 x 340 x 44 mm
Weight (No Modules)	11.7 pounds - 5.3 kilograms
Operating Temperature	32° – 104°F (0° – 40°C)
Humidity	5% – 90% (non-condensing)
Certifications	FCC, IC, CE

* 80W consumption for the main chassis, 20W consumption for the optional module.

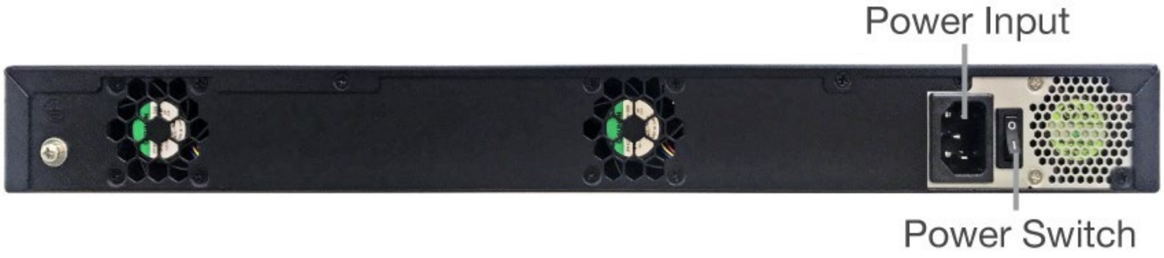
8.2.2 Panel Appearance

Front:



BPL-SDX

Back:



8.2.3 LED Indicators

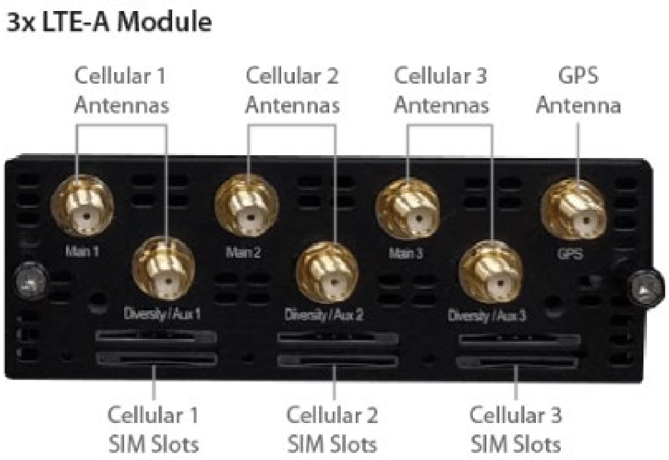
LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

LAN Port, WAN Ports	
Right LED	ORANGE – Enabled as WAN port
	GREEN – PoE enabled
	OFF – Port is not connected
Left LED	Solid – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

Console, MGMT & USB Ports	
Console	CLI console connection

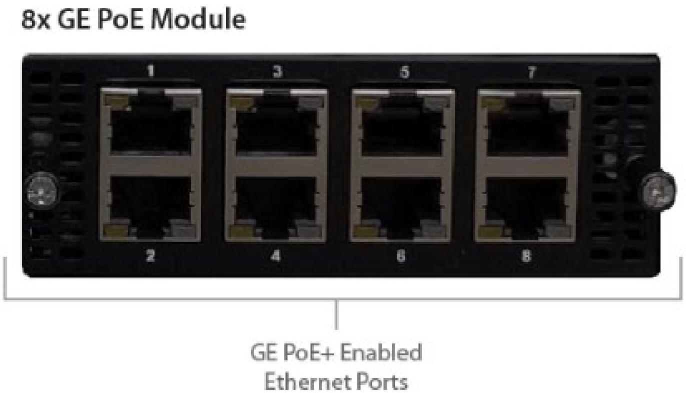
Port	
USB Ports	For connecting 4G/3G USB modems for additional WAN connections
MGMT Port	Management port

8.3 Flex Module Expansion Modules



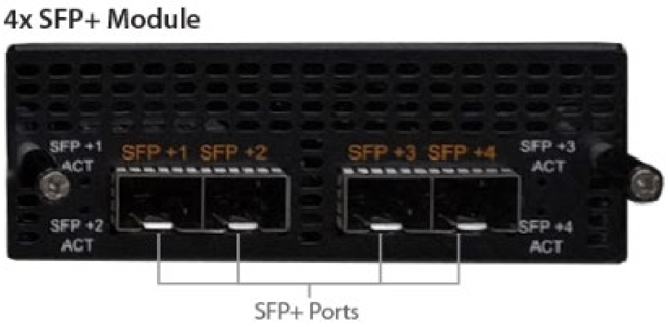
3x LTE-A Module	
Interface	3x Embedded LTE-A Cellular Modems with Redundant SIM Slots

Antenna Connectors	6x SMA Cellular Antenna Connectors 1x SMA GPS Antenna Connector
Power Consumption	20W
Weight	0.83 pounds - 375 grams



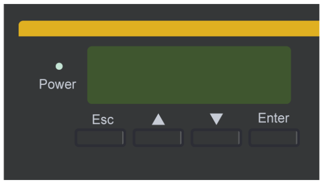
8x GE PoE Module

Interface	8x 10/100/1000M Ethernet Ports Capable of PoE+
Power Consumption	15W (105W max. with 802.3at/af PoE+ Output)
Weight	1.1 pounds 475 grams



4x SFP+ Module	
Interface	4x SFP+ Ports
Power Consumption	11W
Weight	0.83 pounds - 375 grams

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 uptime (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 Transfered (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 11 or above, Mozilla Firefox 24 or above, Apple Safari 7 or above, and Google Chrome 18 or above.

10.2 Constructing the Network

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

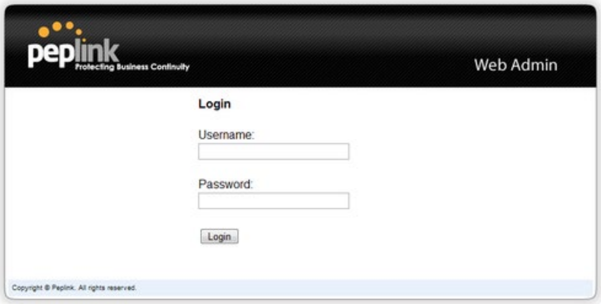
1. With an Ethernet cable, connect a computer to one of the LAN ports on the Peplink Balance. For Peplink Balance models that support multiple connections, repeat with different cables for up to four computers to be connected.
2. With another Ethernet cable, connect the WAN/broadband modem to one of 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

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

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


peplink
Protecting Business Continuity
Web Admin
Login
Username:
Password:
Login
Copyright © Peplink. All rights reserved.

https://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

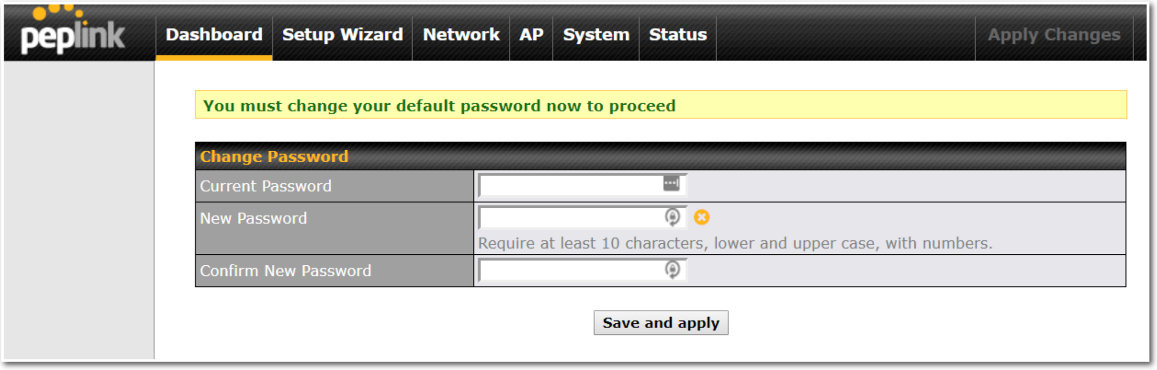
Password: admin

(This is the default admin user login of the Peplink Balance.)

You must change the default password on the first successful logon.

Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.

When HTTP is selected, the URL will be redirected to HTTPS by default.



You must change your default password now to proceed

Change Password	
Current Password	
New Password	Require at least 10 characters, lower and upper case, with numbers.
Confirm New Password	

Save and apply

After successful login, the **Dashboard** of the web admin interface will be displayed.

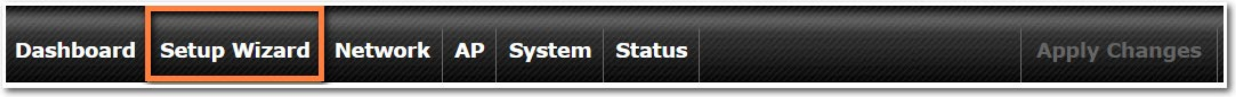
Important Note

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.

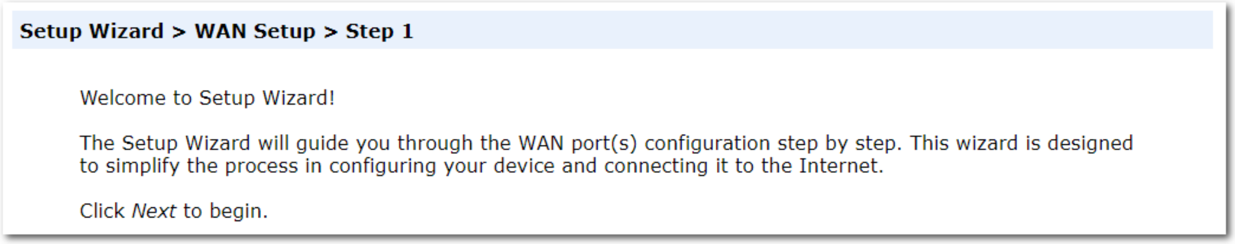
11.2 Configuration with the Setup Wizard

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.



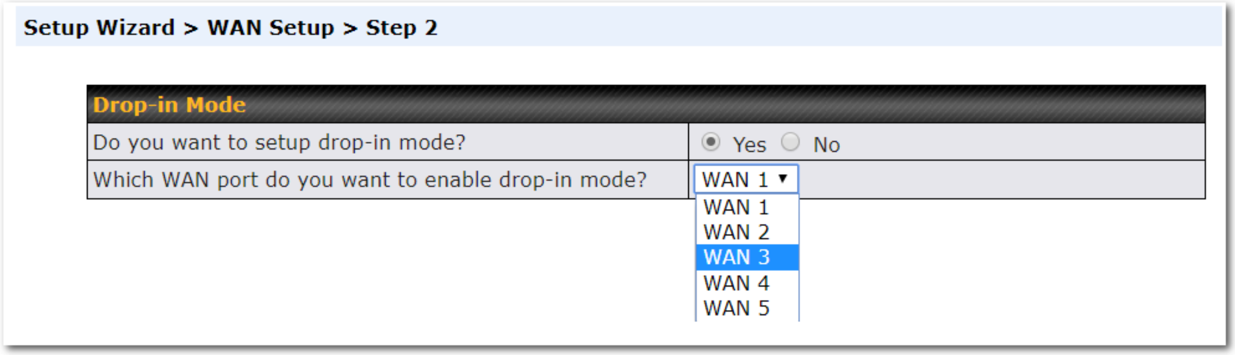
Setup Wizard > WAN Setup > Step 1

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.

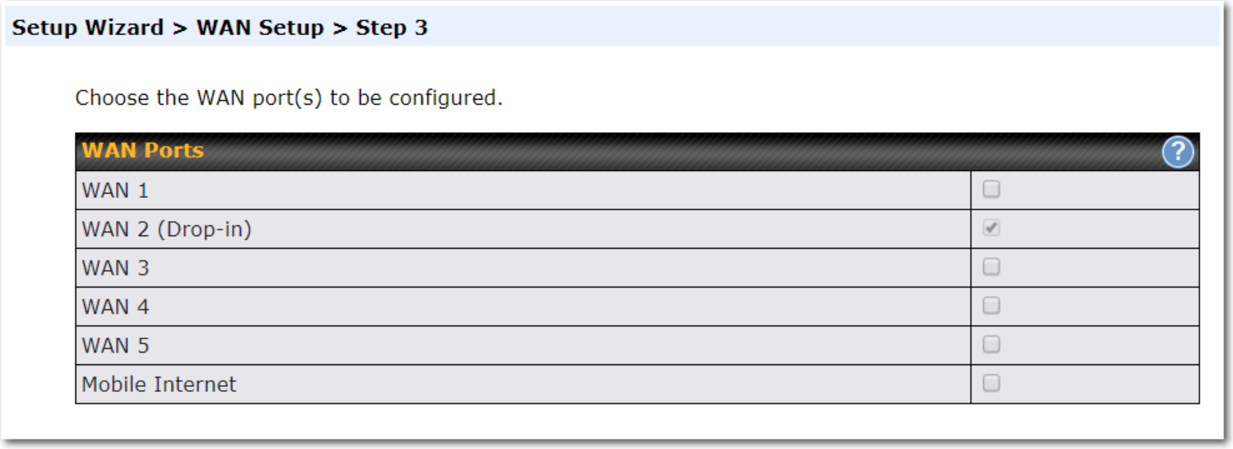
Select **Yes** if you want to set up drop-in mode using the Setup Wizard.



Setup Wizard > WAN Setup > Step 2

Drop-in Mode	
Do you want to setup drop-in mode?	● Yes ○ No
Which WAN port do you want to enable drop-in mode?	WAN 1 ▾

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.

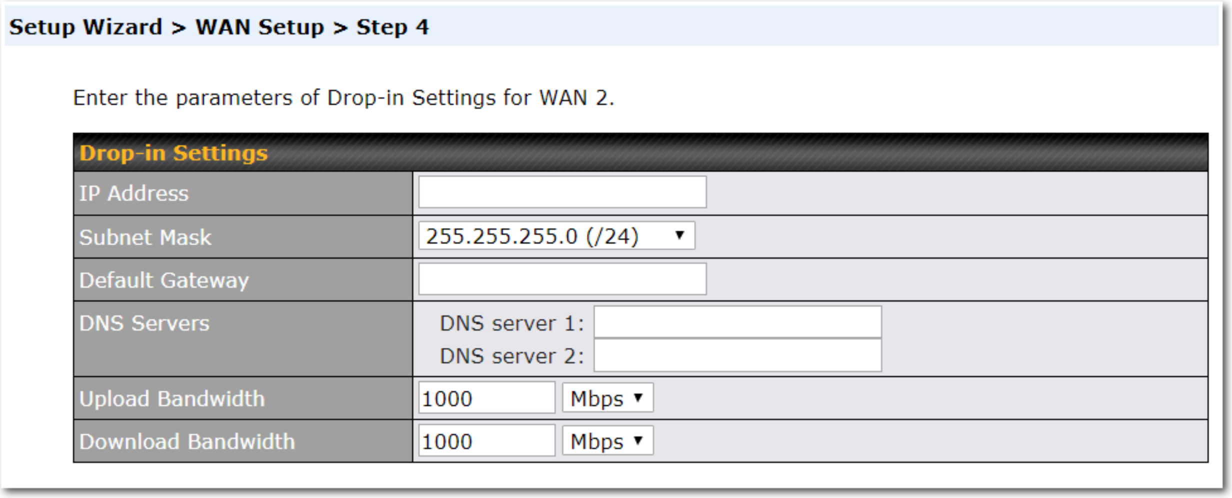


Setup Wizard > WAN Setup > Step 3

Choose the WAN port(s) to be configured.

WAN Ports	
WAN 1	□
WAN 2 (Drop-in)	☑
WAN 3	□
WAN 4	□
WAN 5	□
Mobile Internet	□

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

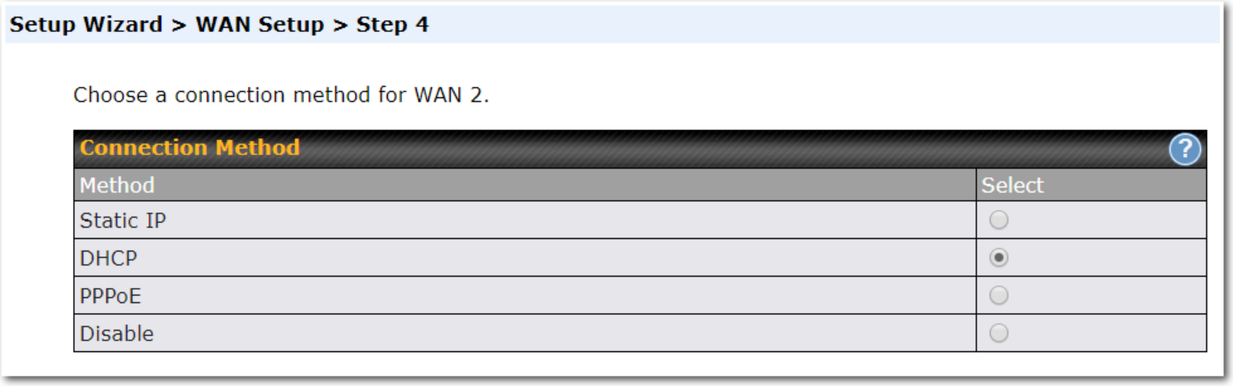


Setup Wizard > WAN Setup > Step 4

Enter the parameters of Drop-in Settings for WAN 2.

Drop-in Settings	
IP Address	
Subnet Mask	255.255.255.0 (/24) ▾
Default Gateway	
DNS Servers	DNS server 1: DNS server 2:
Upload Bandwidth	1000 Mbps ▾
Download Bandwidth	1000 Mbps ▾

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



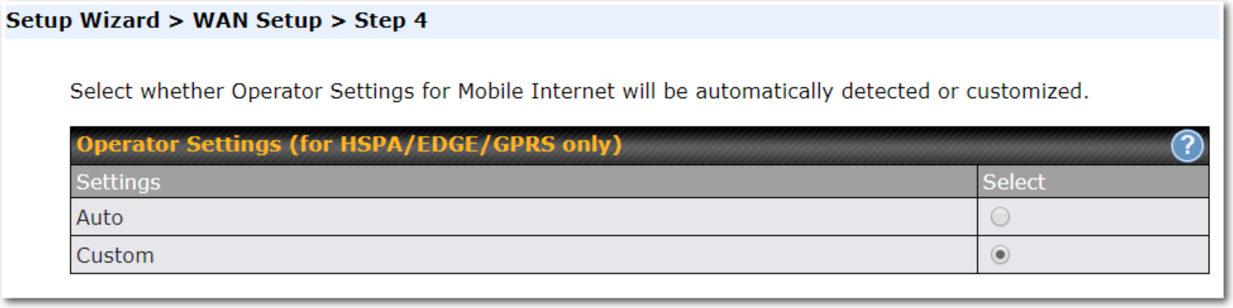
Setup Wizard > WAN Setup > Step 4

Choose a connection method for WAN 2.

Connection Method	
Method	Select
Static IP	○
DHCP	●
PPPoE	○
Disable	○

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**.

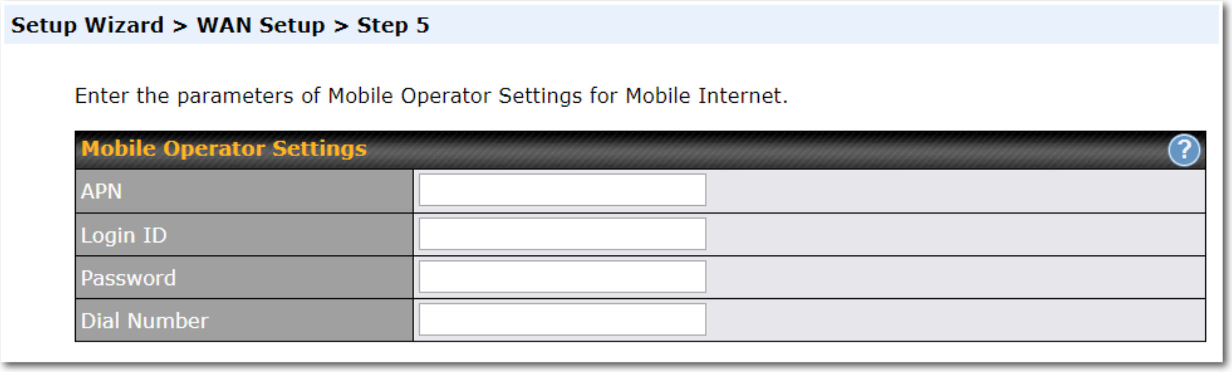


Setup Wizard > WAN Setup > Step 4

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

Operator Settings (for HSPA/EDGE/GPRS only)	
Settings	Select
Auto	○
Custom	●

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.

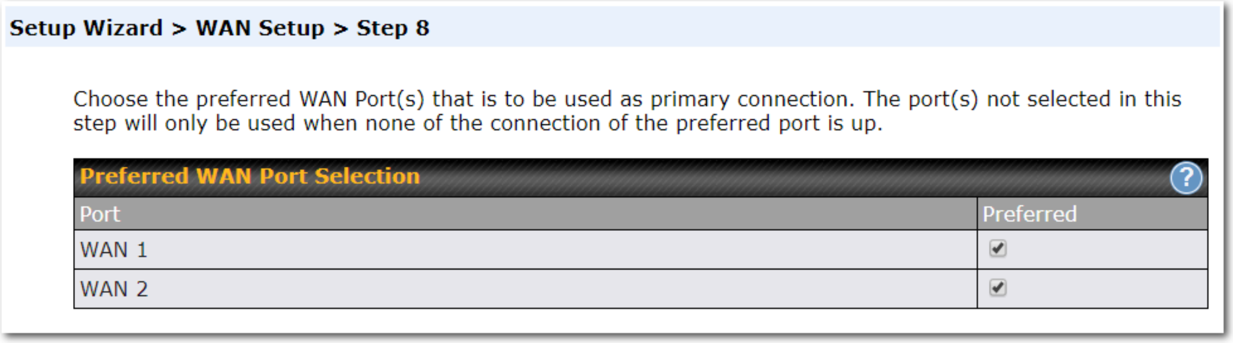


Setup Wizard > WAN Setup > Step 5

Enter the parameters of Mobile Operator Settings for Mobile Internet.

Mobile Operator Settings	
APN	
Login ID	
Password	
Dial Number	

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 a backup only. Click **Next >>** to continue.



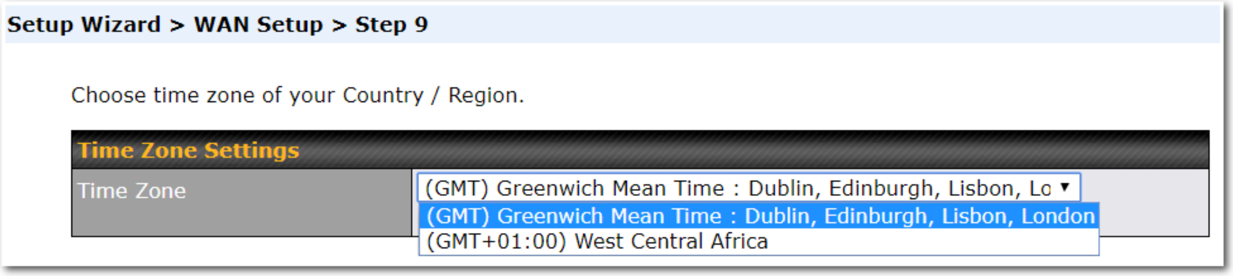
Setup Wizard > WAN Setup > Step 8

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	☑
WAN 2	☑

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



Setup Wizard > WAN Setup > Step 9

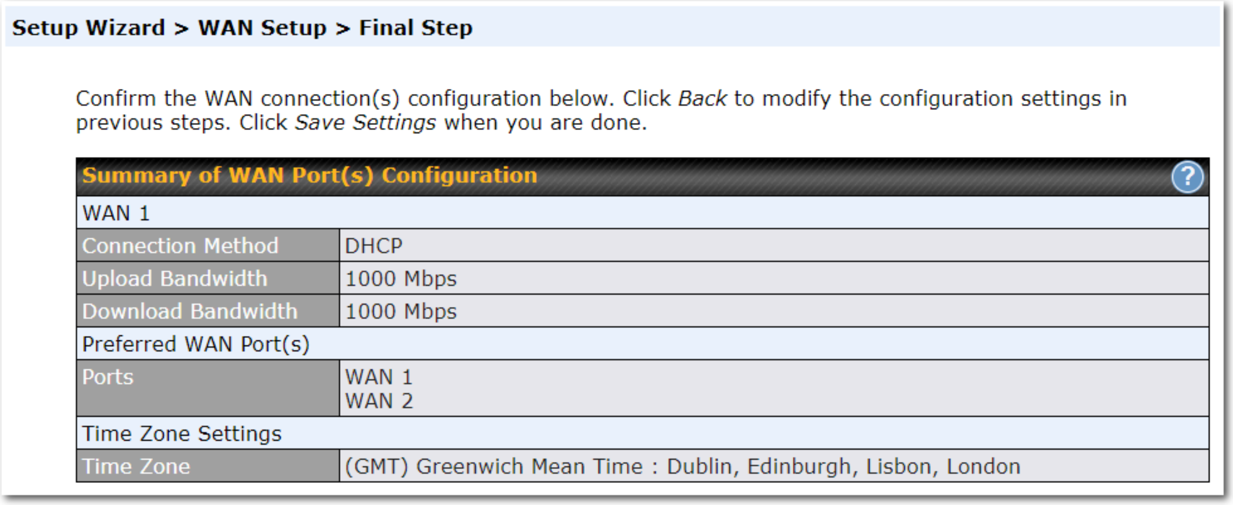
Choose time zone of your Country / Region.

Time Zone Settings

Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lo ▾

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
(GMT+01:00) West Central Africa

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



Setup Wizard > WAN Setup > Final Step

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

Summary of WAN Port(s) Configuration

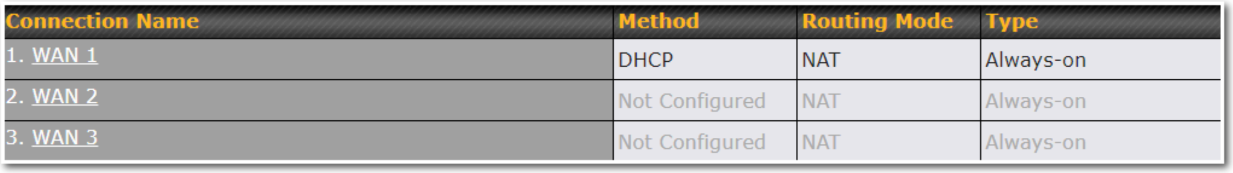
WAN 1	
Connection Method	DHCP
Upload Bandwidth	1000 Mbps
Download Bandwidth	1000 Mbps
Preferred WAN Port(s)	
Ports	WAN 1 WAN 2
Time Zone Settings	
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

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

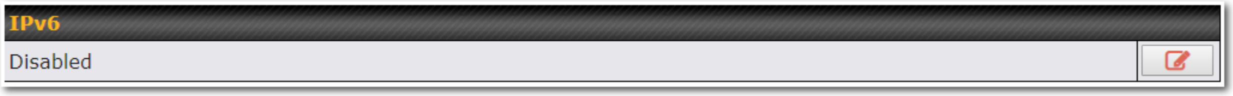
12.1 WAN

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



Connection Name	Method	Routing Mode	Type
1. WAN 1	DHCP	NAT	Always-on
2. WAN 2	Not Configured	NAT	Always-on
3. WAN 3	Not Configured	NAT	Always-on

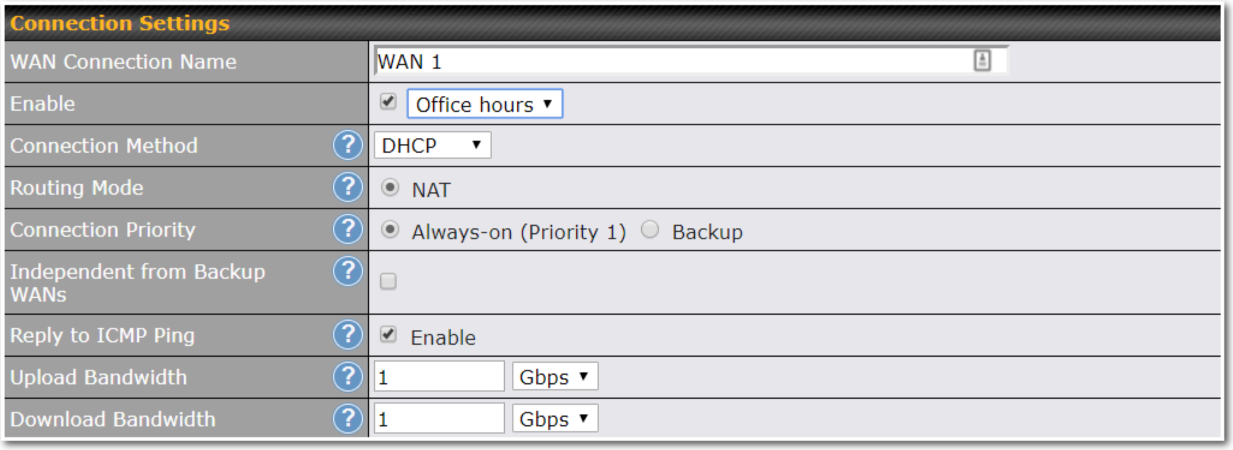
You can also enable IPv6 support in this section



IPv6
Disabled

WAN Connection Settings (Ethernet)

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



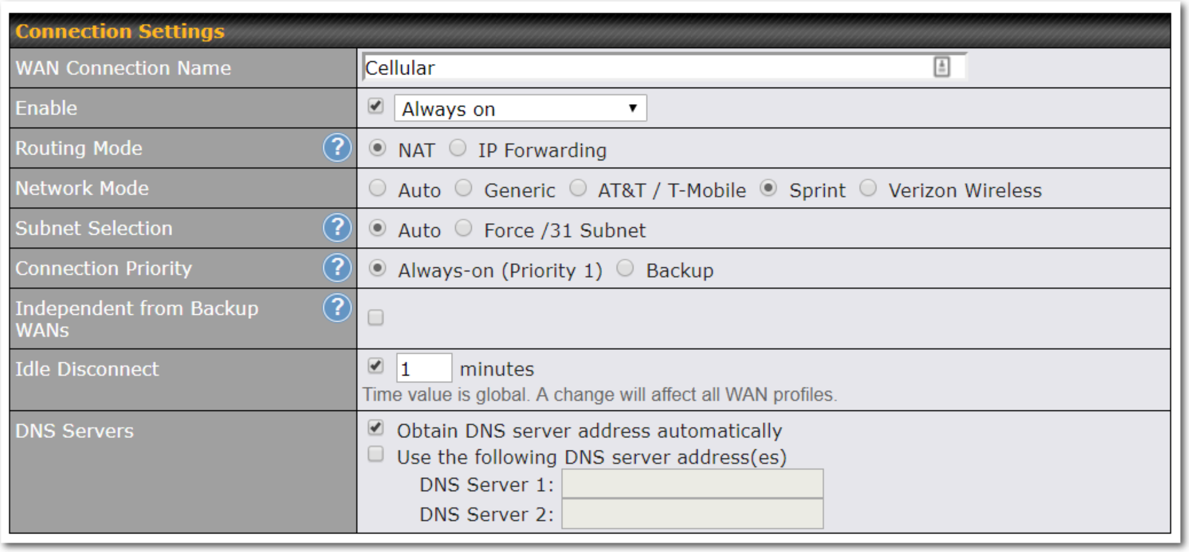
Connection Settings	
WAN Connection Name	WAN 1
Enable	☑ Office hours ▾
Connection Method ?	DHCP ▾
Routing Mode ?	● NAT
Connection Priority ?	● Always-on (Priority 1) ○ Backup
Independent from Backup WANs ?	☐
Reply to ICMP Ping ?	☑ Enable
Upload Bandwidth ?	1 Gbps ▾
Download Bandwidth ?	1 Gbps ▾

WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Enable	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.
Connection Method	There are five possible connection methods for Ethernet WAN: ● **DHCP** ● **Static IP** ● **PPPoE** ● **L2TP** ● **GRE** 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.
Routing Mode	This field shows that **NAT** (network address translation) will be applied to the traffic routed over this WAN connection. **IP Forwarding** is available when you click the link in the help text.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If **Always-on** is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If **Backup** is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Reply to ICMP PING	If the checkbox is **unticked**, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: **ticked** (enabled)
Upload Bandwidth	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.

Download Bandwidth	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)

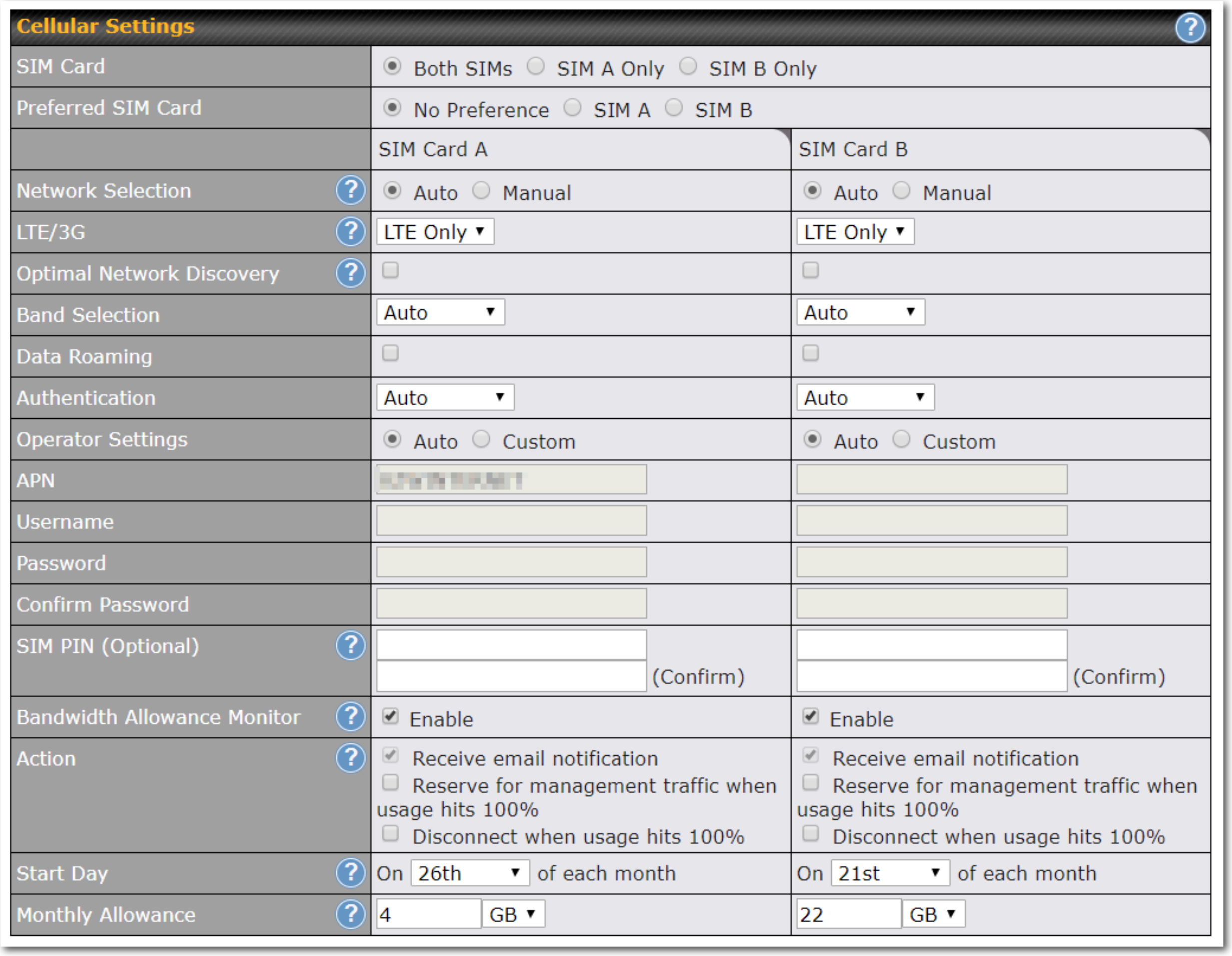
Clicking an Ethernet WAN connection will result in the following screens:



Connection Settings

WAN Connection Name	Cellular
Enable	☑ Always on ▾
Routing Mode	● NAT ○ IP Forwarding
Network Mode	○ Auto ○ Generic ○ AT&T / T-Mobile ● Sprint ○ Verizon Wireless
Subnet Selection	● Auto ○ Force /31 Subnet
Connection Priority	● Always-on (Priority 1) ○ Backup
Independent from Backup WANs	□
Idle Disconnect	☑ 1 minutes Time value is global. A change will affect all WAN profiles.
DNS Servers	☑ Obtain DNS server address automatically □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

Connection Settings	
WAN Connection Name	Indicate a name you wish to give this WAN connection
Enable	Click the checkbox to toggle the on and off state of this connection.
Routing Mode	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding. In the case if you need to choose IP Forwarding for your scenario. Click the ? button to enable IP Forwarding.
Subnet Selection	Choose between: **Auto**: The subnet mask will be set automatically. **Force /31 Subnet**: The subnet mask will be set as 255.255.255.254(/31), and the gateway IP address will be recalculated.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If **Always-on** is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If **Backup** is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Idle Disconnect	If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the 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.



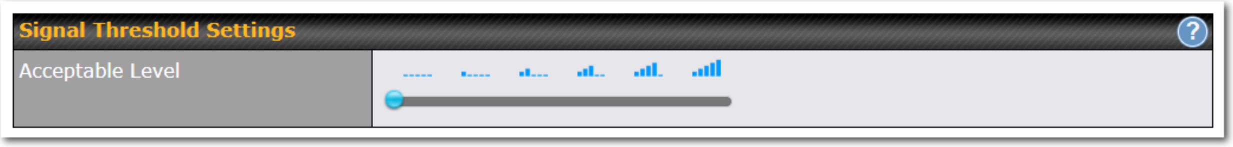
Cellular Settings

SIM Card	● Both SIMs ○ SIM A Only ○ SIM B Only	
Preferred SIM Card	● No Preference ○ SIM A ○ SIM B	
	SIM Card A	SIM Card B
Network Selection	● Auto ○ Manual	● Auto ○ Manual
LTE/3G	LTE Only ▾	LTE Only ▾
Optimal Network Discovery	□	□
Band Selection	Auto ▾	Auto ▾
Data Roaming	□	□
Authentication	Auto ▾	Auto ▾
Operator Settings	● Auto ○ Custom	● Auto ○ Custom
APN	[redacted]	
Username		
Password		
Confirm Password		
SIM PIN (Optional)	(Confirm)	(Confirm)
Bandwidth Allowance Monitor	☑ Enable	☑ Enable
Action	☑ Receive email notification □ Reserve for management traffic when usage hits 100% □ Disconnect when usage hits 100%	☑ Receive email notification □ Reserve for management traffic when usage hits 100% □ Disconnect when usage hits 100%
Start Day	On 26th ▾ of each month	On 21st ▾ of each month
Monthly Allowance	4 GB ▾	22 GB ▾

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

Optimal Network Discovery	Cellular WAsN by default will only handover from 3G to LTE network when there is no active data traffic, enable this option will make it run the handover procedures after fallback to 3G for a defined effective period, even this may interrupt the connectivity for a short while.
Band Selection	When set to **Auto,** band selection allows for automatically connecting to available, supported bands (frequencies) . When set to Manual, you can manually select the bands (frequencies) the SIM will connect to.
Data Roaming	This checkbox enables data roaming on this particular SIM card. When data roaming is enabled this option allows you to select in which countries the SIM has a data connection. The option is configured by using MMC (country) codes.Please check your service provider's data roaming policy before proceeding.
Authentication	Choose from **PAP Only** or **CHAP Only** to use those authentication methods exclusively. Select **Auto** to automatically choose an authentication method.
Operator Settings	This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connections, you may select **Custom** to enter your carrier's **APN**, **Login**, **Password**, and **Dial Number** settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**.
APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Signal Threshold Settings



Signal Threshold Settings

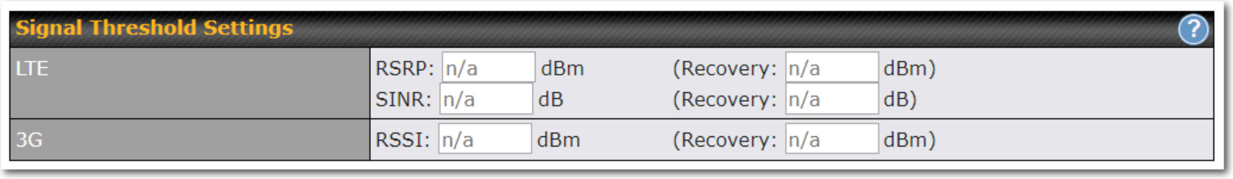
Acceptable Level	

If signal threshold is defined, this connection will be treated as down when a weaker than threshold signal is determined.

The following values are used by the threshold scale:

	0 bars	1 bar	2 bars	3 bars	4 bars	5 bars
LTE / RSSRP	-140	-128	-121	-114	-108	-98
3G / RSSI	-120	-100	-95	-90	-85	-75

To define the threshold manually using specific signal strength values, please click on the question Mark and the following field will be visible.

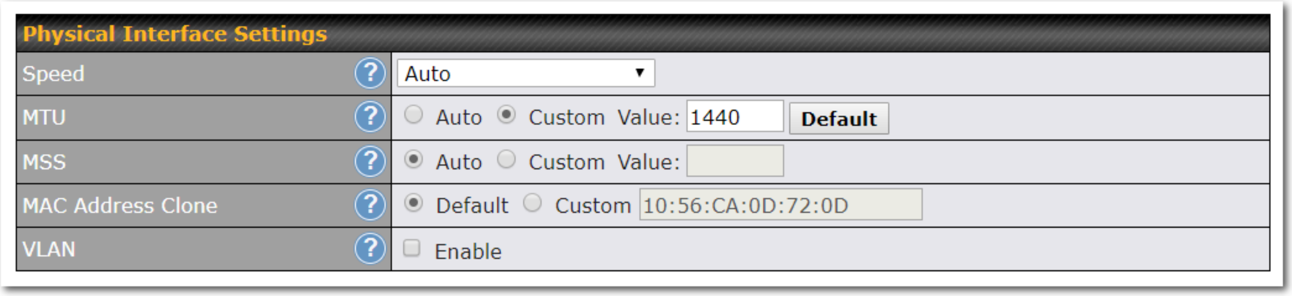


Signal Threshold Settings

LTE	RSRP: n/a dBm SINR: n/a dB	(Recovery: n/a dBm) (Recovery: n/a dB)
3G	RSSI: n/a dBm	(Recovery: n/a dBm)

WAN Connection Settings (Common)

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

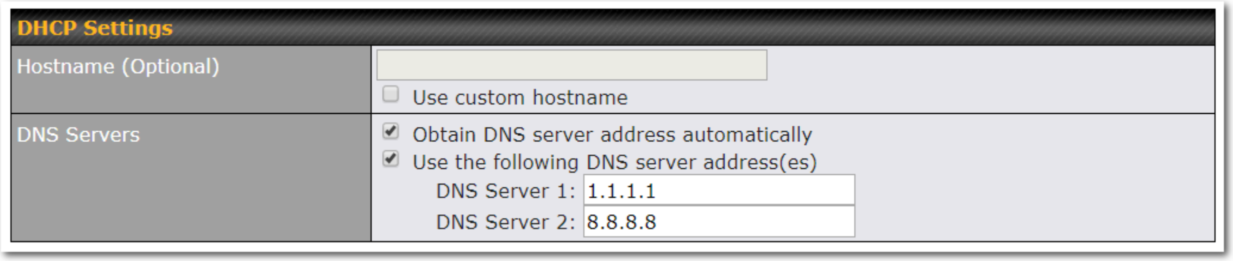


Physical Interface Settings	
Speed	Auto ▾
MTU	○ Auto ● Custom Value: 1440 Default
MSS	● Auto ○ Custom Value:
MAC Address Clone	● Default ○ Custom 10:56:CA:0D:72:0D
VLAN	□ Enable

Physical Interface Settings

Speed	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. 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. Default: Auto
MTU	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. Default value is 1440.
MSS	This field is for specifying the Maximum Segment Size of the WAN connection. 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. Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections. 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. Default: Auto
MAC Address Clone	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.

VLAN	Check the box to assign a VLAN to the interface.



DHCP Settings

Hostname (Optional)	 □ Use custom hostname
DNS Servers	☑ Obtain DNS server address automatically ☑ Use the following DNS server address(es) DNS Server 1: 1.1.1.1 DNS Server 2: 8.8.8.8

DHCP Settings	
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with a hostname, you can safely bypass this option.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the 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.

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.**

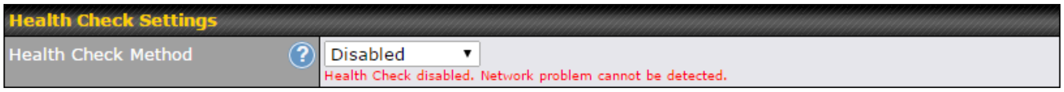
Enable Health Check by selecting PING, DNS Lookup, or HTTP from the Health Check Method drop-down menu.

Health Check Settings

Method

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

Health Check Disabled



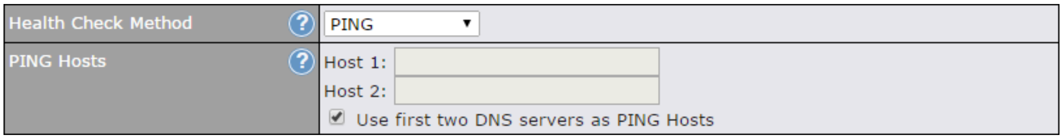
Health Check Settings

Health Check Method: Disabled ▾

Health Check disabled. Network problem cannot be detected.

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

Health Check Method: PING



Health Check Method: PING ▾

PING Hosts: Host 1: Host 2:

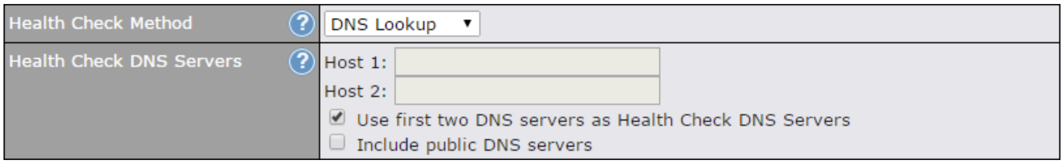
☑ Use first two DNS servers as PING Hosts

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

PING Hosts

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

Health Check Method: DNS Lookup



Health Check Method	DNS Lookup ▾
Health Check DNS Servers	Host 1: Host 2: ☑ Use first two DNS servers as Health Check DNS Servers □ Include public DNS servers

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

Health Check DNS Servers

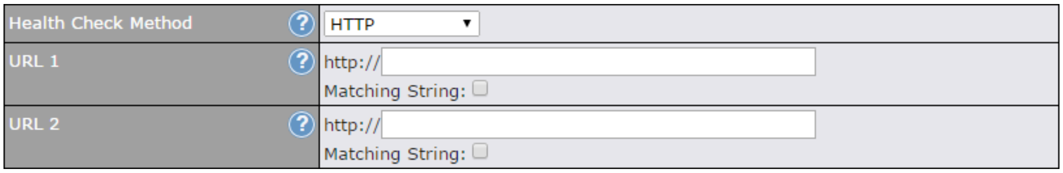
This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS Lookup.

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

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

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

Health Check Method: HTTP



Health Check Method	HTTP ▾
URL 1	http:// Matching String: □
URL 2	http:// Matching String: □

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

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

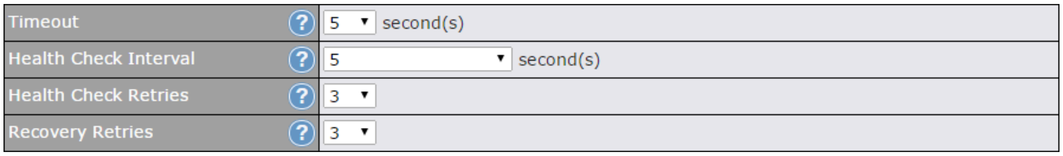
The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass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

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

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

Other Health Check Settings



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

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

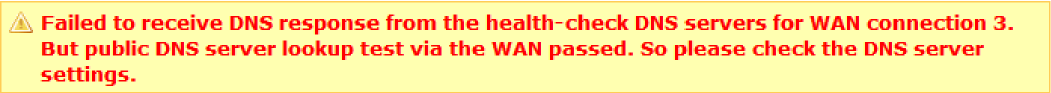
Note

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

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

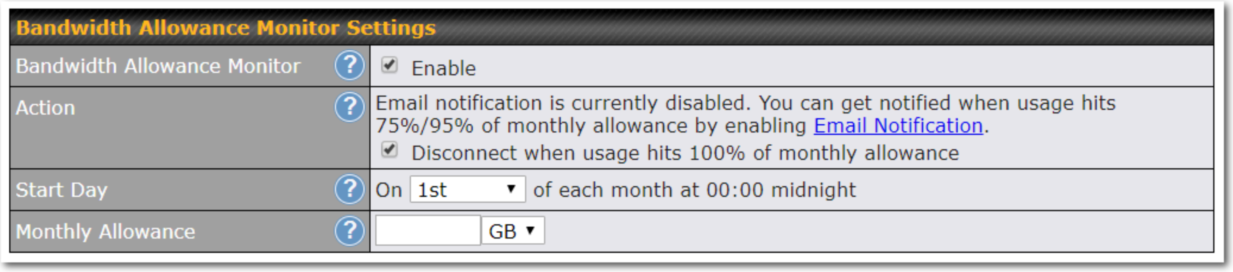
Automatic Public DNS Server Check on DNS Test Failure

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



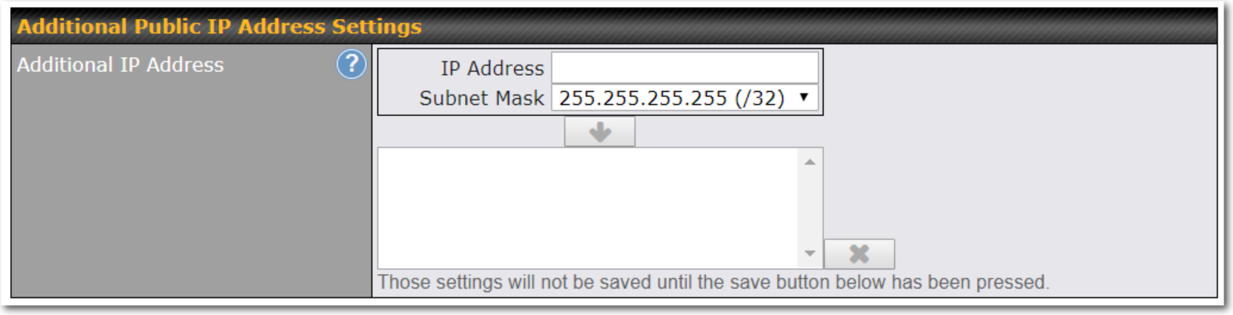
Bandwidth Allowance Monitor Settings	
Bandwidth Allowance Monitor	☑ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st ▾ of each month at 00:00 midnight
Monthly Allowance	GB ▾

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

Disclaimer

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 the use of the numbers shown here.

Additional Public IP Settings



Additional Public IP Address Settings

Additional IP Address

IP Address

Subnet Mask 255.255.255.255 (/32)

Those settings will not be saved until the save button below has been pressed.

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**.

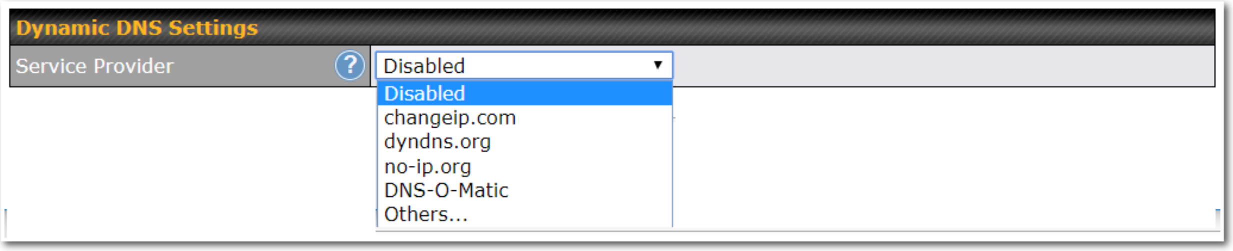
Dynamic DNS Settings

Peplink Balance routers allow 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.

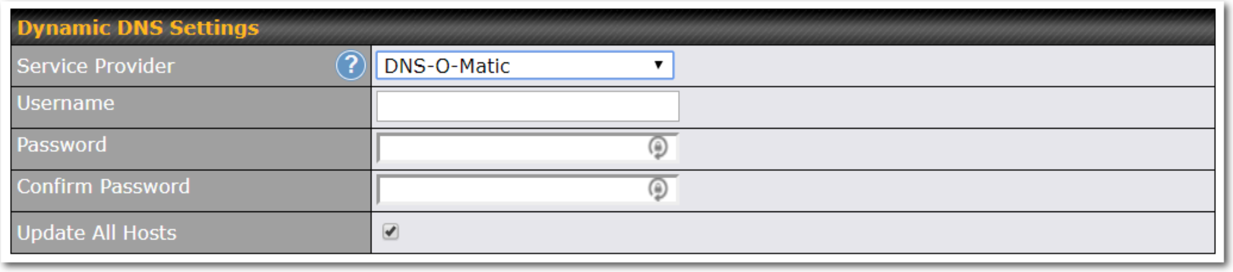
The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network>Interfaces>WAN>*Connection name*>Dynamic DNS Settings**.



Dynamic DNS Settings

Service Provider	Disabled

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



Dynamic DNS Settings	
Service Provider	DNS-O-Matic ▾
Username	
Password	
Confirm Password	
Update All Hosts	☑

Dynamic DNS Settings	
Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are: ● changeip.com ● dyndns.org ● no-ip.org ● tzo.com ● DNS-O-Matic ● Others… support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API. Select **Disabled** to disable this feature.
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.
Password / Pass / TZO Key	This setting specifies the password for the dynamic DNS service.
Update All Hosts	Check this box to automatically update all hosts.
Hosts / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note

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

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

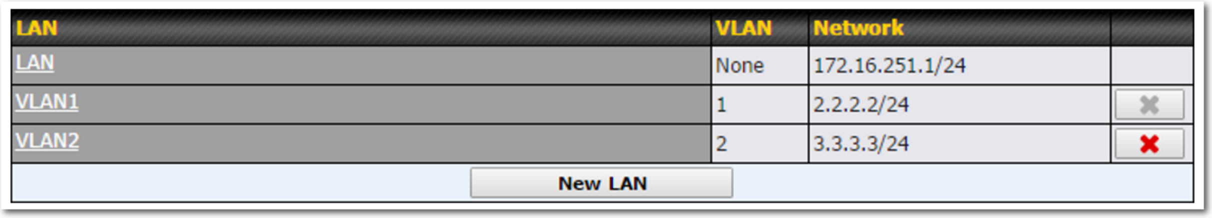
Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been not updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a

WAN's IP address did not change.

12.2 LAN

12.2.1 Network Settings

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

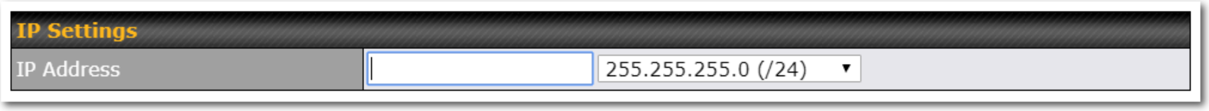


LAN	VLAN	Network	
LAN	None	172.16.251.1/24	
VLAN1	1	2.2.2.2/24	✖
VLAN2	2	3.3.3.3/24	✖

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

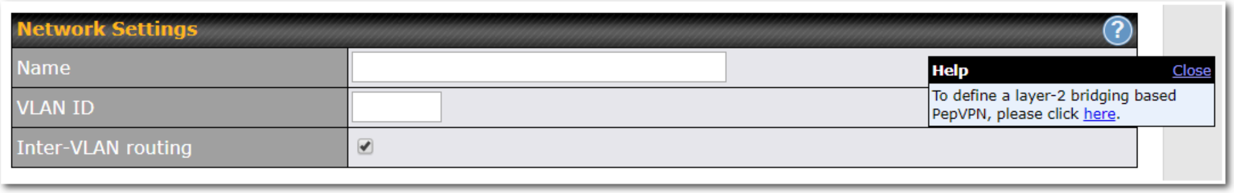
Alternatively, a red "X" means that there are no settings using the VLAN. You can delete that VLAN by clicking the red "X"

Clicking on any of the existing LAN interfaces (or creating a new one) will show the following :



IP Settings	
IP Address	255.255.255.0 (/24) ▾

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

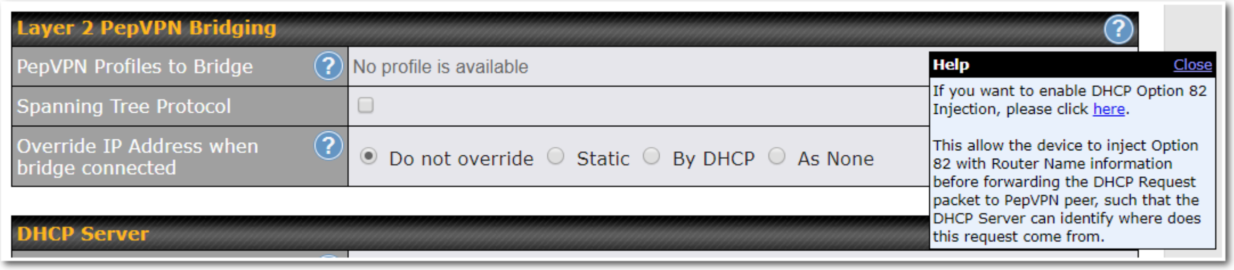


Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☑

Help — Close

To define a layer-2 bridging based PepVPN, please click here.

Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.



Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	No profile is available
Spanning Tree Protocol	□
Override IP Address when bridge connected	● Do not override ○ Static ○ By DHCP ○ As None

DHCP Server

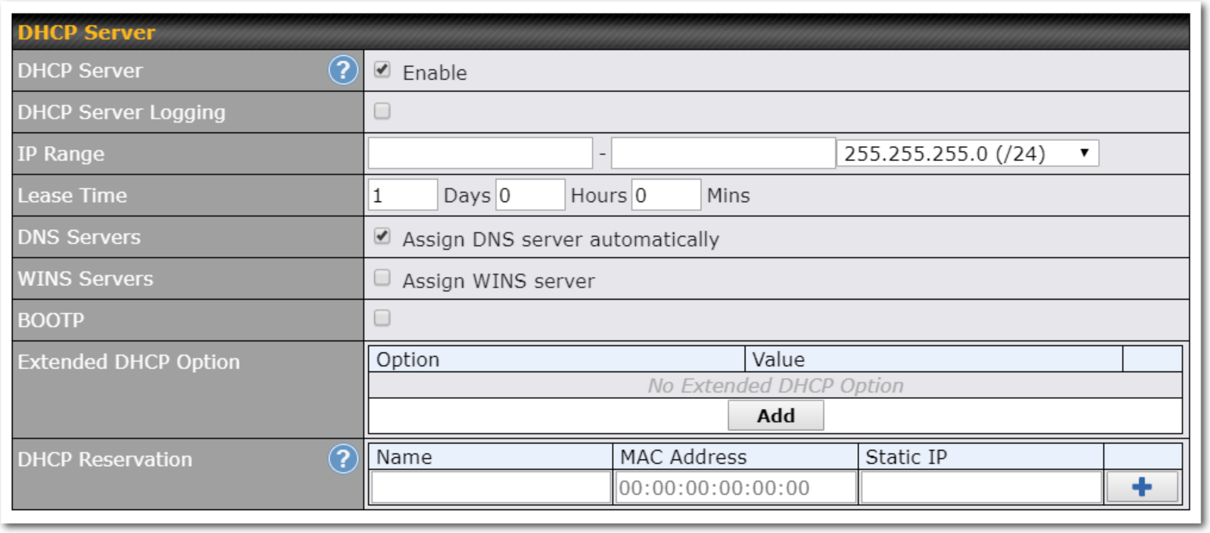
Help — Close

If you want to enable DHCP Option 82 Injection, please click here.

This allow the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to PepVPN peer, such that the DHCP Server can identify where does this request come from.

Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Remote Network Isolation	Enable this option if you want to block network traffic between the remote networks, this will not affect the connectivity between them and this local LAN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
Override IP Address when bridge connected	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.

	If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.
DHCP Option 82	Click on the question Mark if you want to enable DHCP Option 82. This allows the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to a PepVPN peer, such that the DHCP Server can identify where the request originates from.

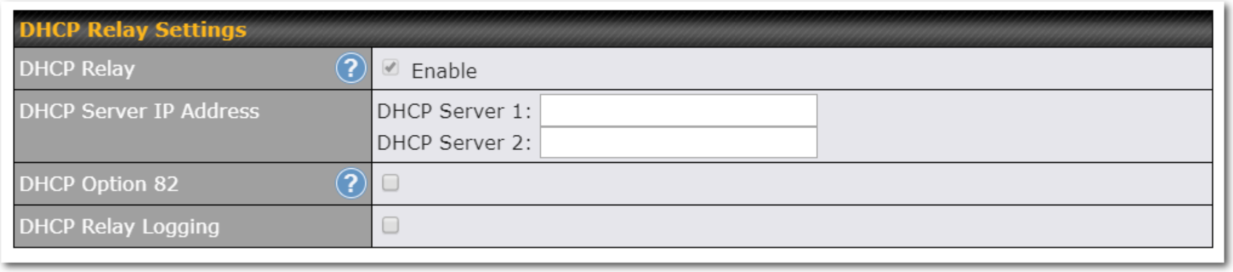


DHCP Server

DHCP Server	☑ Enable
DHCP Server Logging	□
IP Range	- 255.255.255.0 (/24) ▾
Lease Time	1 Days 0 Hours 0 Mins
DNS Servers	☑ Assign DNS server automatically
WINS Servers	□ Assign WINS server
BOOTP	□
Extended DHCP Option	Option | Value *No Extended DHCP Option* Add
DHCP Reservation	Name | MAC Address | Static IP 00:00:00:00:00:00 ✚

DHCP Server Settings	
DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.
DHCP Server Logging	Enable logging of DHCP events in the eventlog by selecting the checkbox.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's

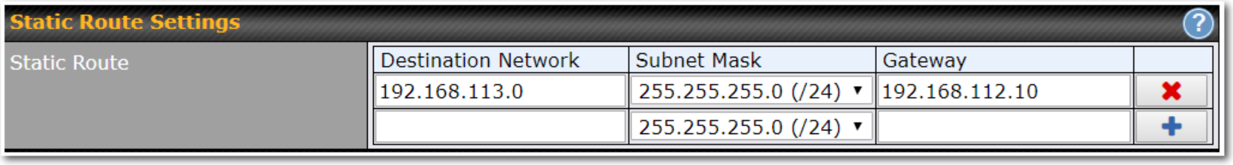
	built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Servers	This option allows you to optionally specify a Windows Internet Name Service (WINS) server. You may choose to use the **built-in WINS server** or **external WINS servers**. When this unit is connected using SpeedFusion^{TM}, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP **WINS Server** setting. Afterward, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press + to create a new record. Press ✖ to remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.**



DHCP Relay Settings	
DHCP Relay ?	☑ Enable
DHCP Server IP Address	DHCP Server 1: DHCP Server 2:
DHCP Option 82 ?	□
DHCP Relay Logging	□

DHCP Relay Settings	
DHCP Relay	Enter the address of the DHCP server here. DHCP requests will be relayed to it.
DHCP Server IP Address	DHCP requests from the LAN are relayed to the entered DHCP server. For active-passive DHCP server configurations, enter active and passive DHCP server IPs into the **DHCP Server 1** and **DHCP Server 2** fields.
DHCP Option 82	This feature includes device information as relay agent for the attached client when forwarding DHCP requests from a DHCP client to a DHCP server. Device MAC address and network name are embedded to circuit ID and Remote ID in option 82.
DHCP Relay Logging	Check this box to log DHCP relay activity.

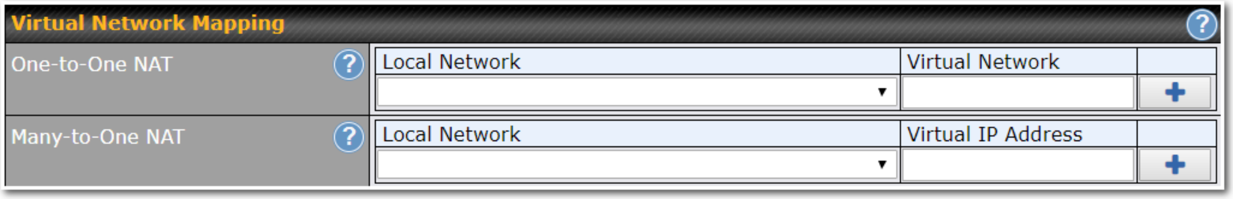
12.2.2 Network Settings (Common Settings)



Static Route Settings

Static Route	Destination Network	Subnet Mask	Gateway	
	192.168.113.0	255.255.255.0 (/24)	192.168.112.10	✖
		255.255.255.0 (/24)		+

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 subnet. Click + to create a new route. Click ✖ to remove a route. Entries in this list will allow traffic to route to a different subnet that is connected to the LAN interface. Any traffic destined for a network/mask pair will be directed to the corresponding gateway instead of routed through WANs.



Virtual Network Mapping

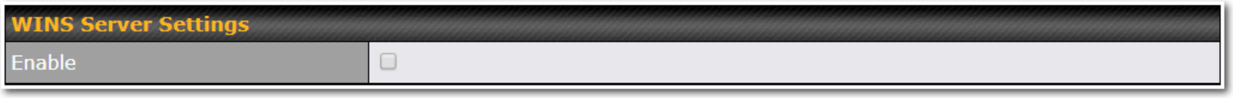
One-to-One NAT	Local Network	Virtual Network	
	▾		✚
Many-to-One NAT	Local Network	Virtual IP Address	
	▾		✚

In case of a network address conflict with remote peers (i.e. PepVPN / IPsec VPN / IP Forwarding WAN are considered as remote connections), you can define Virtual Network Mapping to resolve it.

Note: OSPF & RIPv2 settings should be updated as well to avoid advertising conflicted network.

For further details on virtual network mapping watch this video: https://youtu.be/C1FMdZCn3Z8

Virtual Network Mapping	
One-to-One NAT	Every IP Address in the Local Network has a corresponding unique Virtual IP Address for NAT. Traffic originating from the Local Network to remote connections will be SNAT'ed and behave like coming from the defined Virtual Network. While traffic initiated by remote peers to the Virtual Network will be DNAT'ed accordingly.
Many-to-One NAT	The subnet range defined in Local Network will be mapped to a single Virtual IP Address for NAT. Traffic can only be initiated from local to remote, and these traffic will be NAT'ed and behaves like coming from the same Virtual IP Address.

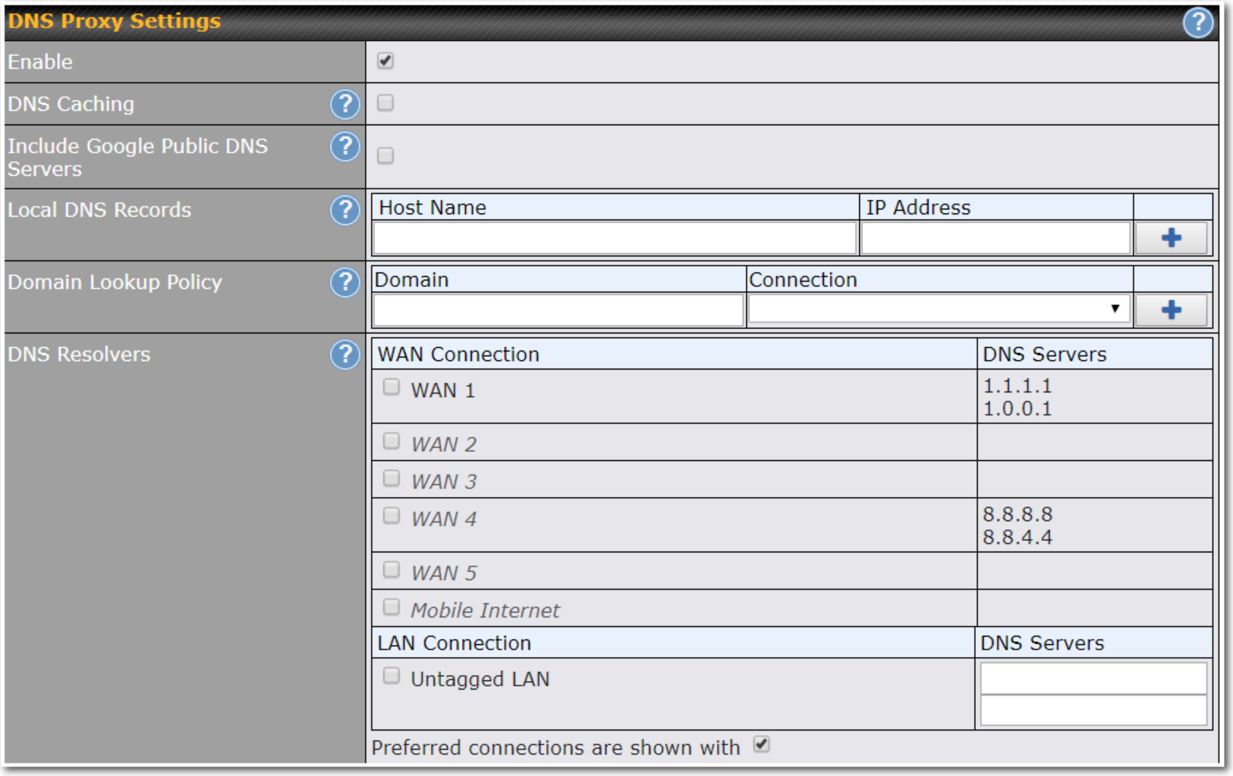


WINS Server Settings

Enable	□

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

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



DNS Proxy Settings

Enable	☑
DNS Caching	☐
Include Google Public DNS Servers	☐
Local DNS Records	Host Name / IP Address / +
Domain Lookup Policy	Domain / Connection ▾ / +
DNS Resolvers	see below

WAN Connection	DNS Servers
☐ WAN 1	1.1.1.1 1.0.0.1
☐ *WAN 2*	
☐ *WAN 3*	
☐ *WAN 4*	8.8.8.8 8.8.4.4
☐ *WAN 5*	
☐ *Mobile Internet*	

LAN Connection	DNS Servers
☐ Untagged LAN	

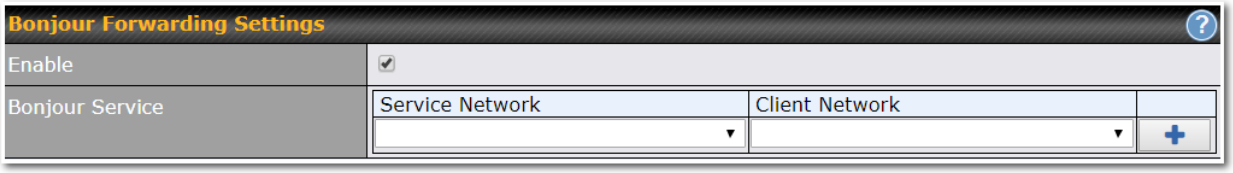
Preferred connections are shown with ☑

DNS Proxy Settings	
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion^{TM} peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN connection.
DNS Caching	This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can improve DNS response time by storing all received DNS results for faster DNS lookup. However, it cannot return the most updated result for frequently updated DNS records. By default, **DNS Caching** is disabled.
Include Google Public DNS Servers	When this option is enabled, the DNS proxy server will forward DNS requests to Google's public DNS servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Peplink Balance, the corresponding IP address will be returned. To display the option to set

	TTL manually, click ?. Click + to create a new record. Click ✖ to remove a record.
Domain Lookup Policy	DNS proxy will look up the domain names defined here using only the specified connections.
DNS Resolvers[A]	Check the box to enable the WINS server. A list of WINS clients will be displayed at **Network>LAN>DNS Proxy Settings>DNS Resolvers**. This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

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

Finally, if needed, configure your Bonjour forwarding settings. Once all settings have been entered, click **Save** to store your changes.



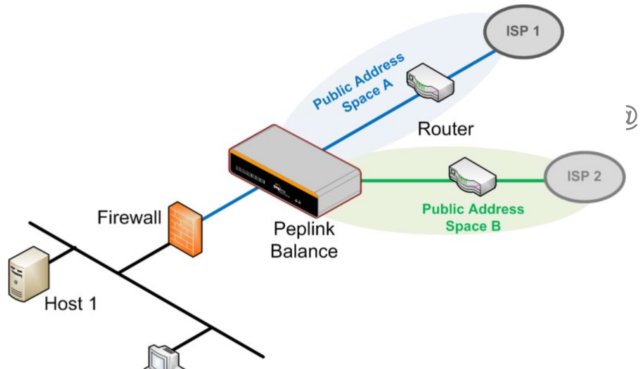
Bonjour Forwarding Settings ?

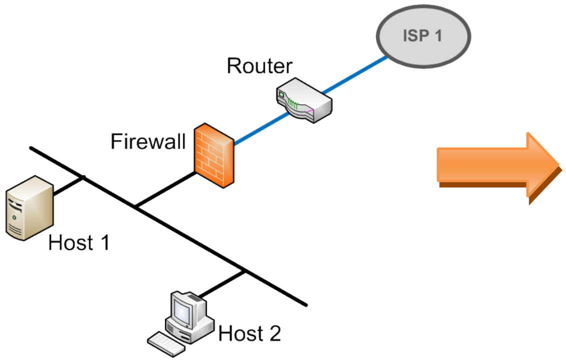
Enable	☑		
Bonjour Service	Service Network	Client Network	
	▾	▾	+

Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	Choose **Service** and **Client** networks from the drop-down menus, and then click + to add the networks. To delete an existing Bonjour listing, click ✖. Bonjour Forwarding is supported on All Balance models, MAX 700, HD2, HD4

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:



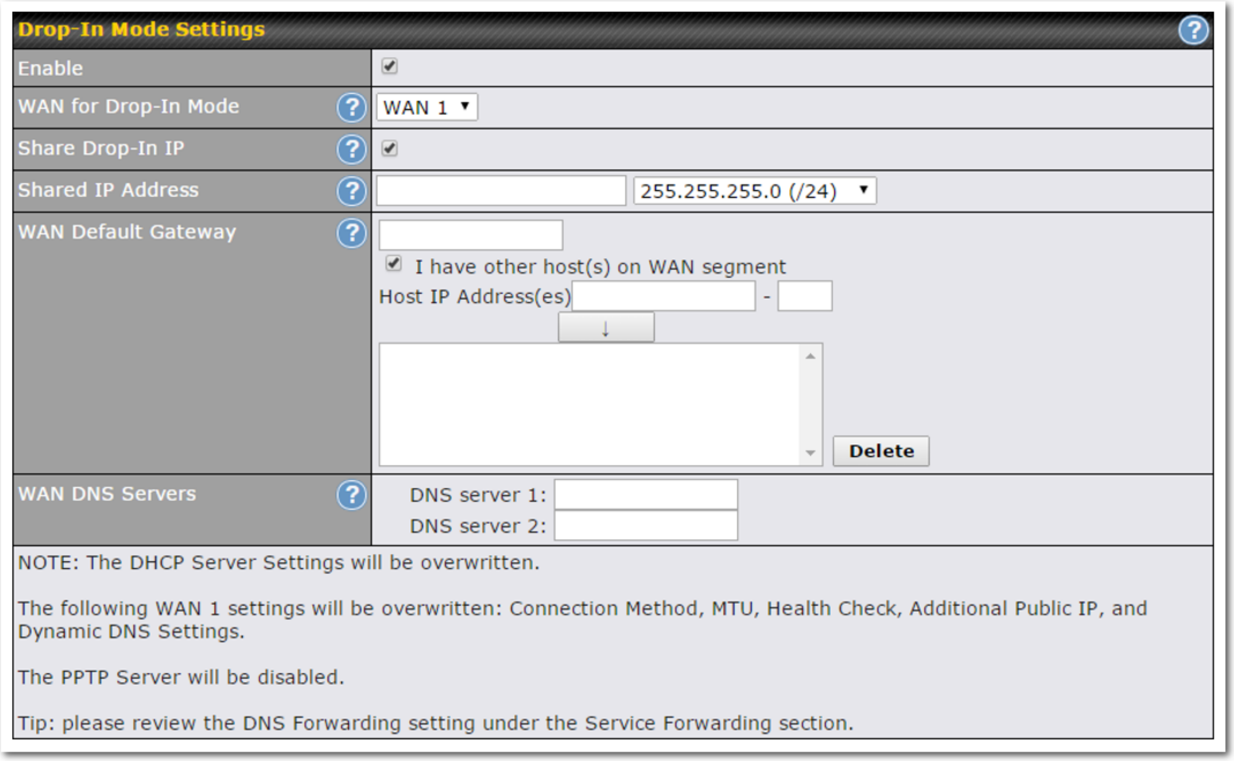


Enable drop-in mode using the Setup Wizard. After enabling this feature and selecting the WAN for drop-in mode, various settings, including the WAN's connection method and IP address, will be automatically updated.

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	☑
WAN for Drop-In Mode	WAN 1 ▾
Share Drop-In IP	☑
Shared IP Address	255.255.255.0 (/24) ▾
WAN Default Gateway	☑ I have other host(s) on WAN segment Host IP Address(es) - ↓ Delete
WAN DNS Servers	DNS server 1: DNS server 2:

NOTE: The DHCP Server Settings will be overwritten.

The following WAN 1 settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.

The PPTP Server will be disabled.

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

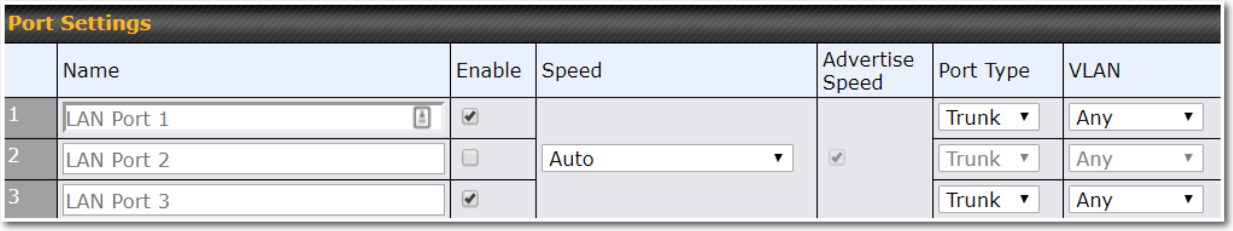
Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of the Peplink Balance on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature. Please refer to **Section 12, Drop-in Mode** for details.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If **WAN 1 with LAN Bypass** is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^{A}	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Balance will listen for this IP address when WAN hosts access services provided by the Balance (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The Balance will listen for this IP address when LAN hosts access services provided by the Balance (web admin access from the WAN, DNS proxy, etc.).
Shared IP Address^{A}	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP

	address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the ? button next to "WAN Default Gateway" and check the I **have other host(s) on WAN segment** box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

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

12.2.3 Port Settings

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



Port Settings

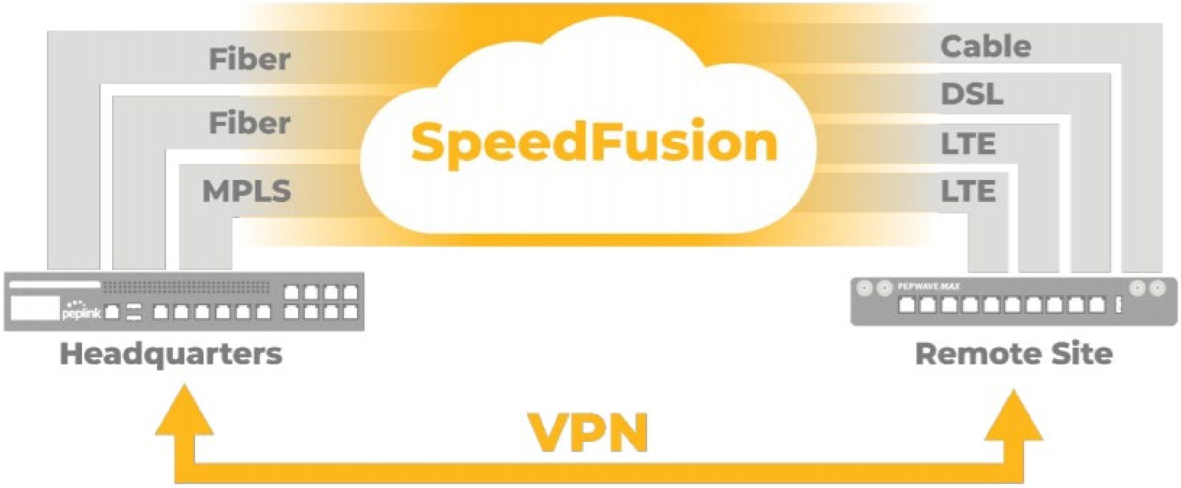
	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port 1	☑	Auto ▾	☑	Trunk ▾	Any ▾
2	LAN Port 2	☐			Trunk ▾	Any ▾
3	LAN Port 3	☑			Trunk ▾	Any ▾

This section allows you to:

- enable or disable specific LAN ports
- Configure the negotiation speed of the LAN ports
- Configure the port type (Trunk or Access)
- Assign a VLAN to a LAN port (in Access mode)

12.3 VPN

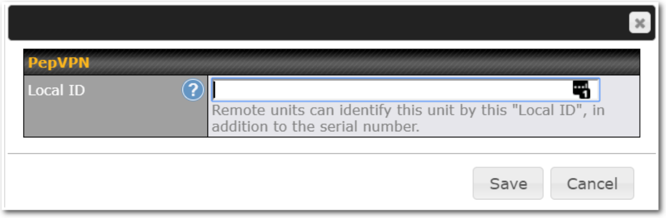
12.3.1 SpeedFusion



Peplink Balance SpeedFusion^{TM} 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.

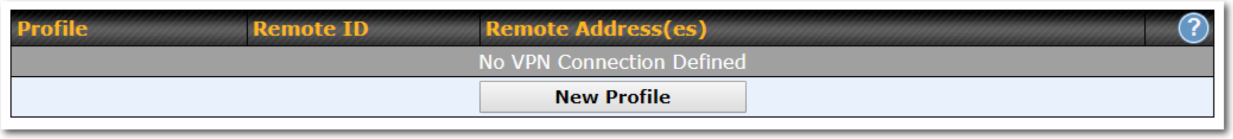
The SpeedFusion^{TM} of the Peplink Balance is specifically designed for multi-WAN environments. With SpeedFusion, in case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic. Peplink Balance routers can bond all WAN connections' bandwidth for routing SpeedFusion^{TM} 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	Remote units can identify this unit by this "Local ID", in addition to the serial number.

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

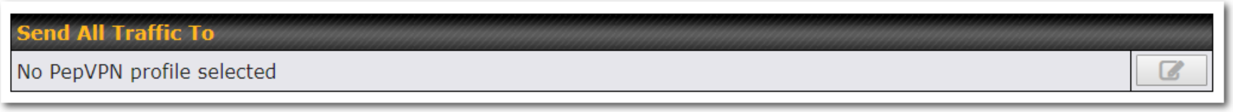


Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		
New Profile		

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.

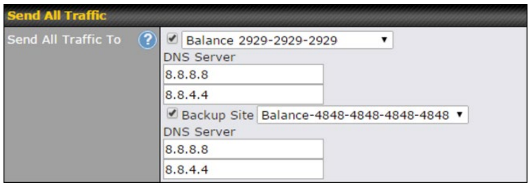


Send All Traffic To

No PepVPN profile selected

Send All Traffic To

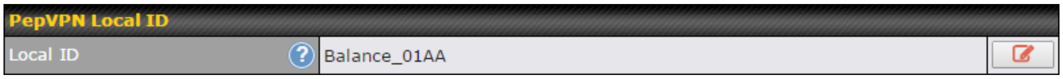
This feature allows you to redirect all traffic to a specified PepVPN connection. Click the ✎ button to select your connection and the following menu will appear:



Send All Traffic

Send All Traffic To: ☑ Balance 2929-2929-2929
DNS Server
8.8.8.8
8.8.4.4
☑ Backup Site Balance-4848-4848-4848-4848
DNS Server
8.8.8.8
8.8.4.4

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

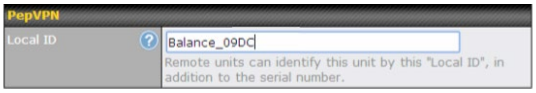


PepVPN Local ID

Local ID: Balance_01AA

PepVPN Local ID

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

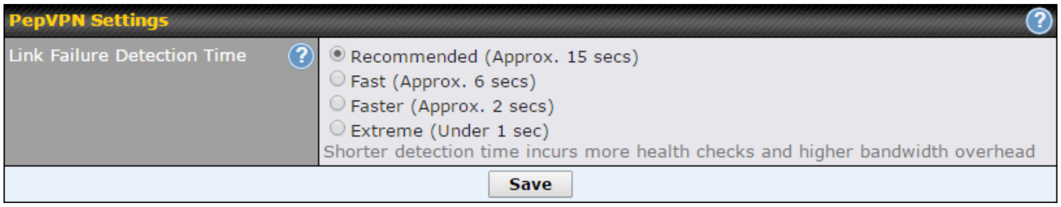


PepVPN

Local ID: Balance_09DC

Remote units can identify this unit by this "Local ID", in addition to the serial number.

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)

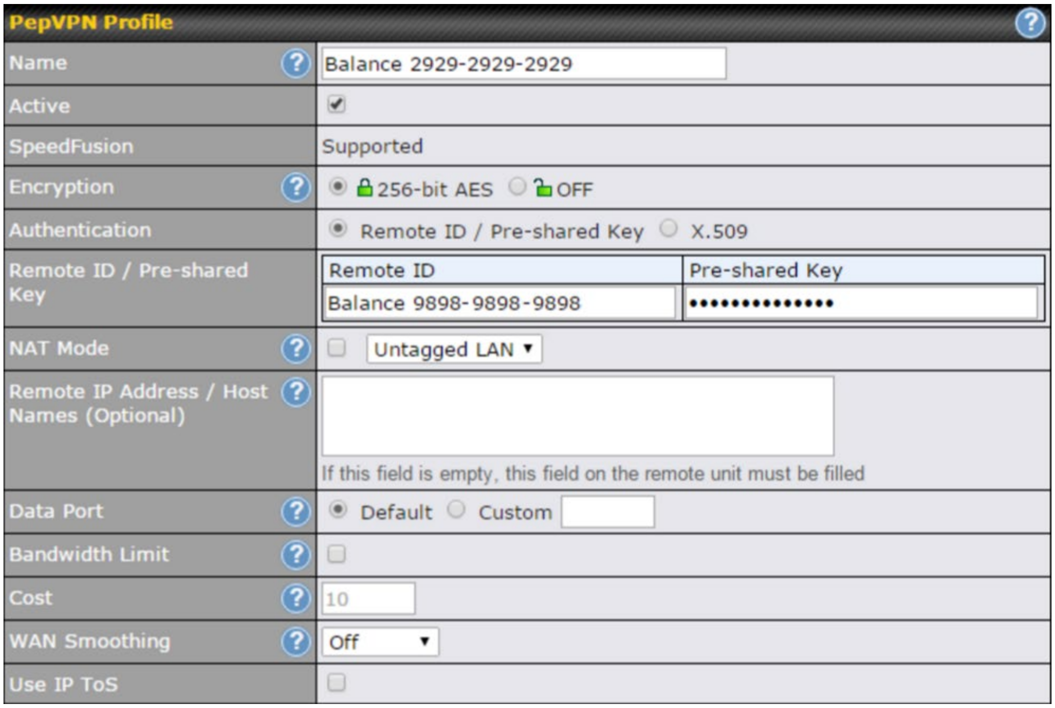
Shorter detection time incurs more health checks and higher bandwidth overhead

Link Failure Detection	
Link Failure Detection Time	The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed. When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds. When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds. When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds. When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

Important Note
Peplink proprietary SpeedFusion^{TM} 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	
Name	Balance 2929-2929-2929
Active	☑
SpeedFusion	Supported
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID: Balance 9898-9898-9898 Pre-shared Key: ••••••••••••••
NAT Mode	□ Untagged LAN ▾
Remote IP Address / Host Names (Optional)	If this field is empty, this field on the remote unit must be filled
Data Port	● Default ○ Custom
Bandwidth Limit	□
Cost	10
WAN Smoothing	Off ▾
Use IP ToS	□

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

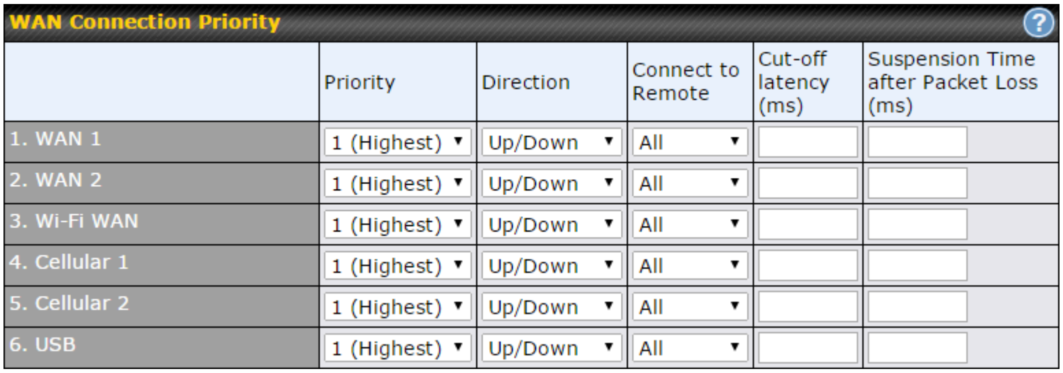
PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ( ). Click the ? icon next to the **PepVPN Profile** title bar to use the IP ToS field of your data packet on PepVPN WAN traffic.
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with **256-bit AES**. If **Off** is selected on both sides of a VPN connection, no encryption will be applied.

Authentication	Select from **By Remote ID Only**, **Preshared Key**, or **X.509** to specify the method the Peplink Balance will use to authenticate peers. When selecting **By Remote ID Only**, be sure to enter a unique peer ID number in the **Remote ID** field.
Remote ID / Pre-shared Key	This optional field becomes available when **Remote ID / Pre-shared Key** is selected as the Peplink Balance's VPN **Authentication** method, as explained above. **Pre-shared Key** defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored. Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the ? icon next to the "Remote ID / Preshared Key" setting.
Remote ID/Remote Certificate	These optional fields become available when **X.509** is selected as the Peplink Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the **Show Details** link below the field.
Allow Shared Remote ID	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When **NAT Mode** is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	If **NAT Mode** is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted. This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established. Click the ? icon to customize the handshake port (TCP)
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If **Default** is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If **Custom** is selected, enter an outgoing port number from 1 to 65535.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10

WAN Smoothing[A]	While using PepVPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN's available bandwidth. 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.

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

To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>*LAN Profile Name***



WAN Connection Priority

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

WAN Connection Priority	
WAN Connection Priority	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.

Peplink also published a whitepaper about Speedfusion which can be downloaded from the following url: http://download.peplink.com/resources/whitepaper-speedfusion-and-best-practices-2019.pdf

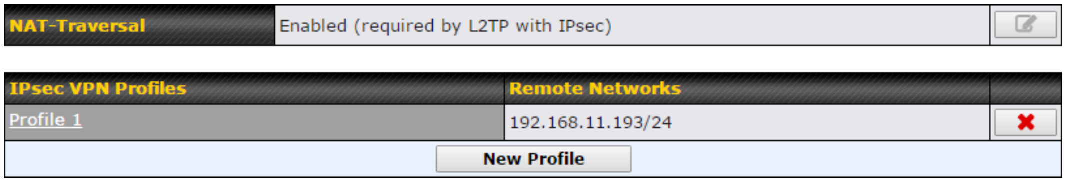
12.3.2 IPsec VPN

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**.



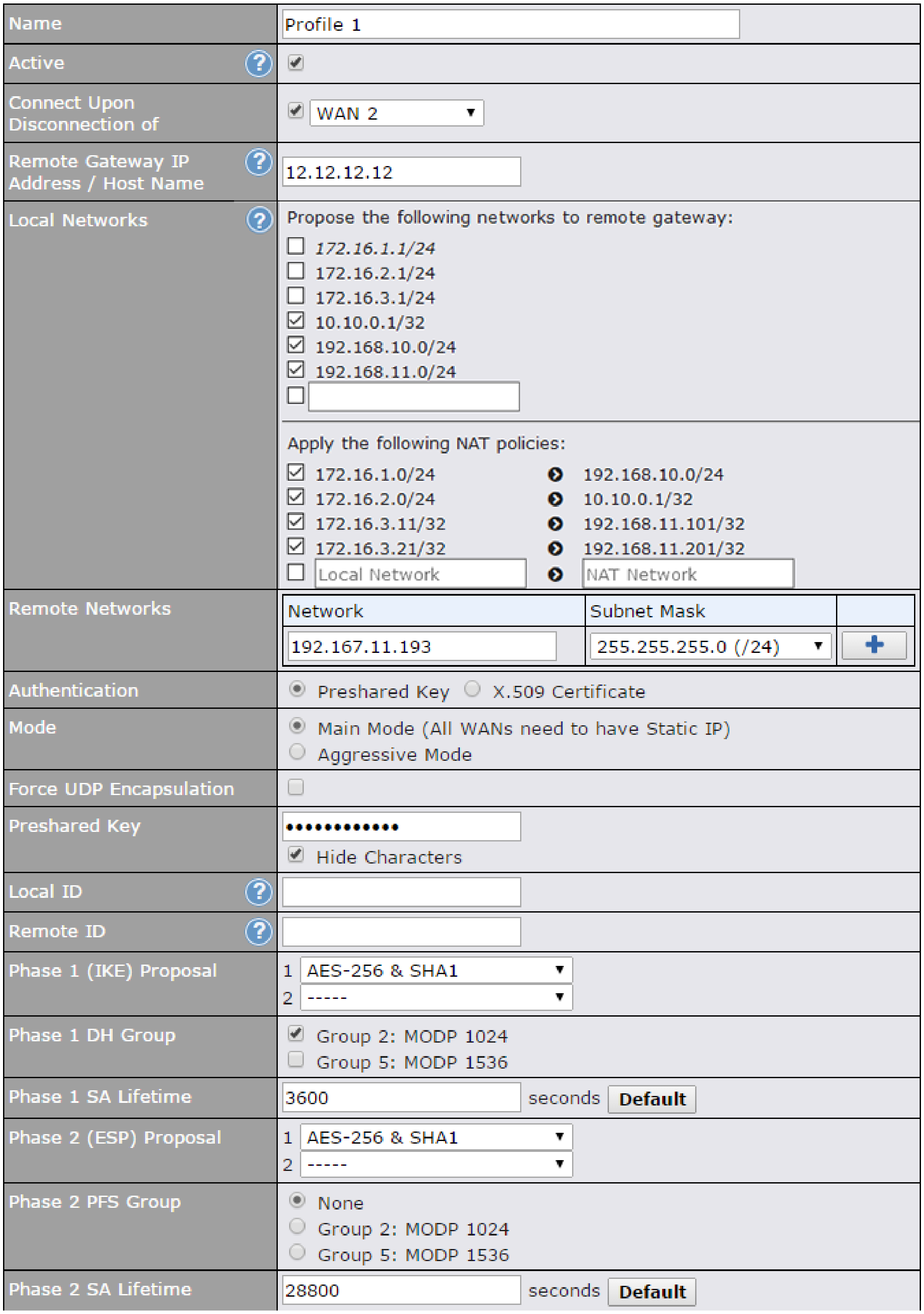
NAT-Traversal	Enabled (required by L2TP with IPsec)

IPsec VPN Profiles	Remote Networks	
Profile 1	192.168.11.193/24	✖

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	☑
Connect Upon Disconnection of	☑ WAN 2 ▼
Remote Gateway IP Address / Host Name	12.12.12.12
Local Networks	Propose the following networks to remote gateway: □ *172.16.1.1/24* □ 172.16.2.1/24 □ 172.16.3.1/24 ☑ 10.10.0.1/32 ☑ 192.168.10.0/24 ☑ 192.168.11.0/24 □ Apply the following NAT policies: ☑ 172.16.1.0/24 ➔ 192.168.10.0/24 ☑ 172.16.2.0/24 ➔ 10.10.0.1/32 ☑ 172.16.3.11/32 ➔ 192.168.11.101/32 ☑ 172.16.3.21/32 ➔ 192.168.11.201/32 □ Local Network ➔ NAT Network
Remote Networks	Network: 192.167.11.193 Subnet Mask: 255.255.255.0 (/24) ▼ +
Authentication	● Preshared Key ○ X.509 Certificate
Mode	● Main Mode (All WANs need to have Static IP) ○ Aggressive Mode
Force UDP Encapsulation	□
Preshared Key	•••••••••••• ☑ Hide Characters
Local ID	
Remote ID	
Phase 1 (IKE) Proposal	1 AES-256 & SHA1 ▼ 2 ----- ▼
Phase 1 DH Group	☑ Group 2: MODP 1024 □ Group 5: MODP 1536
Phase 1 SA Lifetime	3600 seconds Default
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 ▼ 2 ----- ▼
Phase 2 PFS Group	● None ○ Group 2: MODP 1024 ○ Group 5: MODP 1536
Phase 2 SA Lifetime	28800 seconds Default

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

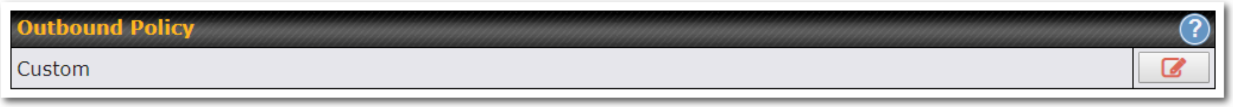
Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate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

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

12.4 Outbound Policy

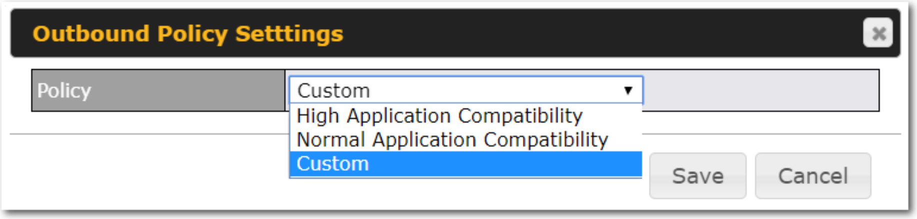
Outbound policies for managing and load balancing outbound traffic are located at

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



Outbound Policy

Custom



Outbound Policy Setttings

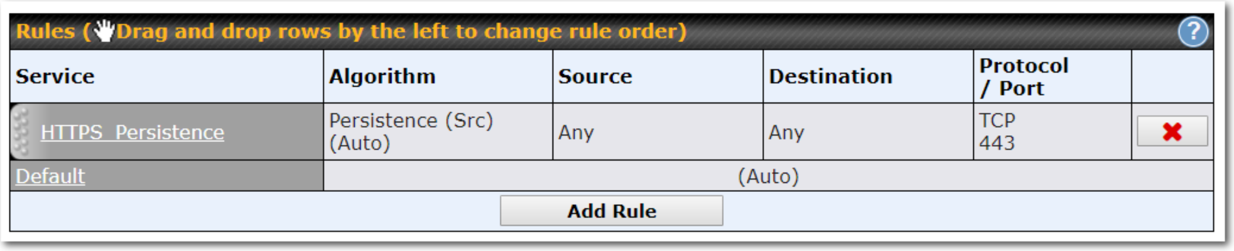
Policy: Custom

High Application Compatibility
Normal Application Compatibility
Custom
Save
Cancel

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

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

The menu underneath enables you to define Outbound policy rules:

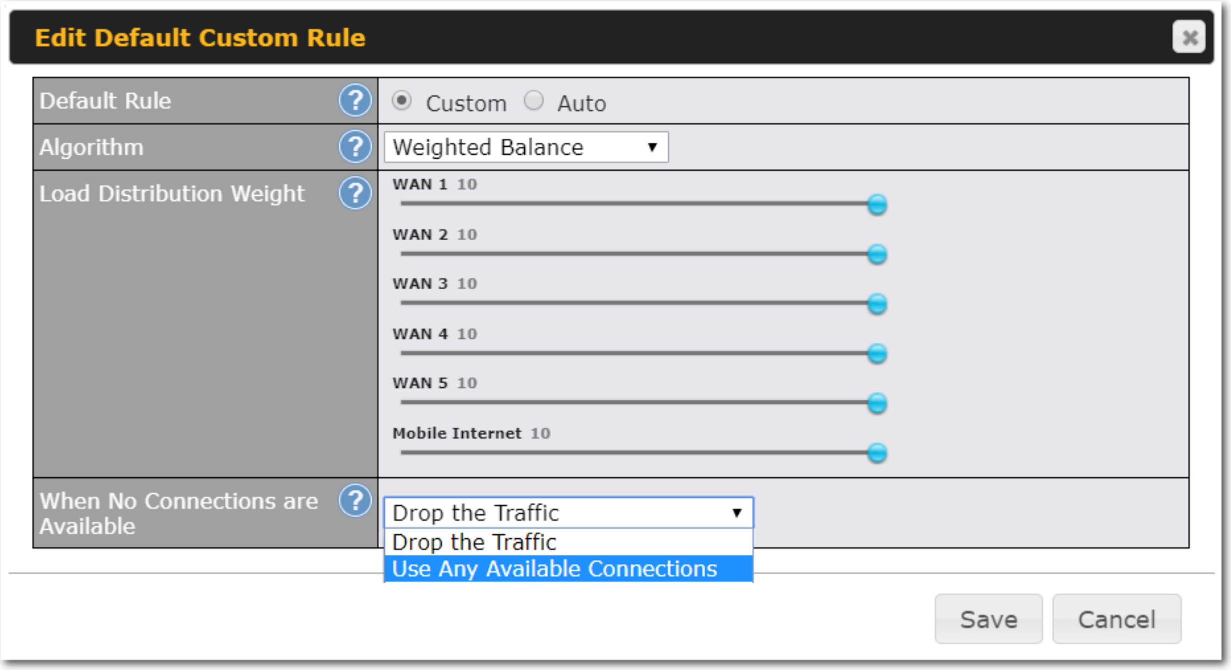


Rules (Drag and drop rows by the left to change rule order)

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

The bottom-most rule is **Default**. Edit this rule to change the device's default manner of controlling outbound traffic for all connections that do not match any of the rules above it. Under the **Service** heading, click **Default** to change these settings.

To rearrange the priority of outbound rules, drag and drop them into the desired sequence.

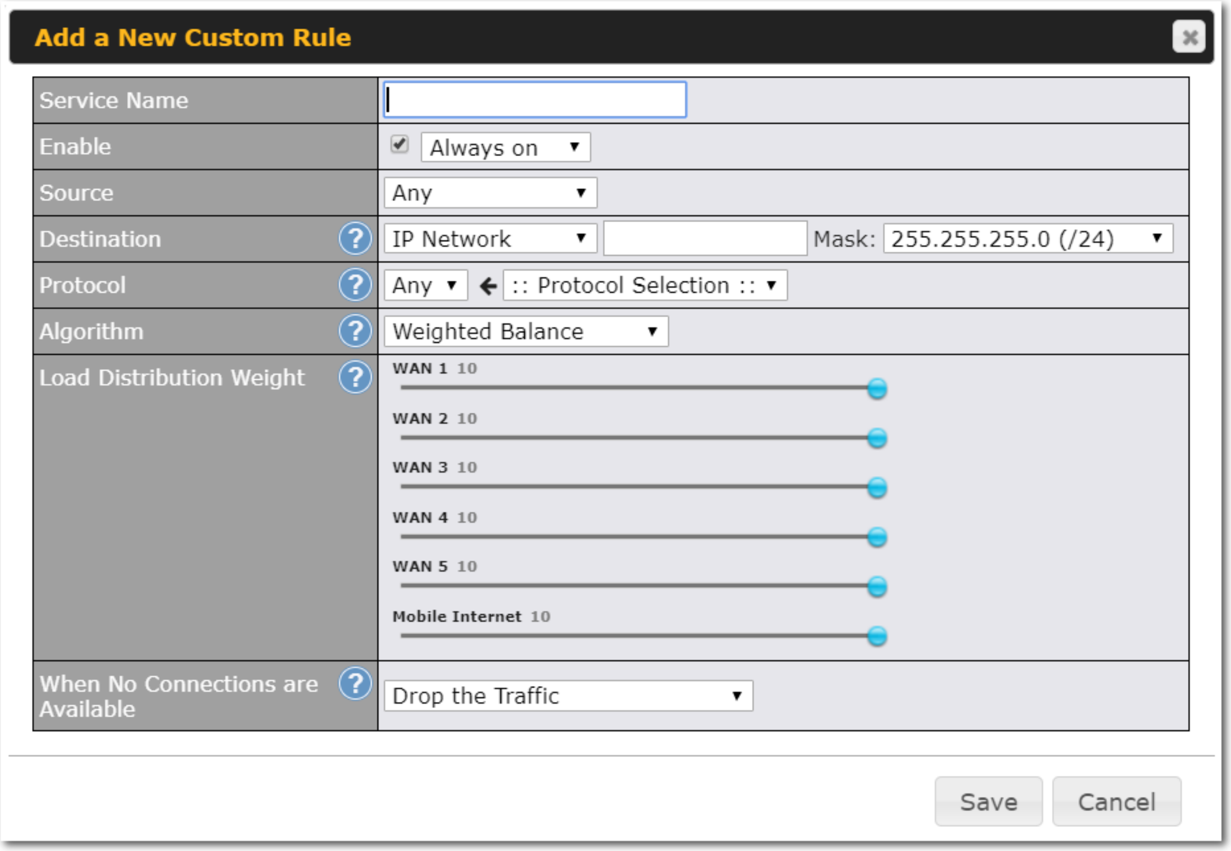


Edit Default Custom Rule

Default Rule	● Custom ○ Auto
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic

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.

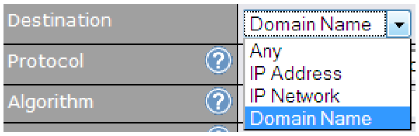
To create a custom rule, click **Add Rule** at the bottom of the table.



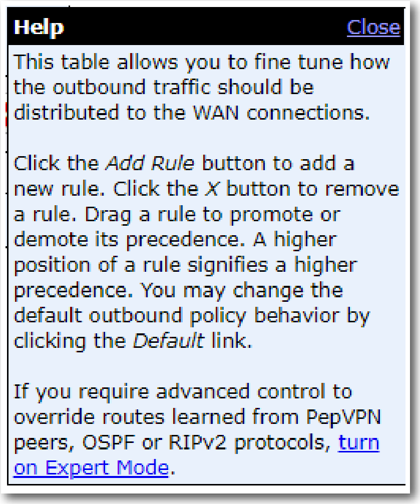
Add a New Custom Rule

Service Name	
Enable	☑ Always on ▾
Source	Any ▾
Destination	IP Network ▾ Mask: 255.255.255.0 (/24) ▾
Protocol	Any ▾ ← :: Protocol Selection :: ▾
Algorithm	Weighted Balance ▾
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic ▾

New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	This setting specifies whether the outbound traffic rule takes effect. When **Enable** is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When **Enable** is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.
Source	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.
Destination	This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.

	 Destination Protocol Algorithm Domain Name Any IP Address IP Network Domain Name If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (.*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *foobar.*,* for example, *www.foobar.com*, *www.foobar.co.jp*, or *foobar.co.uk* will also match. Placing wildcards in any other position is not supported. NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, access to any one of the server names will also match this rule.
Protocol and Port	This setting specifies the IP protocol and port of traffic that matches this rule.
Algorithm	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): ● Weighted Balance ● Persistence ● Enforced ● Priority ● Overflow ● Least Used ● Lowest Latency ● Fastest Response Time For a full explanation of each Algorithm, please see the following article: https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithmns-work/8059
Load Distribution Weight	This is to define the outbound traffic weight ratio for each WAN connection.
Terminate Sessions on Link Recovery	This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the **Weighted, Persistence**, and **Priority** algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.

When No connections are available	This field allows you to configure the default action when all the selected Connections are not available. **Drop the Traffic** - Traffic will be discarded. **Use Any Available Connections** - Traffic will be routed to any available Connection, even it is not selected in the list. **Fall-through to Next Rule** - Traffic will continue to match next Outbound Policy rule just like this rule is inactive.



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

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

If you require advanced control to override routes learned from PepVPN peers, OSPF or RIPv2 protocols, turn on Expert Mode.

Expert Mode is available on some Pepwave routers for use by advanced users. To enable the feature, click on the help icon and click **turn on Expert Mode**.

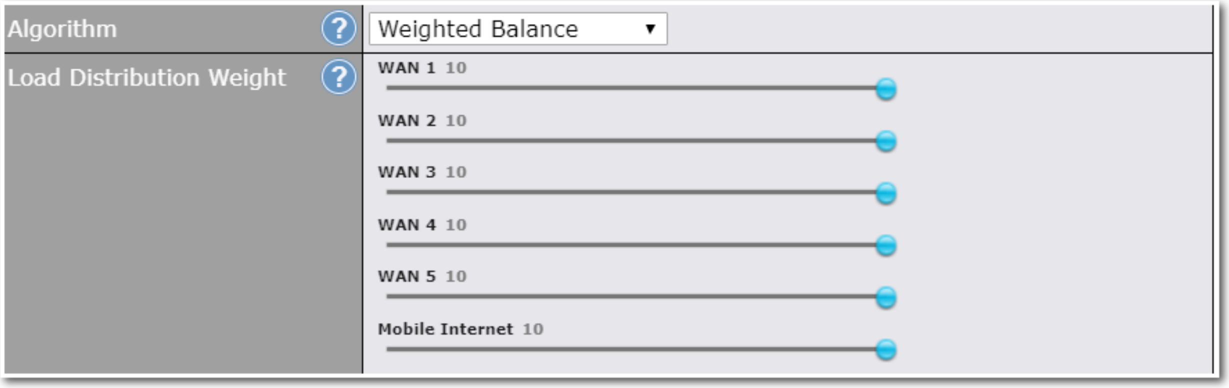
In Expert Mode, a new special rule, **SpeedFusion^{TM} Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion^{TM} routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets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

above the bar to override the SpeedFusion^{TM} routes.

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

Algorithm: Weighted Balance

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



Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10

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

For example, with the following weight settings:

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

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

Matching traffic distributed to Ethernet WAN1 is 16.7% = (10 / 60 x 100%.

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

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

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

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

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

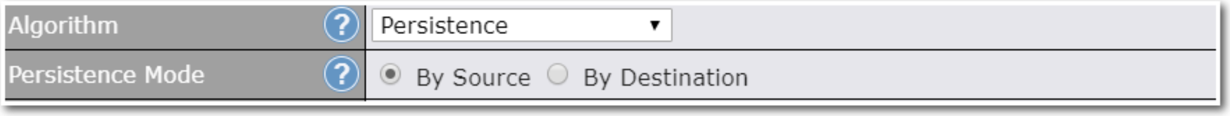
Algorithm: Persistence

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

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

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

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



Algorithm	Persistence ▾
Persistence Mode	● By Source ○ By Destination

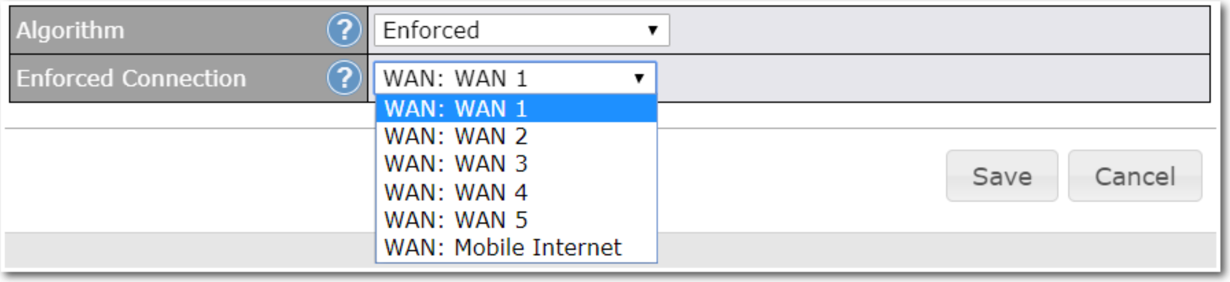
There are two persistent modes: **By Source** and **By Destination**.

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

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

Algorithm: Enforced

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



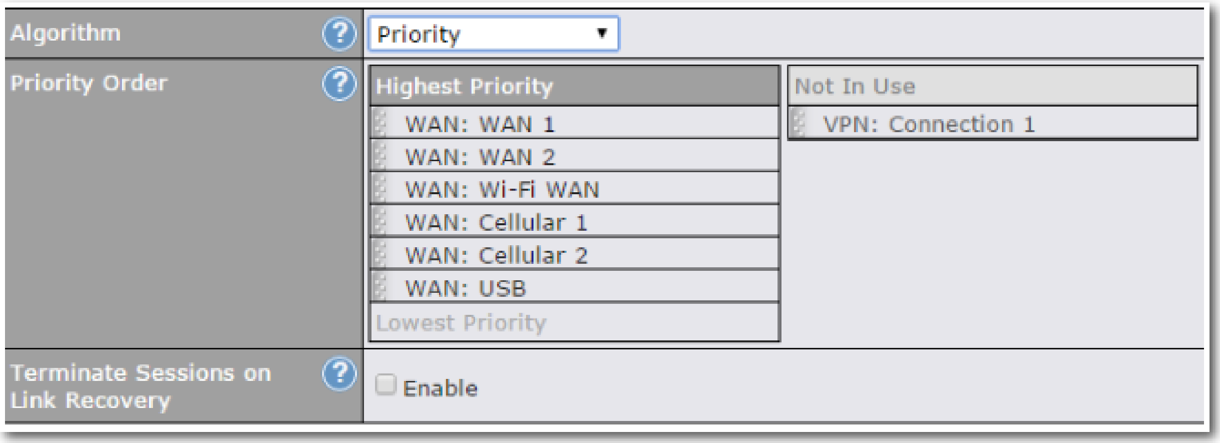
Algorithm	Enforced ▾
Enforced Connection	WAN: WAN 1 ▾

Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Outbound traffic can be also be enforced to go through a specified SpeedFusion™

connection.

Algorithm: Priority

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



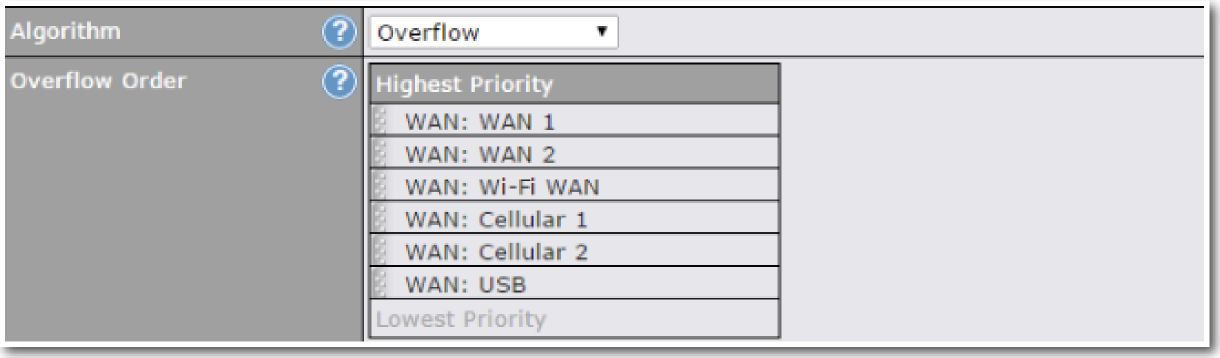
Algorithm	Priority ▾
Priority Order	**Highest Priority** WAN: WAN 1 WAN: WAN 2 WAN: Wi-Fi WAN WAN: Cellular 1 WAN: Cellular 2 WAN: USB Lowest Priority **Not In Use** VPN: Connection 1
Terminate Sessions on Link Recovery	□ Enable

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

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

Algorithm: Overflow

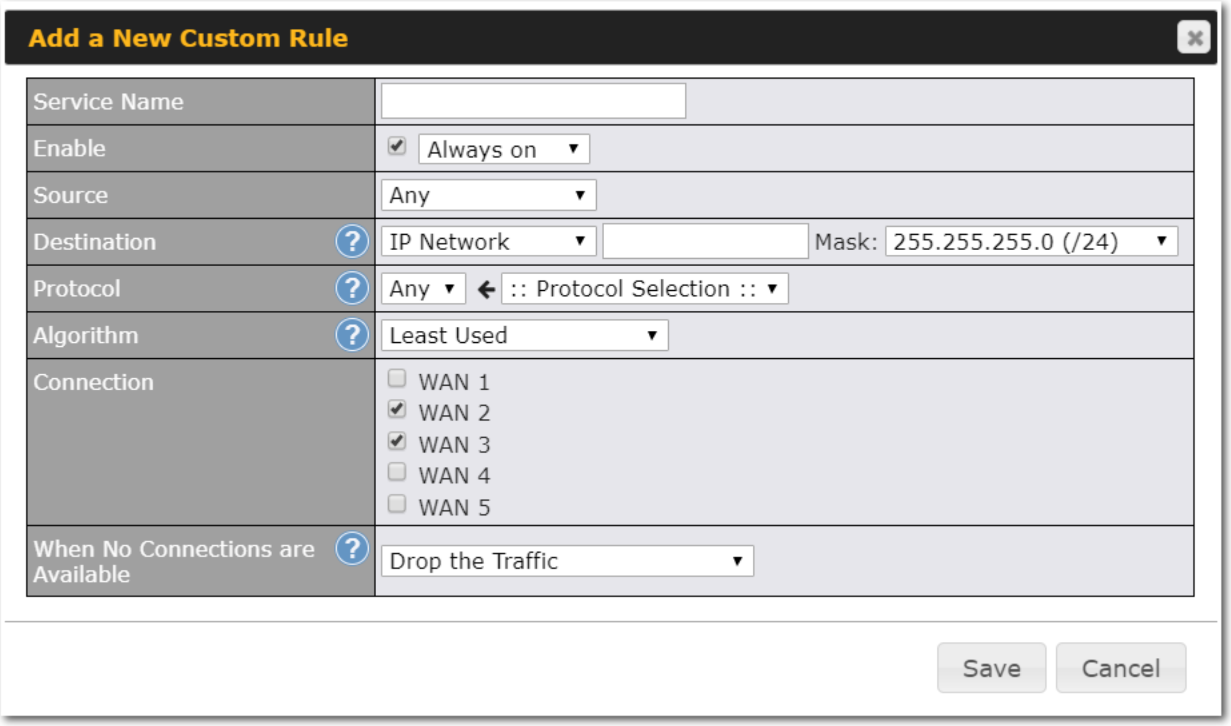
The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.



Algorithm	Overflow ▾
Overflow Order	Highest Priority WAN: WAN 1 WAN: WAN 2 WAN: Wi-Fi WAN WAN: Cellular 1 WAN: Cellular 2 WAN: USB Lowest Priority

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

Algorithm: Least Used

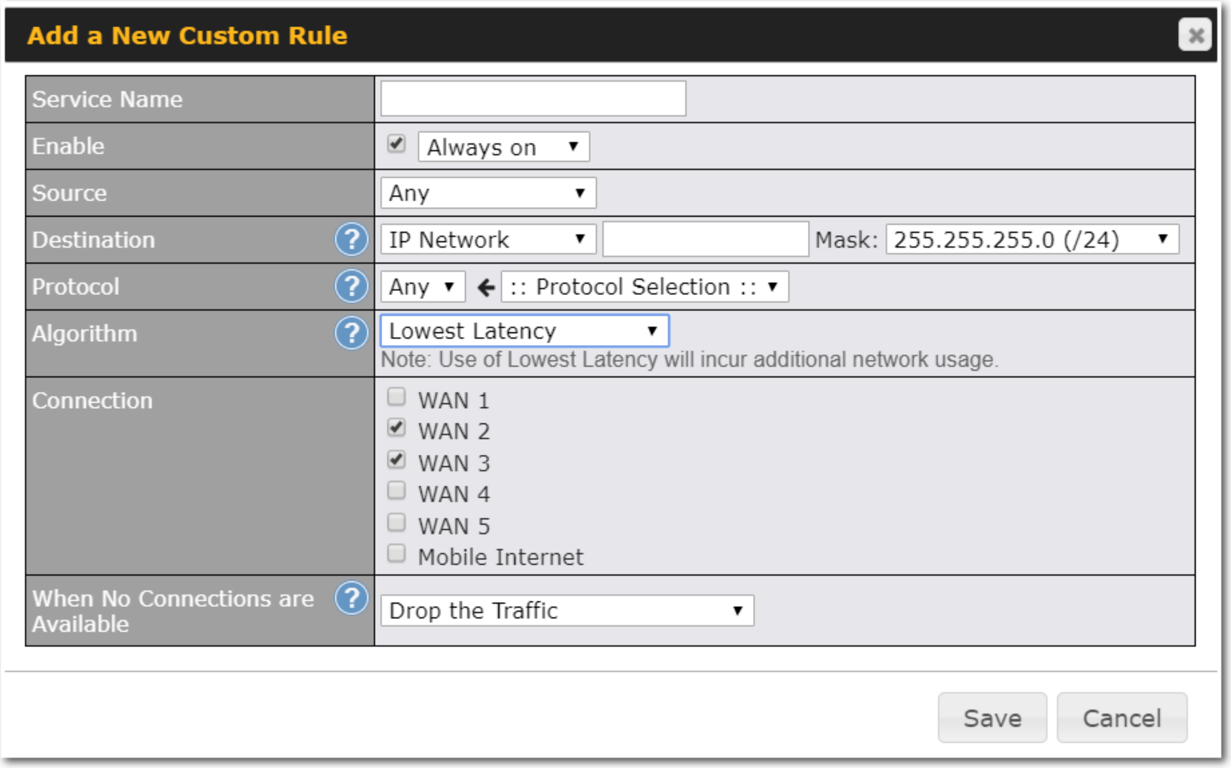


Add a New Custom Rule

Service Name	
Enable	☑ Always on ▾
Source	Any ▾
Destination	IP Network ▾ Mask: 255.255.255.0 (/24) ▾
Protocol	Any ▾ ← :: Protocol Selection :: ▾
Algorithm	Least Used ▾
Connection	☐ WAN 1 ☑ WAN 2 ☑ WAN 3 ☐ WAN 4 ☐ WAN 5
When No Connections are Available	Drop the Traffic ▾

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

Algorithm: Lowest Latency



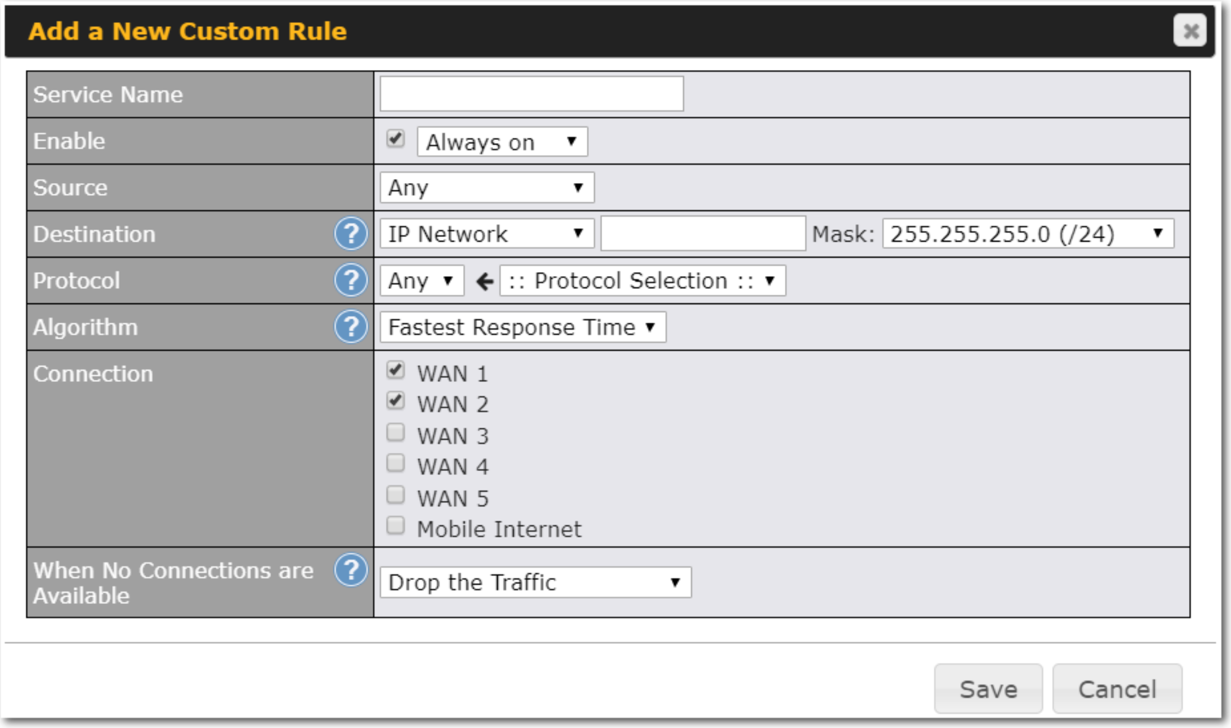
Add a New Custom Rule

Service Name	
Enable	☑ Always on ▾
Source	Any ▾
Destination ?	IP Network ▾ Mask: 255.255.255.0 (/24) ▾
Protocol ?	Any ▾ ← :: Protocol Selection :: ▾
Algorithm ?	Lowest Latency ▾ Note: Use of Lowest Latency will incur additional network usage.
Connection	□ WAN 1 ☑ WAN 2 ☑ WAN 3 □ WAN 4 □ WAN 5 □ Mobile Internet
When No Connections are Available ?	Drop the Traffic ▾

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

Tip
The roundtrip time of a 6M down/640k uplink can be higher than that of a 2M down/2M up link because the overall round trip time is lengthened by its slower upload bandwidth, despite its higher downlink speed. Therefore, this algorithm is good for two scenarios: ● All WAN connections are symmetric; or ● A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN's available bandwidth.

Algorithm : Fastest Response Time



Service Name	
Enable	☑ Always on ▾
Source	Any ▾
Destination	IP Network ▾ Mask: 255.255.255.0 (/24) ▾
Protocol	Any ▾ ← :: Protocol Selection :: ▾
Algorithm	Fastest Response Time ▾
Connection	☑ WAN 1 ☑ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ WAN 5 ☐ Mobile Internet
When No Connections are Available	Drop the Traffic ▾

The Fastest response Time algorithm works as follows: When a network session is created, the first outgoing packet of that particular session is duplicated to all the available WANs.

When the first response is received from a remote server, any further traffic for this session will be routed over that particular WAN connection for the fastest possible response time.

If any slower responses are received on other connections afterwards, they will be discarded.

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.

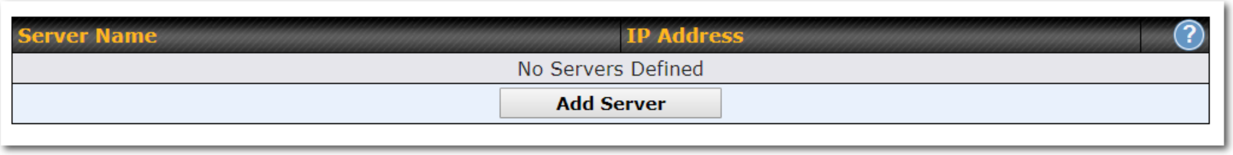
By the custom definition of servers and services for inbound access, Internet users can access the servers behind Peplink Balance. Advanced configurations allow inbound access to be distributed among multiple servers on the LAN.

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

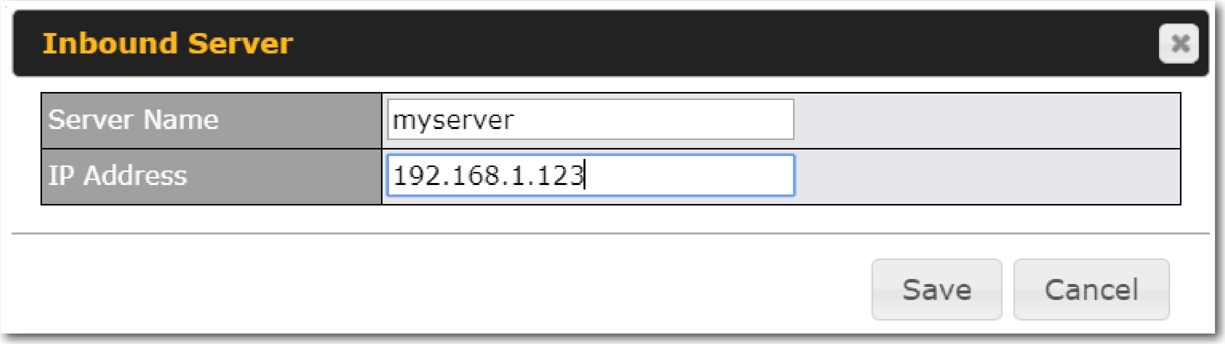
The settings to configure servers on the LAN are located at **Network>Inbound Access>Servers**.

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		

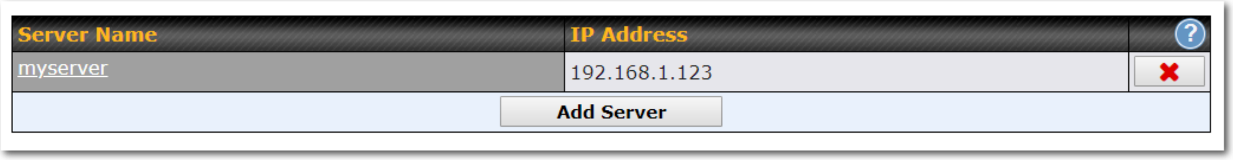
To define a new server, click **Add Server**, which displays the following screen:



Inbound Server

Server Name	myserver
IP Address	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.

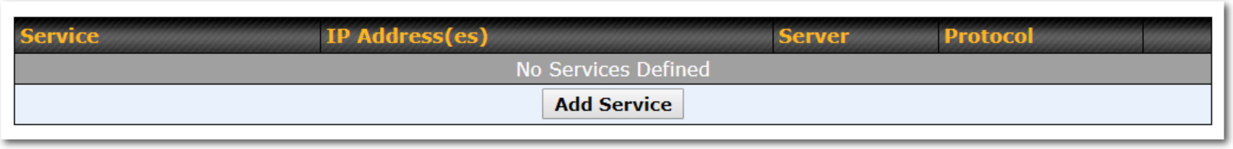


Server Name	IP Address	?
myserver	192.168.1.123	✖

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

12.5.2 Services

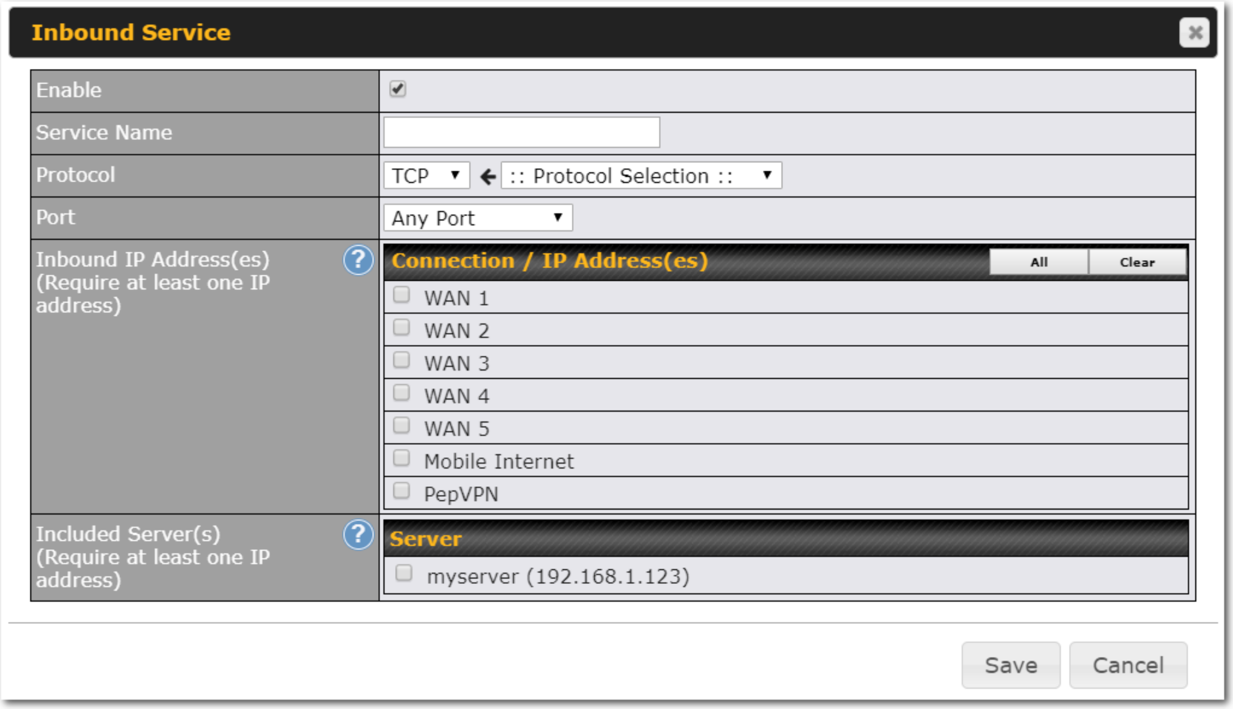
Services are defined at **Network>Inbound Access>Services**.



Service	IP Address(es)	Server	Protocol	
No Services Defined				

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

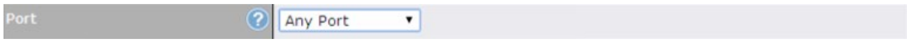
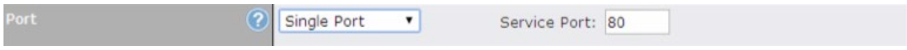
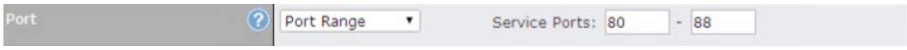
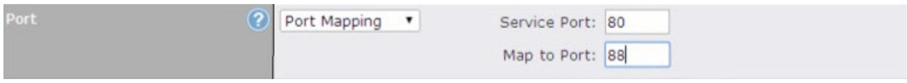
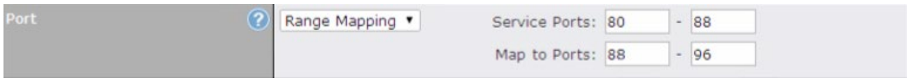
To define a new service, click the **Add Service** button, upon which the following menu appears:



Inbound Service

Enable	☑
Service Name	
Protocol	TCP ▾ ← :: Protocol Selection :: ▾
Port	Any Port ▾
Inbound IP Address(es) (Require at least one IP address)	Connection / IP Address(es) All Clear □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5 □ Mobile Internet □ PepVPN
Included Server(s) (Require at least one IP address)	Server □ myserver (192.168.1.123)

Services Settings	
Enable	This setting specifies whether the inbound service rule takes effect. When **Yes** is selected, the inbound service rule takes effect. If the inbound traffic matches the specified IP protocol and port, action will be taken by the Peplink Balance based on the other parameters of the rule. When **No** is selected, the inbound service rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Only alphanumeric and the underscore "_" characters are valid.
IP Protocol	The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Inbound traffic that matches the specified **IP Protocol** and **Port**(s) will be forwarded to the LAN hosts specified by the **Servers** setting. Upon choosing a protocol, the **Protocol Selection Tool** drop-down menu can be used to automatically the port information of common Internet services (e.g. HTTP, HTTPS, etc.).

	After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and the port number will remain manually modifiable.
Port	The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: **Any Port**, **Single Port**, **Port Range**, **Port Map**, and **Range Mapping**  Port Any Port **Any Port**: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, if I**P Protocol** is set to **TCP** and **Port** is set to **Any Port**, then all TCP traffic will be forwarded to the configured servers.  Port Single Port Service Port: 80 **Single Port**: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, if I**P 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 Port Range Service Ports: 80 - 88 **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 Port Mapping Service Port: 80 Map to Port: 88 **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.)  Port Range Mapping Service Ports: 80 - 88 Map to Ports: 88 - 96 **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

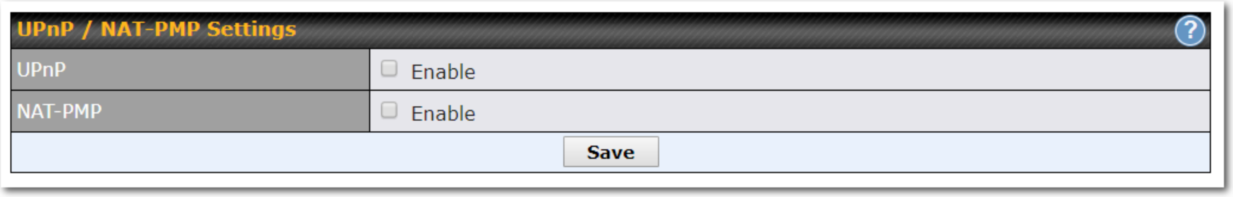
The total weight is 15 = (10 + 5)
Matching traffic distributed to demo_server_1:67% = (10 / 15) x 100%
Matching traffic distributed to demo_server_2:33% = (5 / 15) x 100%

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.



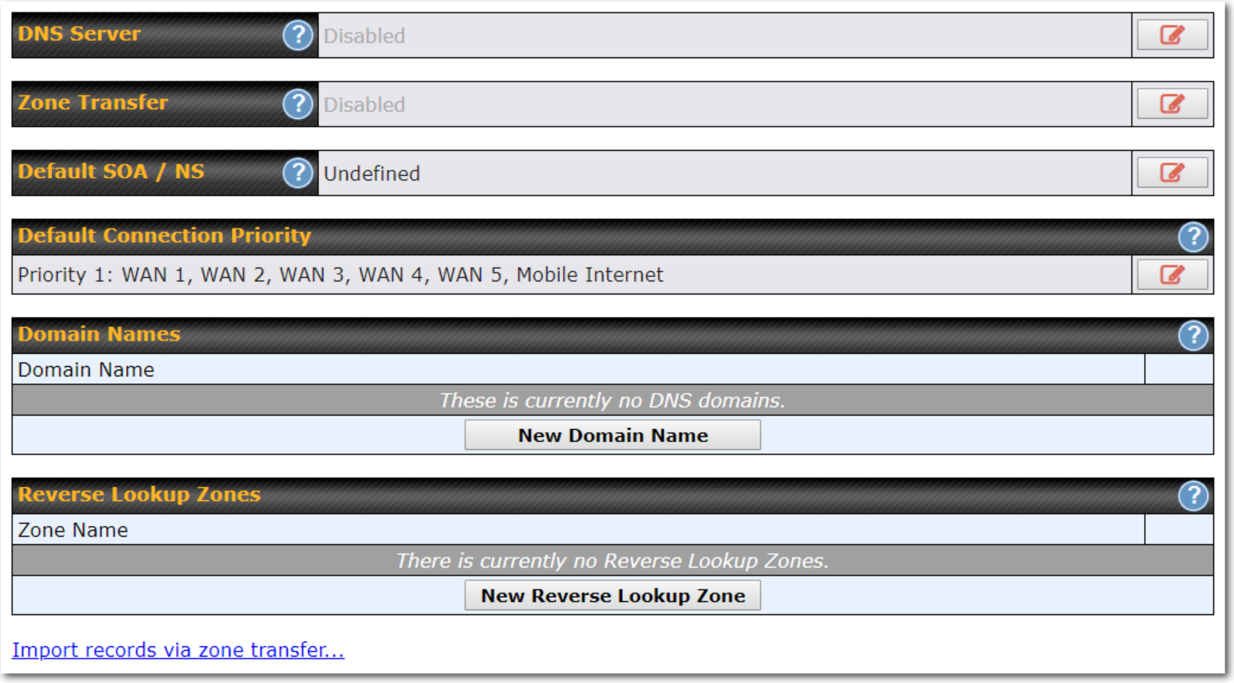
UPnP / NAT-PMP Settings	
UPnP	□ Enable
NAT-PMP	□ Enable

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**.



DNS Server	Disabled	
Zone Transfer	Disabled	
Default SOA / NS	Undefined	

Default Connection Priority

Priority 1: WAN 1, WAN 2, WAN 3, WAN 4, WAN 5, Mobile Internet

Domain Names

Domain Name	
These is currently no DNS domains.	

Reverse Lookup Zones

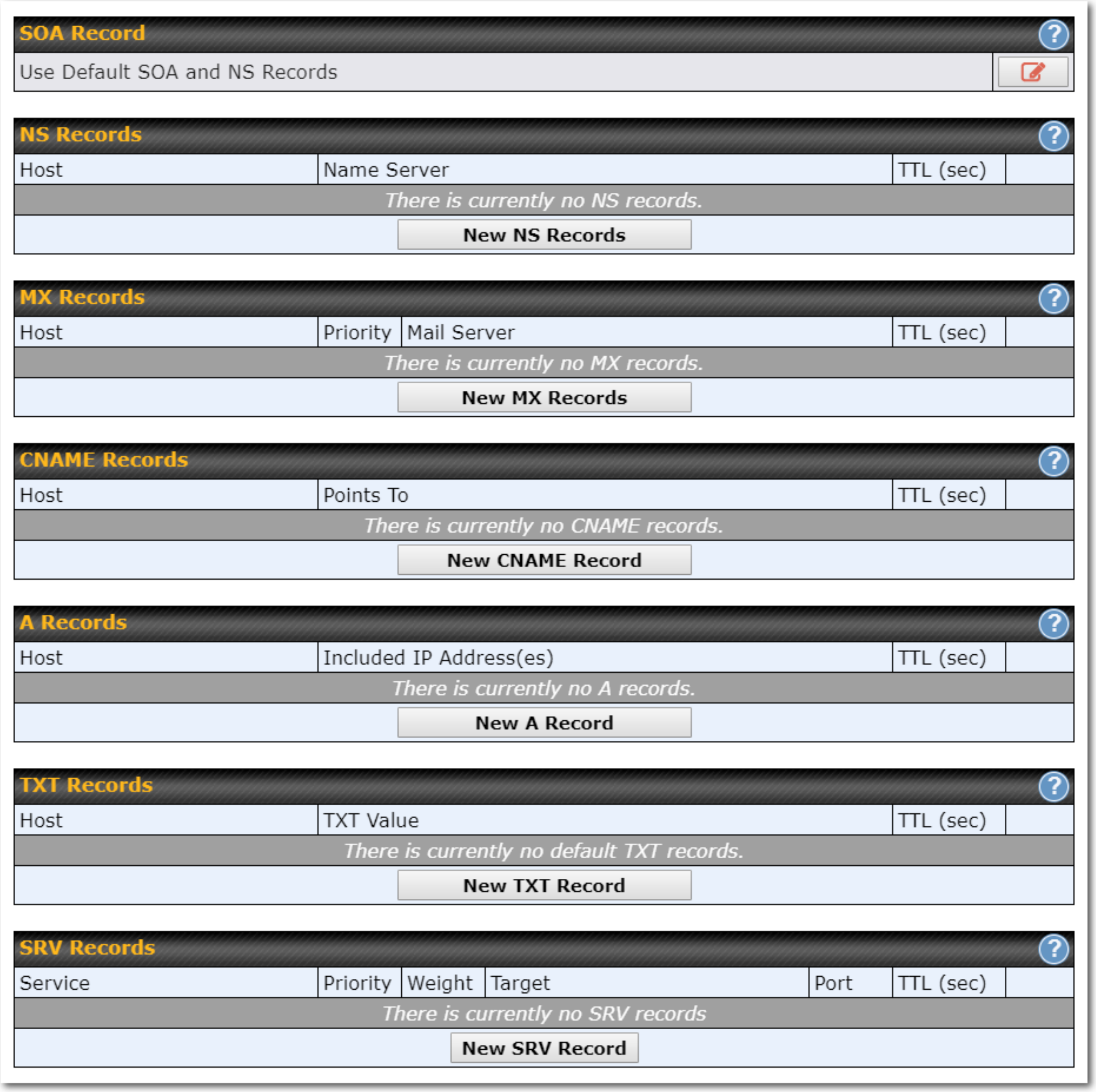
Zone Name	
There is currently no Reverse Lookup Zones.	

DNS Settings	
DNS Servers	This setting specifies the WAN IP addresses on which the DNS server of the Peplink Balance should listen. If no addresses are selected, the inbound link load balancing feature will be disabled and the Peplink Balance will not respond to DNS requests. To specify and/or modify the IP addresses on which the DNS server should listen, click the button that corresponds to **DNS Server**, and a selection screen will be displayed: To specify the Internet IP addresses on which the DNS server should listen, select the desired WAN connection then select the desired associated IP addresses. (Multiple items in the list can be selected by holding CTRL and clicking on the items.) Click **Save** to save the settings when configuration is complete.
Zone Transfer	This setting specifies the IP address(es) of the secondary DNS server(s)authorized to retrieve zone records from the DNS server of the Peplink Balance. The zone transfer server of the Peplink Balance listens on TCP port 53. The Peplink Balance serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing its LAN interface.

Routing Control by Subnet Database	When this function is enabled, the system will check to see if an incoming DNS client is within any WAN's ISP subnet. Only the matched WAN(s)'s IP addresses will be returned. Note that this feature is available only when a subnet database has been defined.
Default SOA / NS	Click the button to define a default SOA / NS record for all domain names. When defining a default SOA record, **Name Server IP Address** is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain. For defining default NS records, the host *[domain]* indicates that this record is for the domain name itself without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the **Host** field left empty. When the entered name server is a fully qualified domain name (FQDN), the **IP Address** field will be disabled.
Default Connection Priority	**Default Connection Priority** defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the **Connection Priority** set to **Default**. Please refer to **Section 17.3.9** for details. The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable. To specify the primary and backup connections, click the button that corresponds to **Default Connection Priority**. A selection screen screen will appear. Each WAN connection is associated with a priority number. Click **Save** to save the settings when configuration is complete.
Domain name	This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its “NS”, “MX” and “TXT” records, and its sub-domains’ “A” and “CNAME” records. Add a new record by clicking the **New Domain Name** button. Click on a domain name to edit. Press the red X to remove a domain name.

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)	
There is currently no NS records.			

MX Records

Host	Priority	Mail Server	TTL (sec)	
There is currently no MX records.				

CNAME Records

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

A Records

Host	Included IP Address(es)	TTL (sec)	
There is currently no A records.			

TXT Records

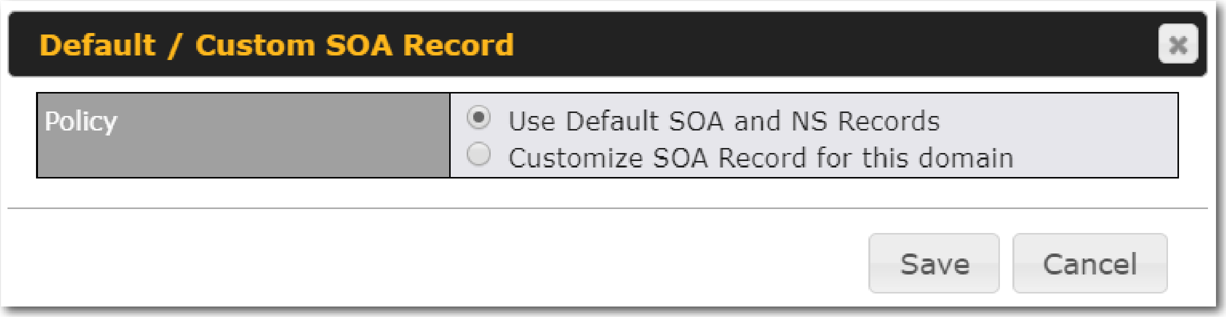
Host	TXT Value	TTL (sec)	
There is currently no default TXT records.			

SRV Records

Service	Priority	Weight	Target	Port	TTL (sec)	
There is currently no SRV records						

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.

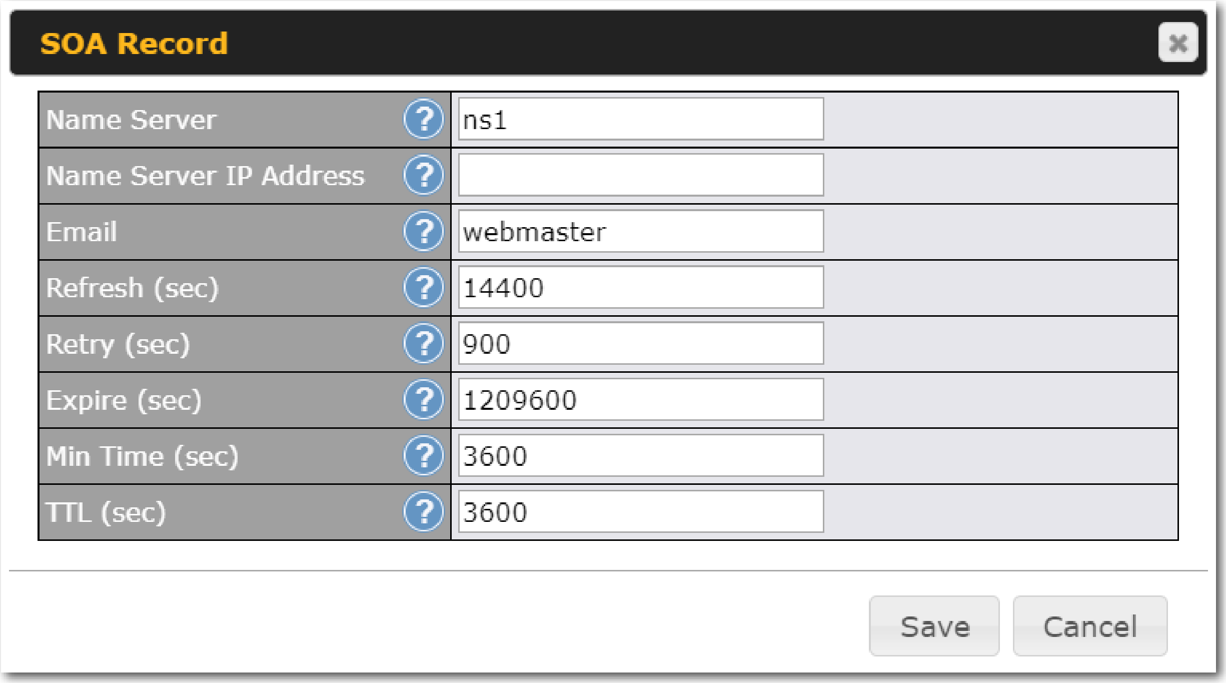
SOA Records



Default / Custom SOA Record

Policy	● Use Default SOA and NS Records ○ 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	ns1
Name Server IP Address	
Email	webmaster
Refresh (sec)	14400
Retry (sec)	900
Expire (sec)	1209600
Min Time (sec)	3600
TTL (sec)	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,

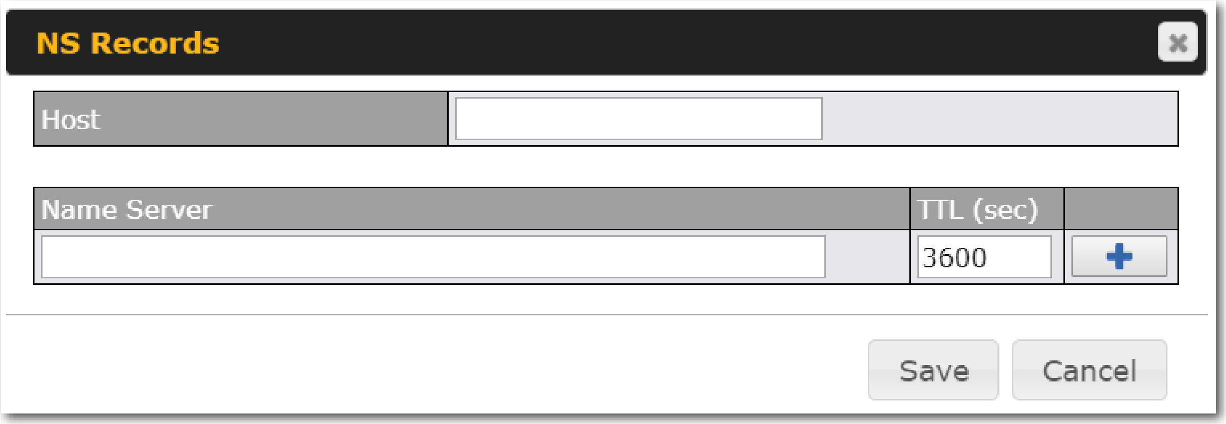
- **Name Server IP Address:** This is the IP address of the authoritative name server. An entry in this field is optional. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If 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.

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:

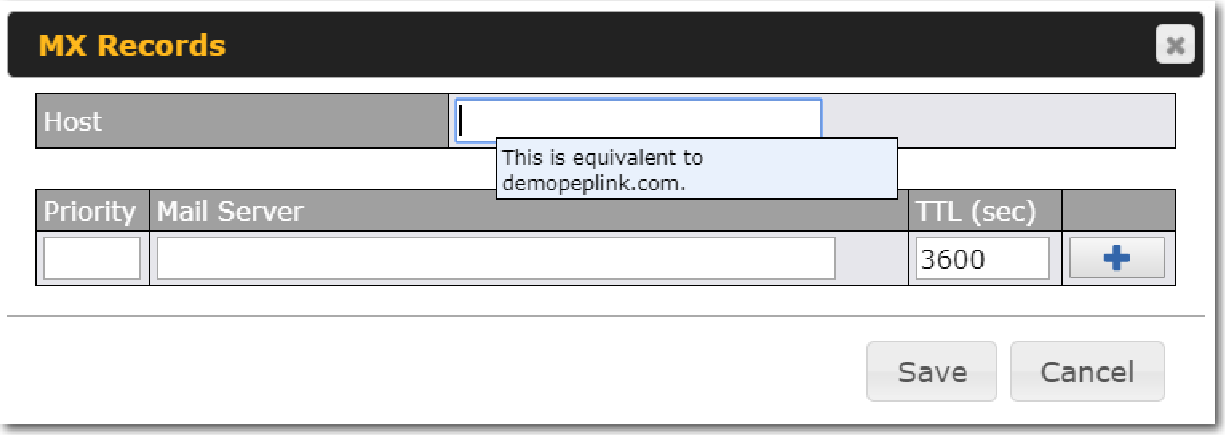


When creating an NS record for the domain itself (not a sub-domain), the **Host** field should be left blank.

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.

MX Records

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



MX Records

Host			
Priority	Mail Server	TTL (sec)	
		3600	+

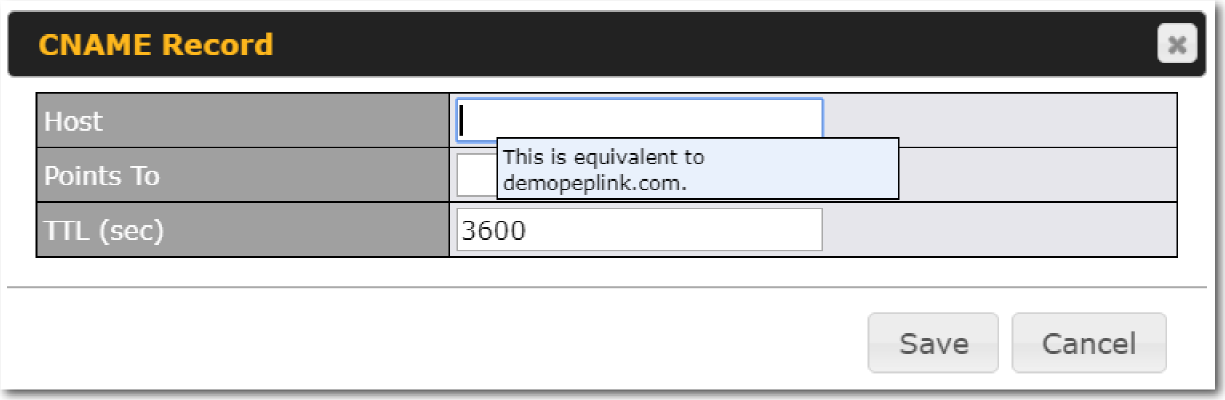
This is equivalent to demopeplink.com.

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 priority. After finishing adding MX records, click the **Save** button.

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:



CNAME Record

Host	
Points To	
TTL (sec)	3600

This is equivalent to demopeplink.com.

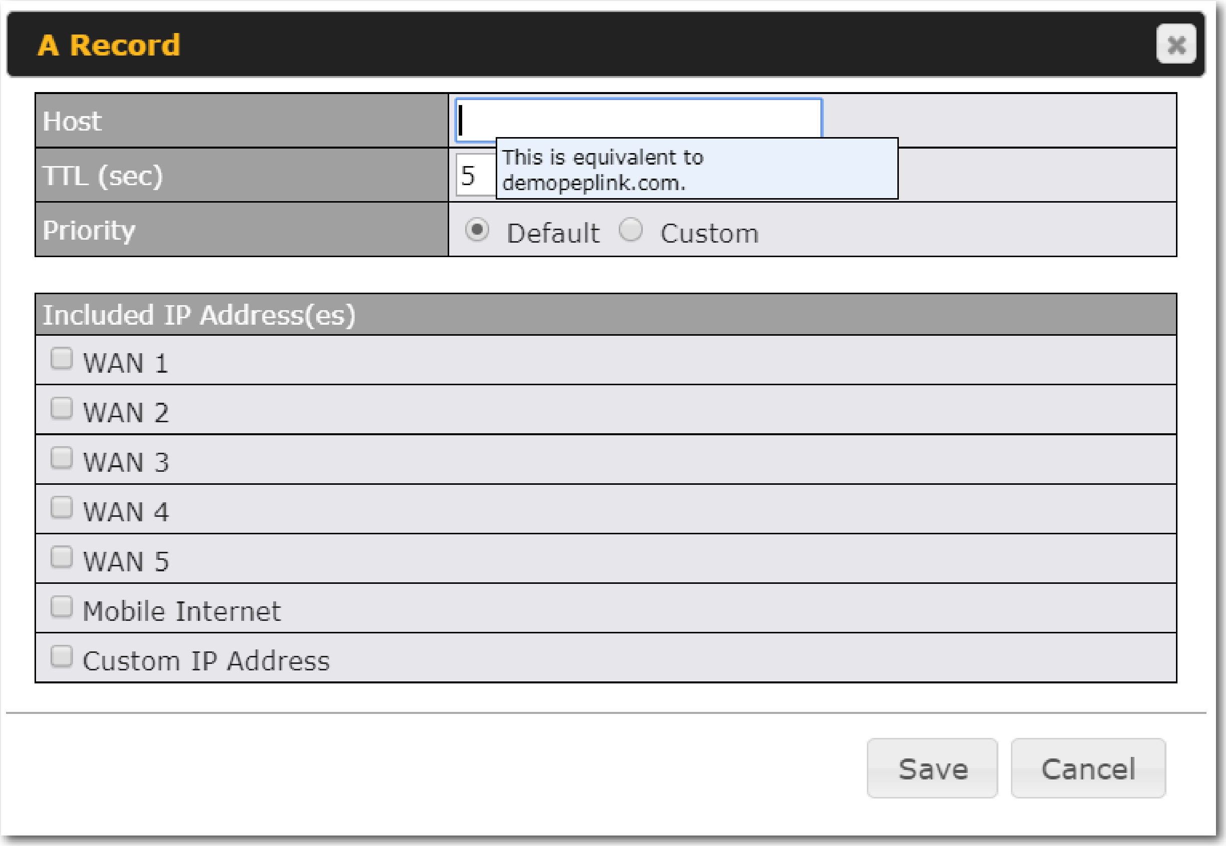
When creating a CNAME record for the domain itself (not a sub-domain), the **Host** field should be left blank.

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.

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	This is equivalent to demopeplink.com.
TTL (sec)	5
Priority	● Default ○ Custom

Included IP Address(es)
□ WAN 1
□ WAN 2
□ WAN 3
□ WAN 4
□ WAN 5
□ Mobile Internet
□ Custom IP Address

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

A Record	
Host Name	This field specifies the A record of this sub-domain to be served by the Peplink Balance. The wildcard character "*" is supported. The IP addresses of "*.*domain.name*" will be returned for every name ending with *".domain.name"* except names that have their own records.
TTL	This setting specifies the time to live of this record in external DNS caches. In order to reflect any dynamic changes on the IP addresses in case of link failure and recovery, this value should be set to a smaller value, e.g., 5 secs, 60 secs, etc.
Priority	This option specifies the priority of different connections. Select the **Default** option to apply the **Default Connection Priority** (refer to the table shown on the main DNS settings page) to an A record. To customize priorities, choose the **Custom** option and a priority selection table will be shown at the bottom.
Included IP	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

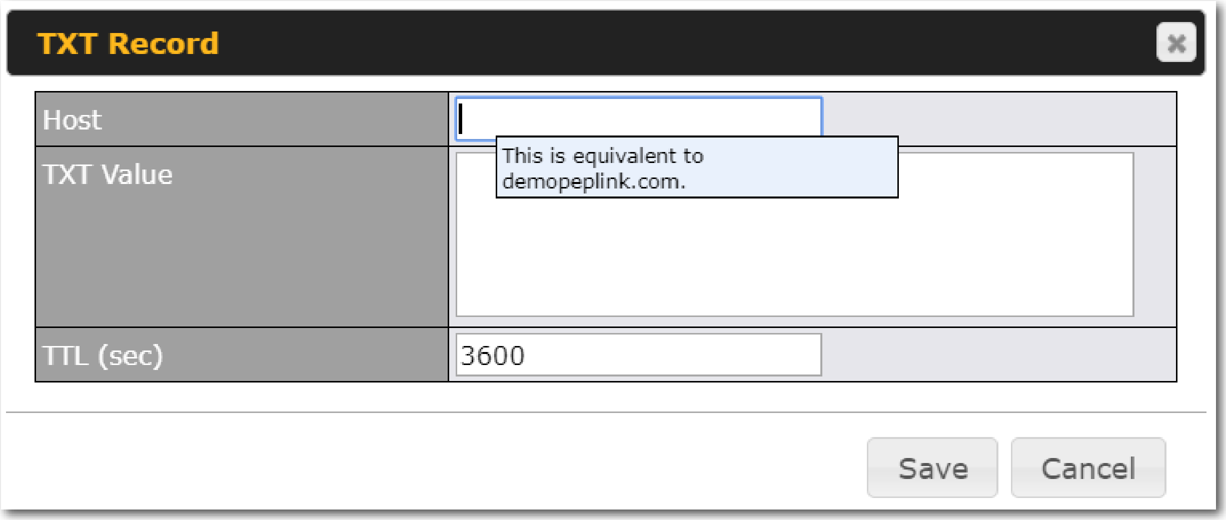
Address(es)	by **Host Name**. The IP addresses listed in each box as **default** are the Internet IP addresses associated with each of the WAN connections. Static IP addresses that are not associated with any WAN can be entered into the **Custom IP** list. A PTR record is also created for each custom IP. For WAN connections that operate under drop-in mode, there may be other routable IP addresses in addition to the default IP address. Therefore, the Peplink Balance allows custom Internet IP addresses to be added manually via filling the text box on the right-hand side and clicking the + button. Only the checked IP addresses in the lists are candidates to be returned when responding to a DNS query. If a WAN connection is down, the corresponding set of IP addresses will not be returned. However, the IP addresses in the **Custom IP Address** field will always be returned. If the **Connection Priority** field is set to **Custom**, you can also specify the usage priority of each WAN connection. Only selected IP address(es) of available connection(s) with the highest priority, and custom IP addresses will be returned. By default, **Connection Priority** is set to **Default**.

PTR Records

PTR records are created along with A records pointing to custom IPs. 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.

TXT Records

This table shows the TXT record of the domain name.



TXT Record

Host	
TXT Value	
TTL (sec)	3600

This is equivalent to demopeplink.com.

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.

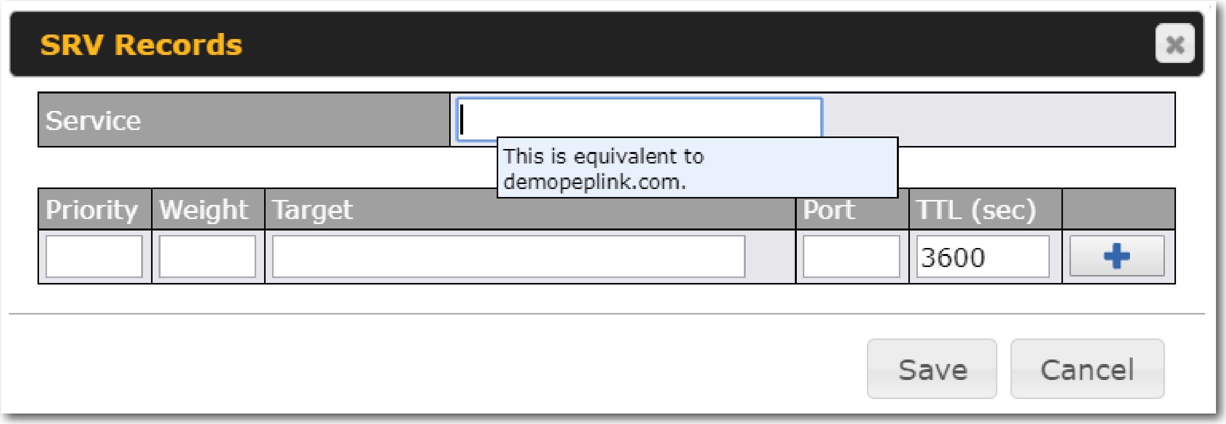
When creating a TXT record for the domain itself (not a sub-domain), the **Host** field should be left blank.

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.

SRV Records

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



SRV Records

Service	

This is equivalent to demopeplink.com.

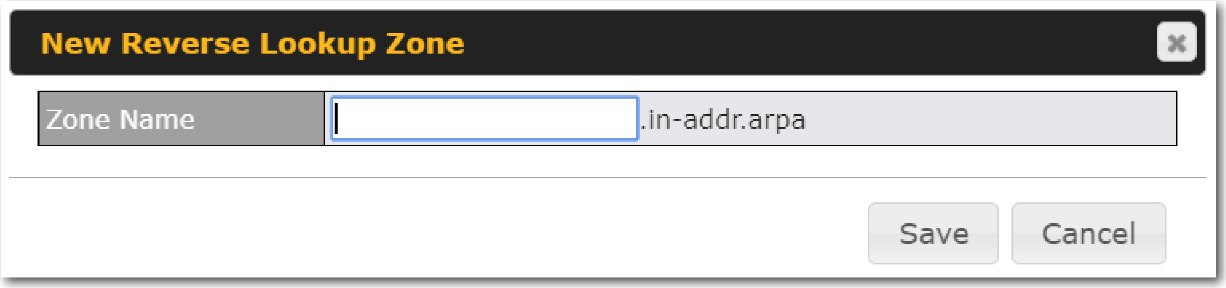
Priority	Weight	Target	Port	TTL (sec)	
				3600	+

- **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**.



Zone Name	.in-addr.arpa

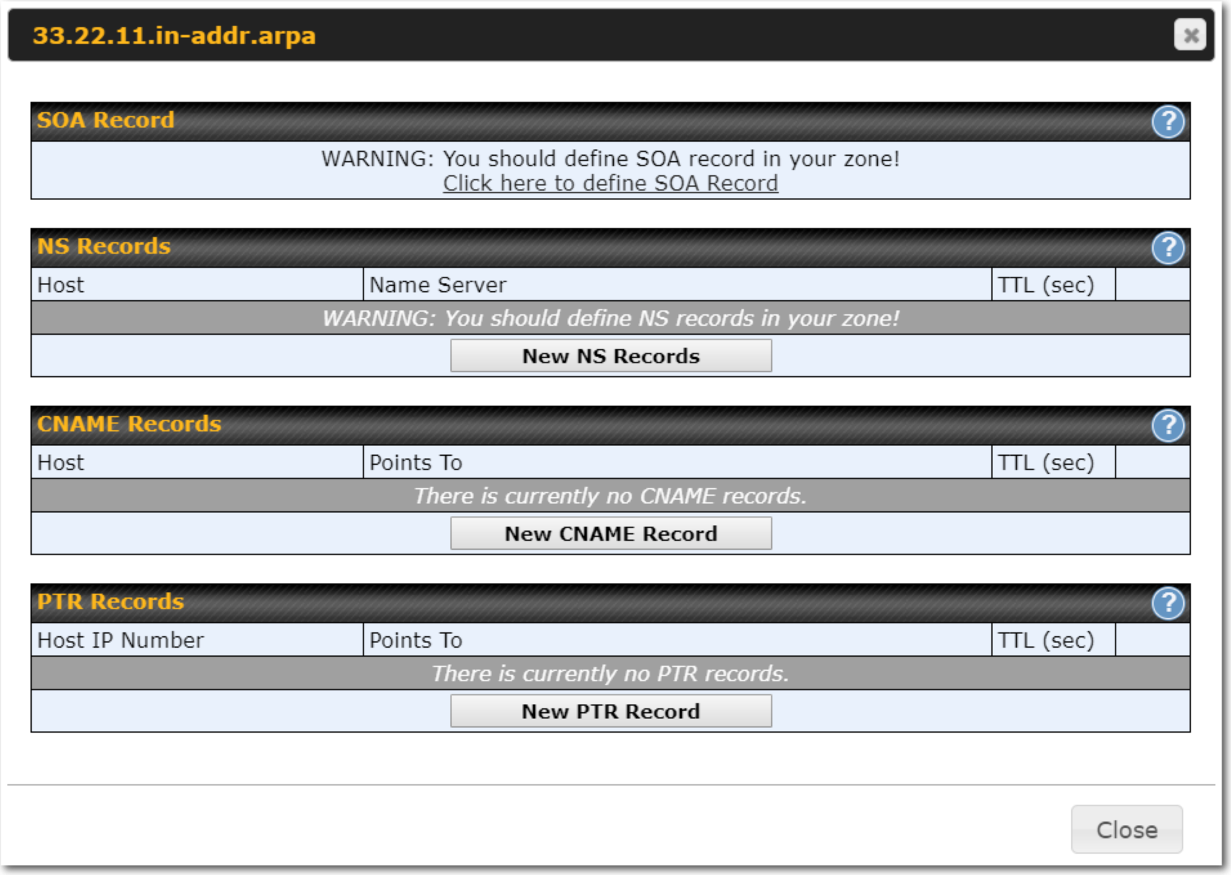
Reverse lookup refers to performing a DNS query to find one or more DNS names associated with a given IP address.

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-arpa.add*r. 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!			

CNAME Records

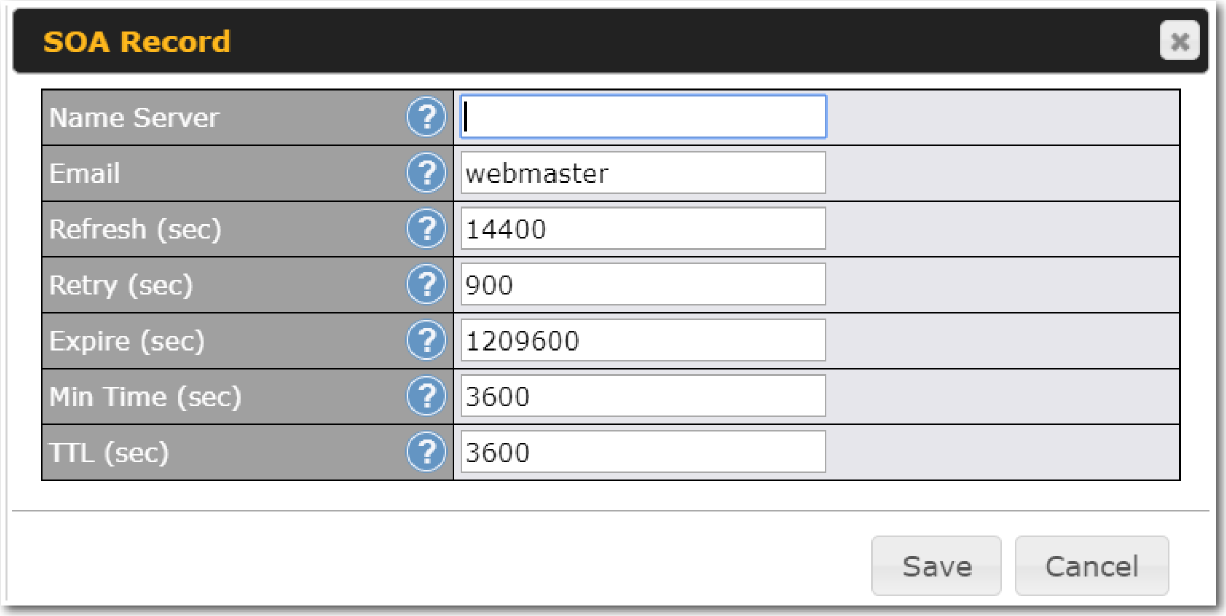
Host	Points To	TTL (sec)	
There is currently no CNAME records.			

PTR Records

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

SOA Record

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



SOA Record

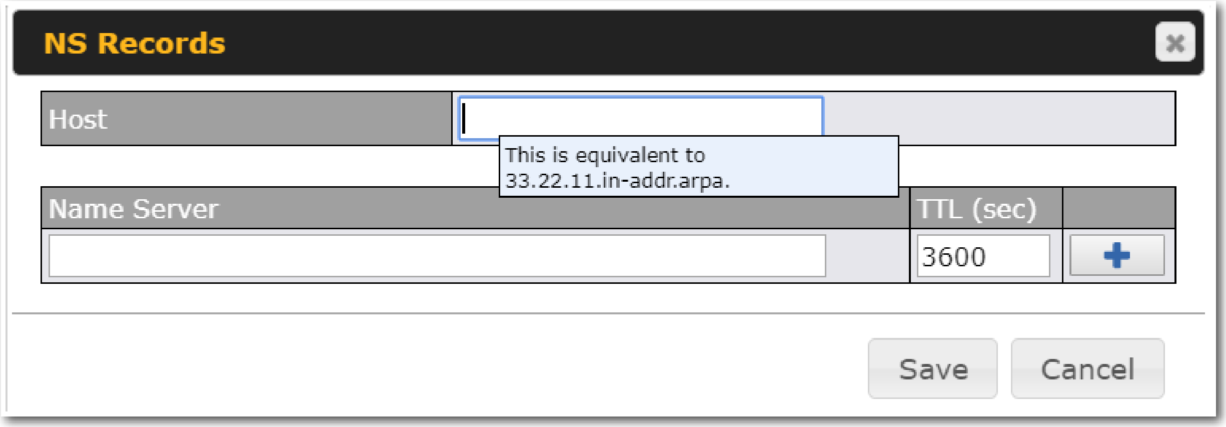
Name Server	
Email	webmaster
Refresh (sec)	14400
Retry (sec)	900
Expire (sec)	1209600
Min Time (sec)	3600
TTL (sec)	3600

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	

This is equivalent to 33.22.11.in-addr.arpa.

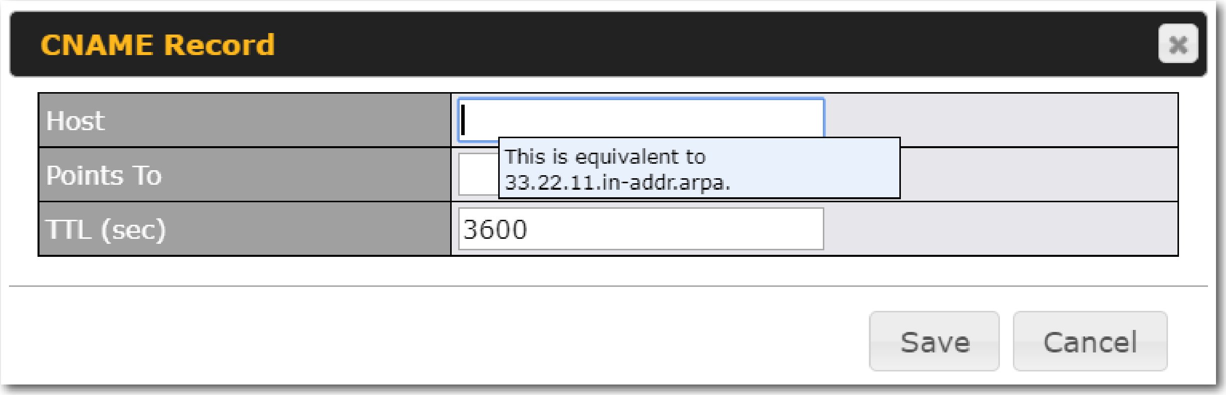
Name Server	TTL (sec)	
	3600	+

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

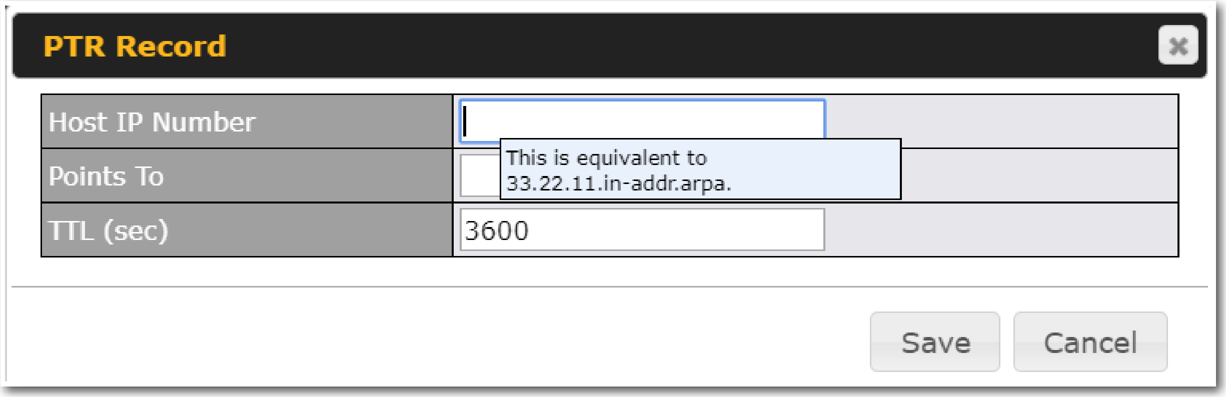
Host	
Points To	
TTL (sec)	3600

This is equivalent to 33.22.11.in-addr.arpa.

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



PTR Record

Host IP Number	
Points To	
TTL (sec)	3600

This is equivalent to 33.22.11.in-addr.arpa.

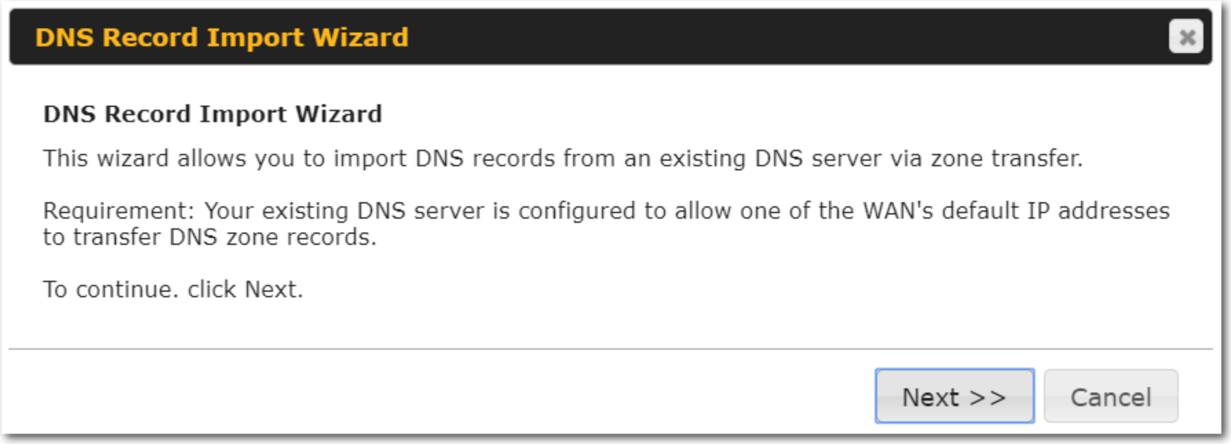
To create a new PTR record, click the **New PTR Record** button.

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.



DNS Record Import Wizard

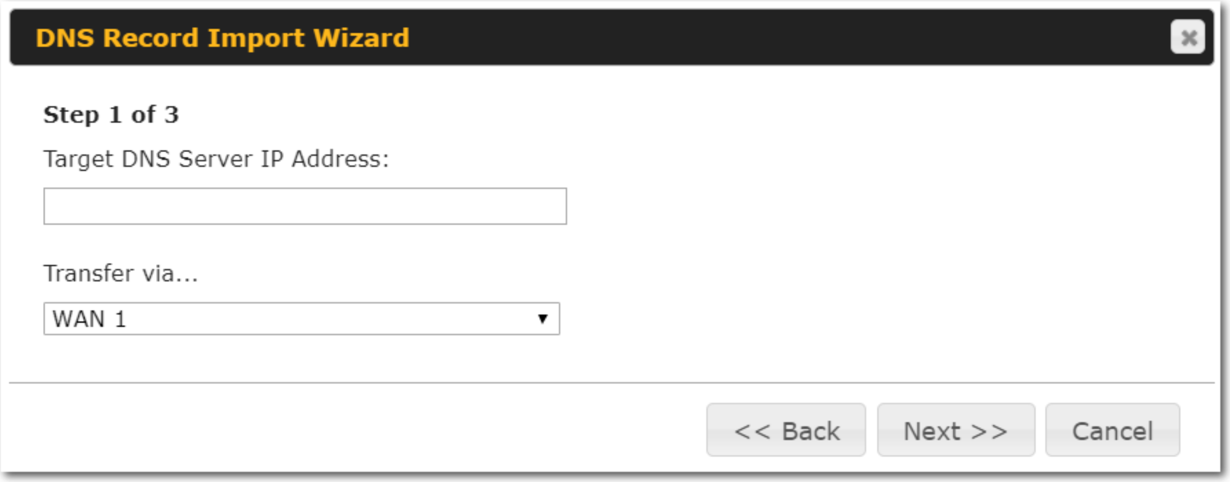
DNS Record Import Wizard

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.

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



DNS Record Import Wizard

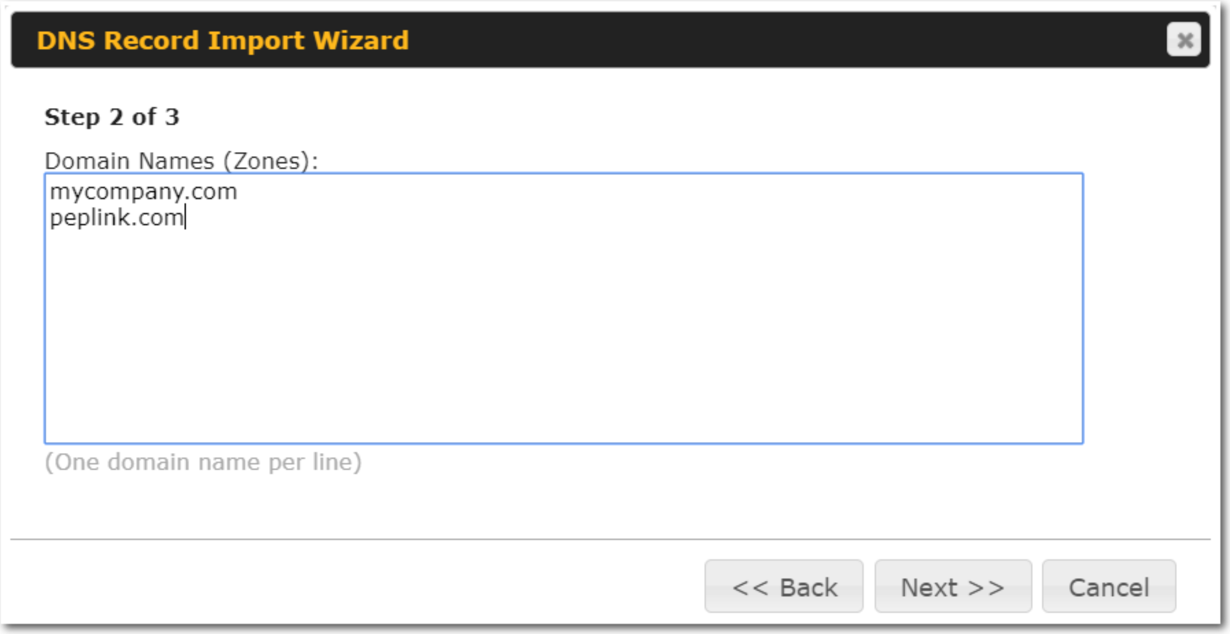
Step 1 of 3

Target DNS Server IP Address:

Transfer via...

WAN 1

- 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):

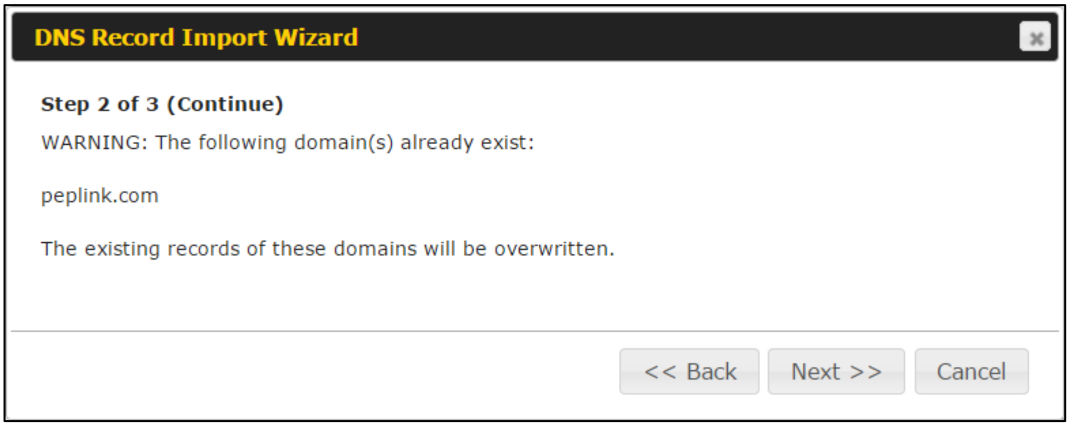
mycompany.com
peplink.com

(One domain name per line)

- 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.



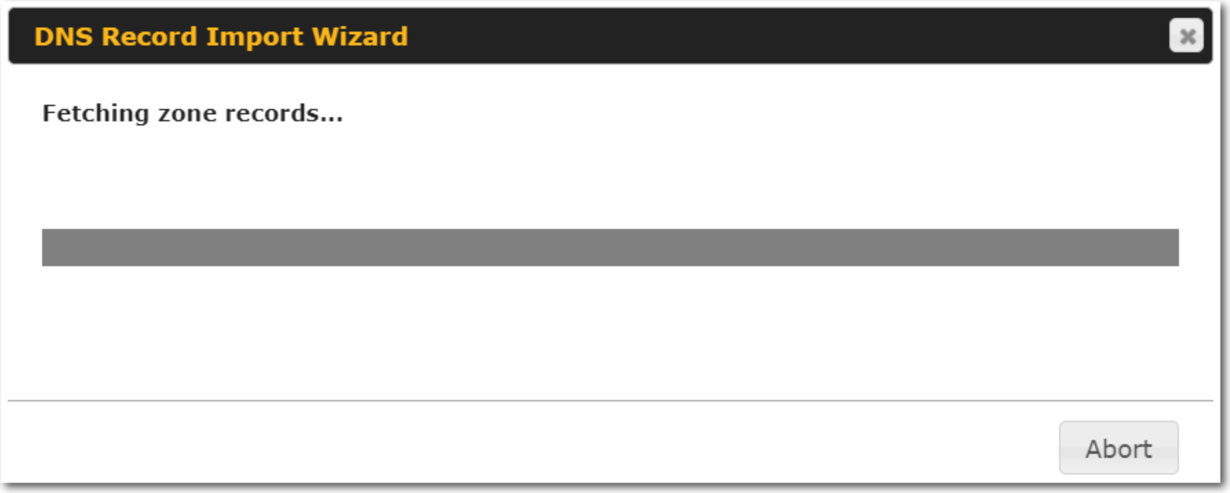
DNS Record Import Wizard

Step 2 of 3 (Continue)

WARNING: The following domain(s) already exist:

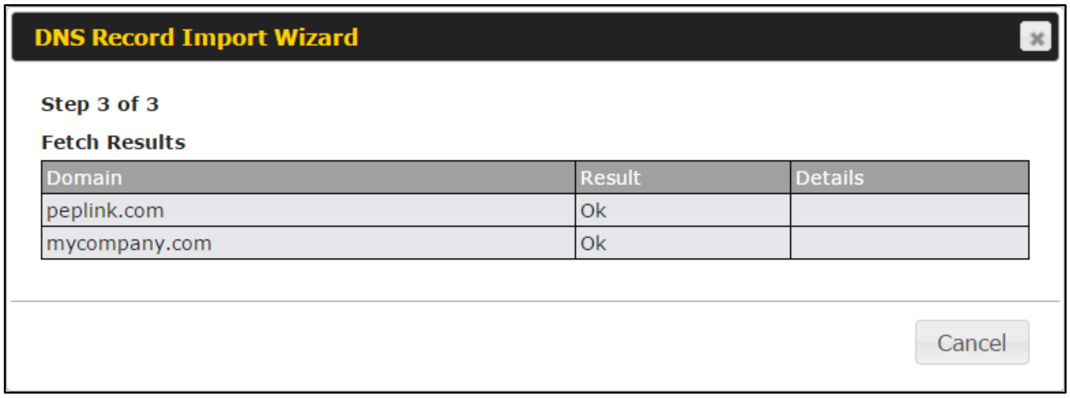
peplink.com

The existing records of these domains will be overwritten.



DNS Record Import Wizard

Fetching zone records...



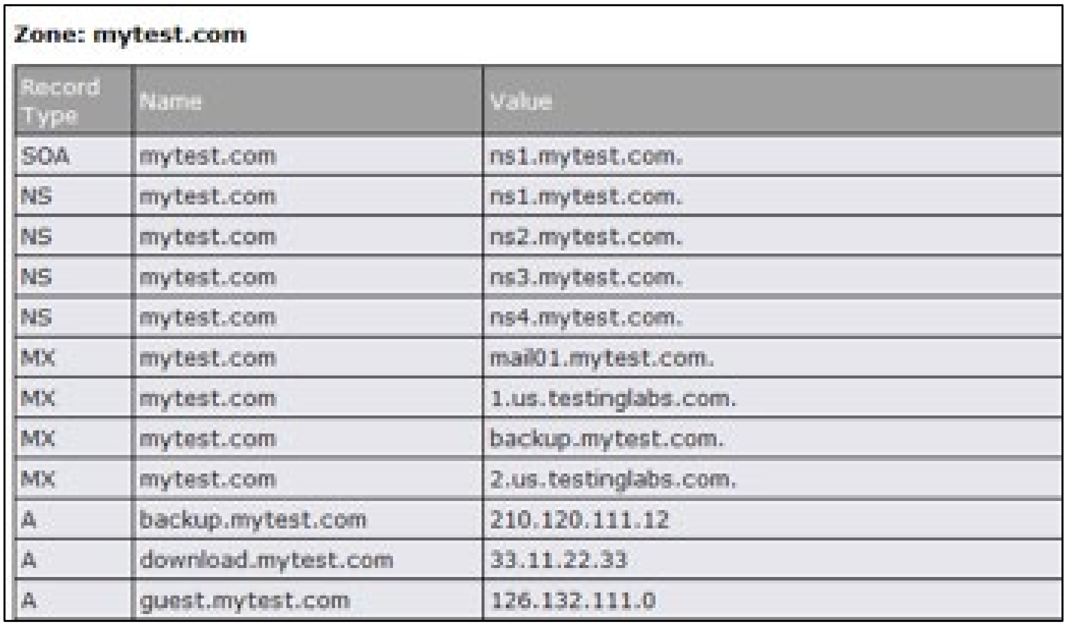
DNS Record Import Wizard

Step 3 of 3

Fetch Results

Domain	Result	Details
peplink.com	Ok	
mycompany.com	Ok	

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.



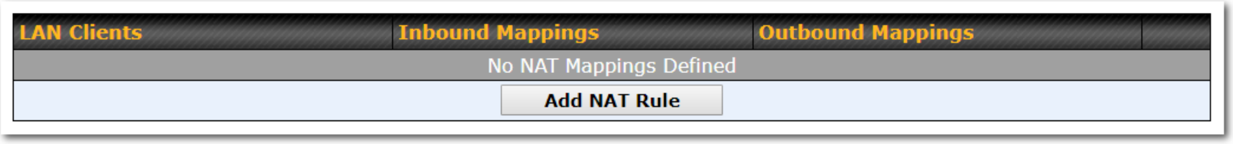
Zone: mytest.com

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

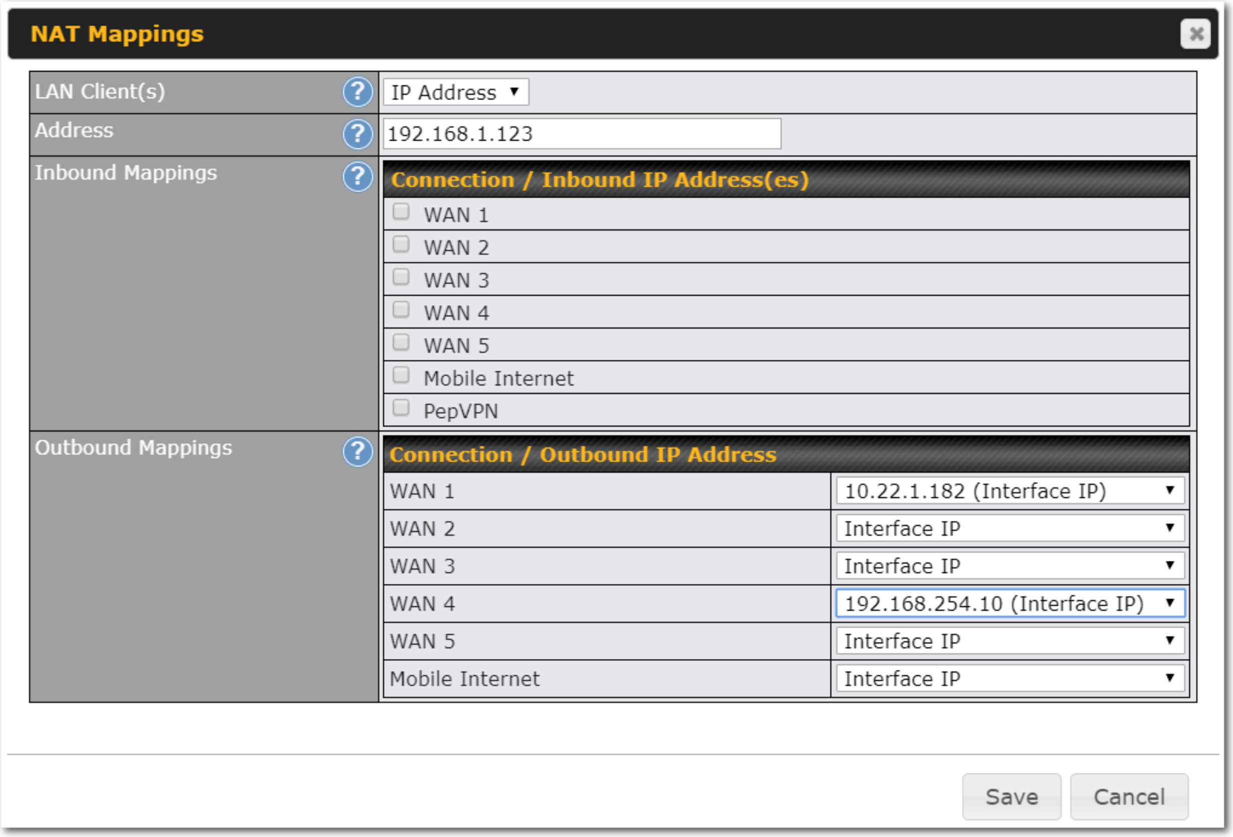
The Peplink Balance allows the IP address mapping of all inbound and outbound NATed traffic to and from an internal client IP address.

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



LAN Clients	Inbound Mappings	Outbound Mappings	
No NAT Mappings Defined			

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



NAT Mappings

LAN Client(s)	IP Address ▾
Address	192.168.1.123
Inbound Mappings	**Connection / Inbound IP Address(es)** □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5 □ Mobile Internet □ PepVPN

Outbound Mappings

Connection / Outbound IP Address	
WAN 1	10.22.1.182 (Interface IP) ▾
WAN 2	Interface IP ▾
WAN 3	Interface IP ▾
WAN 4	192.168.254.10 (Interface IP) ▾
WAN 5	Interface IP ▾
Mobile Internet	Interface IP ▾

NAT Mapping Settings	
LAN Client(s)	NAT Mapping rules can be defined for a single LAN **IP Address**, an **IP Range**, or an **IP Network**.
Address	This refers to the LAN host’s private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when **IP Address** is selected.

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

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

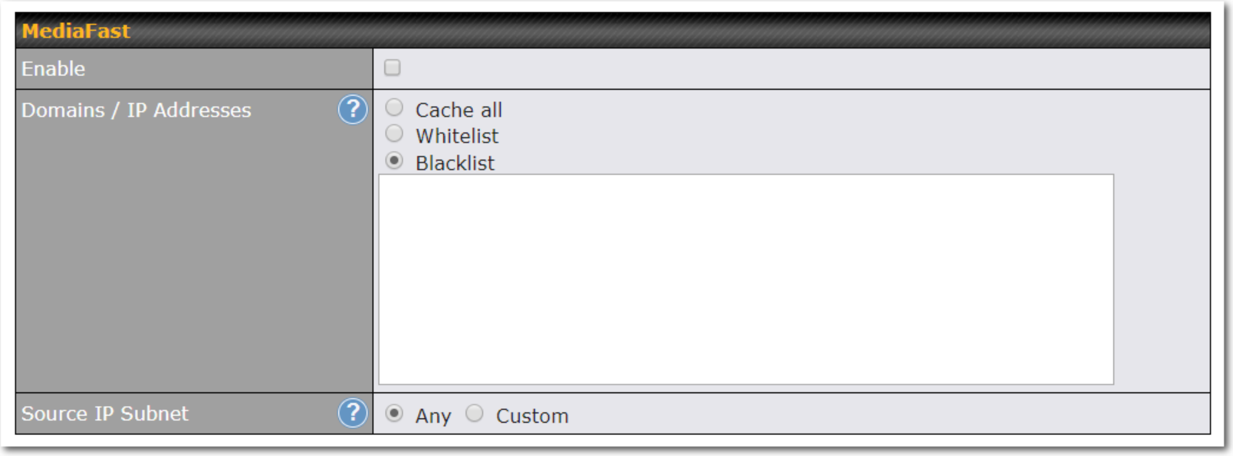
Important Note
Inbound firewall rules override inbound mapping settings.

12.7 MediaFast

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

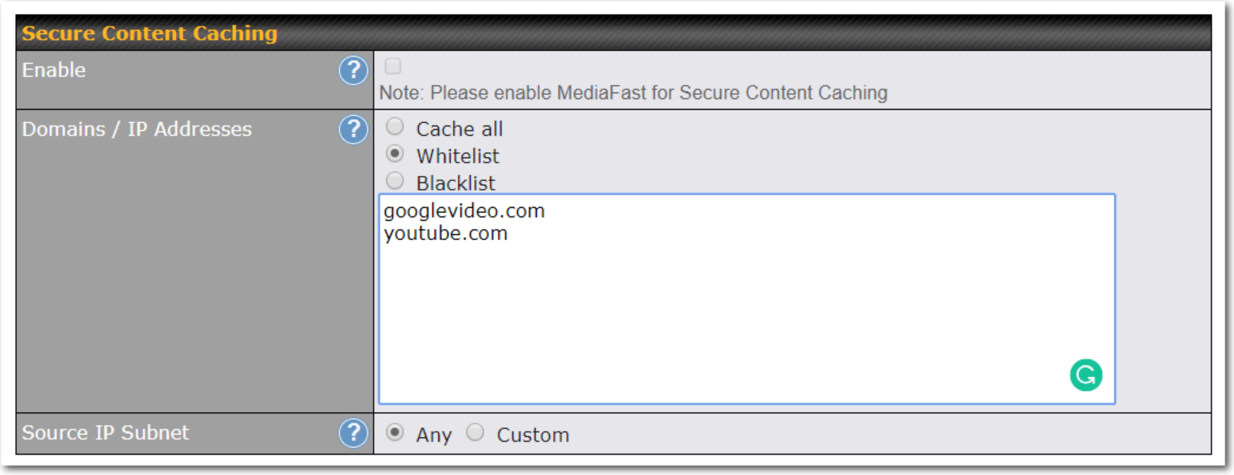
Setting Up MediaFast Content Caching

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



MediaFast	
Enable	□
Domains / IP Addresses	○ Cache all ○ Whitelist ● Blacklist
Source IP Subnet	● Any ○ Custom

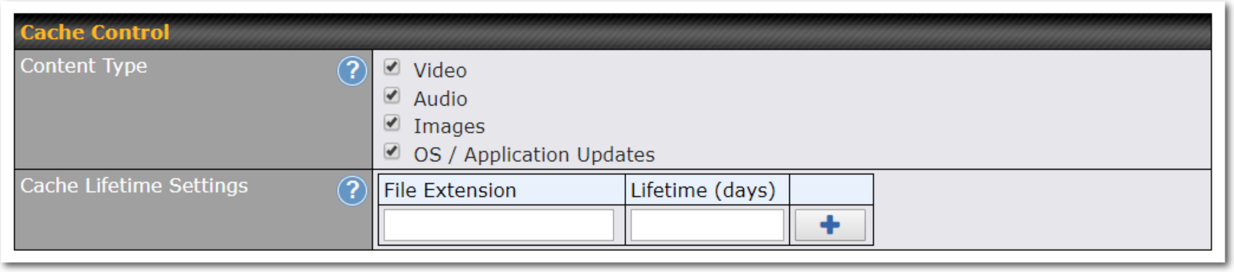
MediaFast	
Enable	Click the checkbox to enable MediaFast content caching.
Domains / IP Addresses	Choose to **Cache on all domains**, or enter domain names and then choose either **Whitelist** (cache the specified domains only) or **Blacklist** (do not cache the specified domains).
Source IP Subnet	This setting allows caching to be enabled on custom subnets only. If "Any" is selected, then caching will apply to all subnets.



Secure Content Caching	
Enable	□ Note: Please enable MediaFast for Secure Content Caching
Domains / IP Addresses	○ Cache all ● Whitelist ○ Blacklist googlevideo.com youtube.com
Source IP Subnet	● Any ○ Custom

The **Secure Content Caching** menu operates identically to the **MediaFast** menu, except it is for secure content cachting accessible through https://. In order for Mediafast devices to cache and deliver HTTPS content, every client needs to have the necessary certificates installed*.

*See https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/



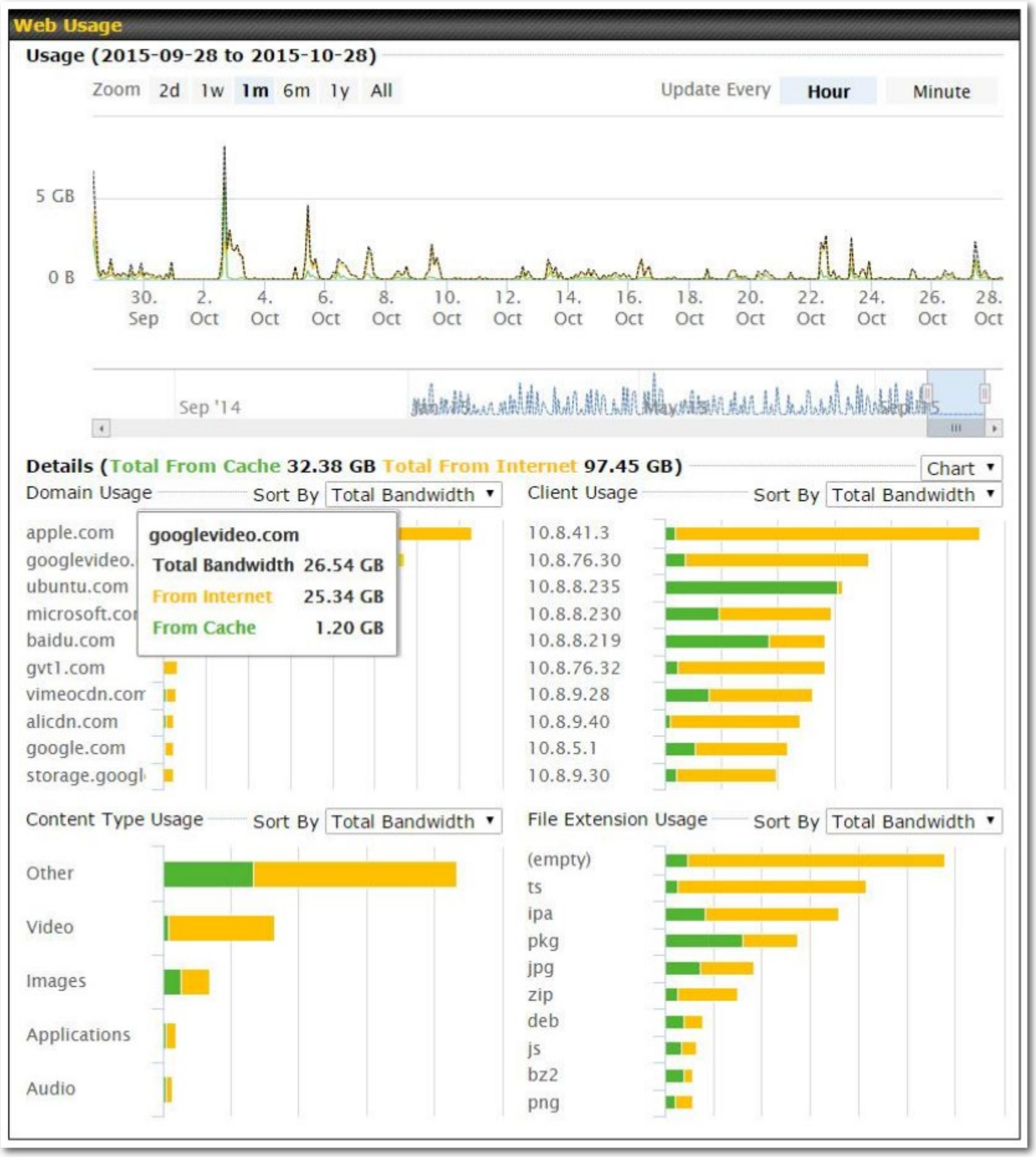
Cache Control

Content Type	☑ Video ☑ Audio ☑ Images ☑ OS / Application Updates
Cache Lifetime Settings	File Extension | Lifetime (days)

Cache Control	
Content Type	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
Cache Lifetime Settings	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.

Viewing MediaFast Statistics

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



Web Usage

Usage (2015-09-28 to 2015-10-28)

Update Every: Hour

Details (Total From Cache 32.38 GB Total From Internet 97.45 GB)

googlevideo.com
Total Bandwidth 26.54 GB
From Internet 25.34 GB
From Cache 1.20 GB

Domain Usage: Sort By Total Bandwidth

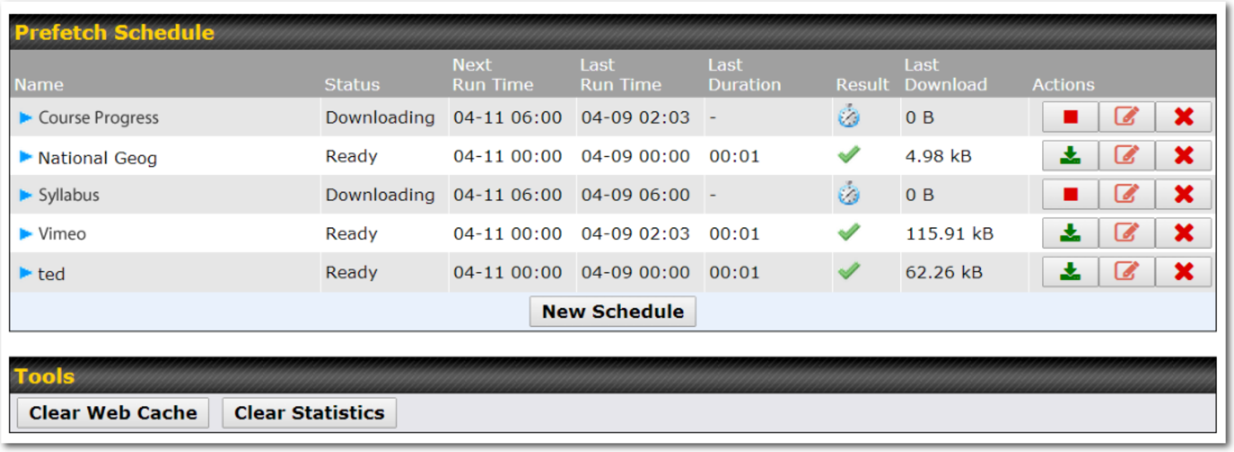
Client Usage: Sort By Total Bandwidth

Content Type Usage: Sort By Total Bandwidth

File Extension Usage: Sort By Total Bandwidth

Prefetch Schedule

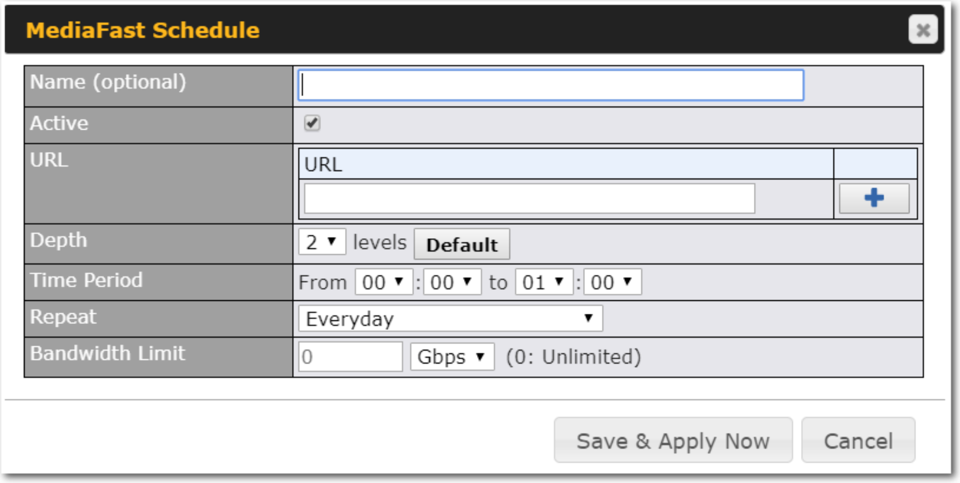
Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Network > MediaFast > Prefetch Schedule**.



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	⬇ ✎ ✖

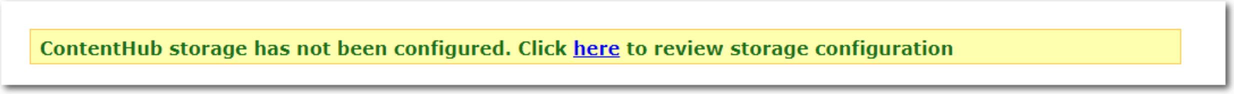
Prefetch Schedule Settings	
Name	This field displays the name given to the scheduled download.
Status	Check the status of your scheduled download here.
Next Run Time/Last Run Time	These fields display the date and time of the next and most recent occurrences of the scheduled download.
Last Duration	Check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

	To delete a scheduled download, click ✖.
New Schedule	Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:  MediaFast Schedule Name (optional): Active: ☑ URL: URL Depth: 2 ▾ levels Default Time Period: From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾ Repeat: Everyday ▾ Bandwidth Limit: 0 Gbps ▾ (0: Unlimited) Save & Apply Now Cancel Simply provide the requested information to create your schedule.
Clear Web Cache	Click to clear all cached content. Note that this action cannot be undone.
Clear Statistics	Click to clear all prefetch and status page statistics.

12.8 ContentHub

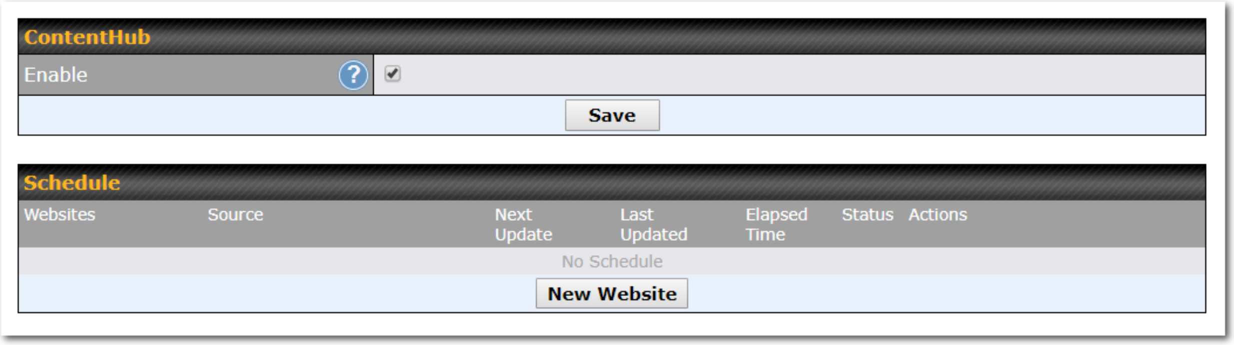
Integrated into MediaFast-enabled routers, ContentHub allows you to deliver webpages and applications using the local storage on your router. Users will be able to access news, articles, videos, and access your web app, without the need for internet access.

ContentHub Storage needs to be configured before content can be uploaded to the ContentHub. Follow the link on the information panel to configure storage.



ContentHub storage has not been configured. Click here to review storage configuration

To access ContentHub, navigate to **Network > ContentHub** and check the **Enable** box.:



ContentHub	
Enable	☑

Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
No Schedule						

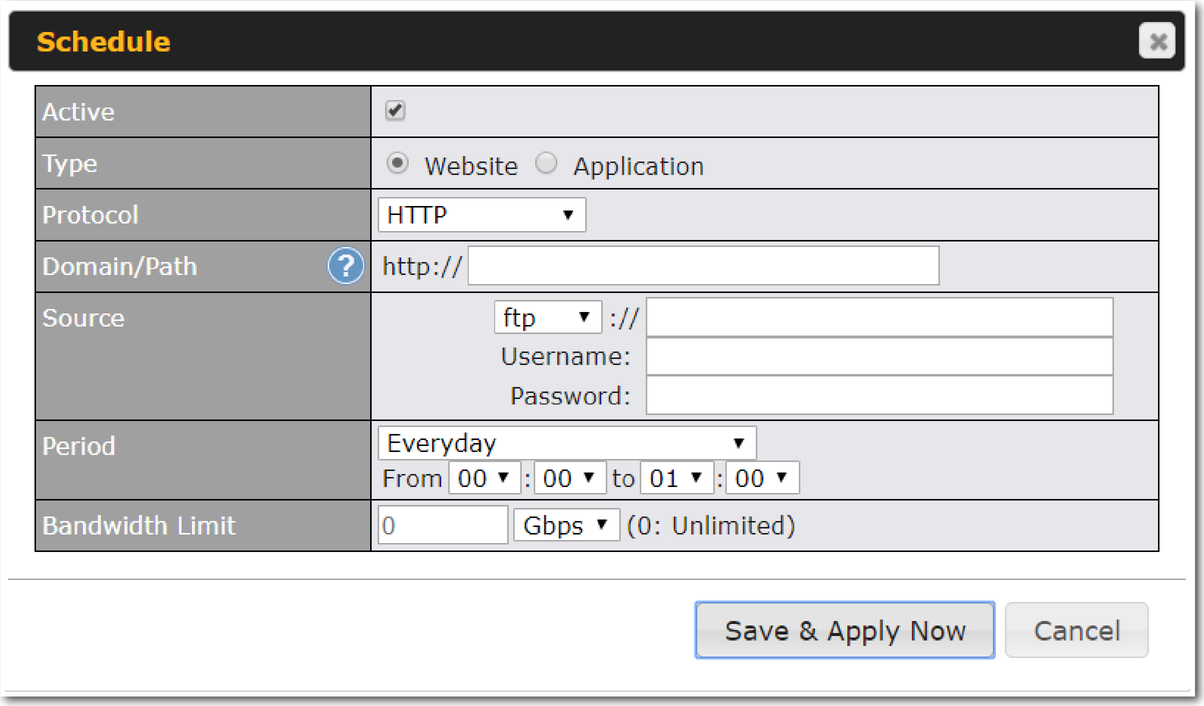
On an external server configure content (a website or application) that will be synced to the ContentHub; for example a html5 website.

To configure a website or application as content follow these steps.

Configure a website to be published from the ContentHub

This option allows you to sync a website to the Peplink router, this website will then be published with the specified domain from the router itself and makes the content available to the client via the HTTP/HTTPS protocol.
Only FTP sync is supported for this type of ContentHub content.
The content should be uploaded to an FTP server before.

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



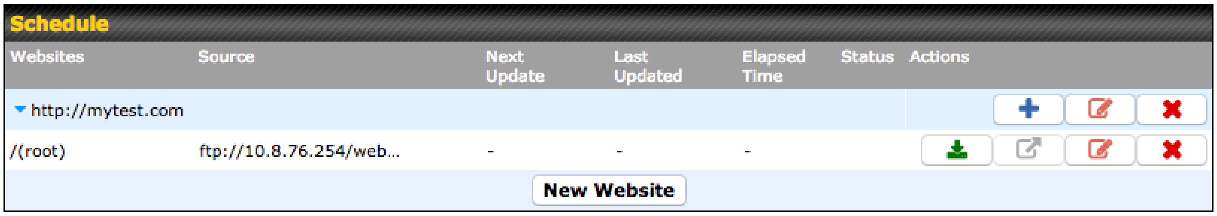
Schedule

Active	☑
Type	● Website ○ Application
Protocol	HTTP ▾
Domain/Path ?	http://
Source	ftp ▾ :// Username: Password:
Period	Everyday ▾ From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾
Bandwidth Limit	0 Gbps ▾ (0: Unlimited)

The Active checkbox toggles the activation of the content.
For type, select Website.

Type	HTTP,HTTPS or both
Domain/Path	The contenhub uses this as the domain name for client access (such as http://mytest.com).
Source	Enter the server details that the content will be downloaded from. Enter your credentials under **Username** and **Password**.
Period	This field determines how often the Router will search for updates to the source content.
Method	Only applicable for application: Choose between sync or file upload
Bandwidth Limit	Used to limit the bandwidth for each client to access the web server.

Click “Save & Apply Now” to activate the changes. Below is a screenshot after configuration:

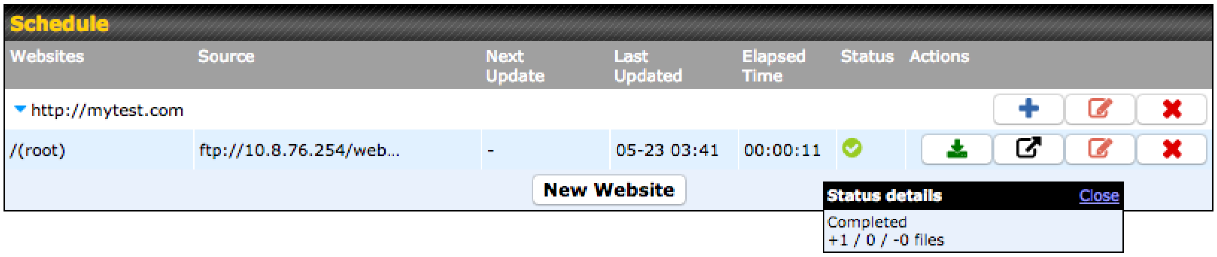


Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						✚ ✎ ✖
/(root)	ftp://10.8.76.254/web...	-	-	-		⬇ ↗ ✎ ✖

The content will be synced based on the **Period** that is configured before. If you want to trigger the sync manually, you can click “⬇”. The “Status” column shows the sync progress.

When the sync is completed,you’ll see a summary as shown in the screenshot below:



Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						✚ ✎ ✖
/(root)	ftp://10.8.76.254/web...	-	05-23 03:41	00:00:11	✓	⬇ ↗ ✎ ✖

Status details Close

Completed
+1 / 0 / -0 files

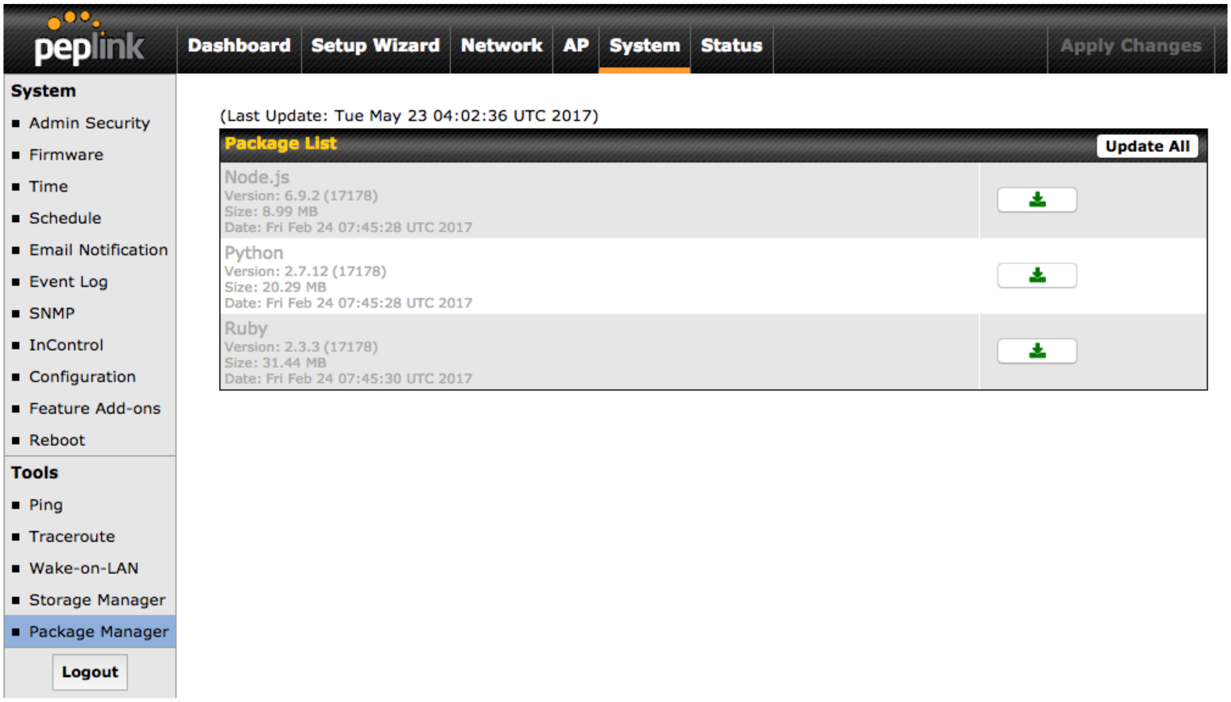
To access the content, open a browser in MFA’s client and enter the domain configured before (such as http://mytest.com).

Configure an application to be published from the ContentHub

Mediafast Routers allow you to configure and publish ant application from the router itself by using the supported framework

- Python (version 2.7.12)
- Ruby (version 2.3.3)
- Node.js (version 6.9.2)

First install the desired framework in “Package Manager” as below:

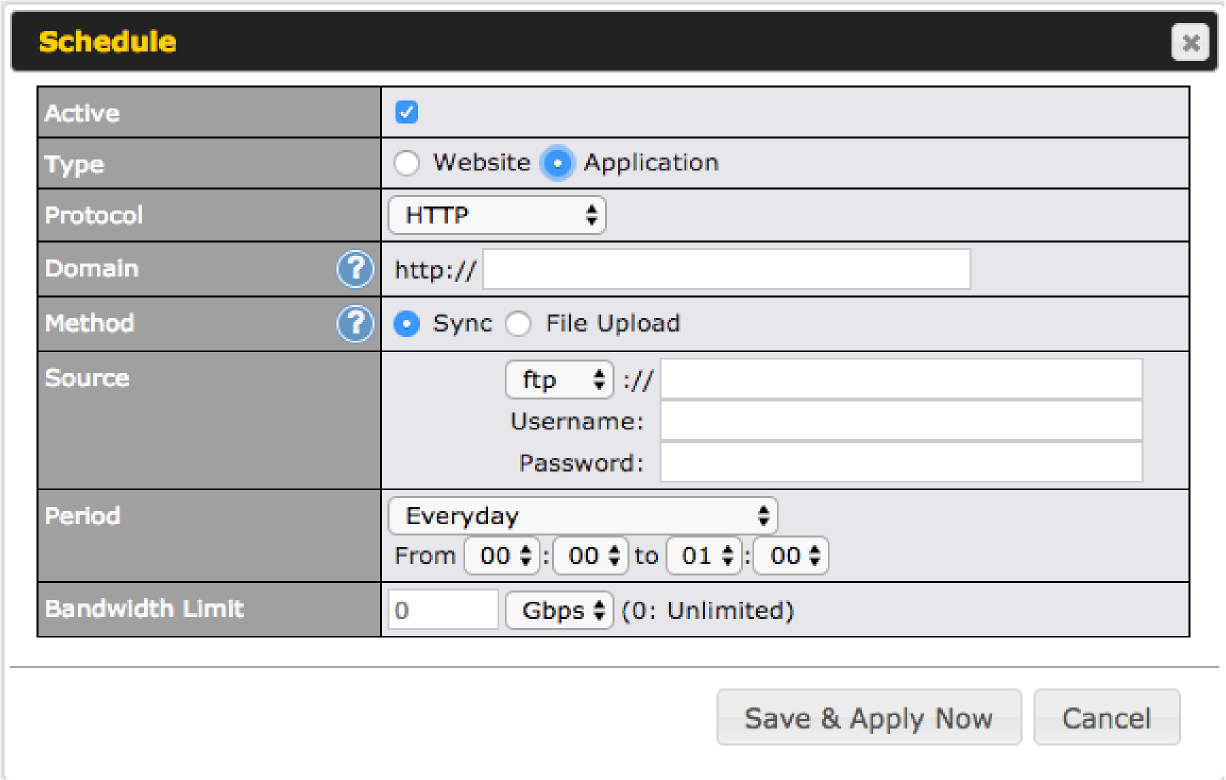


(Last Update: Tue May 23 04:02:36 UTC 2017)

Package List

Node.js Version: 6.9.2 (17178) Size: 8.99 MB Date: Fri Feb 24 07:45:28 UTC 2017	
Python Version: 2.7.12 (17178) Size: 20.29 MB Date: Fri Feb 24 07:45:28 UTC 2017	
Ruby Version: 2.3.3 (17178) Size: 31.44 MB Date: Fri Feb 24 07:45:30 UTC 2017	

After installing the framework, you can select the type to “Application” and configure the website:



Schedule

Active	☑
Type	○ Website ● Application
Protocol	HTTP
Domain	http://
Method	● Sync ○ File Upload
Source	ftp :// Username: Password:
Period	Everyday From 00 : 00 to 01 : 00
Bandwidth Limit	0 Gbps (0: Unlimited)

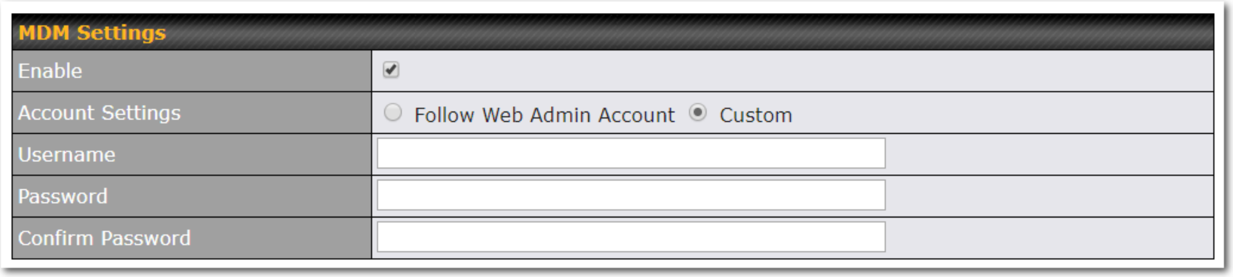
The setting is the same as Website type and you can refer to the description in the above section

For the Application type, you need to pack your application as below:

1. Implement two bash script files, start.sh and stop.sh in root folder, to start and stop your application. the Mediafast router will only execute start.sh and stop.sh when the corresponding website is enabled and disabled respectively.
2. Compress your application files and the bash script to tar.gz format.
3. Upload this tar file to the router.

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	☑
Account Settings	○ Follow Web Admin Account ● Custom
Username	
Password	
Confirm Password	

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

Please refer to the knowledgebase for information about enrolling client devices to MDM:
https://forum.peplink.com/t/how-to-enroll-a-device-to-the-mdm-server/8454

Docker

MediaFast enabled routers can host Docker containers when running firmware 7.1 or later.

Docker is an open platform for developing, shipping, and running applications.

From firmware version 7.1.0 upwards it is possible to install and run Docker Containers on your Peplink Mediafast 500 or 750 router.

Due to the nature of Docker and its unlimited variables; this feature is supported by Peplink up to the point of creating a running Docker Container.

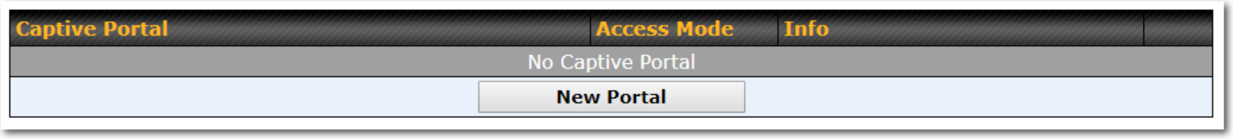
Information about Docker can be found on the Docker Documentation site: https://docs.docker.com/ 2

This will allow you to run for example a file sharing platform (Owncloud), a web server (Wordpress, Joomla) , a learning platform (Moodle) or a visualisation tool for viewing large scale data (Kibana).

The Peplink router will search through the Docker Hub repository when creating a new Docker Container.
https://hub.docker.com/explore/ 7

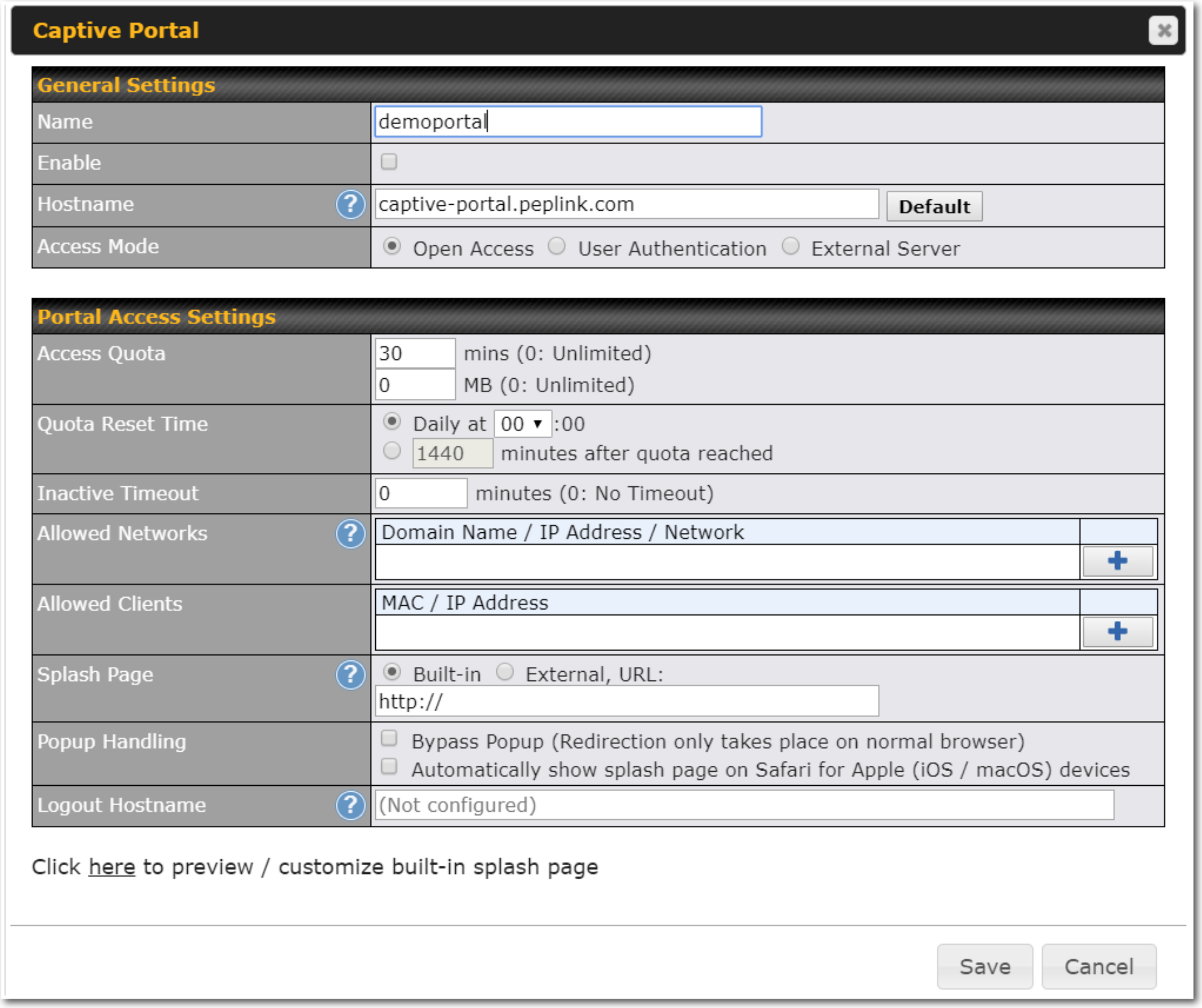
For detailed configuration instructions please refer to our knowledge base:
https://forum.peplink.com/t/how-to-run-a-docker-application-on-a-peplink-mediafast-router/16021

12.9 Captive Portal



Captive Portal	Access Mode	Info
No Captive Portal		

The captive portal serves as a 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

General Settings

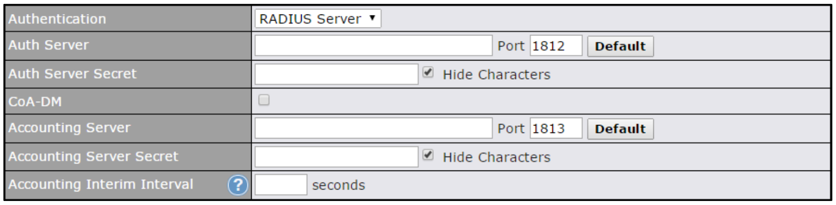
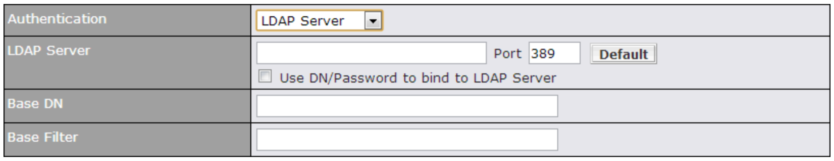
Name	demoportal
Enable	□
Hostname	captive-portal.peplink.com [Default]
Access Mode	● Open Access ○ User Authentication ○ External Server

Portal Access Settings

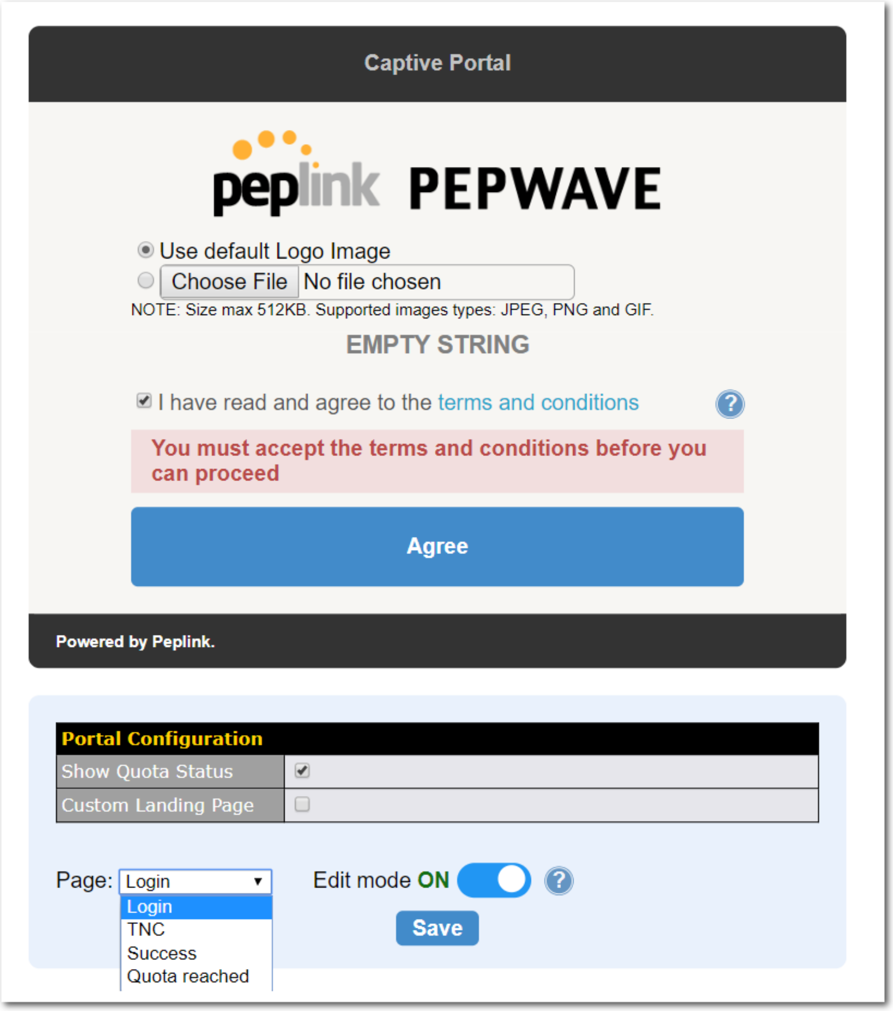
Access Quota	30 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	● Daily at 00 :00 ○ 1440 minutes after quota reached
Inactive Timeout	0 minutes (0: No Timeout)
Allowed Networks	Domain Name / IP Address / Network
Allowed Clients	MAC / IP Address
Splash Page	● Built-in ○ External, URL: http://
Popup Handling	□ Bypass Popup (Redirection only takes place on normal browser) □ Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	(Not configured)

Click here to preview / customize built-in splash page

Captive Portal Settings

Enable	Check **Enable** and then, optionally, select the LANs/VLANs that will use the captive portal.
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click **Default**.
Access Mode	Click **Open Access** to allow clients to freely access your router. Click **User Authentication** to force your clients to authenticate before accessing your router. Select **External Server** to use the Captive Portal with a HotSpot system**.** As described in the following knowledgebase article: https://forum.peplink.com/t/using-hotspotsystem-wi-fi-on-pepwave-max-routers/
RADIUS Server	This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:  Authentication RADIUS Server ▾ Auth Server Port 1812 Default Auth Server Secret ☑ Hide Characters CoA-DM ☐ Accounting Server Port 1813 Default Accounting Server Secret ☑ Hide Characters Accounting Interim Interval ? seconds Fill in the necessary information to complete your connection to the server and enable authentication.
LDAP Server	This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:  Authentication LDAP Server ▾ LDAP Server Port 389 Default ☐ Use DN/Password to bind to LDAP Server Base DN Base Filter Fill in the necessary information to complete your connection to the server and enable authentication.
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.

Inactive Timeout	Clients will get disconnected when the inactive the configured time is reached. Default 0: no timeout
Allowed Networks	To whitelist a network, enter the domain name / IP address here and click + . To delete an existing network from the list of allowed networks, click the ✖ button next to the listing.
Allowed Clients	To whitelist a client, enter the MAC address / IP address here and click + . To delete an existing client from the list of allowed clients, click the ✖ button next to the listing.
Splash Page	Here, you can choose between using the Balance's built-in captive portal and redirecting clients to a URL you define.
Popup Handling	Configurable options for popup handling: - Bypass Popup (Redirection only takes place on normal browser) - Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostnan	A hostname that can be used to logout captive portal when being accessed on browser.
Customize splash page	Click on the provided link in the Captive portal profile to customize the splash page. A new browser tab is opened with a WYSIWYG editor of the splash page o edit the content, click on the corresponding element after switching Edit Mode to ON.



Captive Portal

● Use default Logo Image
○ Choose File No file chosen
NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.

EMPTY STRING

☑ I have read and agree to the terms and conditions

You must accept the terms and conditions before you can proceed

Agree

Powered by Peplink.

Portal Configuration	
Show Quota Status	☑
Custom Landing Page	□

Page: Login ▾   Edit mode ON

Login
TNC
Success
Quota reached

Save

12.10 QoS

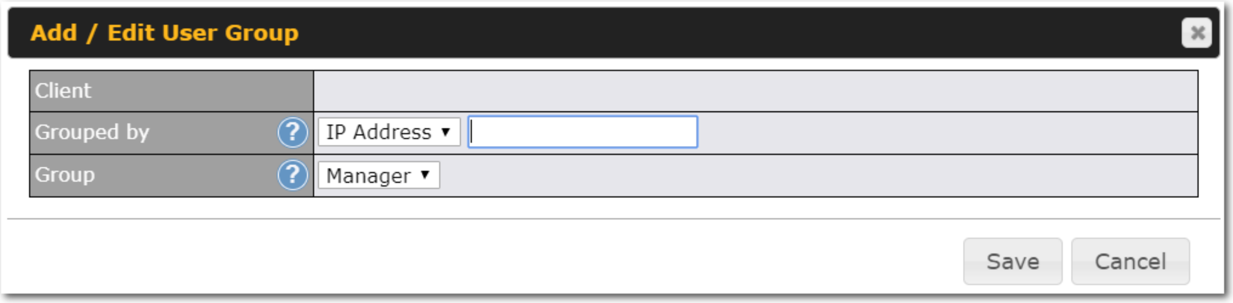
12.10.1 User Groups

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 predefined 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

Client	
Grouped by	IP Address ▾
Group	Manager ▾

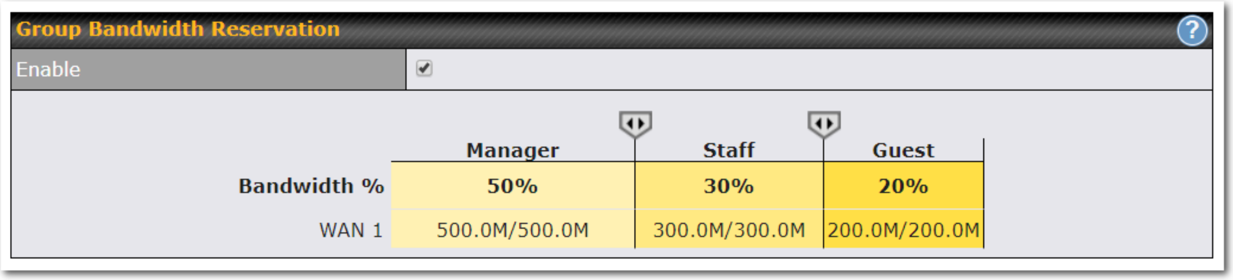
Add / Edit User Group	
Subnet / IP Address	From the drop-down menu, choose whether you are going to define the client(s) by an **IP Address** or a **Subnet**. If **IP Address** is selected, enter a name defined in DHCP reservation table or a LAN client's IP address. If **Subnet** is selected, enter a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

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

12.10.2 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.

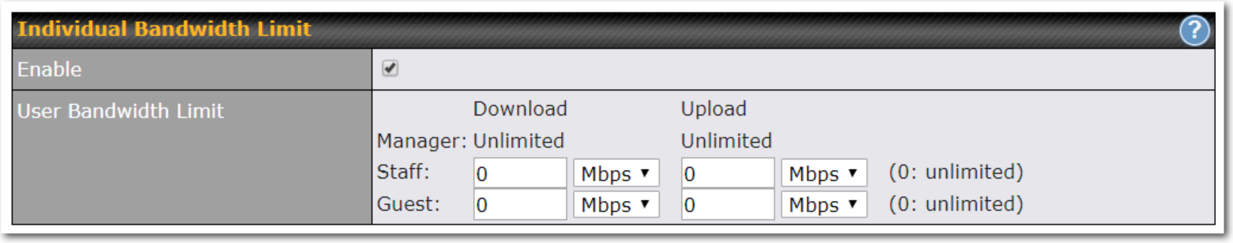


Group Bandwidth Reservation

Enable ☑

	Manager	Staff	Guest
Bandwidth %	50%	30%	20%
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M

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**).

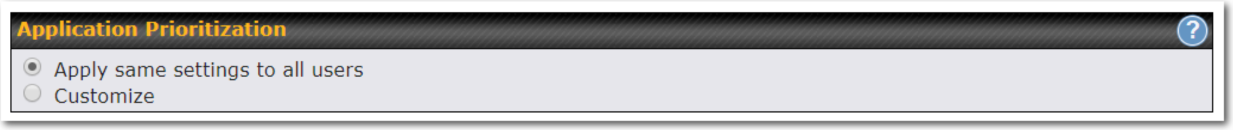


Individual Bandwidth Limit

Enable	☑			
User Bandwidth Limit		Download	Upload	
	Manager:	Unlimited	Unlimited	
	Staff:	0 Mbps ▾	0 Mbps ▾	(0: unlimited)
	Guest:	0 Mbps ▾	0 Mbps ▾	(0: unlimited)

12.10.3 Application

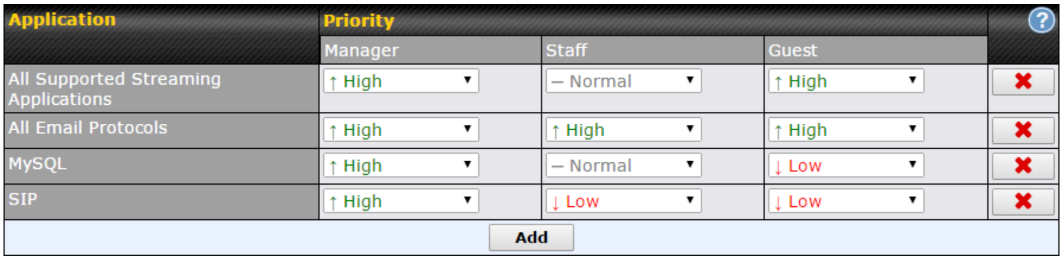
You can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.



Application Prioritization

● Apply same settings to all users
○ Customize

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



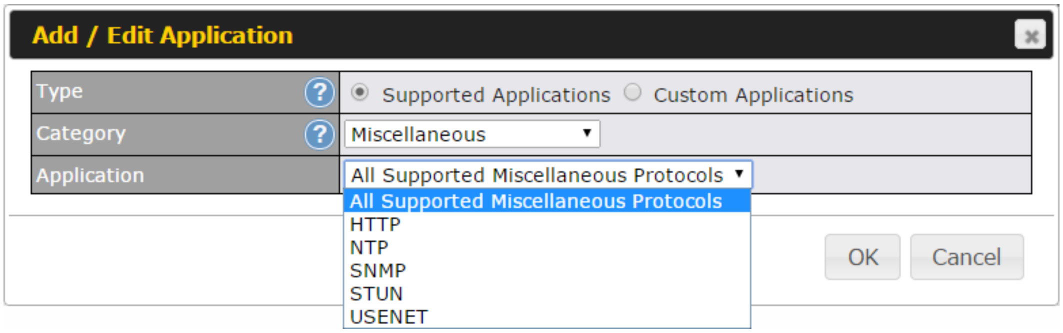
Application	Priority			
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High ▾	– Normal ▾	↑ High ▾	✖
All Email Protocols	↑ High ▾	↑ High ▾	↑ High ▾	✖
MySQL	↑ High ▾	– Normal ▾	↓ Low ▾	✖
SIP	↑ High ▾	↓ Low ▾	↓ Low ▾	✖

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

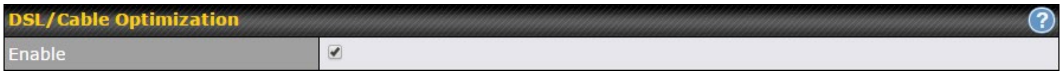
Type	● Supported Applications ○ Custom Applications
Category	Miscellaneous
Application	All Supported Miscellaneous Protocols

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.



DSL/Cable Optimization	
Enable	☑

12.11 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)

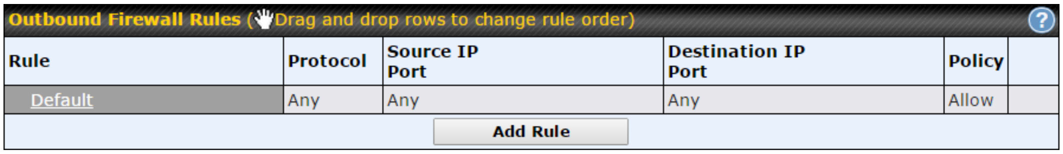
The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

12.11.1 Access Rules

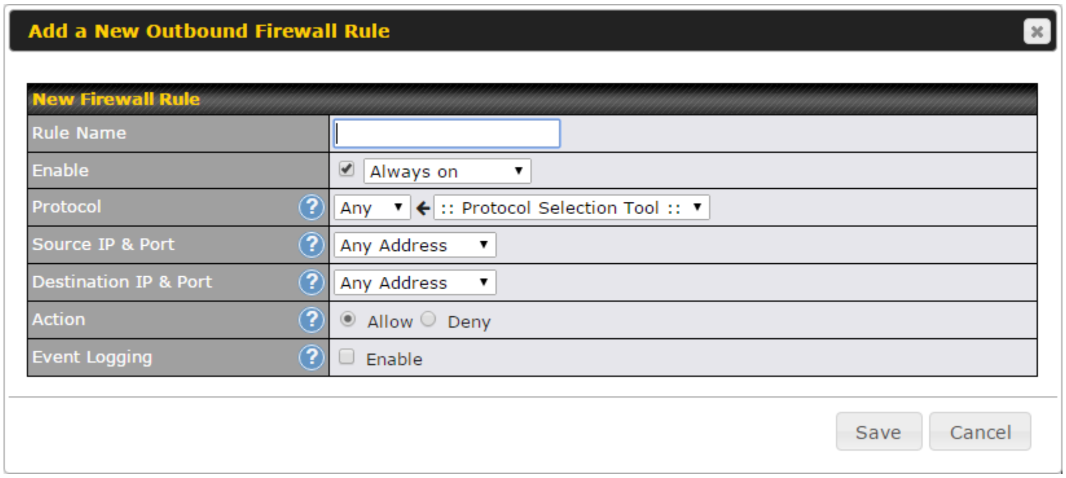
The outbound firewall settings are located at **Network>Firewall>Access Rules**.



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

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

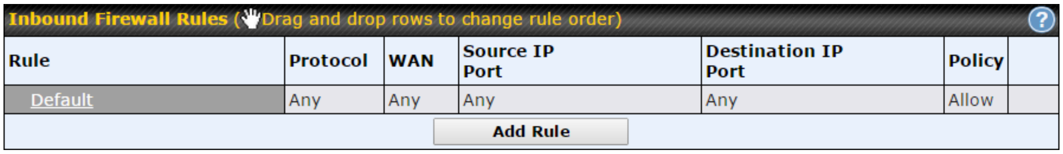
Click **Add Rule** to display the following screen:



Add a New Outbound Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑ Always on
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	□ Enable

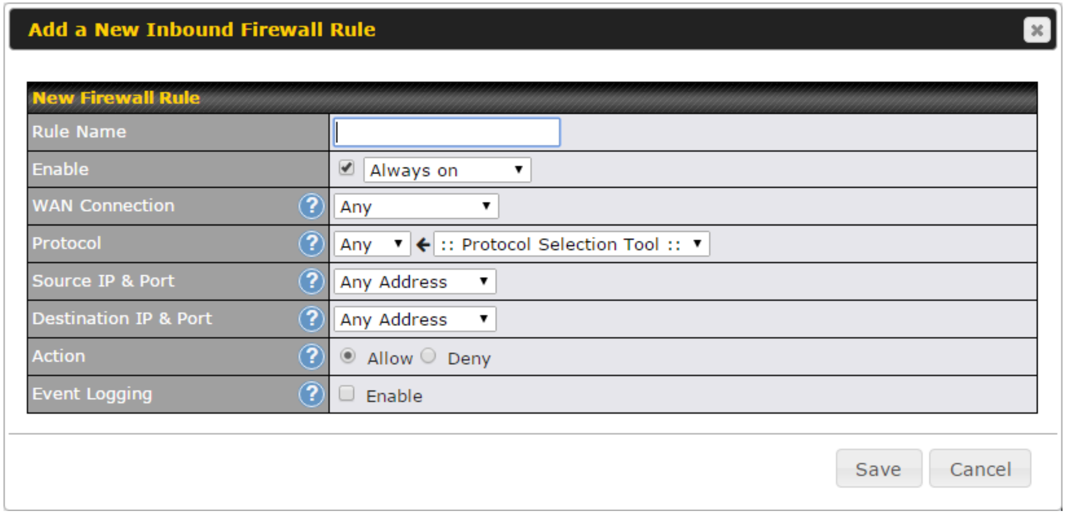
The inbound firewall settings are located at **Network>Firewall>Access Rules**.



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

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

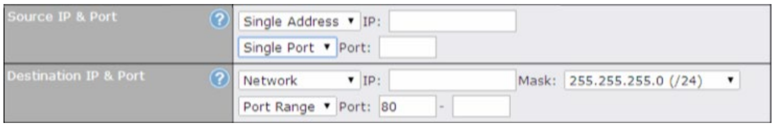
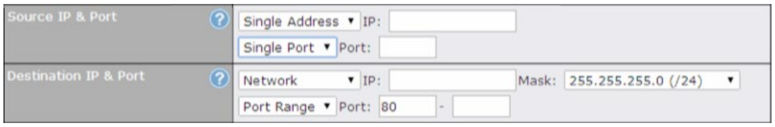
Click **Add Rule** to display the following window:



Add a New Inbound Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑ Always on
WAN Connection	Any
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	□ Enable

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

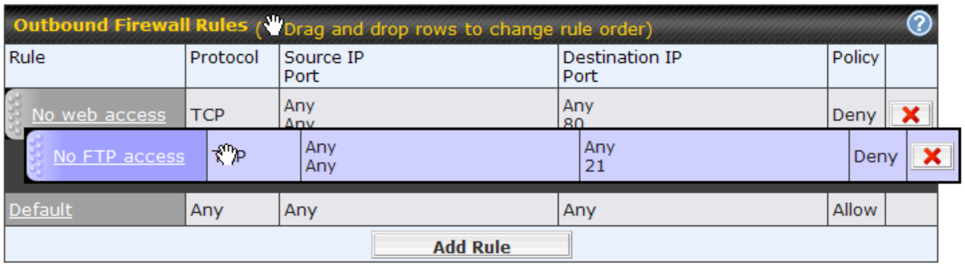
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule. Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: ● **TCP** ● **UDP** ● **ICMP** ● **IP** Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.
Source IP & Port	This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Source IP & Port** setting, as indicated with the following screenshots:  Source IP & Port: Single Address ▾ IP: Single Port ▾ Port: Destination IP & Port: Network ▾ IP: Mask: 255.255.255.0 (/24) ▾ Port Range ▾ Port: 80 - In addition, a single port, or a range of ports, can be specified for the **Source IP & Port** settings.
Destination IP & Port	This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Destination IP & Port** setting, as indicated with the following screenshots:  Source IP & Port: Single Address ▾ IP: Single Port ▾ Port: Destination IP & Port: Network ▾ IP: Mask: 255.255.255.0 (/24) ▾ Port Range ▾ Port: 80 - In addition, a single port, or a range of ports, can be specified for the **Destination IP & Port** settings.

Action	This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following: ● Source IP & port ● Destination IP & port With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded).
Event Logging	This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows: Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80 ● **CONN:** The connection where the log entry refers to ● **SRC:** Source IP address ● **DST:** Destination IP address ● **LEN:** Packet length ● **PROTO:** Protocol ● **SPT:** Source port ● **DPT:** Destination port

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

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

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



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

Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	✖
No FTP access	P	Any Any	Any 21	Deny	✖
Default	Any	Any	Any	Allow	

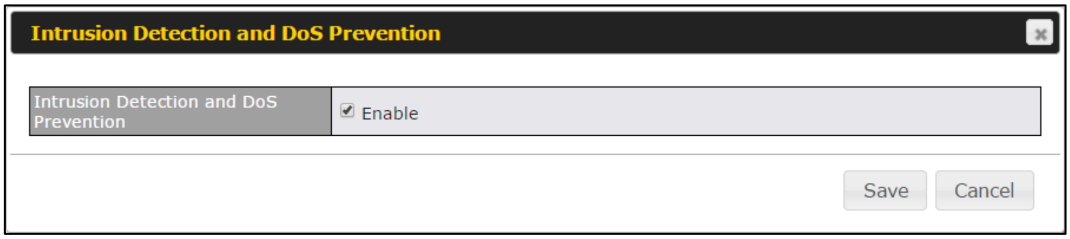
To remove a rule, click the ✖ button.

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



Intrusion Detection and DoS Prevention

Intrusion Detection and DoS Prevention	☑ Enable

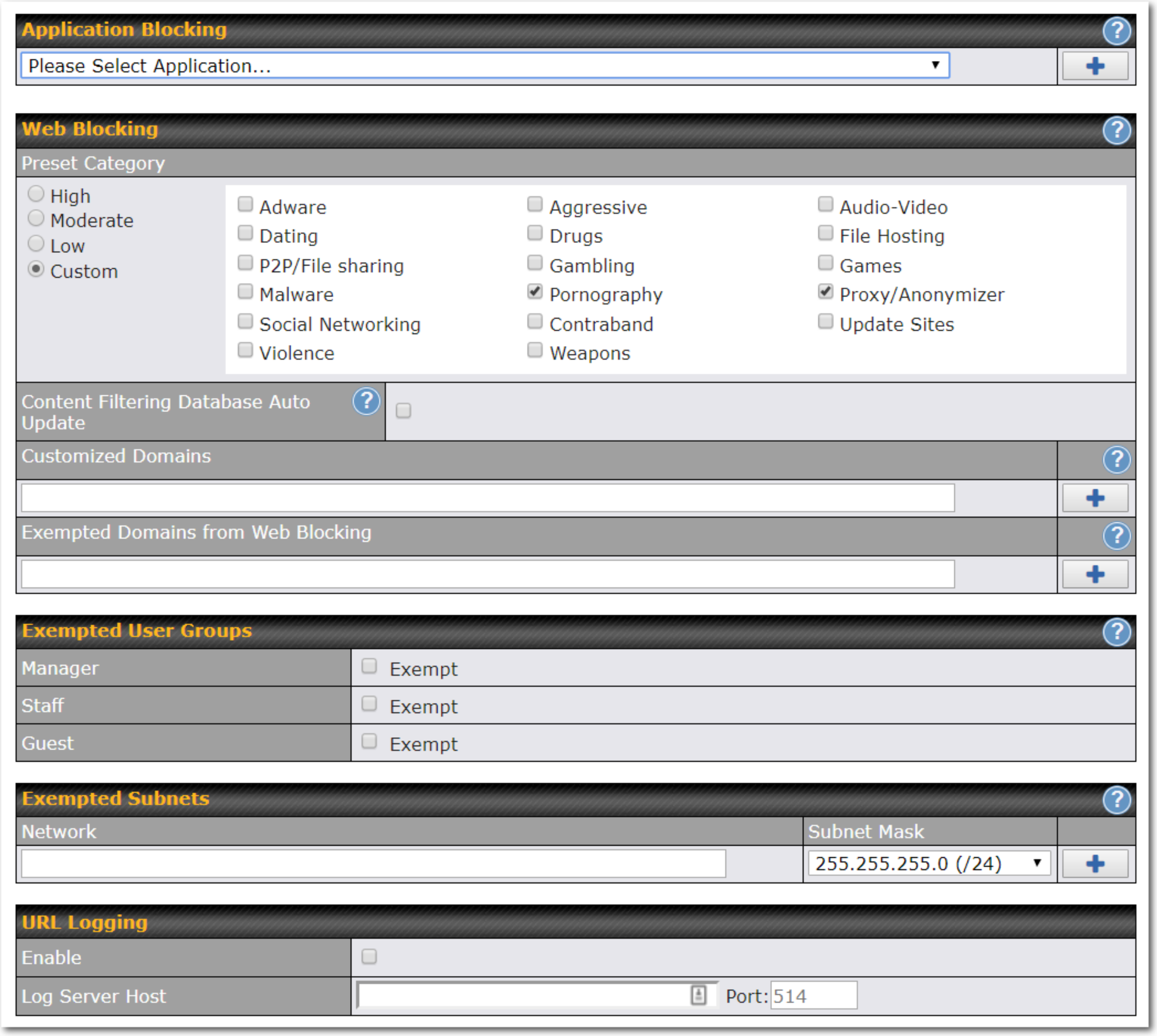
The Balance can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click ✎, check the **Enable** check box for the **Intrusion Detection and DoS Prevention**, and press the **Save** button.

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

- Port scan
  - NMAP FIN/URG/PSH
  - Xmas tree

  - Another Xmas tree
  - Null scan
  - SYN/RST
  - SYN/FIN
- SYN flood prevention
- Ping flood attack prevention

12.11.2 Content Blocking



Application Blocking

Please Select Application... ▾ +

Web Blocking

Preset Category

○ High
○ Moderate
○ Low
● Custom

□ Adware	□ Aggressive	□ Audio-Video
□ Dating	□ Drugs	□ File Hosting
□ P2P/File sharing	□ Gambling	□ Games
□ Malware	☑ Pornography	☑ Proxy/Anonymizer
□ Social Networking	□ Contraband	□ Update Sites
□ Violence	□ Weapons	

Content Filtering Database Auto Update □

Customized Domains +

Exempted Domains from Web Blocking +

Exempted User Groups

Manager	□ Exempt
Staff	□ Exempt
Guest	□ Exempt

Exempted Subnets

Network	Subnet Mask
	255.255.255.0 (/24) ▾ +

URL Logging

Enable	□
Log Server Host	Port: 514

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 website 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 and HTTPS traffic.

Customized Domains

Enter an appropriate website address, and the Peplink Balance will block and disallow LAN/PPTP/SpeedFusion^{TM} 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

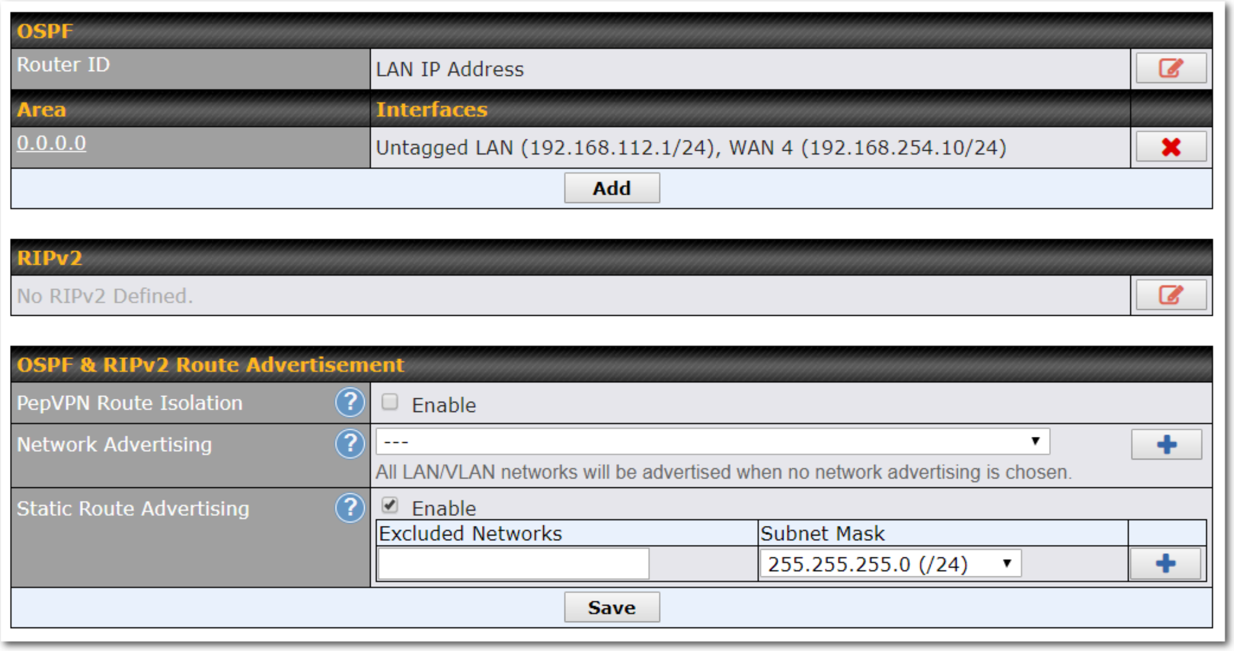
With the subnet defined in the field, clients on the particular subnet(s) can be exempted from the access blocking rules.

URL Logging

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

12.12 OSPF & RIPv2

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



OSPF		
Router ID	LAN IP Address	
Area	**Interfaces**	
0.0.0.0	Untagged LAN (192.168.112.1/24), WAN 4 (192.168.254.10/24)	✖

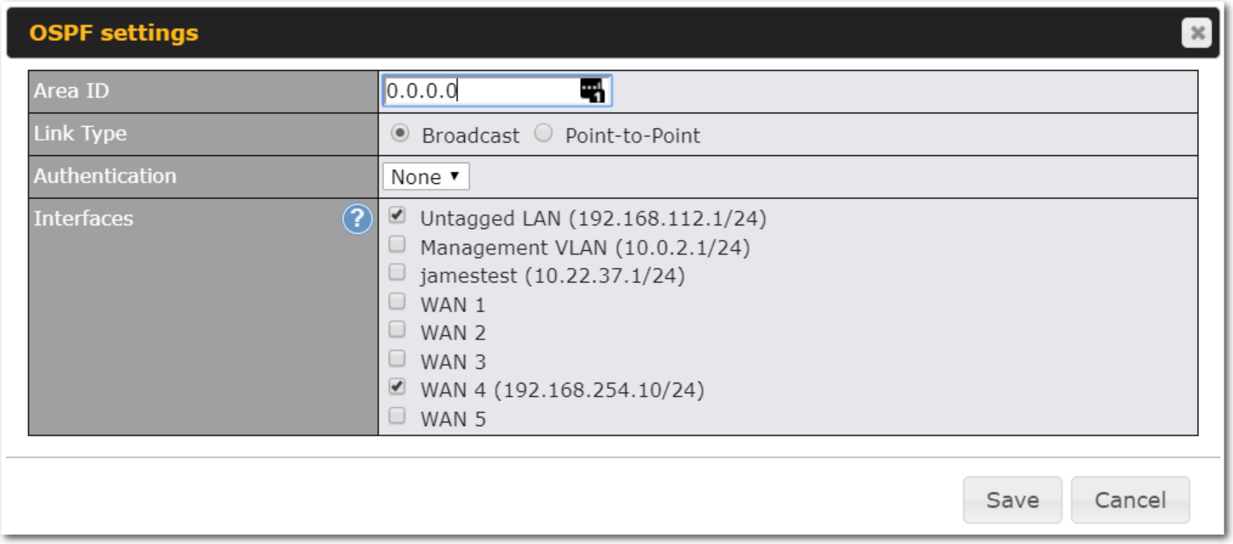
RIPv2

No RIPv2 Defined.

OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation	□ Enable		
Network Advertising	--- All LAN/VLAN networks will be advertised when no network advertising is chosen.		+
Static Route Advertising	☑ Enable		
	Excluded Networks	Subnet Mask	
		255.255.255.0 (/24)	+

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

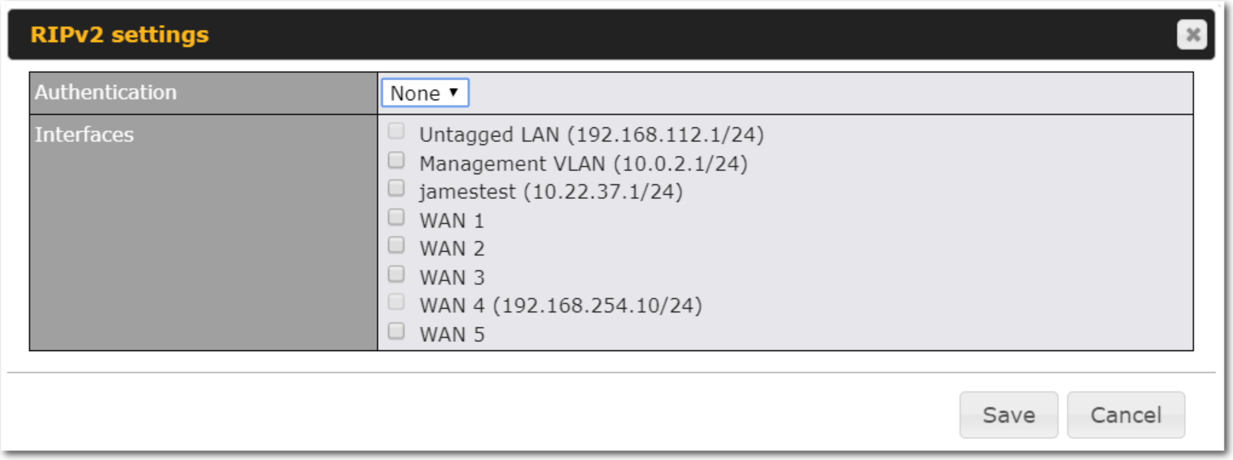


OSPF settings

Area ID	0.0.0.0
Link Type	● Broadcast ○ Point-to-Point
Authentication	None ▾
Interfaces	☑ Untagged LAN (192.168.112.1/24) ☐ Management VLAN (10.0.2.1/24) ☐ jamestest (10.22.37.1/24) ☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☑ WAN 4 (192.168.254.10/24) ☐ WAN 5

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

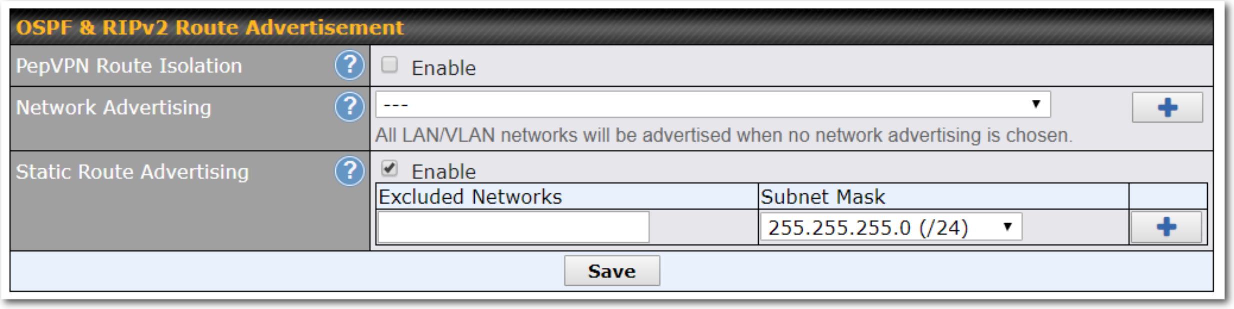
To access RIPv2 settings, click ✎.



RIPv2 settings

Authentication	None ▾
Interfaces	□ Untagged LAN (192.168.112.1/24) □ Management VLAN (10.0.2.1/24) □ jamestest (10.22.37.1/24) □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 (192.168.254.10/24) □ WAN 5

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



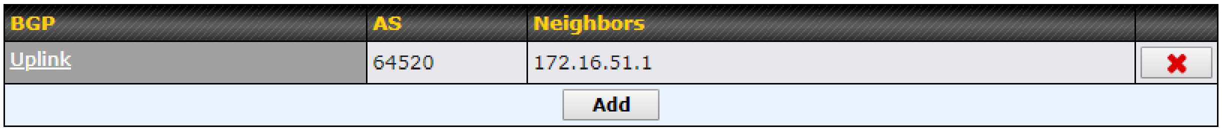
OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation	□ Enable
Network Advertising	--- ▾ All LAN/VLAN networks will be advertised when no network advertising is chosen.
Static Route Advertising	☑ Enable Excluded Networks / Subnet Mask: 255.255.255.0 (/24) ▾

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

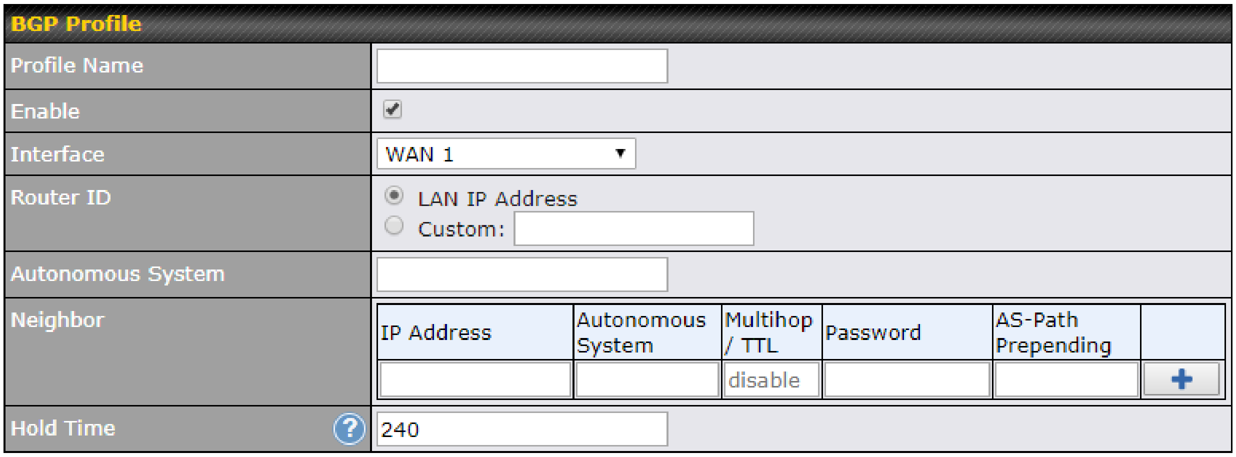
12.13 BGP

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	✖

Click "x" to delete a BGP profile
Click "Add" to add a new BGP profile

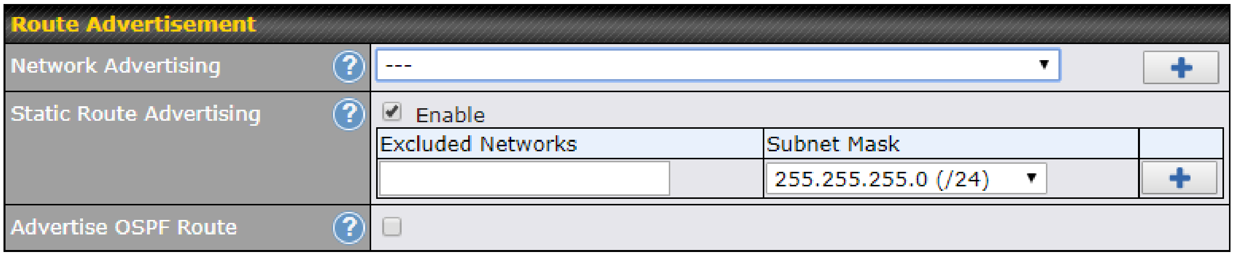


BGP Profile

Profile Name	
Enable	☑
Interface	WAN 1 ▾
Router ID	● LAN IP Address ○ Custom:
Autonomous System	
Neighbor	IP Address / Autonomous System / Multihop / TTL: disable / Password / AS-Path Prepending / +
Hold Time ?	240

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

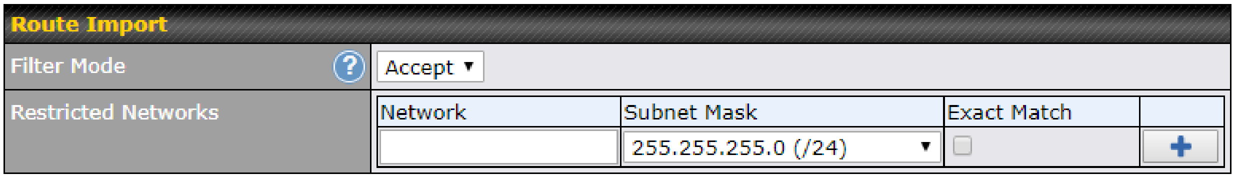
Multihop/TTL	Time-to-live (TTL) of BGP packet. Leave it blank if BGP neighbor is directly connected, otherwise you must specify a TTL value. Accurately, this option should be used if the configured neighbor IP address does not match the selected Interface's network subnets. TTL value must be between 2 to 255.
Password	Optional password for MD5 authentication of BGP sessions.
AS-Path Prepending:	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.
Hold Time	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	☑ Enable Excluded Networks / Subnet Mask: 255.255.255.0 (/24)
Advertise OSPF Route	□

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

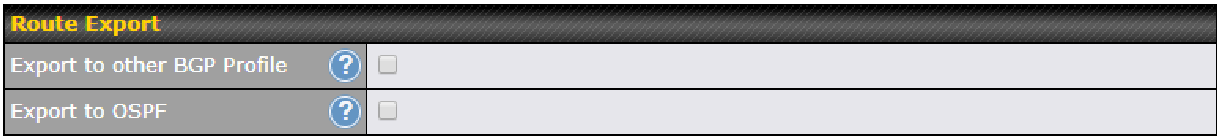


Route Import

Filter Mode	Accept
Restricted Networks	Network / Subnet Mask: 255.255.255.0 (/24) / Exact Match: □

Filter Mode	This option selects the route import filter mode.

	None: all BGP routes will be accepted. **Accept**: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. **Reject**: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks	This specifies the network in the "route import" entry **Exact Match:** 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.



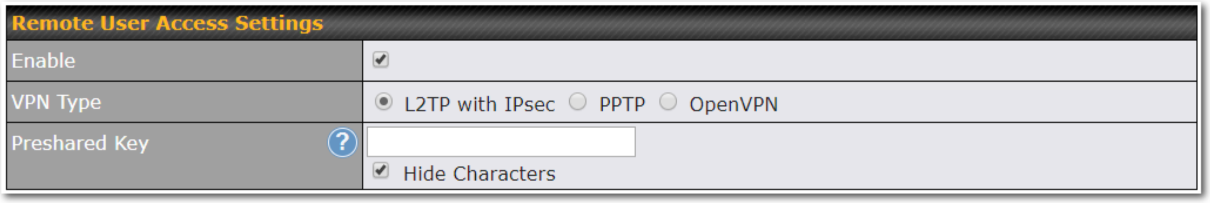
Route Export	
Export to other BGP Profile ?	□
Export to OSPF ?	□

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

12.14 Remote User Access

A remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the Internet. Networks routed by a Peplink router can be remotely accessed via OpenVPN, L2TP with IPsec or PPTP. To configure this feature, navigate to **Network > Remote User Access** and choose the required VPN type.

12.14.1 L2TP with IPsec



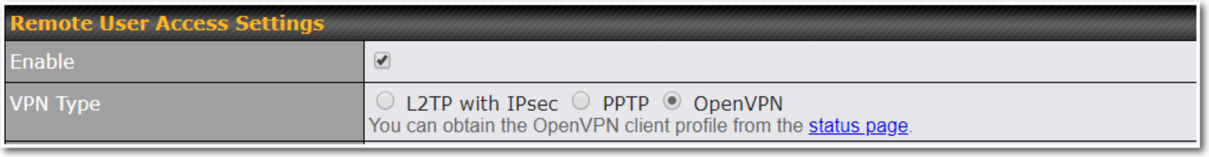
Remote User Access Settings	
Enable	☑
VPN Type	● L2TP with IPsec ○ PPTP ○ OpenVPN
Preshared Key ?	 ☑ Hide Characters

L2TP with IPsec Remote User Access Settings

Pre-shared Key	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
Listen On	This setting is for specifying the WAN IP addresses that allow remote user access.
Disable Weak Ciphers	Click the ? button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.

Continue to configure the authentication method.

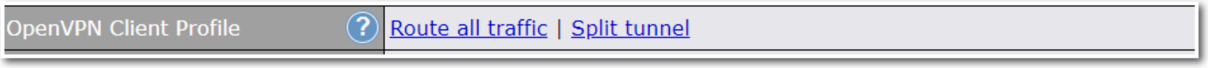
12.14.2 OpenVPN



Remote User Access Settings	
Enable	☑
VPN Type	○ L2TP with IPsec ○ PPTP ● OpenVPN You can obtain the OpenVPN client profile from the status page.

Select OpenVPN and continue to configure the authentication method.

The OpenVPN Client profile can be downloaded from the **Status > device** page after the configuration has been saved.



OpenVPN Client Profile ?	Route all traffic | Split tunnel

You have a choice between 2 different OpenVPN Client profiles.

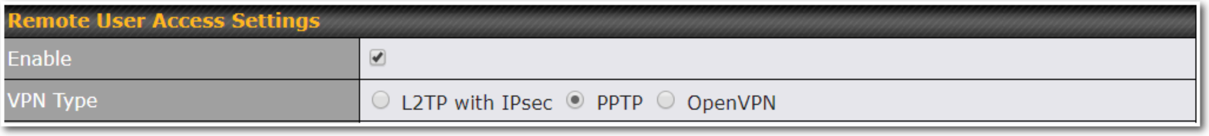
13 "route all traffic" profile

Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel

14 "split tunnel" profile

Using this profile, VPN clients will ONLY send those traffic designated to the untagged LAN and VLAN segment through the OpenVPN tunnel.

14.1.1 PPTP



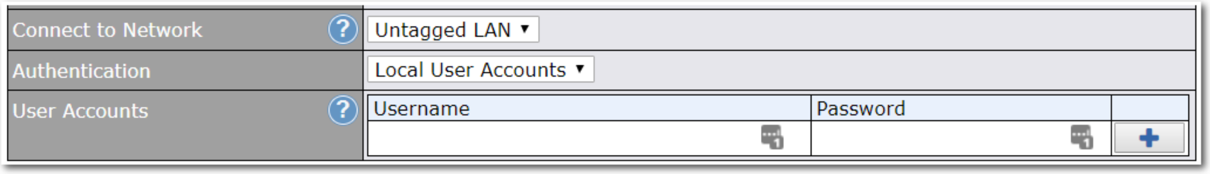
Remote User Access Settings	
Enable	☑
VPN Type	○ L2TP with IPsec ● PPTP ○ OpenVPN

No additional configuration required.

The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private

networks. PPTP has many well known security issues
Continue to configure authentication method.

14.1.2 Authentication Methods



Connect to Network ?	Untagged LAN ▾
Authentication	Local User Accounts ▾
User Accounts ?	Username | Password | +

Authentication Method	
Connect to Network	Select the VLAN network for remote users to enable remote user access on.
Authentication	Determine the method of authenticating remote users

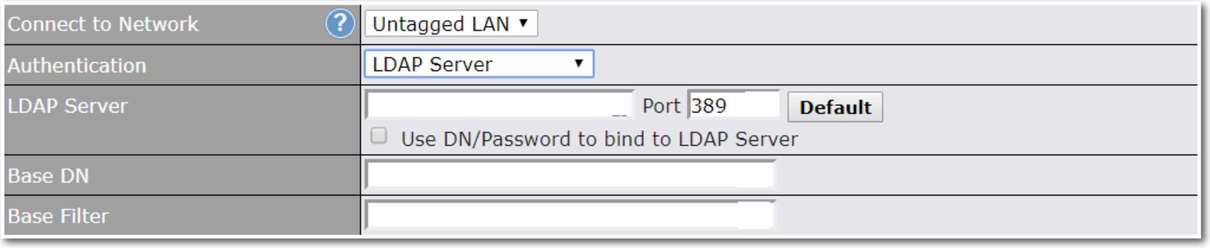
User accounts:

This setting allows you to define the Remote 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.

Note:

The username must contain lowercase letters, numerics, underscore(_), dash(-), at sign(@), and period(.) only.
The password must be between 8 and 12 characters long.

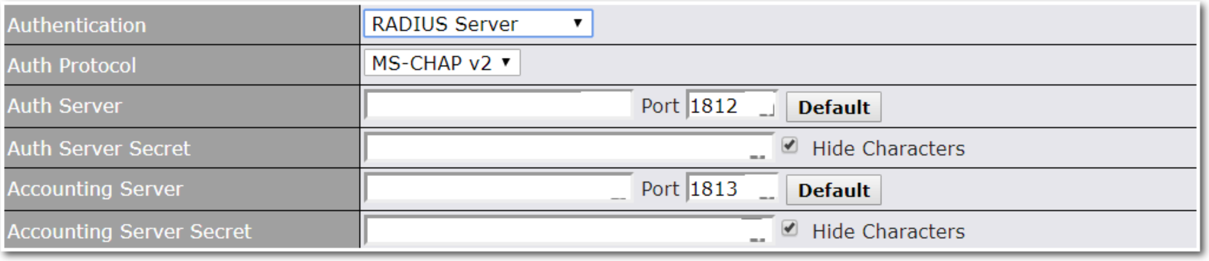
LDAP Server:



Connect to Network ?	Untagged LAN ▾
Authentication	LDAP Server ▾
LDAP Server	Port 389 Default □ Use DN/Password to bind to LDAP Server
Base DN	
Base Filter	

Enter the matching LDAP server details to allow for LDAP server authentication.

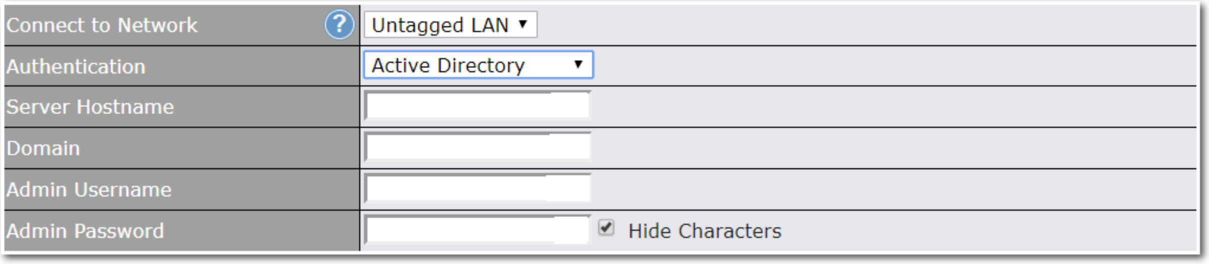
Radius Server:



Authentication	RADIUS Server ▾
Auth Protocol	MS-CHAP v2 ▾
Auth Server	Port 1812 Default
Auth Server Secret	☑ Hide Characters
Accounting Server	Port 1813 Default
Accounting Server Secret	☑ Hide Characters

Enter the matching Radius server details to allow for Radius server authentication.

Active Directory:



Connect to Network ?	Untagged LAN ▾
Authentication	Active Directory ▾
Server Hostname	
Domain	
Admin Username	
Admin Password	☑ Hide Characters

Enter the matching Active Directory details to allow for Active Directory server authentication.

14.2 Misc. Settings

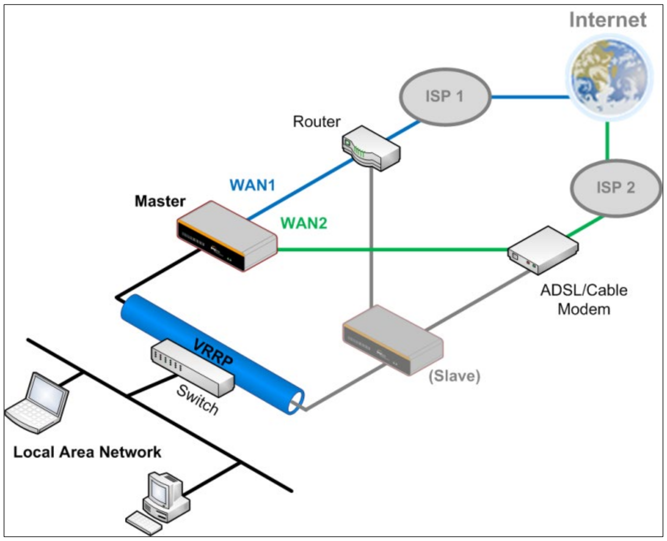
14.2.1 High Availability

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:



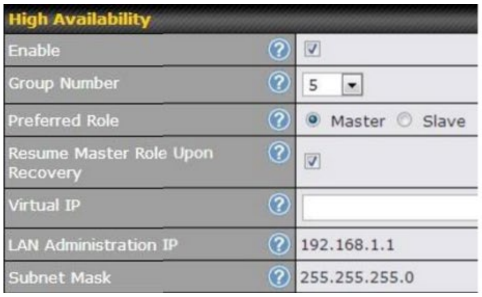
In the diagram, the WAN ports of each Peplink Balance unit connect to the router and to the modem. Both Peplink Balance units connect to the same LAN switch via a LAN port.

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.

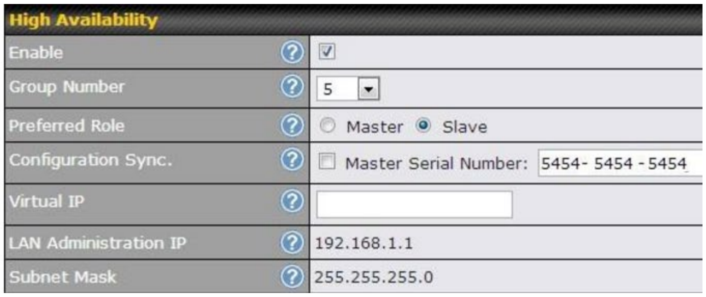
You can configure high availability at **Network>Misc. Settings>High Availability**.

Interface for Master Router



High Availability	
Enable	☑
Group Number	5
Preferred Role	● Master ○ Slave
Resume Master Role Upon Recovery	☑
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

Interface for Slave Router

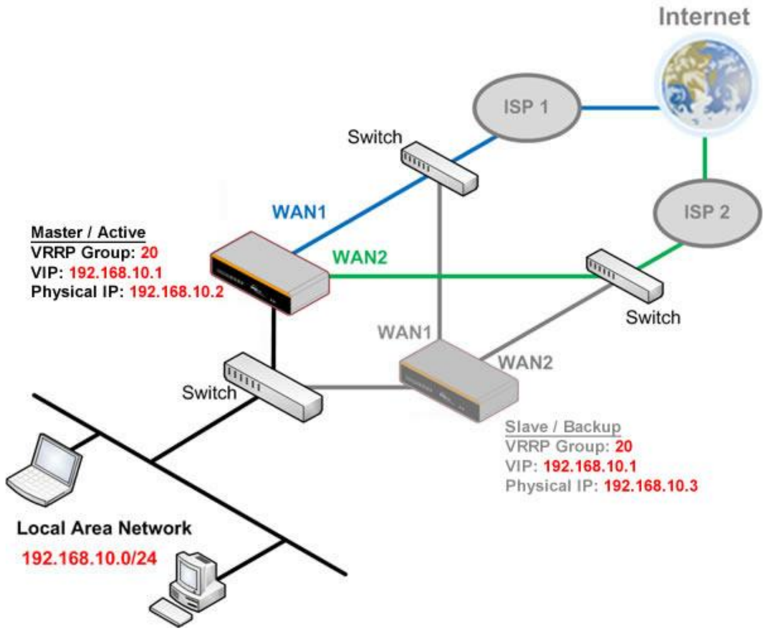


High Availability	
Enable	☑
Group Number	5
Preferred Role	○ Master ● Slave
Configuration Sync.	☐ Master Serial Number: 5454- 5454 - 5454
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

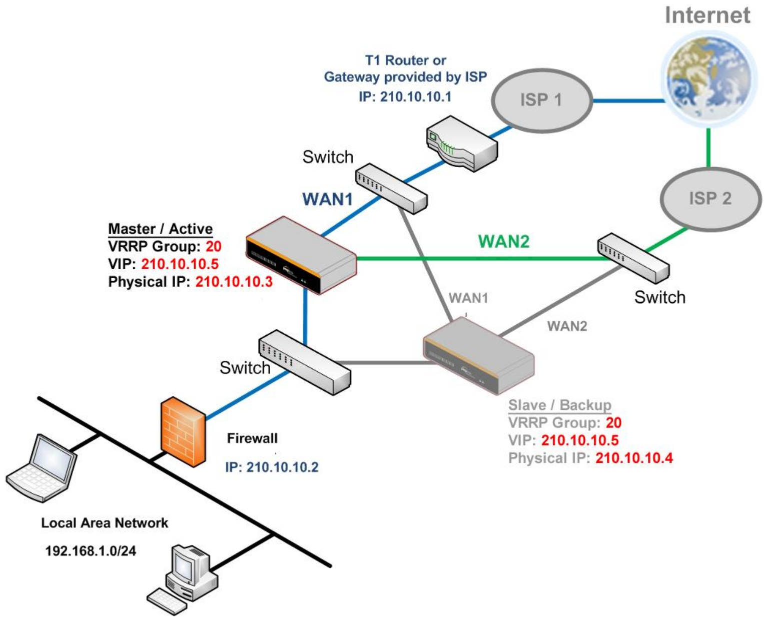
High Availability	
Enable	Checking this box specifies that the Peplink Balance unit is part of a high availability configuration.
Group Number	This number identifies a pair of Peplink Balance units operating in a high availability configuration. The two Peplink Balance units in the pair must have the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

Important Note

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

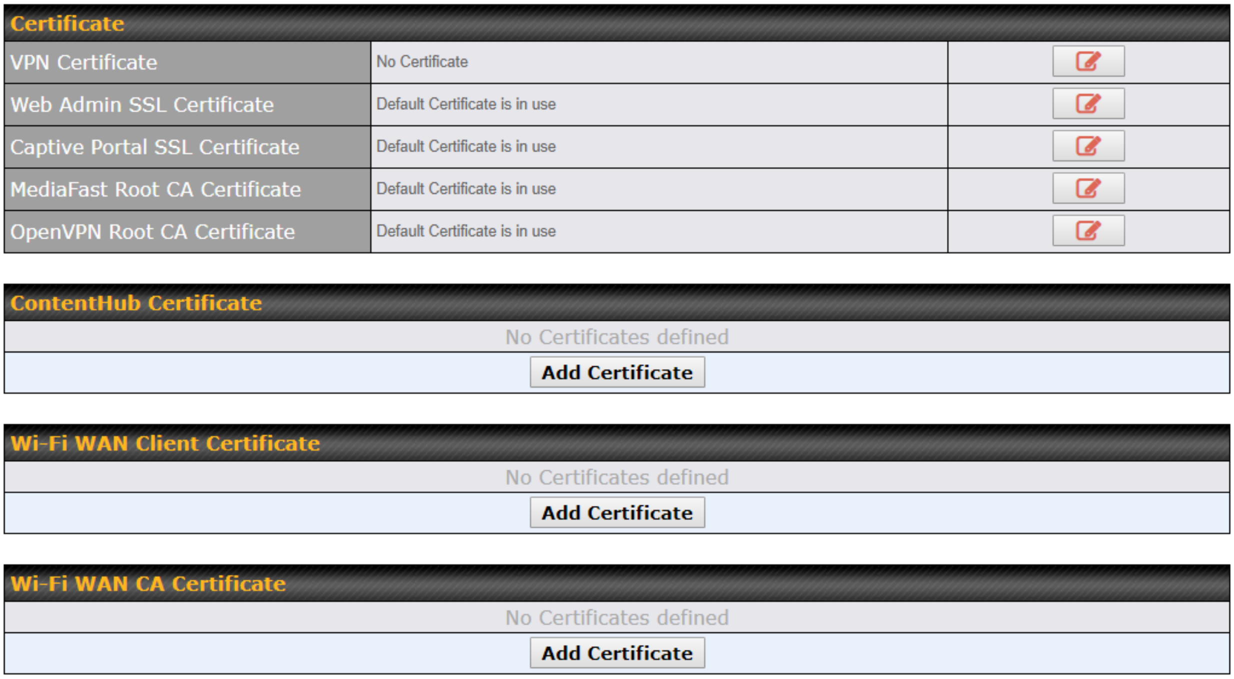


In drop-in mode, no other configuration needs to be set.



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

14.2.2 Certificate Manager



Certificate		
VPN Certificate	No Certificate	✎
Web Admin SSL Certificate	Default Certificate is in use	✎
Captive Portal SSL Certificate	Default Certificate is in use	✎
MediaFast Root CA Certificate	Default Certificate is in use	✎
OpenVPN Root CA Certificate	Default Certificate is in use	✎

ContentHub Certificate
No Certificates defined
Add Certificate

Wi-Fi WAN Client Certificate
No Certificates defined
Add Certificate

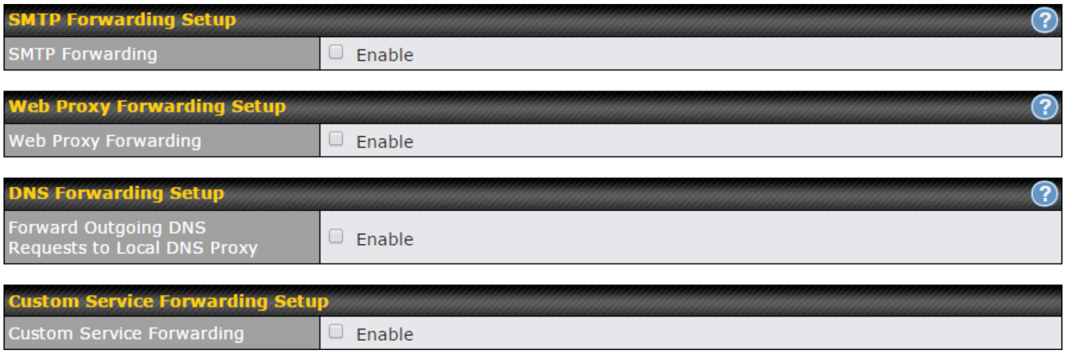
Wi-Fi WAN CA Certificate
No Certificates defined
Add Certificate

This section allows you to assign certificates for the local VPN, OpenVPN, Captive Portal, Mediafast, ContentHub, Wi-Fi WAN (Client and CA) and web admin SSL for extra security.

Read the following knowledgebase article for full instructions on how to create and import a self-signed certificate: https://forum.peplink.com/t/how-to-create-a-self-signed-certificate-and-import-it-to-a-peplink-product/

14.2.3 Service Forwarding

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



SMTP Forwarding Setup	?
SMTP Forwarding	□ Enable

Web Proxy Forwarding Setup	?
Web Proxy Forwarding	□ Enable

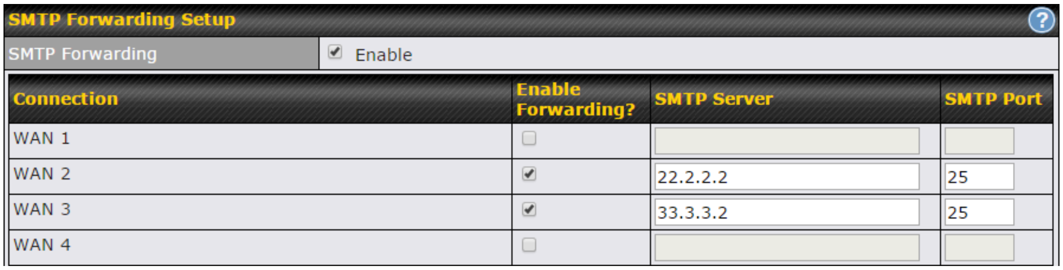
DNS Forwarding Setup	?
Forward Outgoing DNS Requests to Local DNS Proxy	□ Enable

Custom Service Forwarding Setup	
Custom Service Forwarding	□ Enable

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

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	☑ Enable

Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	☐		
WAN 2	☑	22.2.2.2	25
WAN 3	☑	33.3.3.2	25
WAN 4	☐		

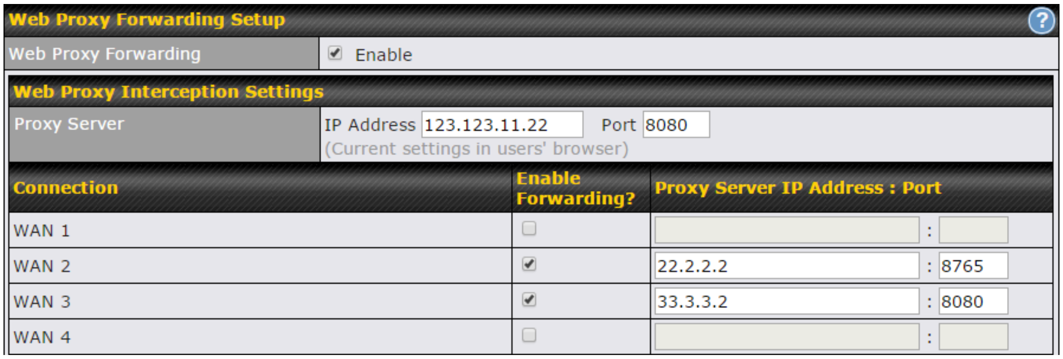
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

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	☑ Enable

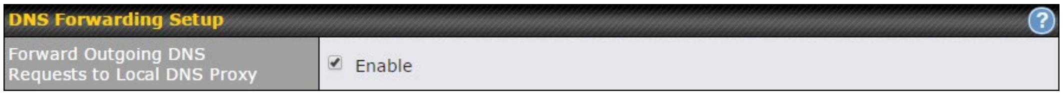
Web Proxy Interception Settings

Proxy Server	IP Address 123.123.11.22 Port 8080 (Current settings in users' browser)

Connection	Enable Forwarding?	Proxy Server IP Address : Port
WAN 1	☐	:
WAN 2	☑	22.2.2.2 : 8765
WAN 3	☑	33.3.3.2 : 8080
WAN 4	☐	:

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.

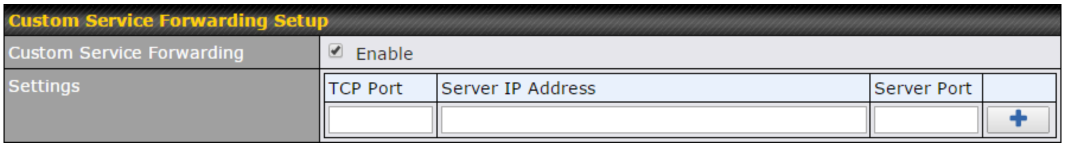
DNS Forwarding



DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	☑ 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

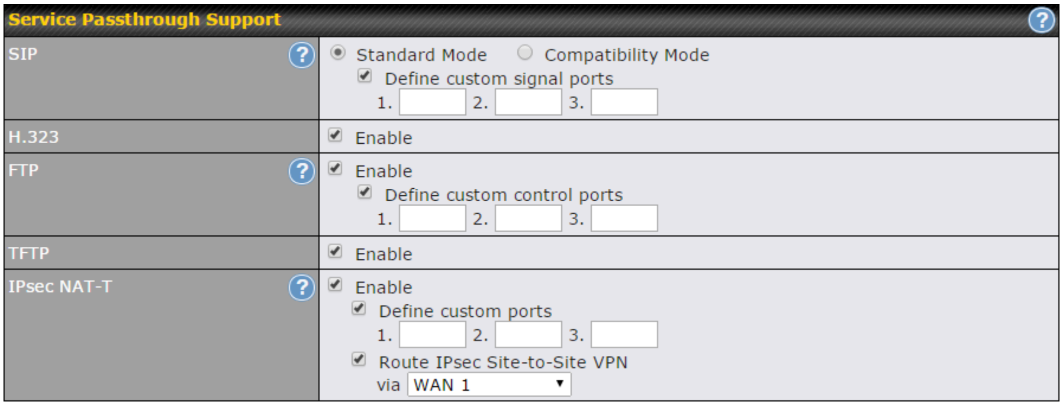


Custom Service Forwarding Setup	
Custom Service Forwarding	☑ Enable
Settings	TCP Port / Server IP Address / Server Port / +

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.

14.2.4 Service Passthrough

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



Service Passthrough Support	
SIP	● Standard Mode ○ Compatibility Mode ☑ Define custom signal ports 1. 2. 3.
H.323	☑ Enable
FTP	☑ Enable ☑ Define custom control ports 1. 2. 3.
TFTP	☑ Enable
IPsec NAT-T	☑ Enable ☑ Define custom ports 1. 2. 3. ☑ Route IPsec Site-to-Site VPN via WAN 1

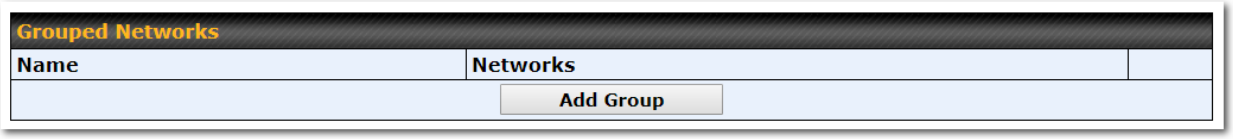
(Registered trademarks are copyrighted by their respective owner)

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

Service Passthrough Support	
SIP	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Peplink Balance can act as a SIP application layer gateway (ALG) which binds connections for the same SIP

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

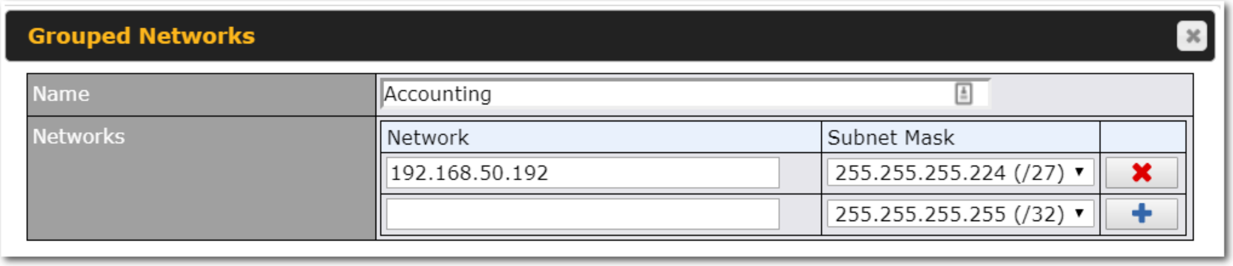
14.2.5 Grouped Networks


Grouped Networks

Name	Networks	

Using "Grouped Networks" you can group and name a range of IP addresses, which can then be used to define firewall rules or outbound policies.

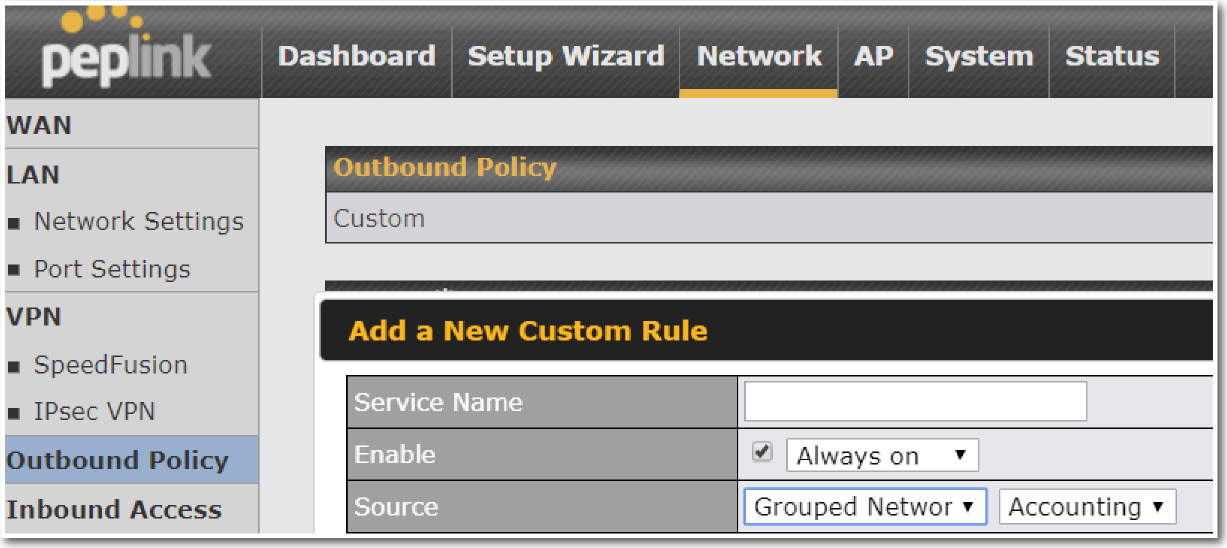
Start by clicking on “add group” then fill in the appropriate field. In this example we’ll create a group “accounting” Click save when you have finished adding the required networks.



Name	Accounting
Networks	

Network	Subnet Mask	
192.168.50.192	255.255.255.224 (/27) ▾	✖
	255.255.255.255 (/32) ▾	✚

The grouped network “accounting” can now be used to configure a group policy or firewall rule.



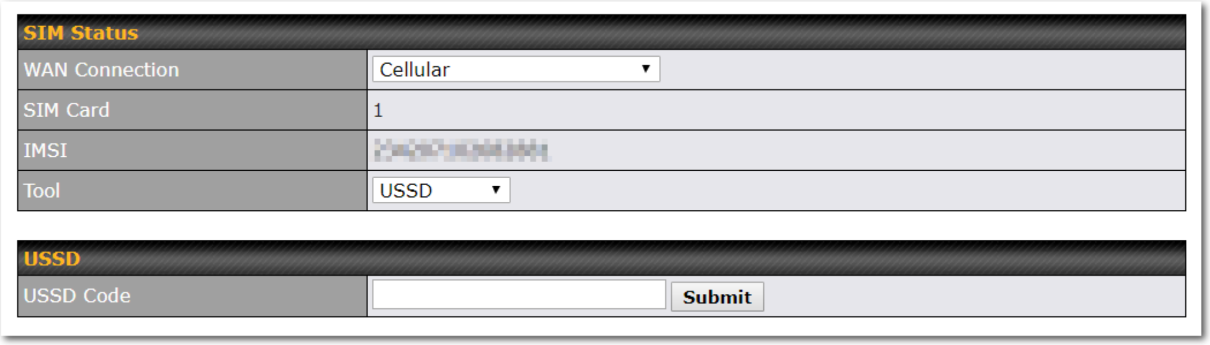
Service Name	
Enable	☑ Always on ▾
Source	Grouped Networ ▾ Accounting ▾

14.2.6 SIM Toolkit

The SIM Toolkit ,accessible via **Networks > Misc Settings > SIM Toolkit**, supports two functionalities, USSD and SMS.

USSD

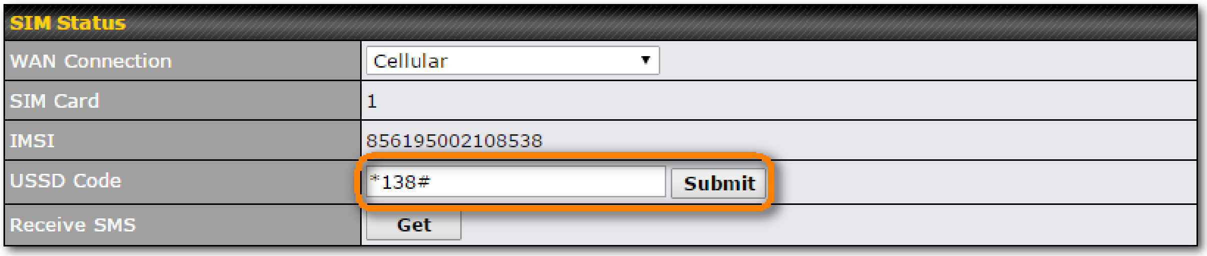
Unstructured Supplementary Service Data (USSD) is a protocol used by mobile phones to communicate with their service provider’s computers. One of the most common uses is to query the available balance.



SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	[redacted]
Tool	USSD ▾

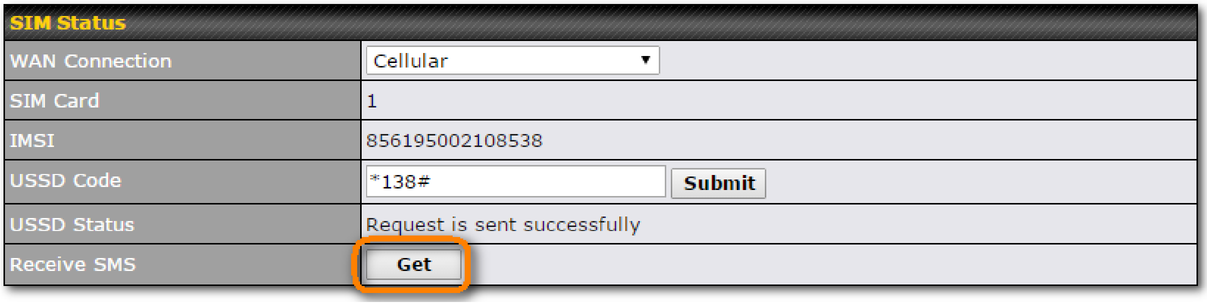
USSD	
USSD Code	Submit

Enter your USSD code under the **USSD Code** text field and click **Submit**.



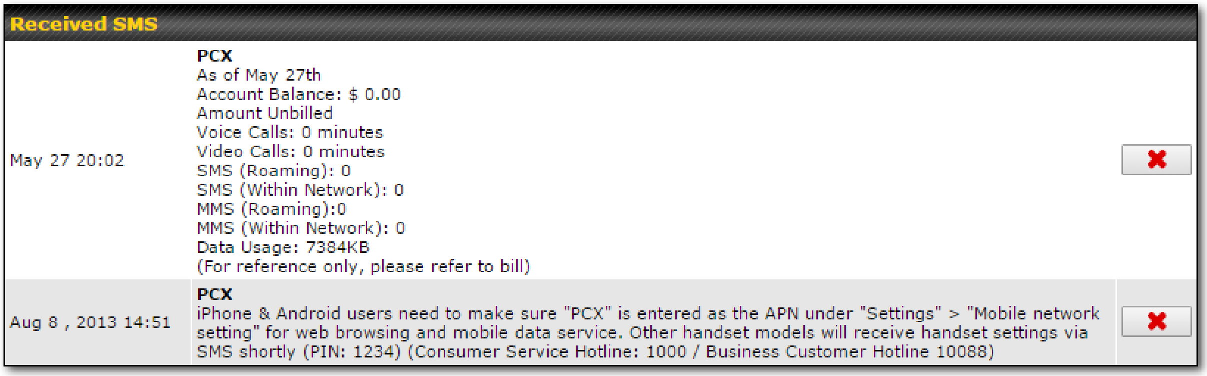
SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
Receive SMS	Get

You will receive a confirmation. To check the SMS response, click **Get**.



SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
USSD Status	Request is sent successfully
Receive SMS	Get

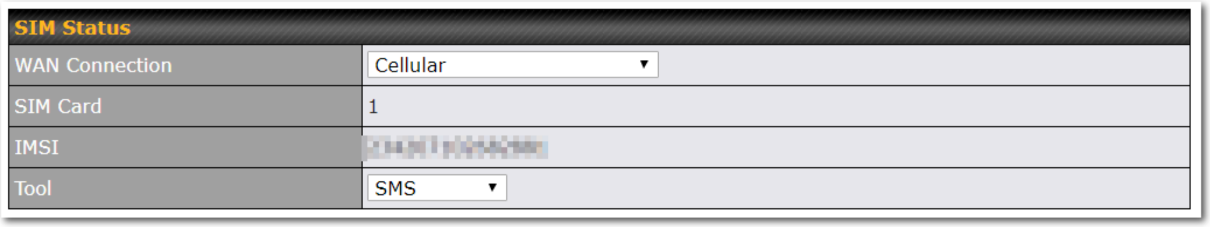
After a few minutes you will receive a response to your USSD code



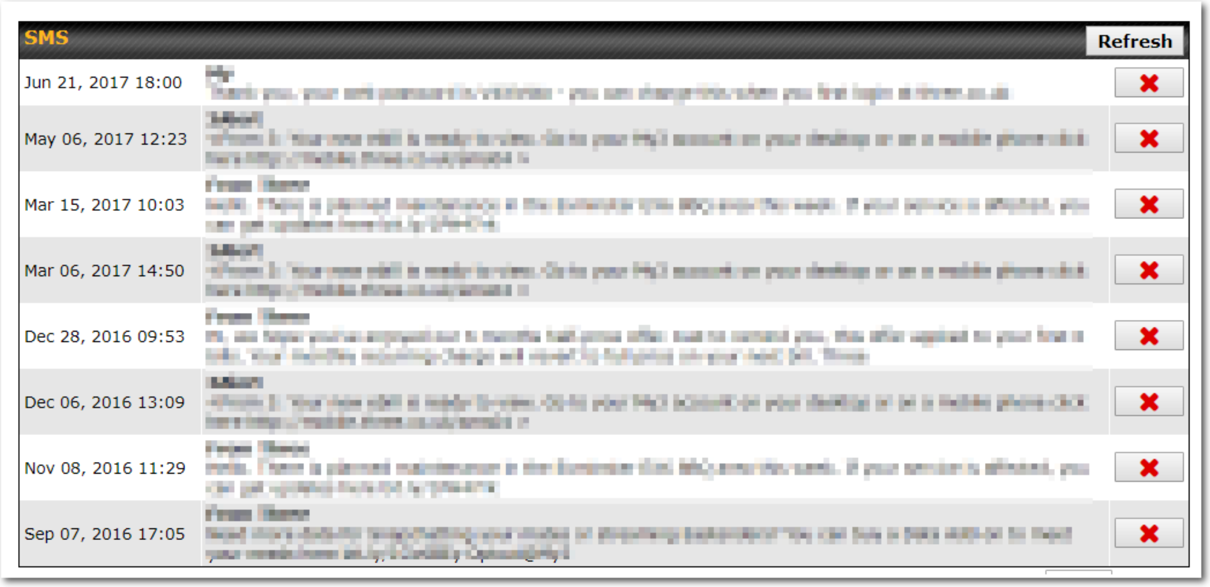
Received SMS		
May 27 20:02	**PCX** As of May 27th Account Balance: $ 0.00 Amount Unbilled Voice Calls: 0 minutes Video Calls: 0 minutes SMS (Roaming): 0 SMS (Within Network): 0 MMS (Roaming):0 MMS (Within Network): 0 Data Usage: 7384KB (For reference only, please refer to bill)	✖
Aug 8 , 2013 14:51	**PCX** iPhone & Android users need to make sure "PCX" is entered as the APN under "Settings" > "Mobile network setting" for web browsing and mobile data service. Other handset models will receive handset settings via SMS shortly (PIN: 1234) (Consumer Service Hotline: 1000 / Business Customer Hotline 10088)	✖

SMS

The SMS option allows you to read SMS (text) messages that have been sent to the SIM in your Peplink router.



SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	[redacted]
Tool	SMS ▾



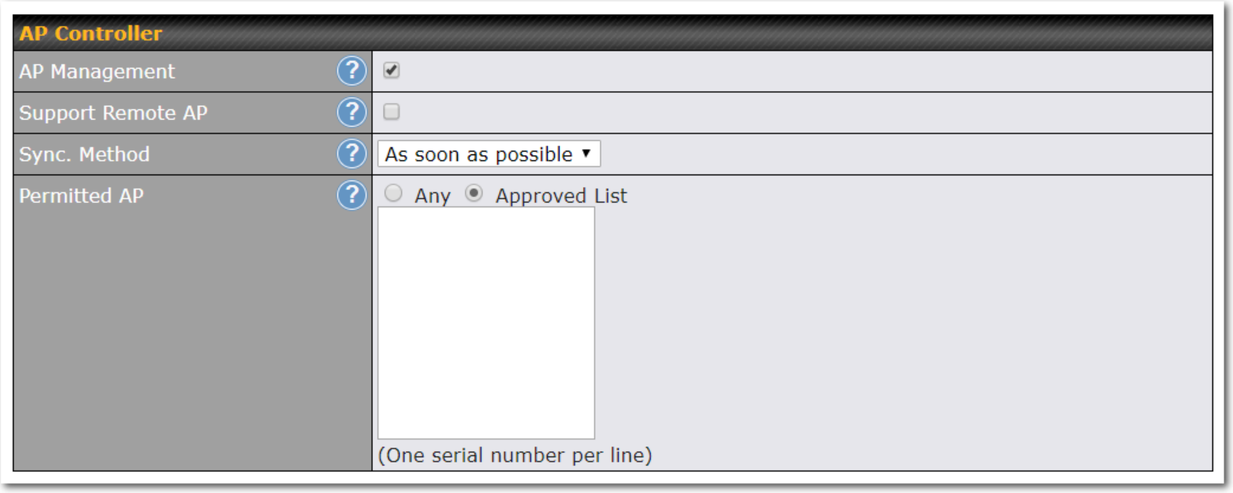
SMS		Refresh
Jun 21, 2017 18:00	[redacted]	✖
May 06, 2017 12:23	[redacted]	✖
Mar 15, 2017 10:03	[redacted]	✖
Mar 06, 2017 14:50	[redacted]	✖
Dec 28, 2016 09:53	[redacted]	✖
Dec 06, 2016 13:09	[redacted]	✖
Nov 08, 2016 11:29	[redacted]	✖
Sep 07, 2016 17:05	[redacted]	✖

15 AP Tab

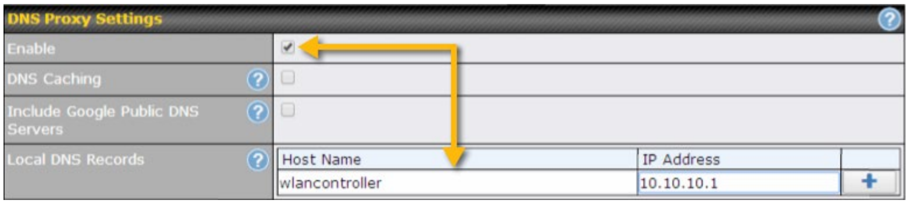
15.1 AP

15.1.1 AP Controller

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

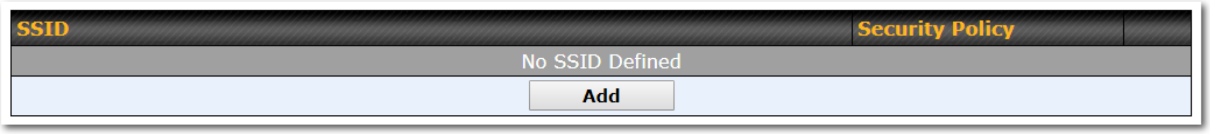


AP Controller	
AP Management	☑
Support Remote AP	□
Sync. Method	As soon as possible ▾
Permitted AP	○ Any ● Approved List (One serial number per line)

AP Controller	
AP Management	The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, **CAPWAP Access Controller addresses** (field 138), will be added to the DHCP server. A local DNS record, **AP Controller**, will be added to the local DNS proxy.
Support Remote AP	The AP controller supports remote management of Pepwave APs. When this option is enabled, the AP controller will wait for management connections originating from remote APs over the WAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. The DHCP server and/or local DNS server of the remote AP's network should be configured in the **DNS Proxy Settings menu** under **Network>LAN**. The procedure is as follows: 1. Define an extended DHCP option, **CAPWAP Access Controller addresses** (field 138), in the DHCP server, where the values are the AP controller's public IP addresses; and/or 2. Create a local DNS record for the AP controller with a value corresponding to the AP controller's public IP address.  DNS Proxy Settings Enable ☑ DNS Caching □ Include Google Public DNS Servers □ Local DNS Records: Host Name: wlancontroller; IP Address: 10.10.10.1
Sync. Method	Select the required option to synchronize the managed AP's. Options are: ● As soon as possible (default)

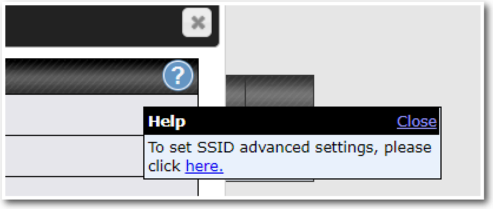
	- Progressively (synchronize AP's in groups) - One at a time (synchronize one AP at a time)
Permitted AP	Access points to manage can be specified here. If **Any** is selected, the AP controller will manage any AP that reports to it. If **Approved List** is selected, only APs with serial numbers listed in the provided text box will be managed.

15.1.2 Wireless SSID



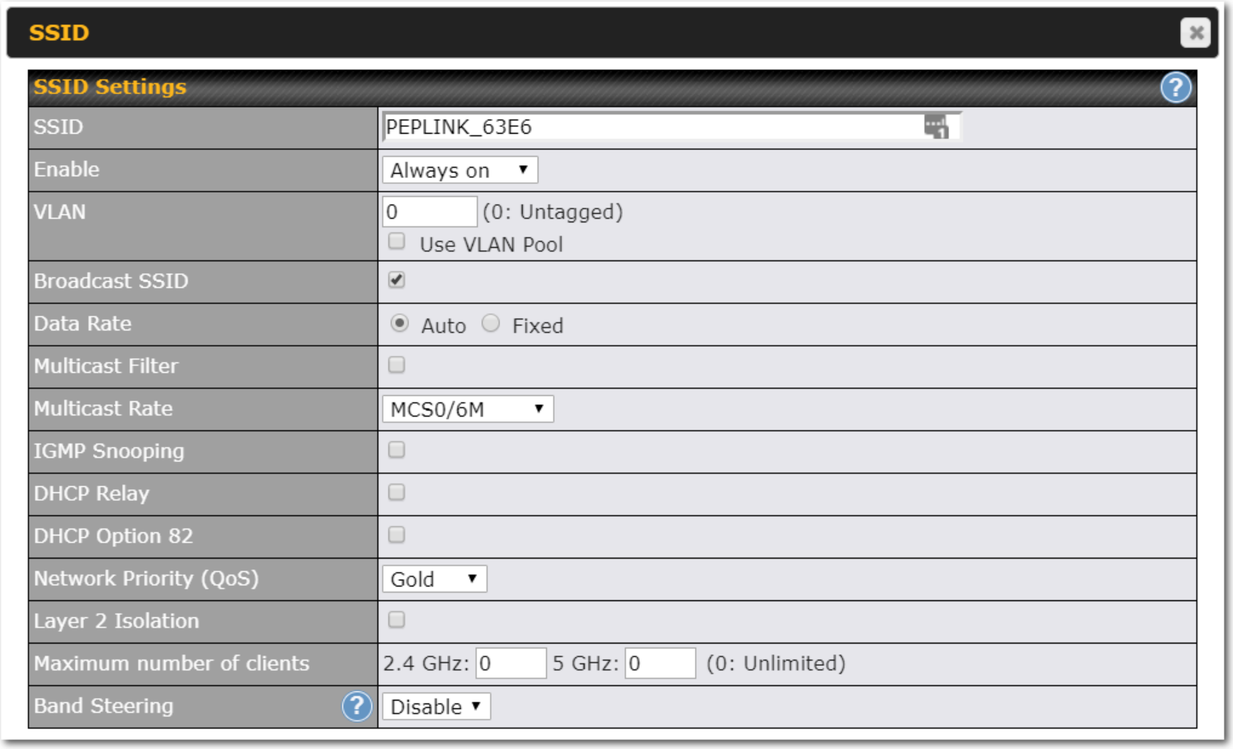
SSID	Security Policy	
No SSID Defined		

Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model. The below settings ishows a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).



Help Close

To set SSID advanced settings, please click here.



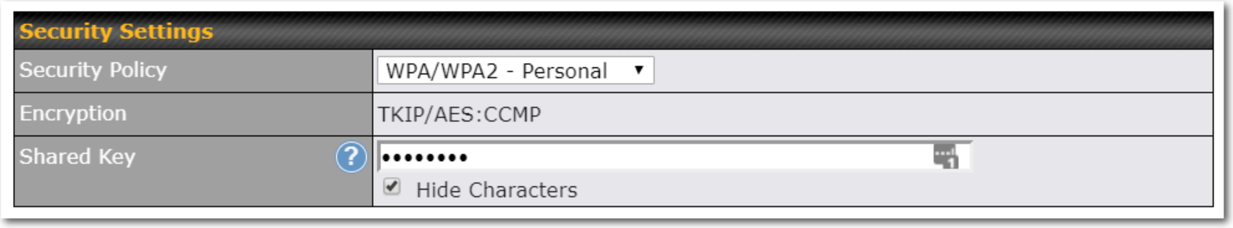
SSID

SSID Settings	
SSID	PEPLINK_63E6
Enable	Always on ▾
VLAN	0 (0: Untagged) □ Use VLAN Pool
Broadcast SSID	☑
Data Rate	● Auto ○ Fixed
Multicast Filter	□
Multicast Rate	MCS0/6M ▾
IGMP Snooping	□
DHCP Relay	□
DHCP Option 82	□
Network Priority (QoS)	Gold ▾
Layer 2 Isolation	□
Maximum number of clients	2.4 GHz: 0 5 GHz: 0 (0: Unlimited)
Band Steering	Disable ▾

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Enable	Click the drop-down menu to apply a time schedule to this interface
VLAN	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is **0**, which means VLAN tagging is disabled (instead of tagged with zero). Use of a VLAN pool is enabled by selecting the checkbox.
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. **Broadcast SSID** is enabled by default.
Data Rate ^{A}	Select **Auto** to allow the Pepwave router to set the data rate automatically, or select **Fixed** and choose a rate from the displayed drop-down menu.
Multicast Filter^{A}	This setting enables the filtering of multicast network traffic to the wireless SSID.

Multicast Rate^A	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected **Protocol** and **Channel Bonding** settings will affect the rate options and values available here.
IGMP Snooping ^A	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
DHCP Relay	Put the address of the DHCP server in this field.. DHCP requests will be relayed to this DHCP server
DHCP Option 82 ^A	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
Layer 2 Isolation ^A	**Layer 2** refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
Maximum Number of Clients	Indicate the maximum number of clients that should be able to connect to each frequency.
Band Steering	To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency. Choose between: **Force** - Clients capable of 5 GHz operation are only offered with 5 GHz frequency. **Prefer** - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered. **Disable** - Default

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

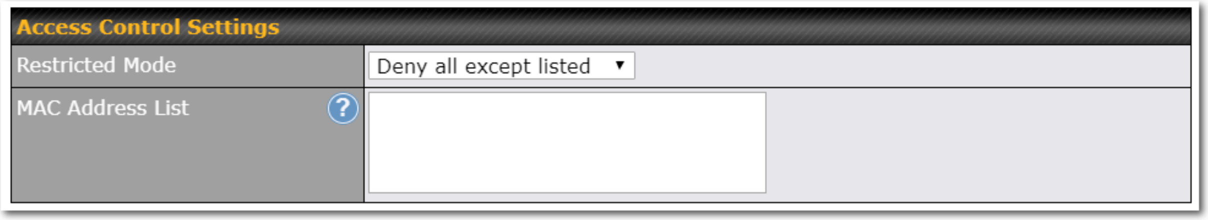


Security Settings

Security Policy	WPA/WPA2 - Personal ▾
Encryption	TKIP/AES:CCMP
Shared Key ?	•••••••• ☑ Hide Characters

Security Settings

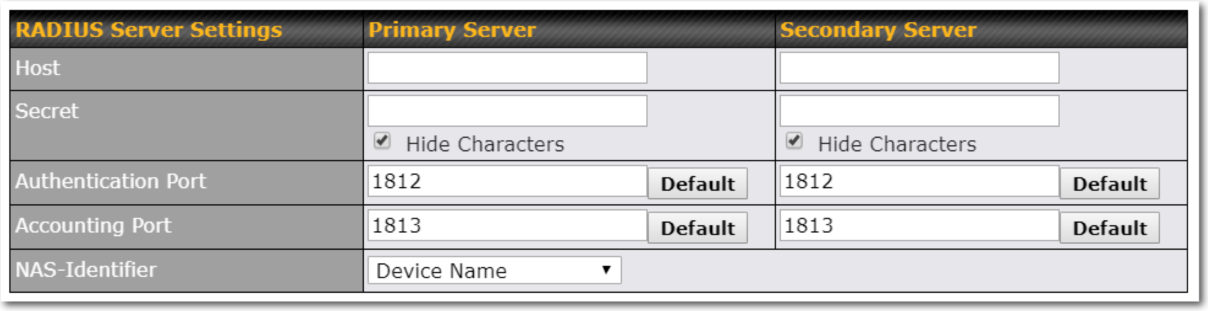
Security Policy	This setting configures the wireless authentication and encryption methods. Available options are : ● **Open (**No Encryption) ● **WPA2 -Personal** (AES:CCMP) ● **WPA2 – Enterprise** ● **WPA/WPA2 - Personal** (TKIP/AES: CCMP) ● **WPA/WPA2 – Enterprise** When **WPA/WPA2 - Enterprise** 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.



Access Control Settings

Restricted Mode	Deny all except listed ▾
MAC Address List ?	

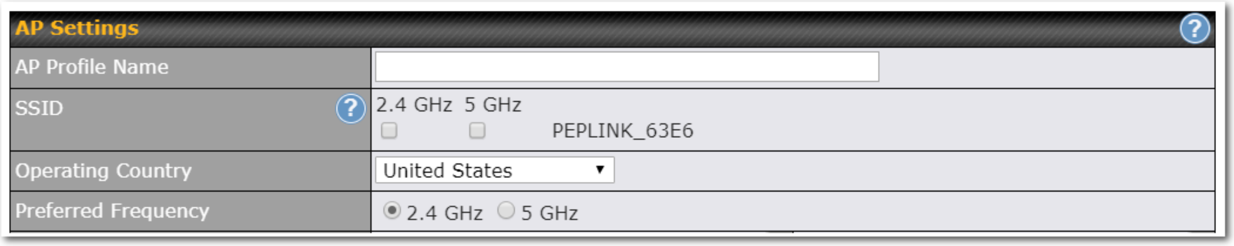
Access Control	
Restricted Mode	The settings allow administrator to control access using MAC address filtering. Available options are **None**, **Deny all except listed**, and **Accept all except listed**
MAC Address List	Connections coming from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field. If more than one MAC address needs to be entered, you can use a carriage return to separate them.



RADIUS Server Settings	Primary Server		Secondary Server	
Host				
Secret	 ☑ Hide Characters		 ☑ Hide Characters	
Authentication Port	1812	Default	1812	Default
Accounting Port	1813	Default	1813	Default
NAS-Identifier	Device Name ▾			

RADIUS Server Settings	
Host	Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.
Secret	Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
Authentication Port	In field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the **Default** button to enter **1812**.
Accounting Port	In field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the **Default** button to enter **1813**.
NAS-Identifier	Choose between **Device Name**, **LAN MAC address**, **Device Serial Number** and **Custom Value**

15.1.3 AP > Profiles

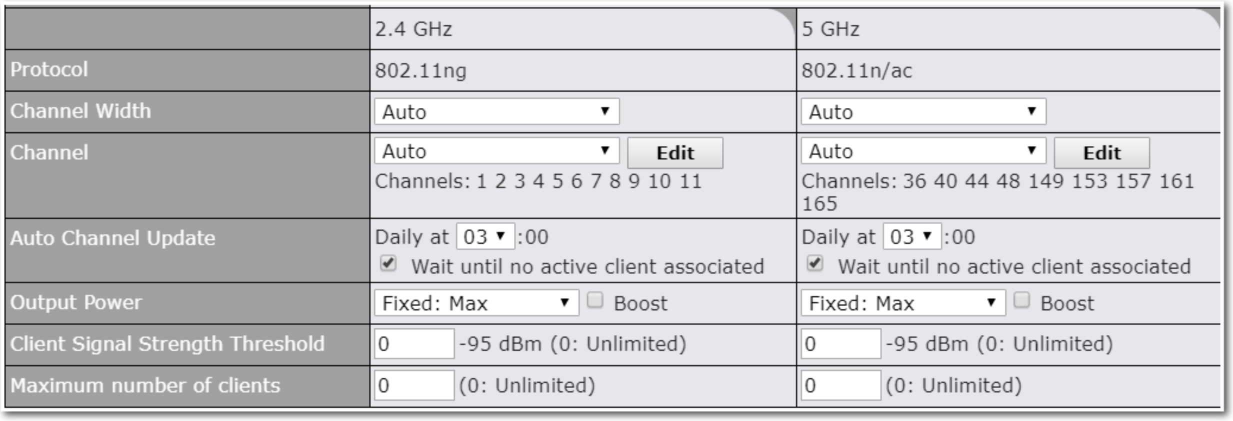


AP Settings	
AP Profile Name	
SSID	2.4 GHz 5 GHz □ □ PEPLINK_63E6
Operating Country	United States ▾
Preferred Frequency	● 2.4 GHz ○ 5 GHz

AP Settings

AP Profile Name	Ap Profile name
SSID	You can select the wireless networks for 2.4 GHz or 5 GHz separately for each SSID.
Operating Country	This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow. ● If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). ● If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). NOTE: Users are required to choose an option suitable to local laws and regulations.
Preferred Frequency	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.

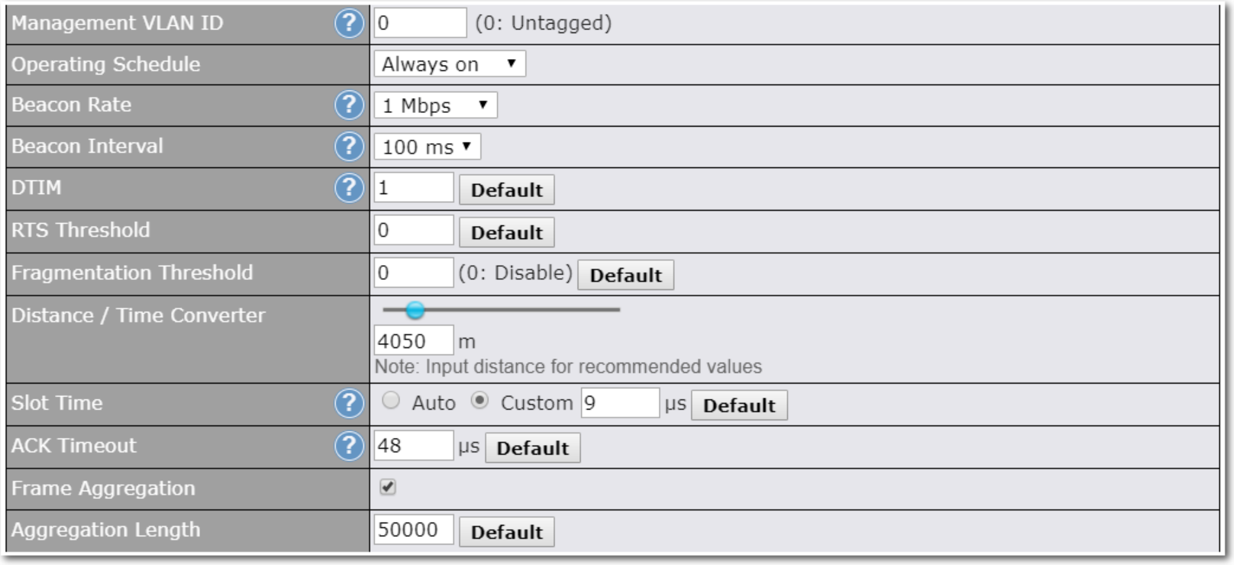


	2.4 GHz	5 GHz
Protocol	802.11ng	802.11n/ac
Channel Width	Auto ▾	Auto ▾
Channel	Auto ▾ Edit Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto ▾ Edit Channels: 36 40 44 48 149 153 157 161 165
Auto Channel Update	Daily at 03 ▾ :00 ☑ Wait until no active client associated	Daily at 03 ▾ :00 ☑ Wait until no active client associated
Output Power	Fixed: Max ▾ □ Boost	Fixed: Max ▾ □ Boost
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)	0 (0: Unlimited)

AP Settings (part 2)	
Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, **802.11ng** is selected.
Channel Width	Available options are **20 MHz**, **40 MHz**, and **Auto (20/40 MHz)** . Default is **Auto (20/40 MHz),** which allows both widths to be used simultaneously.
Channel	This option allows you to select which 802.11 RF channel will be utilized. **Channel 1**

	(2.412 GHz) is selected by default.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country.
Client Signal Strength Threshold	This setting determines the maximum strength at which the Wi-Fi AP can broadcast
Maximum number of clients	This setting determines the maximum number of clients that can connect to this Wi-Fi frequency.

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

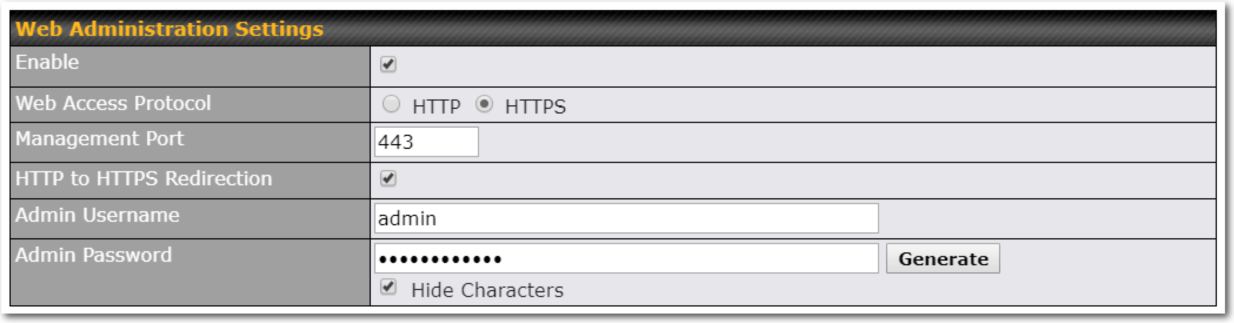


Management VLAN ID ?	0 (0: Untagged)
Operating Schedule	Always on ▾
Beacon Rate ?	1 Mbps ▾
Beacon Interval ?	100 ms ▾
DTIM ?	1 Default
RTS Threshold	0 Default
Fragmentation Threshold	0 (0: Disable) Default
Distance / Time Converter	4050 m Note: Input distance for recommended values
Slot Time ?	○ Auto ● Custom 9 μs Default
ACK Timeout ?	48 μs Default
Frame Aggregation	☑
Aggregation Length	50000 Default

Advanced AP Settings	
Management	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

VLAN ID	that no VLAN tagging will be applied. NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller.
Operating Schedule	Choose from the schedules that you have defined in System>Schedule. Select the schedule for the integrated AP to follow from the drop-down menu.
Beacon Rate [A]	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.
Beacon Interval [A]	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DTIM [A]	This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to **1 ms**.
RTS Threshold [A]	The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500.
Fragmentation Threshold [A]	This setting determines the maximum size of a packet before it gets fragmented into multiple pieces.
Distance / Time Convertor	Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout.
Slot Time [A]	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to **9 μs**.
ACK Timeout [A]	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to **48 μs**.
Frame Aggregation [A]	This option allows you to enable frame aggregation to increase transmission throughput.

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



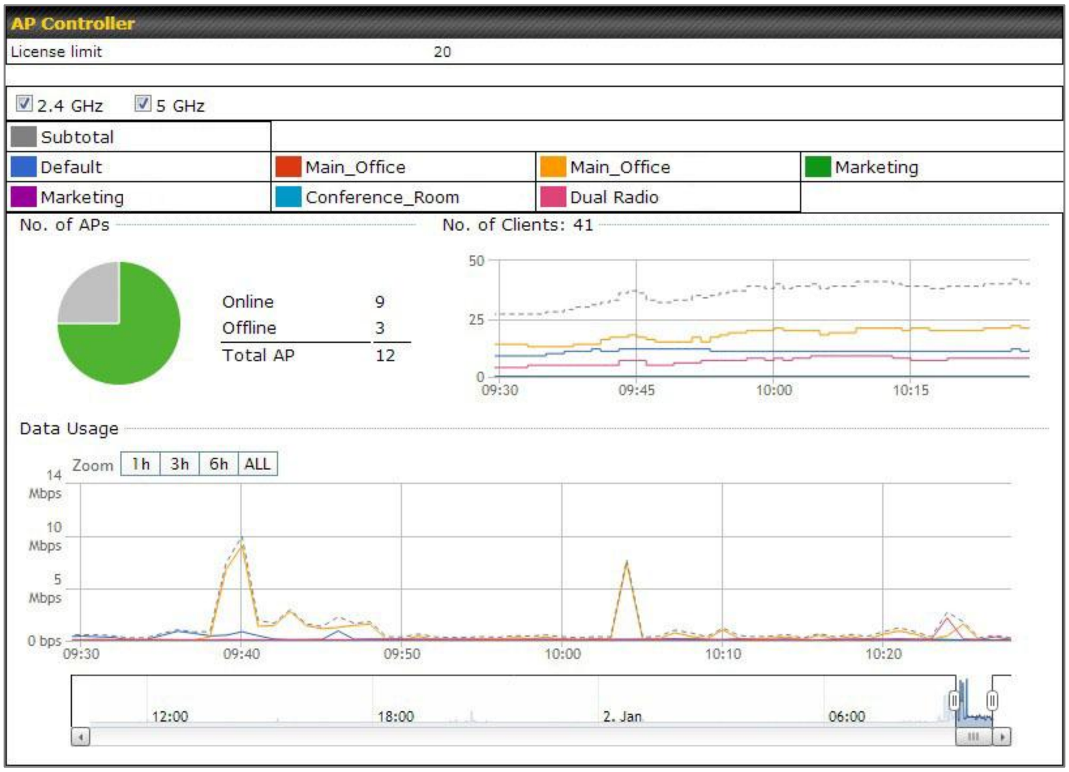
Web Administration Settings	
Enable	☑
Web Access Protocol	○ HTTP ● HTTPS
Management Port	443
HTTP to HTTPS Redirection	☑
Admin Username	admin
Admin Password	•••••••••••• Generate ☑ Hide Characters

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

15.2 AP Controller Status

15.2.1 Info

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



AP Controller

License limit	20

☑ 2.4 GHz ☑ 5 GHz

⬛ Subtotal			
🟦 Default	🟥 Main_Office	🟧 Main_Office	🟩 Marketing
🟪 Marketing	🟦 Conference_Room	🟥 Dual Radio	

No. of APs

Online	9
Offline	3
Total AP	12

No. of Clients: 41

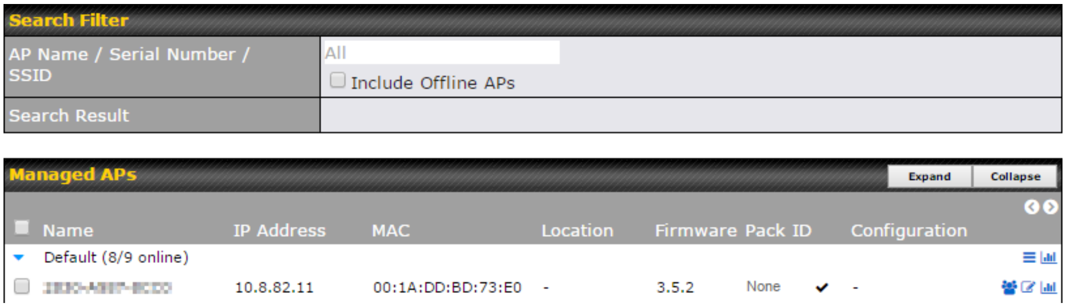
Data Usage

Zoom 1h 3h 6h ALL

AP Controller	
License Limit	This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage.
Frequency	Underneath, there are two check boxes labeled **2.4 Ghz** and **5 Ghz**. Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.
SSID	The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs.
No. of APs	This pie chart and table indicates how many APs are online and how many are offline.
No.of Clients	This graph displays the number of clients connected to each network at any given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time.
Data Usage	This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to **Zoom** to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

15.2.2 Access Points (Usage)

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



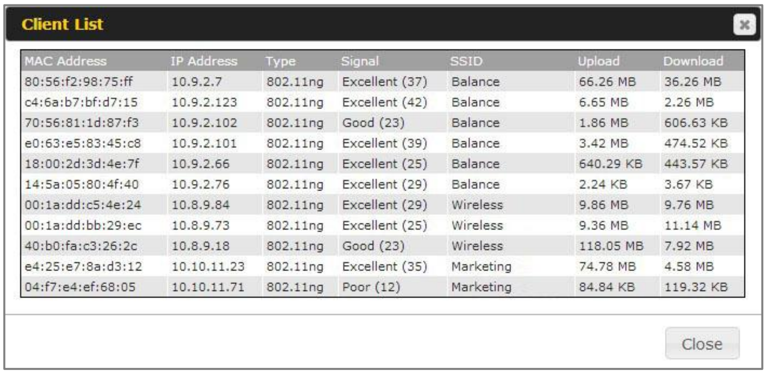
Search Filter

AP Name / Serial Number / SSID	All □ Include Offline APs
Search Result	

Managed APs

□	Name	IP Address	MAC	Location	Firmware	Pack ID		Configuration	
▾	Default (8/9 online)								☰ 📊
□	[redacted]	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None	✓	-	👥 ✎ 📊

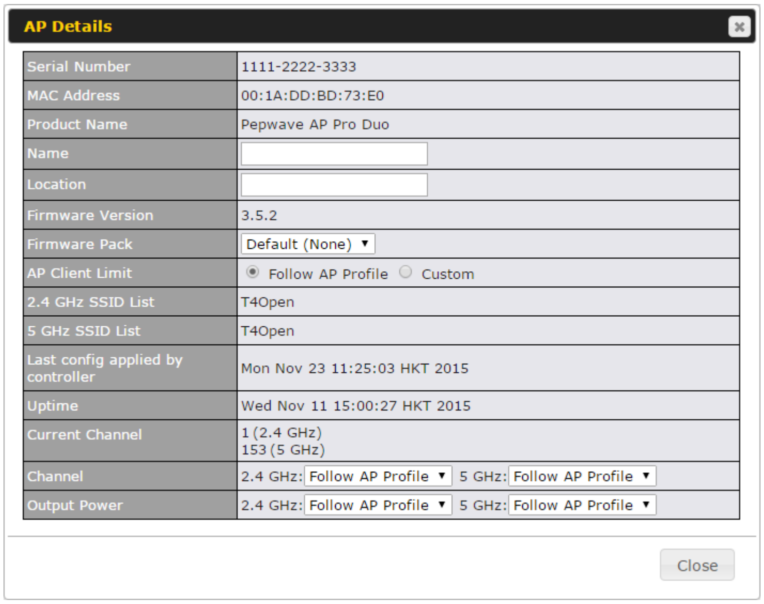
Usage	
AP Name/Serial Number	This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.
Online Status	This button toggles whether your search will include offline devices.
Managed Wireless 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

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

Click the icon to configure each client

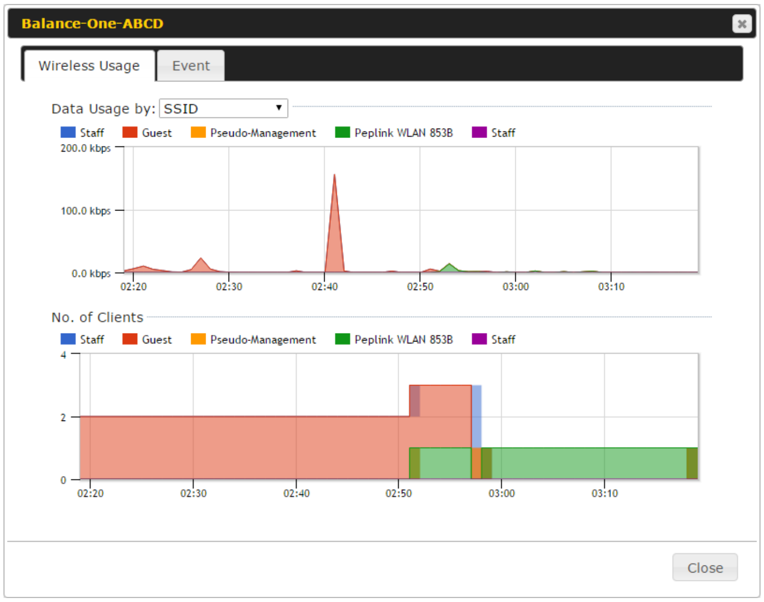


AP Details

Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:E0
Product Name	Pepwave AP Pro Duo
Name	
Location	
Firmware Version	3.5.2
Firmware Pack	Default (None) ▾
AP Client Limit	● Follow AP Profile ○ 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 ▾

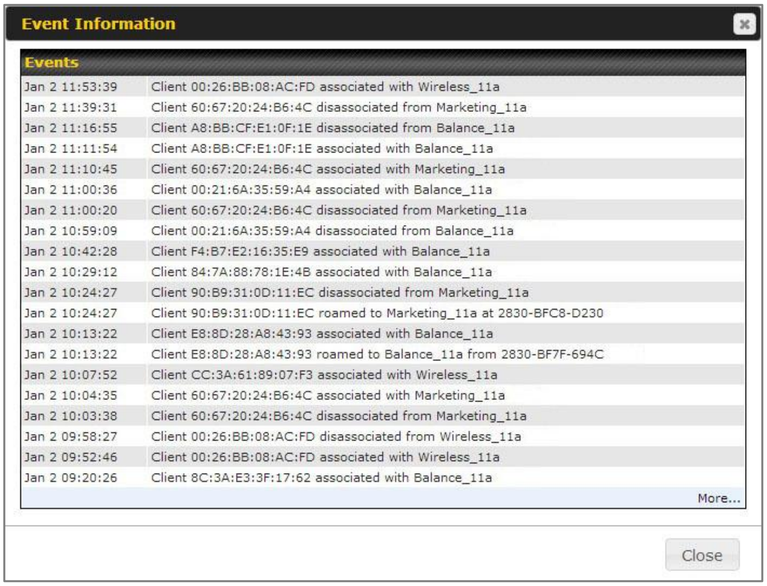
For easier network management, you can give each client a name and designate its location. You can also designate which firmware pack (if any) this client will follow, as well as the channels on which the client will broadcast.

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.

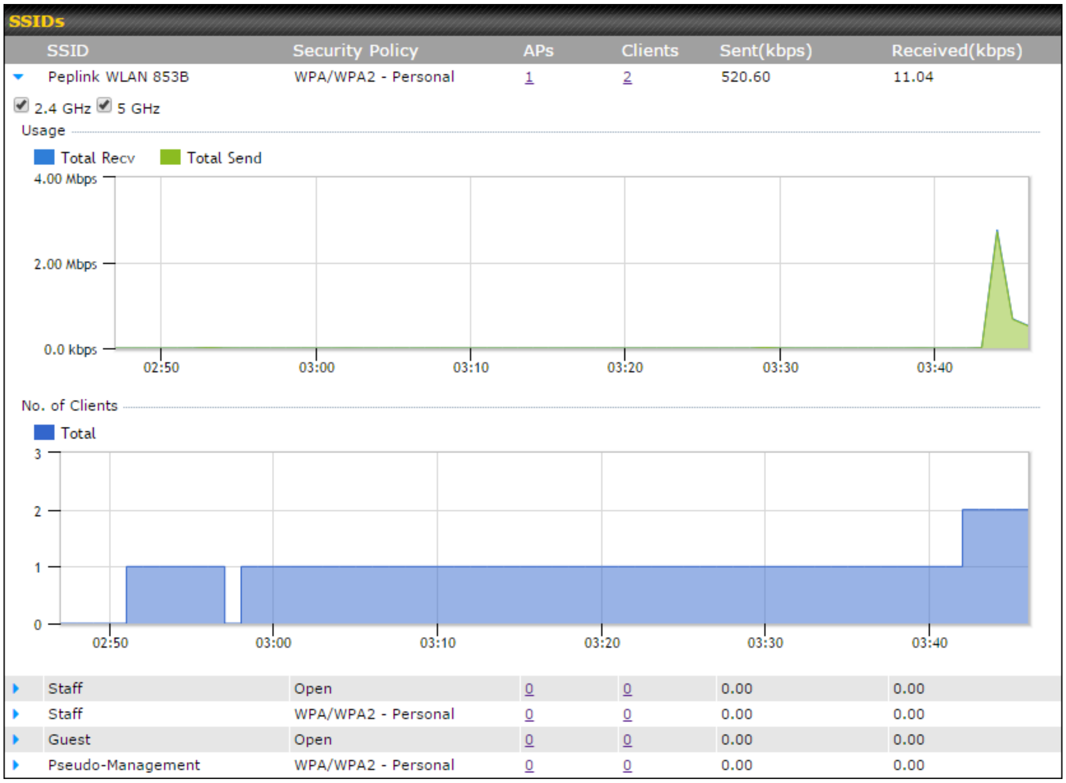
Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:



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

15.2.3 Wireless SSID

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



SSIDs

	SSID	Security Policy	APs	Clients	Sent(kbps)	Received(kbps)
▼	Peplink WLAN 853B	WPA/WPA2 - Personal	1	2	520.60	11.04

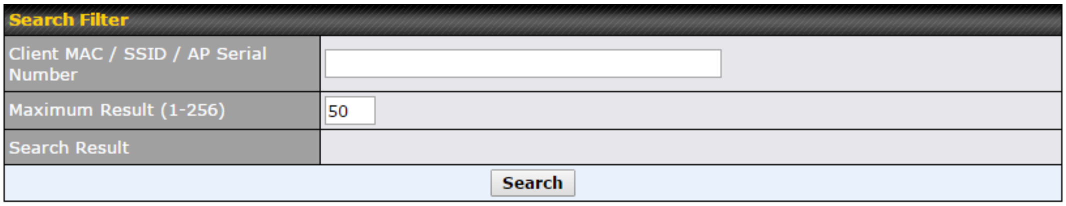
☑ 2.4 GHz ☑ 5 GHz

	SSID	Security Policy	APs	Clients	Sent(kbps)	Received(kbps)
▶	Staff	Open	0	0	0.00	0.00
▶	Staff	WPA/WPA2 - Personal	0	0	0.00	0.00
▶	Guest	Open	0	0	0.00	0.00
▶	Pseudo-Management	WPA/WPA2 - Personal	0	0	0.00	0.00

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

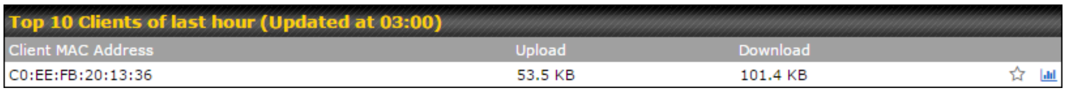
15.2.4 Wireless Client

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



Search Filter

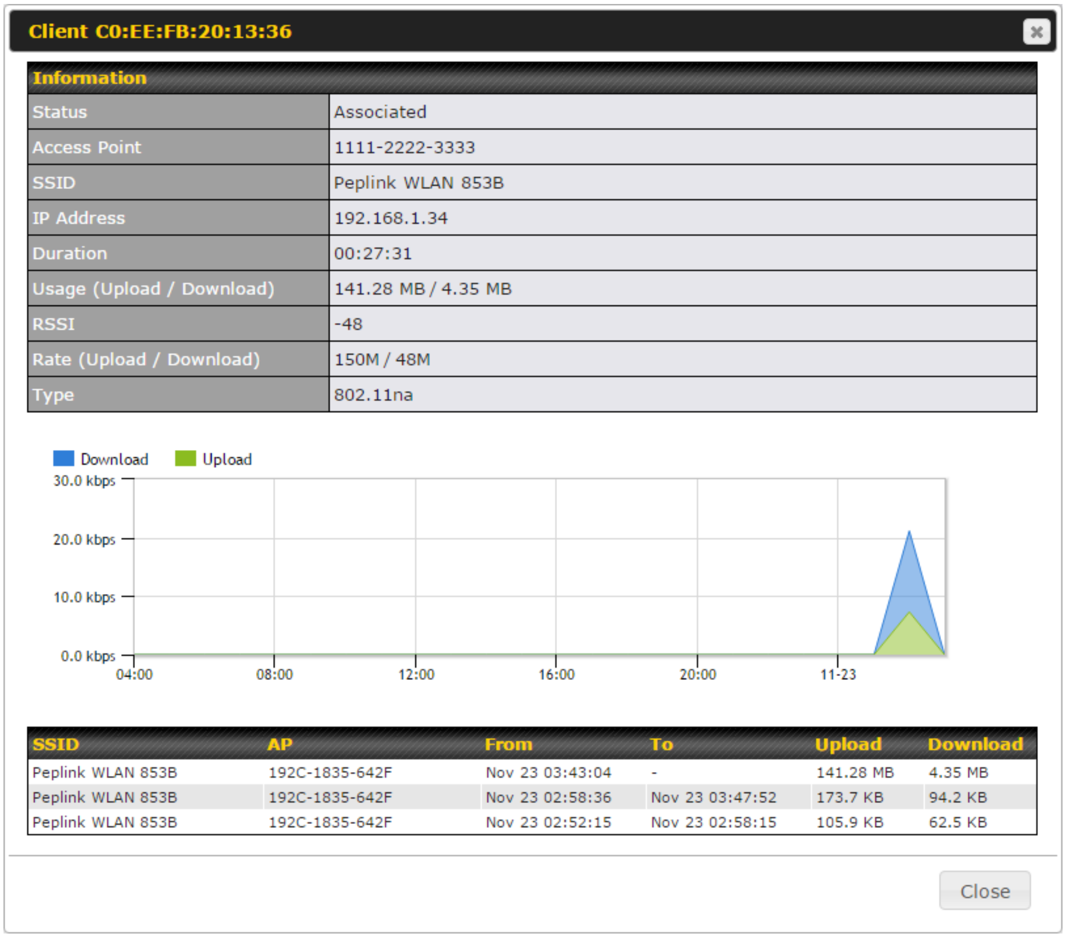
Client MAC / SSID / AP Serial Number	
Maximum Result (1-256)	50
Search Result	



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:



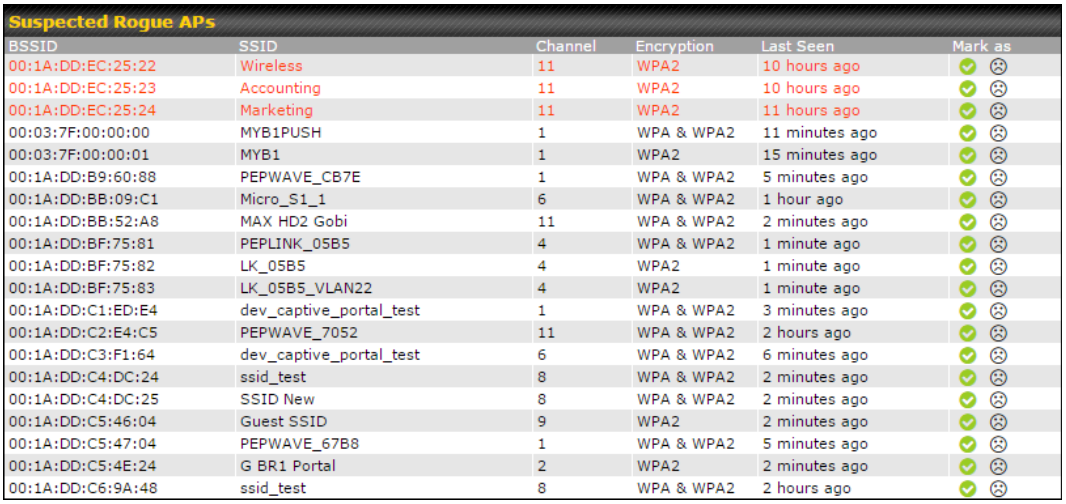
Client C0:EE:FB:20:13:36

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

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

15.2.5 Nearby Device

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



Suspected Rogue APs

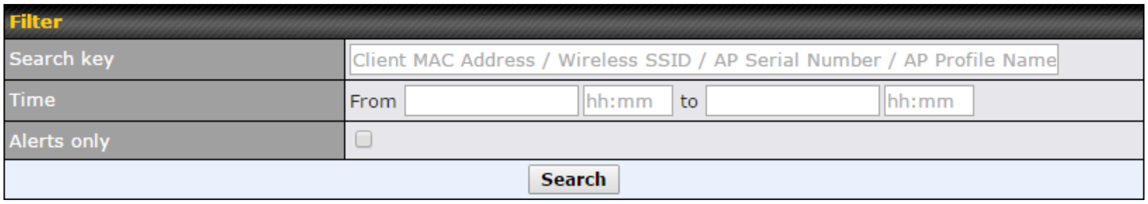
BSSID	SSID	Channel	Encryption	Last Seen	Mark as
00:1A:DD:EC:25:22	Wireless	11	WPA2	10 hours ago	✓ ☹
00:1A:DD:EC:25:23	Accounting	11	WPA2	10 hours ago	✓ ☹
00:1A:DD:EC:25:24	Marketing	11	WPA2	11 hours ago	✓ ☹
00:03:7F:00:00:00	MYB1PUSH	1	WPA & WPA2	11 minutes ago	✓ ☹
00:03:7F:00:00:01	MYB1	1	WPA2	15 minutes 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.

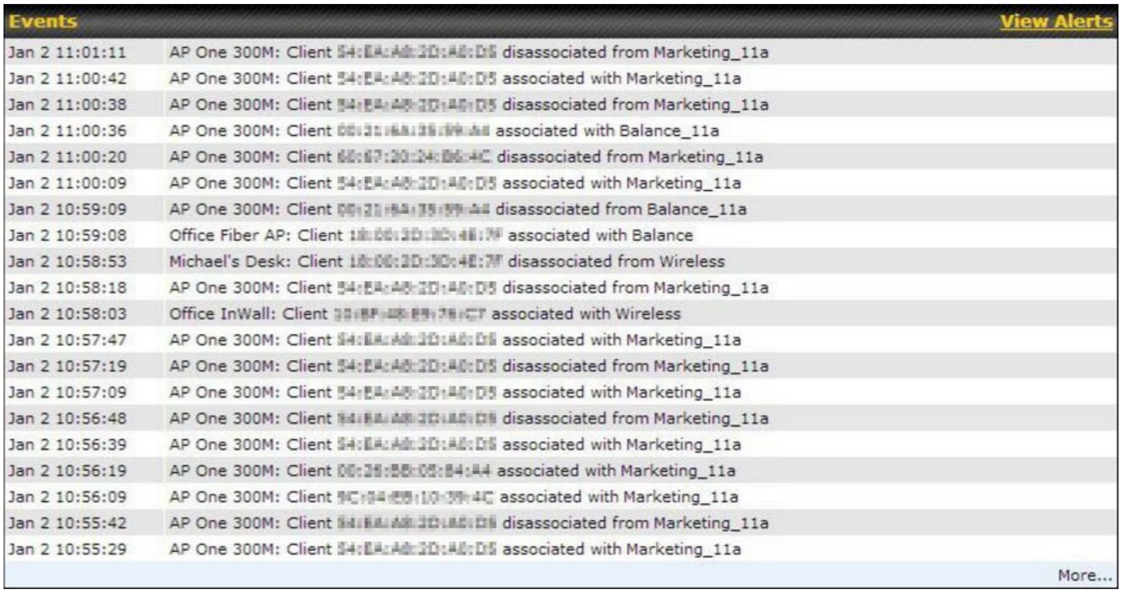
15.2.6 Event Log

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



Filter

Search key	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name
Time	From [ ] hh:mm to [ ] hh:mm
Alerts only	□

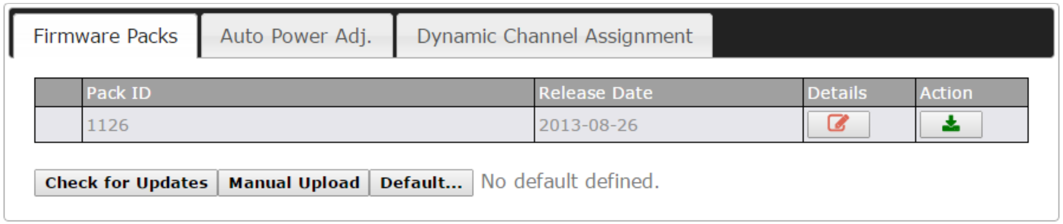


```
Events                                                                      View Alerts
Jan 2 11:01:11   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:42   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 11:00:38   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:36   AP One 300M: Client [redacted] associated with Balance_11a
Jan 2 11:00:20   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:59:09   AP One 300M: Client [redacted] disassociated from Balance_11a
Jan 2 10:59:08   Office Fiber AP: Client [redacted] associated with Balance
Jan 2 10:58:53   Michael's Desk: Client [redacted] disassociated from Wireless
Jan 2 10:58:18   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:58:03   Office InWall: Client [redacted] associated with Wireless
Jan 2 10:57:47   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:57:19   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:57:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:48   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:56:39   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:19   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:55:42   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:55:29   AP One 300M: Client [redacted] 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.

15.3 Toolbox

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



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

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.

16 System Tab

16.1 System

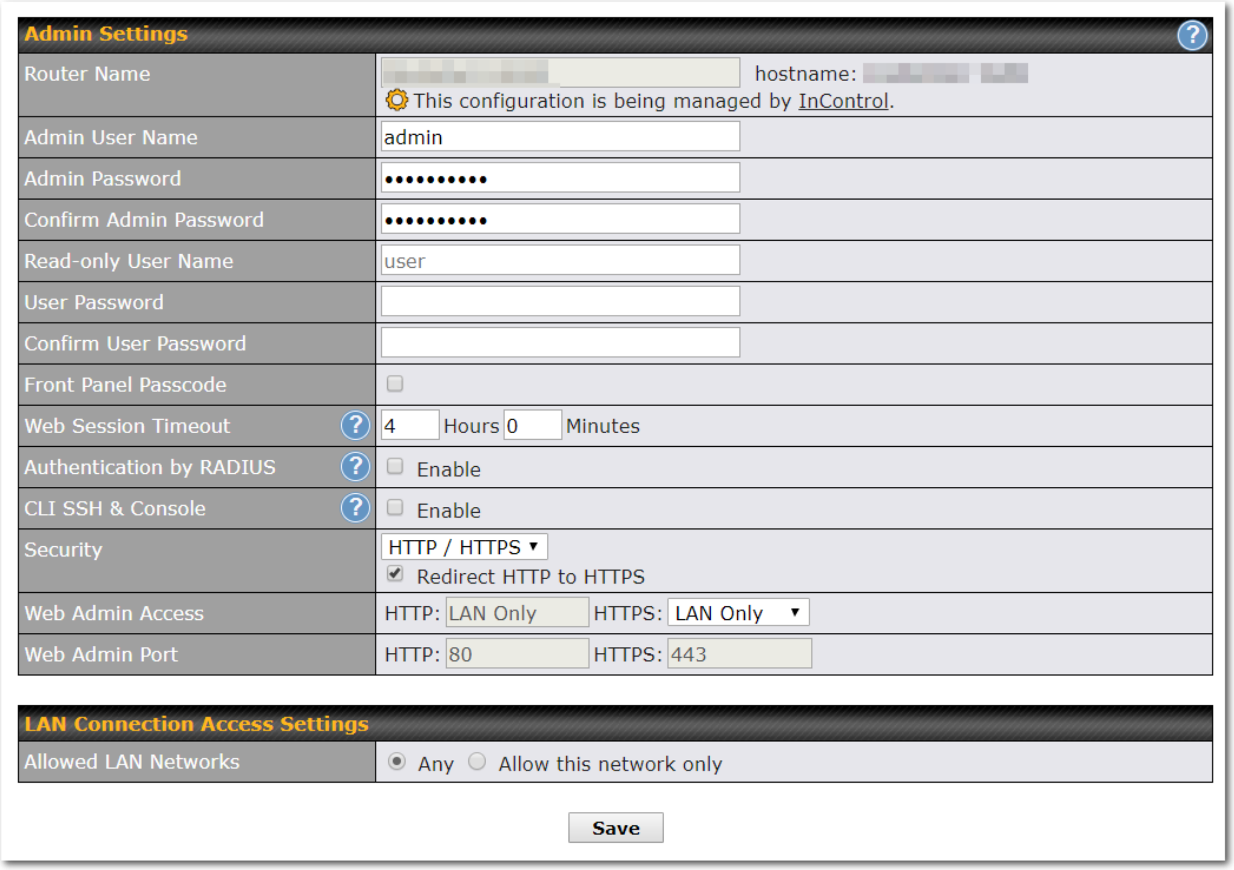
16.1.1 Admin Security

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

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

0 hours 0 minutes signifies an unlimited session time. This setting should be used only in special situations, as it will lower the system security level if users do not log out before closing the browser. The **default** is 4 hours, 0 minutes.

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



Admin Settings

Router Name	[redacted] hostname: [redacted] This configuration is being managed by InControl.
Admin User Name	admin
Admin Password	••••••••••
Confirm Admin Password	••••••••••
Read-only User Name	user
User Password	
Confirm User Password	
Front Panel Passcode	□
Web Session Timeout	4 Hours 0 Minutes
Authentication by RADIUS	□ Enable
CLI SSH & Console	□ Enable
Security	HTTP / HTTPS ▾ ☑ Redirect HTTP to HTTPS
Web Admin Access	HTTP: LAN Only HTTPS: LAN Only ▾
Web Admin Port	HTTP: 80 HTTPS: 443

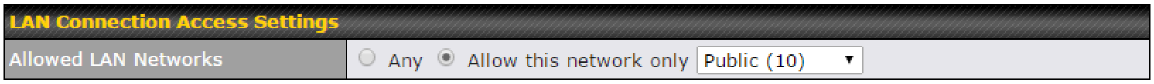
LAN Connection Access Settings

Allowed LAN Networks	● Any ○ Allow this network only

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

Confirm User Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to **4 hours**.
Authentication by RADIUS	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or “user” with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.
Auth Protocol	This specifies the authentication protocol used. Available options are **MS-CHAP v2** and **PAP**.
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.
Network Connection	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
CLI SSH	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to **Section 30.5.**
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: ● HTTP ● HTTPS ● HTTP/HTTPS

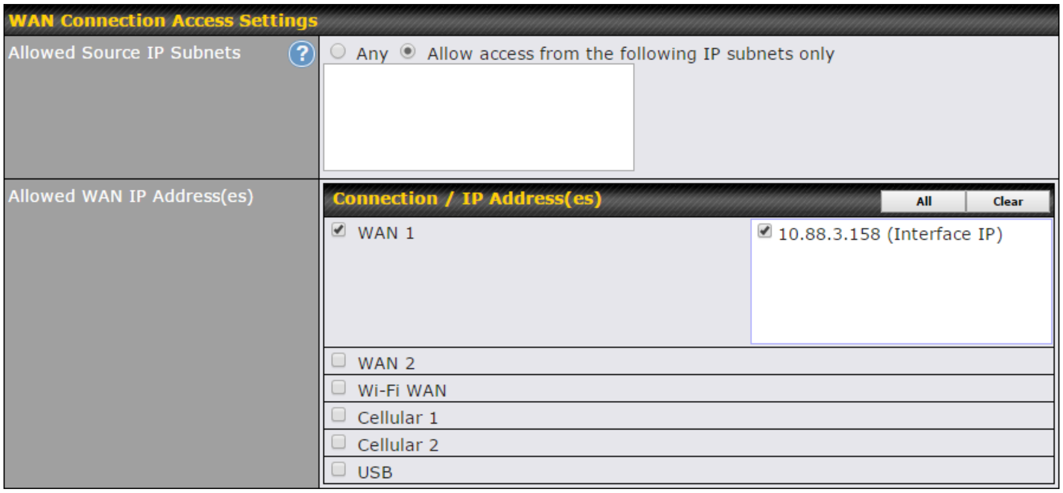
	HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
Web Admin Access	This option is for specifying the network interfaces through which the web admin interface can be accessed: ● LAN only ● LAN/WAN If LAN/WAN is chosen, the **WAN Connection Access Settings** form will be displayed.



LAN Connection Access Settings

Allowed LAN Networks	○ Any ● Allow this network only Public (10) ▾

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



WAN Connection Access Settings

Allowed Source IP Subnets	○ Any ● Allow access from the following IP subnets only
Allowed WAN IP Address(es)	**Connection / IP Address(es)** All Clear ☑ WAN 1 ☑ 10.88.3.158 (Interface IP) □ WAN 2 □ Wi-Fi WAN □ Cellular 1 □ Cellular 2 □ USB

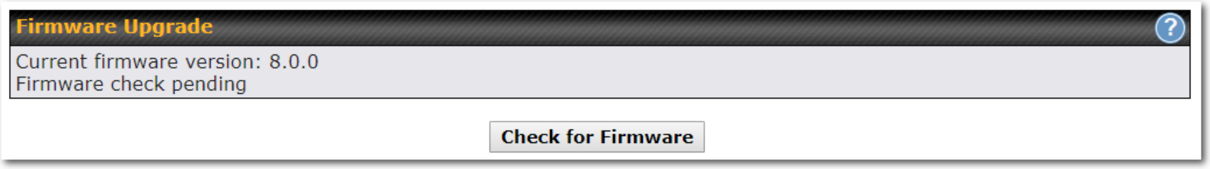
WAN Connection Access Settings	
Allowed Source IP Subnets	This field allows you to restrict web admin access only from defined IP subnets. ● **Any** - Allow web admin accesses to be from anywhere, without IP address restriction. ● **Allow access from the following IP subnets only** - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input

	area will be displayed beneath: The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of *w.x.y.z/m*, where *w.x.y.z* is an IP address (e.g., *192.168.0.0*), and *m* is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, *192.168.0.0/24*). To define multiple subnets, separate each IP subnet one in a line. For example: ● 192.168.0.0/24 ● 10.8.0.0/16
Allowed WAN IP Address(es)	This is to choose which WAN IP address(es) the web server should listen on.

16.1.2 Firmware

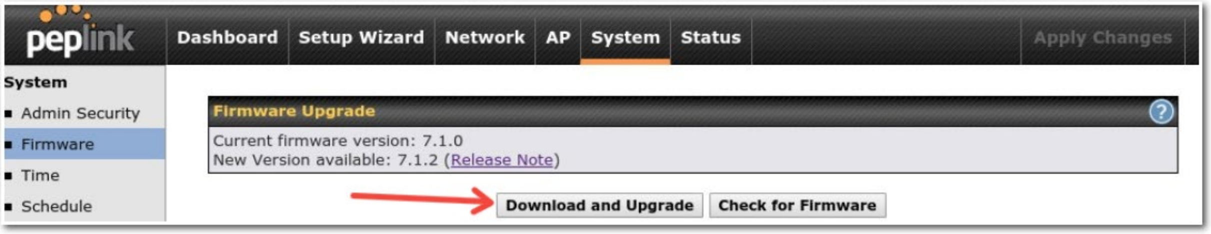
Upgrading firmware can be done in one of three ways. Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

The automatic upgrade can be done from **System** > **Firmware**.



Current firmware version: 8.0.0
Firmware check pending

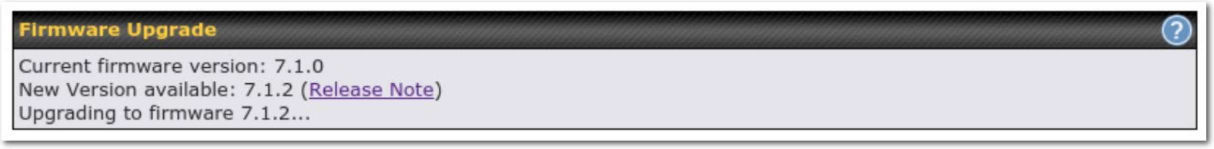
If an update is found the buttons will change to allow you to **Download and Update** the firmware.



Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)

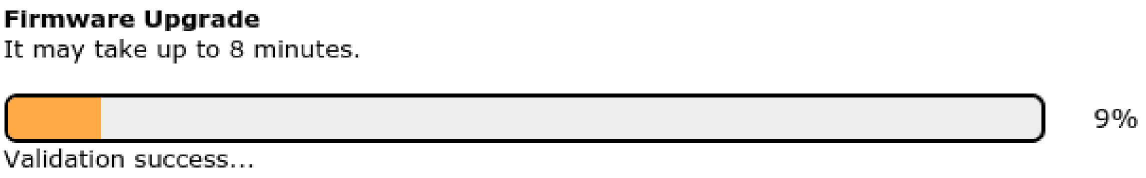
Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

The router will download and then apply the firmware. The time that this process takes will depend on your internet connection's speed.



Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)
Upgrading to firmware 7.1.2...

The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will also depend on the router that’s being upgraded.



Firmware Upgrade

It may take up to 8 minutes.

9%

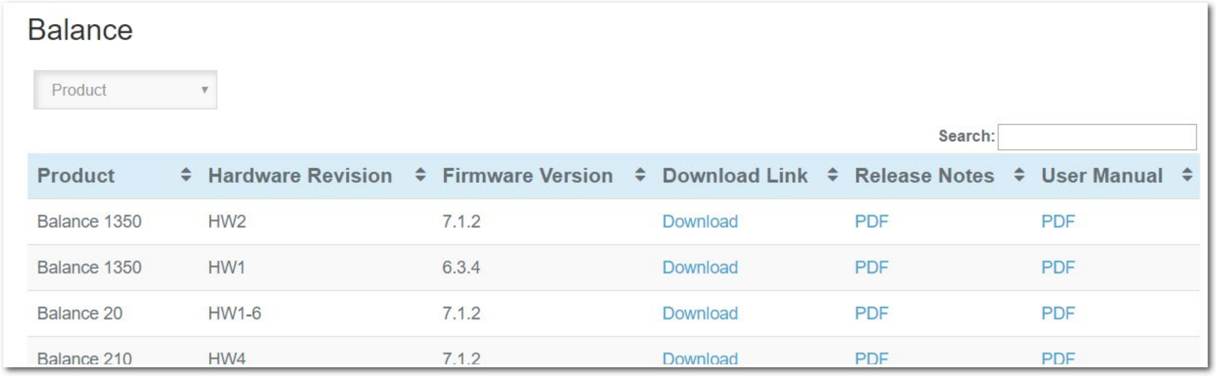
Validation success...

***Upgrading the firmware will cause the router to reboot.**

Web admin interface : install updates manually

In some cases, a special build may be provided via a ticket or it may be found in the forum. Upgrading to the special build can be done using this method, or using IC2 if you are using that to manage your firmware upgrades. A manual upgrade using the GA firmware posted on the site may also be recommended or required for a couple of reasons.

All of the Peplink/Pepwave GA firmware can be found here Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the Balance line.



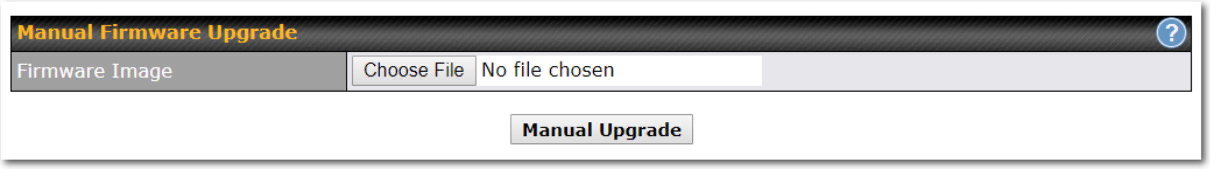
Balance

Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual
Balance 1350	HW2	7.1.2	Download	PDF	PDF
Balance 1350	HW1	6.3.4	Download	PDF	PDF
Balance 20	HW1-6	7.1.2	Download	PDF	PDF
Balance 210	HW4	7.1.2	Download	PDF	PDF

If the device has more than one firmware version the current hardware revision will be required to know what firmware to download.

Navigate to System > Firmware and click the Choose File button under the Manual Firmware Upgrade section. Navigate to the location that the firmware was downloaded to select the “.img” file and click the Open button.

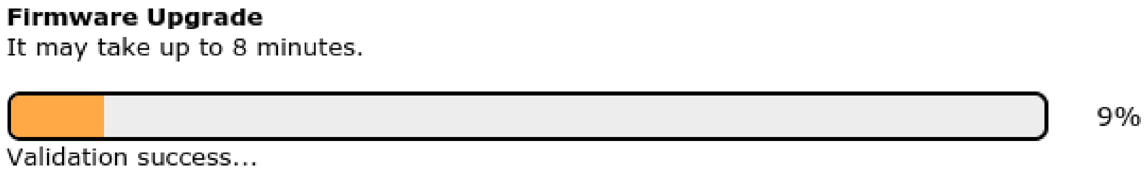
Click on the Manual Upgrade button to start the upgrade process.



Manual Firmware Upgrade

Firmware Image	Choose File No file chosen

A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the Ok button to start the upgrade process. The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will depend on the router that's being upgraded.



Firmware Upgrade

It may take up to 8 minutes.

9%

Validation success...

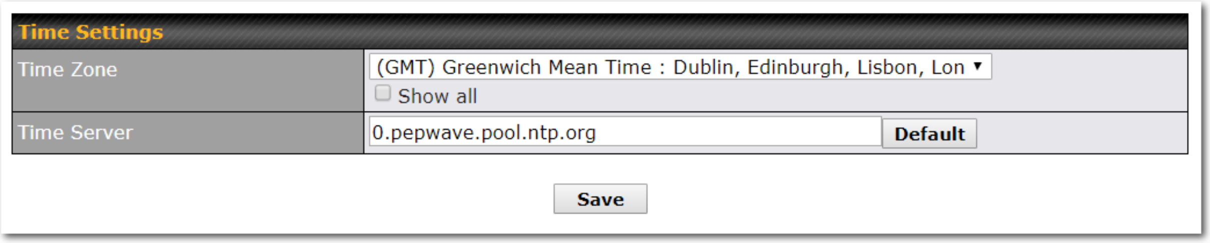
***Upgrading the firmware will cause the router to reboot.**

The InControl method

[Described in this knowledgebase article on our forum.]

16.1.3 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

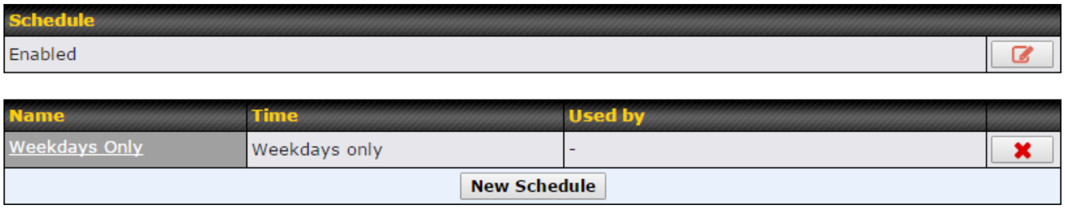
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▾ □ Show all
Time Server	0.pepwave.pool.ntp.org Default

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

Time Server	This setting specifies the NTP network time server to be utilized by the Peplink Balance.

16.1.4 Schedule

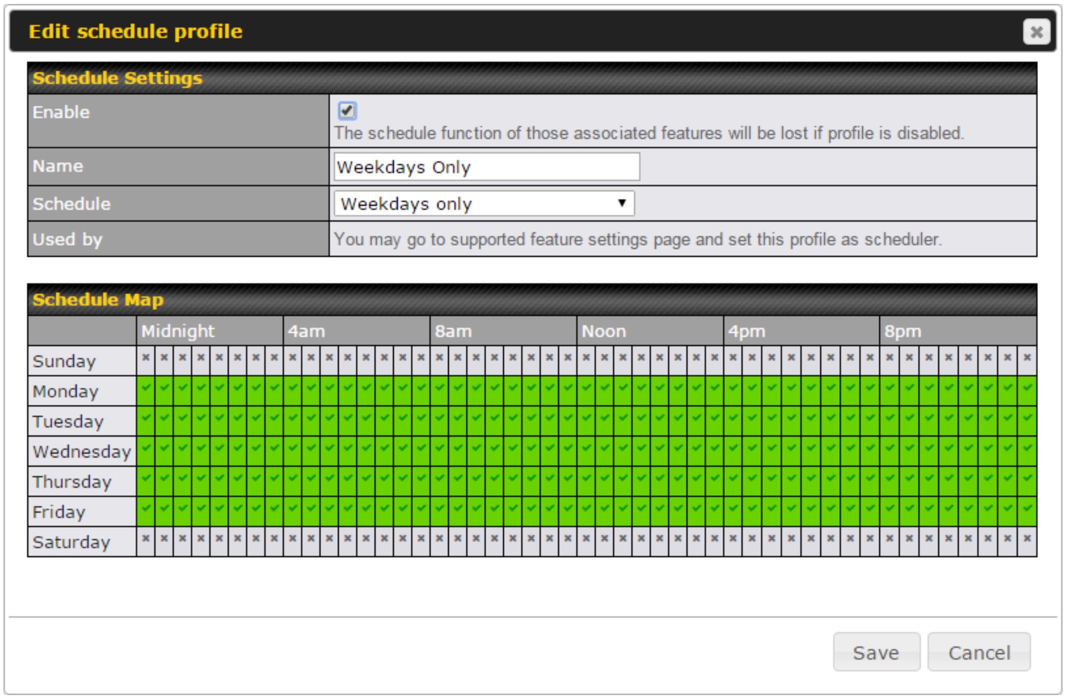
Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**



Schedule	
Enabled	

Name	Time	Used by	
Weekdays Only	Weekdays only	-	✖

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



Edit schedule profile

Schedule Settings	
Enable	☑ The schedule function of those associated features will be lost if profile is disabled.
Name	Weekdays Only
Schedule	Weekdays only ▾
Used by	You may go to supported feature settings page and set this profile as scheduler.

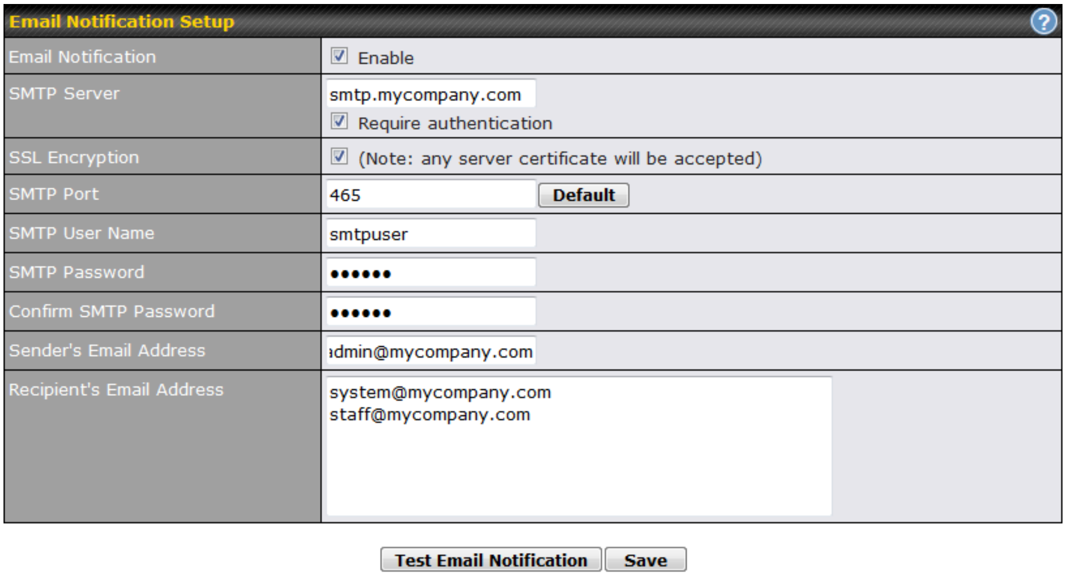
Schedule Map

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

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

16.1.5 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**.



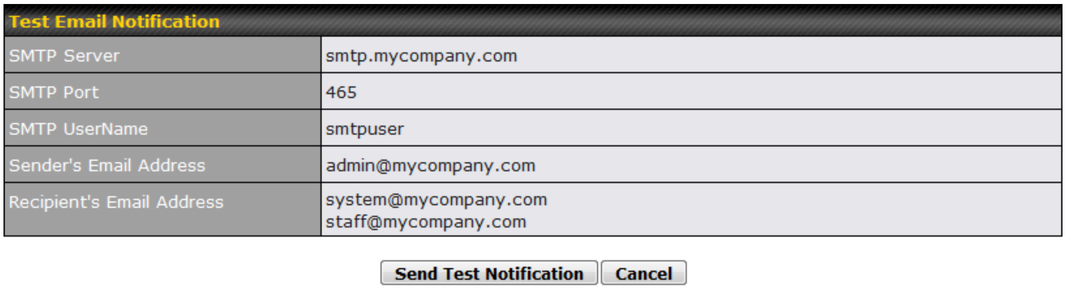
Email Notification Setup

Email Notification	☑ Enable
SMTP Server	smtp.mycompany.com ☑ Require authentication
SSL Encryption	☑ (Note: any server certificate will be accepted)
SMTP Port	465 Default
SMTP User Name	smtpuser
SMTP Password	••••••
Confirm SMTP Password	••••••
Sender's Email Address	ıdmin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

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

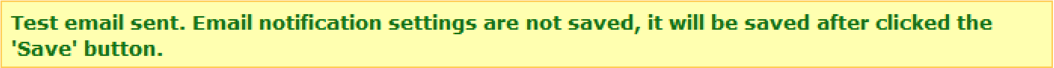
	authentication, check **Require authentication**.
SSL Encryption	Check the box to enable SMTPS. When the box is checked, **SMTP Port** will be changed to **465** automatically.
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to **25**; when **SSL Encryption** is checked,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

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

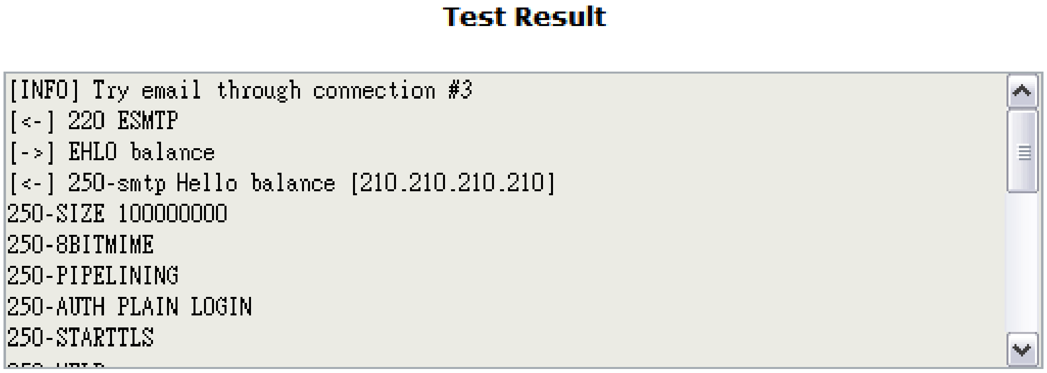


Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

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.

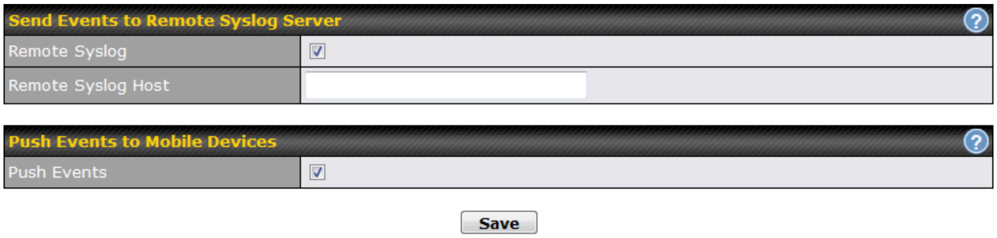


Test Result

```
[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
```

16.1.6 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**.



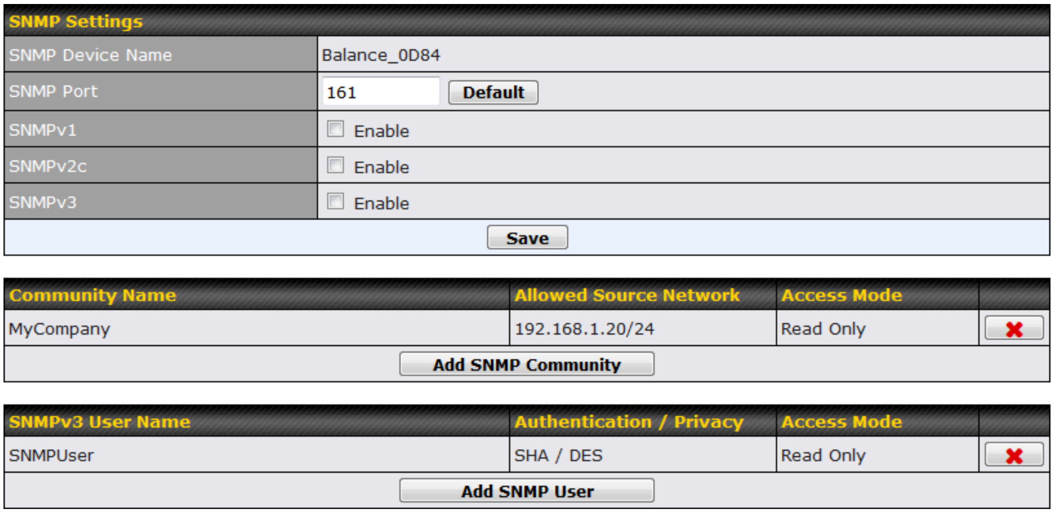
Send Events to Remote Syslog Server	
Remote Syslog	☑
Remote Syslog Host	

Push Events to Mobile Devices	
Push Events	☑

Remote Syslog Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
Push Events	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.
peplink PEPWAVE	For more information on the Router Utility, go to: www.peplink.com/products/router-utility

16.1.7 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**.



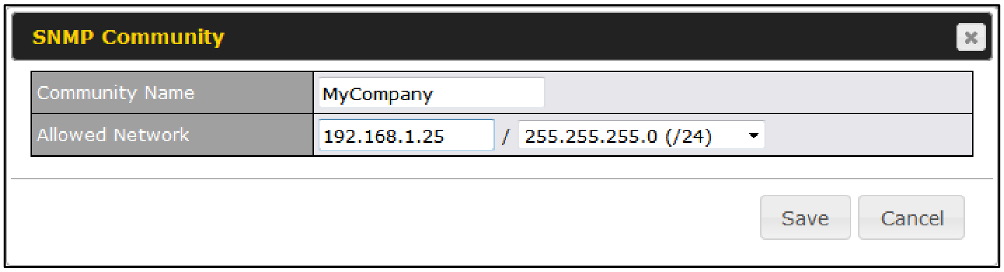
SNMP Settings	
SNMP Device Name	Balance_0D84
SNMP Port	161 Default
SNMPv1	□ Enable
SNMPv2c	□ Enable
SNMPv3	□ Enable
	Save

Community Name	Allowed Source Network	Access Mode	
MyCompany	192.168.1.20/24	Read Only	✖
Add SNMP Community			

SNMPv3 User Name	Authentication / Privacy	Access Mode	
SNMPUser	SHA / DES	Read Only	✖
Add SNMP User			

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

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

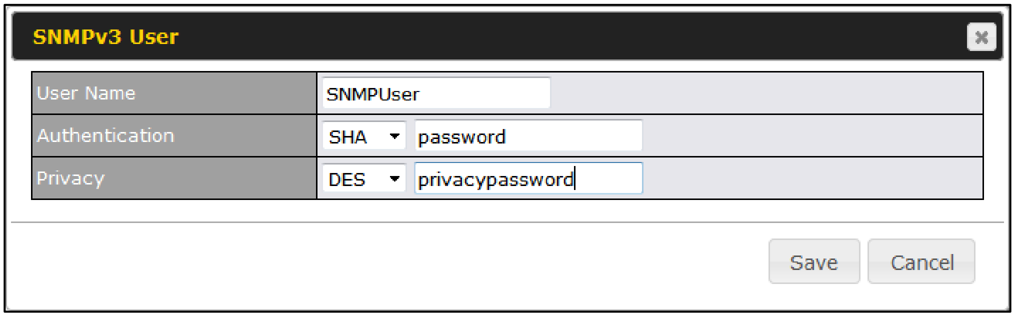


SNMP Community

Community Name	MyCompany
Allowed Network	192.168.1.25 / 255.255.255.0 (/24)

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

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



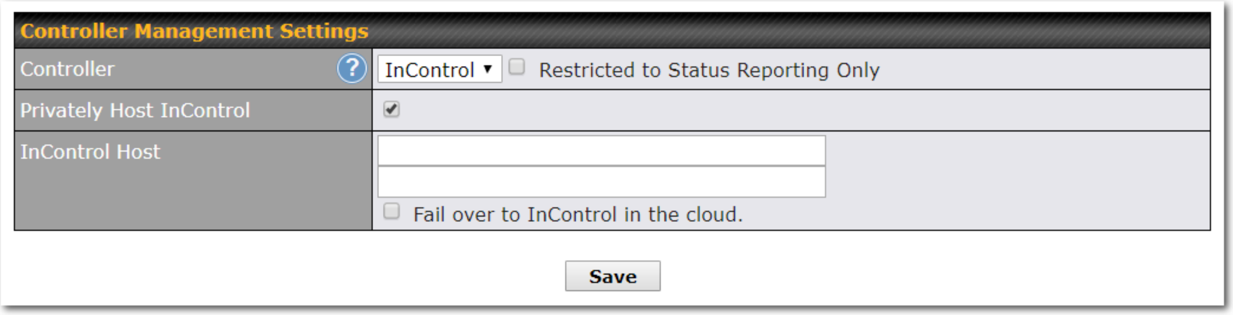
SNMPv3 User

User Name	SNMPUser
Authentication	SHA password
Privacy	DES privacypassword

SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols: ● NONE ● MD5

	- SHA When MD5 or SHA is selected, an entry field will appear for the password.
Privacy Protocol	This setting specifies via a drop-down menu one of the following valid privacy protocols: - NONE - DES When DES is selected, an entry field will appear for the password.

16.1.8 InControl



Controller Management Settings

Controller	InControl ▾ □ Restricted to Status Reporting Only
Privately Host InControl	☑
InControl Host	□ Fail over to InControl in the cloud.

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 checkbox 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.

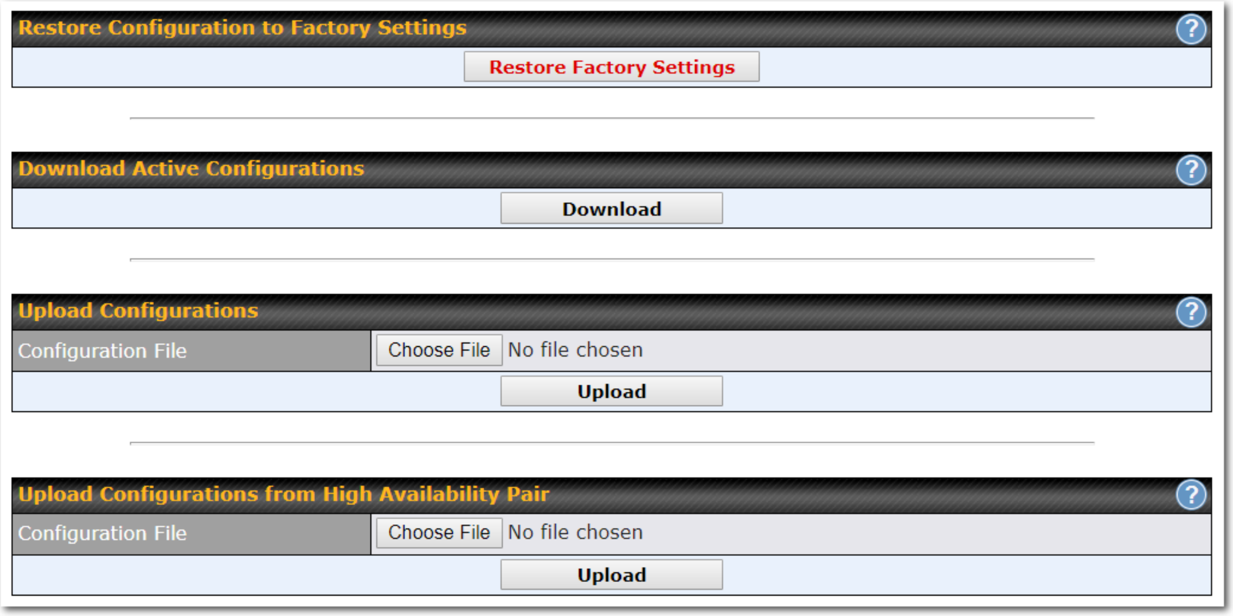
When the box **Restricted to Status Reporting Only** is ticked, the router will only report its status, but can’t be managed or configured by InControl.

Alternatively, you can 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.

16.1.9 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**.



Restore Configuration to Factory Settings

Restore Factory Settings

Download Active Configurations

Download

Upload Configurations

Configuration File: Choose File No file chosen

Upload

Upload Configurations from High Availability Pair

Configuration File: Choose File No file chosen

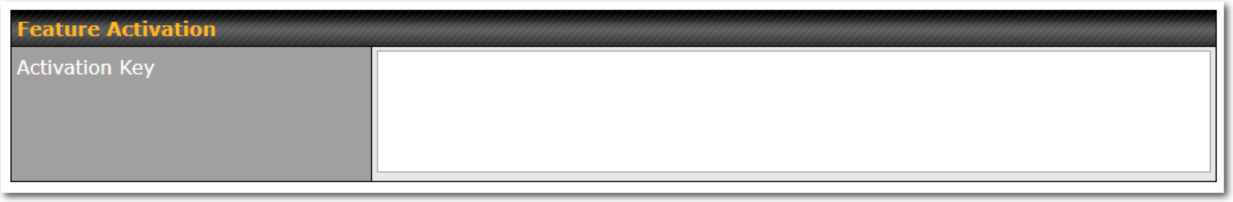
Upload

Configuration	
Restore Configuration to Factory Settings	The **Restore Factory Settings** button is to reset the configuration to factory default settings. After clicking the button, you will need to click the **Apply Changes** button on the top right corner to make the settings effective.
Download Active Configurations	Click **Download** to backup the current active settings.
Upload Configurations	To restore or change settings based on a configuration file, click **Choose File** to locate the configuration file on the local computer, and then click **Upload**. The new settings can then be applied by clicking the **Apply Changes** button on the page header, or you can cancel the procedure by pressing **discard** on the main page of the web admin interface.

Upload Configurations from High Availability Pair	In a high availability (HA) configuration, the Balance unit can quickly load the configuration of its HA counterpart. To do so, click the **Upload** button. After loading the settings, configure the LAN IP address of the Peplink Balance unit so that it is different from the HA counterpart.

16.1.10 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**.



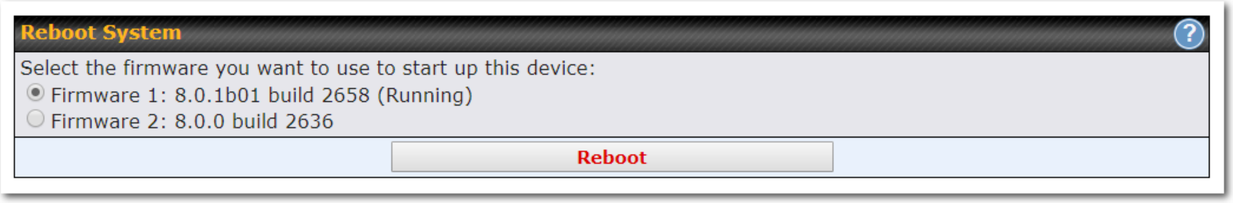
Feature Activation

Activation Key	

16.1.11 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.



Reboot System

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

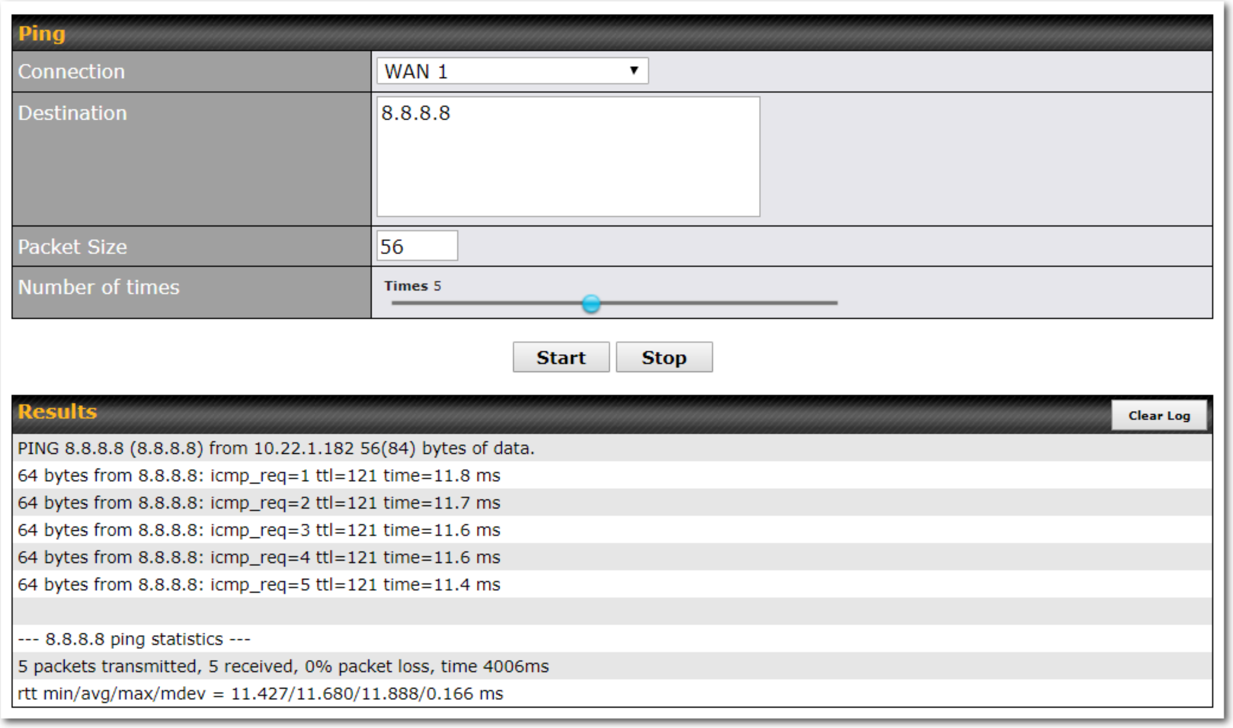
● Firmware 1: 8.0.1b01 build 2658 (Running)

○ Firmware 2: 8.0.0 build 2636

16.2 Tools

16.3 Ping

The ping test tool sends pings through a specific Ethernet interface or a SpeedFusion^{TM} 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:



Connection	WAN 1
Destination	8.8.8.8
Packet Size	56
Number of times	Times 5

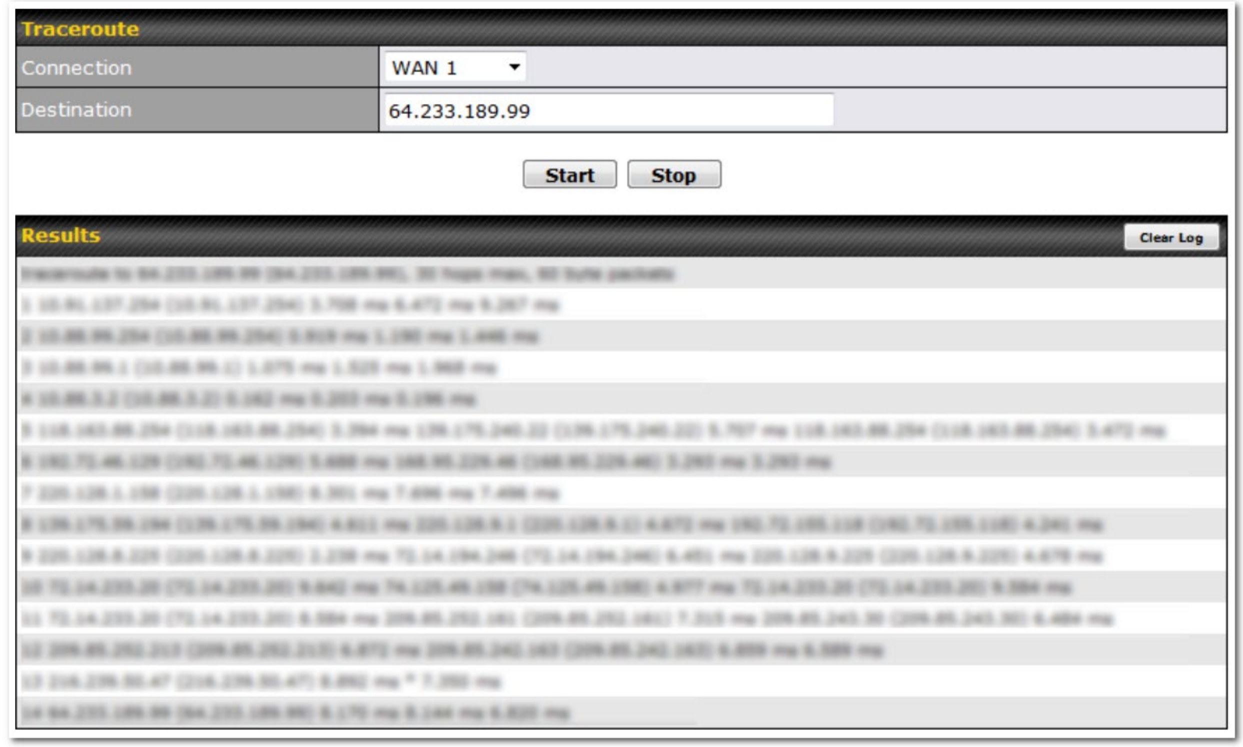
```
PING 8.8.8.8 (8.8.8.8) from 10.22.1.182 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=121 time=11.8 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=121 time=11.7 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=121 time=11.4 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 11.427/11.680/11.888/0.166 ms
```

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

16.4 Traceroute

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



Traceroute

Connection	WAN 1
Destination	64.233.189.99

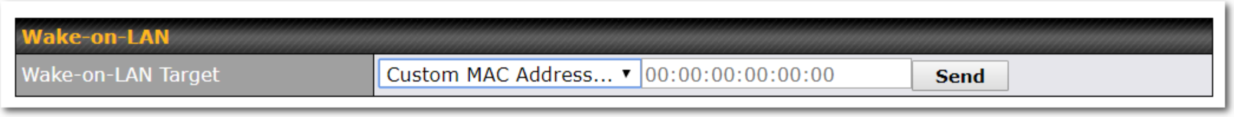
```
traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 60 byte packets
1 10.91.137.254 (10.91.137.254) 3.708 ms 6.472 ms 9.267 ms
2 10.88.99.254 (10.88.99.254) 0.919 ms 1.190 ms 1.446 ms
3 10.88.99.1 (10.88.99.1) 1.075 ms 1.525 ms 1.968 ms
4 10.88.3.2 (10.88.3.2) 0.162 ms 0.203 ms 0.196 ms
5 118.143.88.254 (118.143.88.254) 3.394 ms 139.175.240.22 (139.175.240.22) 5.707 ms 118.143.88.254 (118.143.88.254) 3.472 ms
6 192.72.46.129 (192.72.46.129) 5.688 ms 168.95.229.46 (168.95.229.46) 3.293 ms 3.293 ms
7 220.128.1.158 (220.128.1.158) 8.301 ms 7.496 ms 7.496 ms
8 139.175.59.194 (139.175.59.194) 4.611 ms 220.128.8.1 (220.128.8.1) 4.672 ms 192.72.155.118 (192.72.155.118) 4.241 ms
9 220.128.8.225 (220.128.8.225) 1.238 ms 72.14.194.246 (72.14.194.246) 6.451 ms 220.128.8.225 (220.128.8.225) 4.678 ms
10 72.14.233.20 (72.14.233.20) 9.842 ms 74.125.49.158 (74.125.49.158) 4.977 ms 72.14.233.20 (72.14.233.20) 9.384 ms
11 72.14.233.20 (72.14.233.20) 6.584 ms 209.85.252.161 (209.85.252.161) 7.315 ms 209.85.243.30 (209.85.243.30) 6.484 ms
12 209.85.252.213 (209.85.252.213) 6.872 ms 209.85.242.163 (209.85.242.163) 6.859 ms 6.589 ms
13 216.239.50.47 (216.239.50.47) 6.892 ms * 7.350 ms
14 64.233.189.99 (64.233.189.99) 8.170 ms 8.144 ms 6.820 ms
```

Tip

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

16.5 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

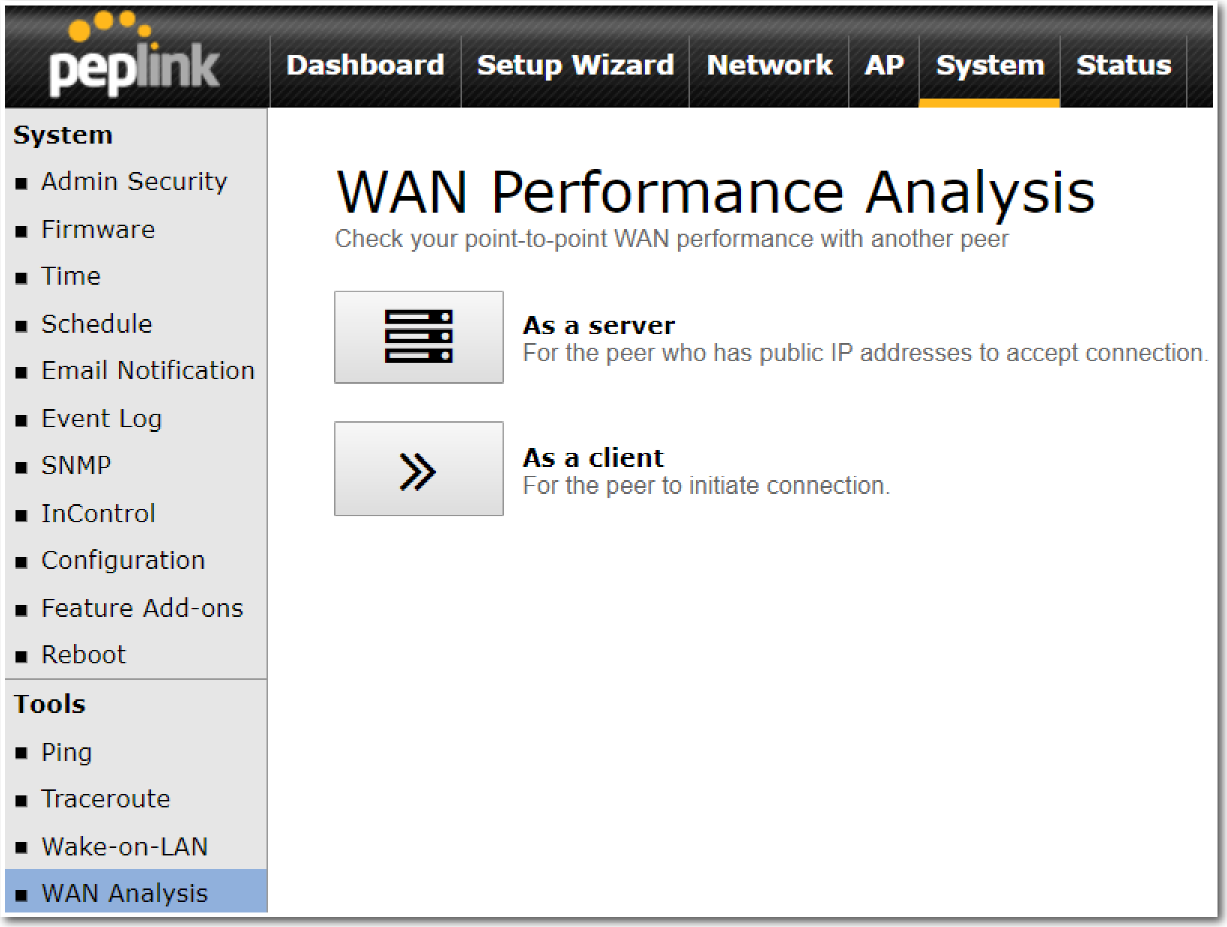
Wake-on-LAN Target	Custom MAC Address... 00:00:00:00:00:00

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

16.6 WAN Analysis

The WAN Analysis feature allows you to run a WAN to WAN speed test between 2 Peplink devices .

You can set a device up as a **Server** or a **Client**. One device must be set up as a server to run the speed tests and the server must have a public IP address.



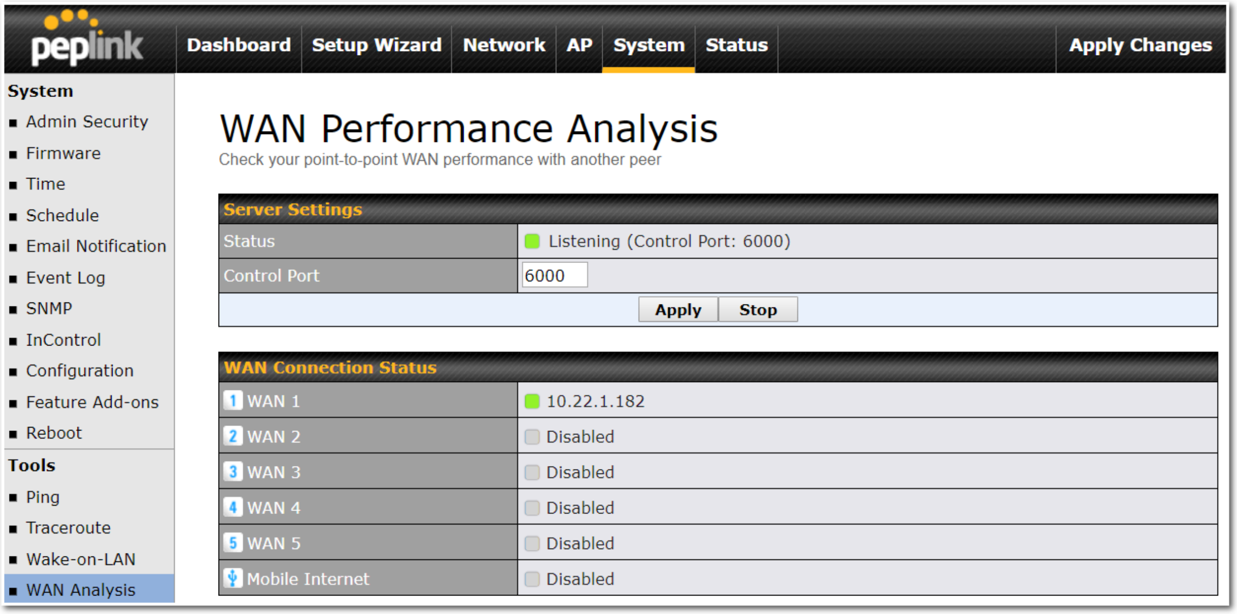
WAN Performance Analysis

Check your point-to-point WAN performance with another peer

As a server
For the peer who has public IP addresses to accept connection.

As a client
For the peer to initiate connection.

The default port is 6000 and can be changed if required. The IP address of the WAN interface will be shown in the **WAN Connection Status** section.



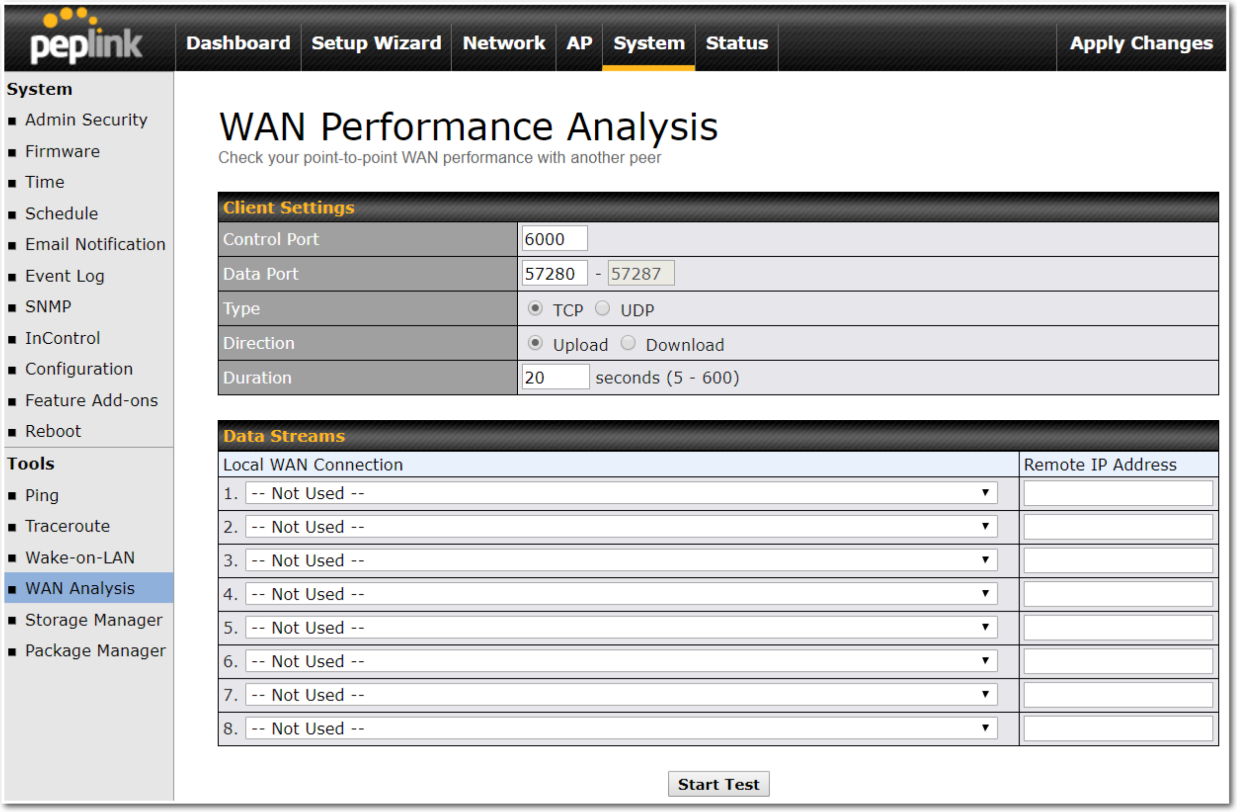
WAN Performance Analysis

Check your point-to-point WAN performance with another peer

Server Settings	
Status	🟩 Listening (Control Port: 6000)
Control Port	6000

WAN Connection Status	
1 WAN 1	🟩 10.22.1.182
2 WAN 2	□ Disabled
3 WAN 3	□ Disabled
4 WAN 4	□ Disabled
5 WAN 5	□ Disabled
Mobile Internet	□ Disabled

The client side has a few more settings that can be changed. Make sure that the **Control Port** matches what's been entered on the server side. Select the WAN(s) that will be used for testing and enter the Servers WAN IP address. Once all of the options have been set, click the **Start Test** button.



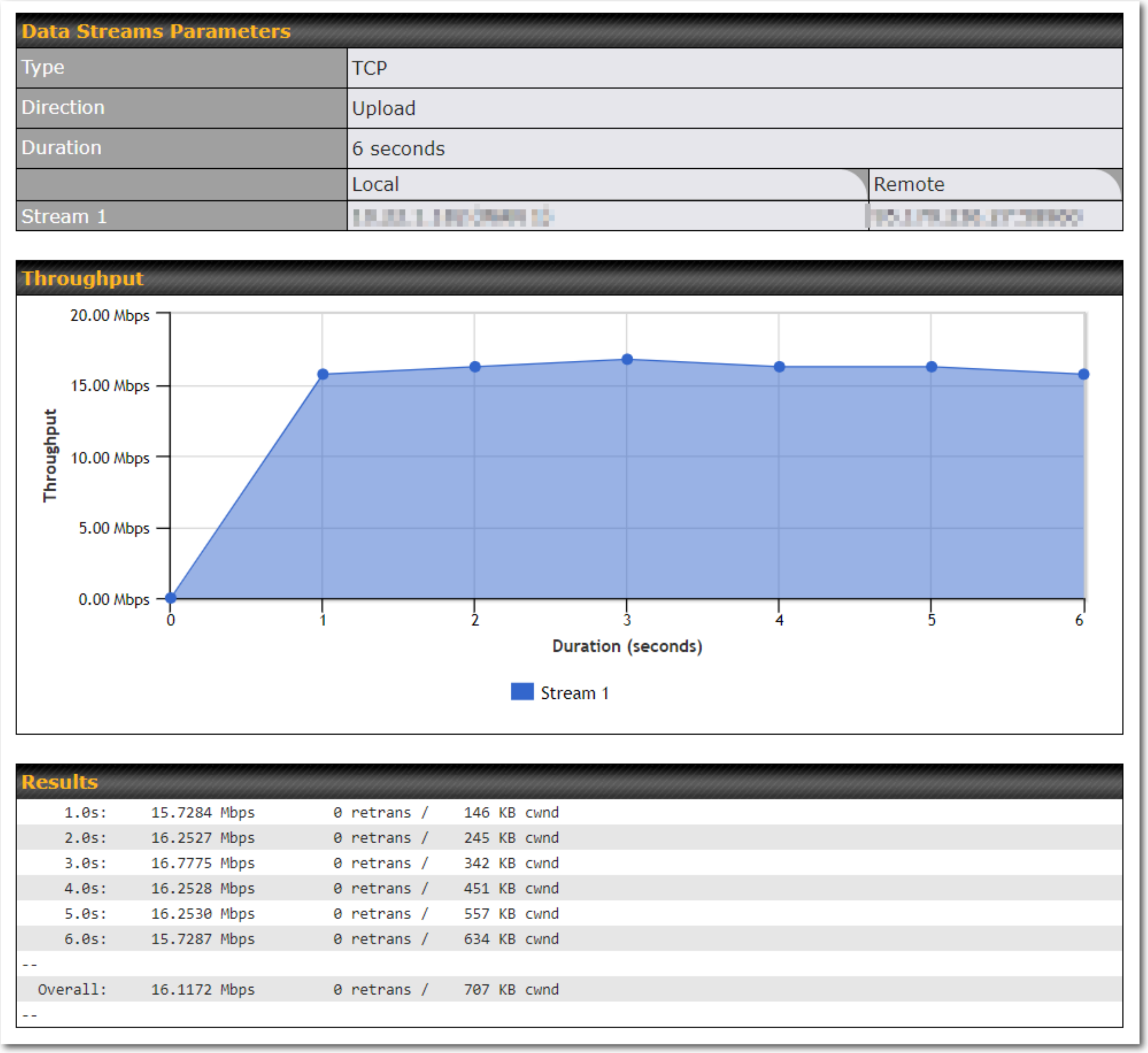
WAN Performance Analysis

Check your point-to-point WAN performance with another peer

Client Settings	
Control Port	6000
Data Port	57280 - 57287
Type	● TCP ○ UDP
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

Local WAN Connection	Remote IP Address
1. -- Not Used --	
2. -- Not Used --	
3. -- Not Used --	
4. -- Not Used --	
5. -- Not Used --	
6. -- Not Used --	
7. -- Not Used --	
8. -- Not Used --	

The test output will show the **Data Streams Parameters**, the **Throughput** as a graph, and the **Results**.



Data Streams Parameters

Type	TCP	
Direction	Upload	
Duration	6 seconds	
	Local	Remote
Stream 1	[redacted]	[redacted]

Throughput

Results

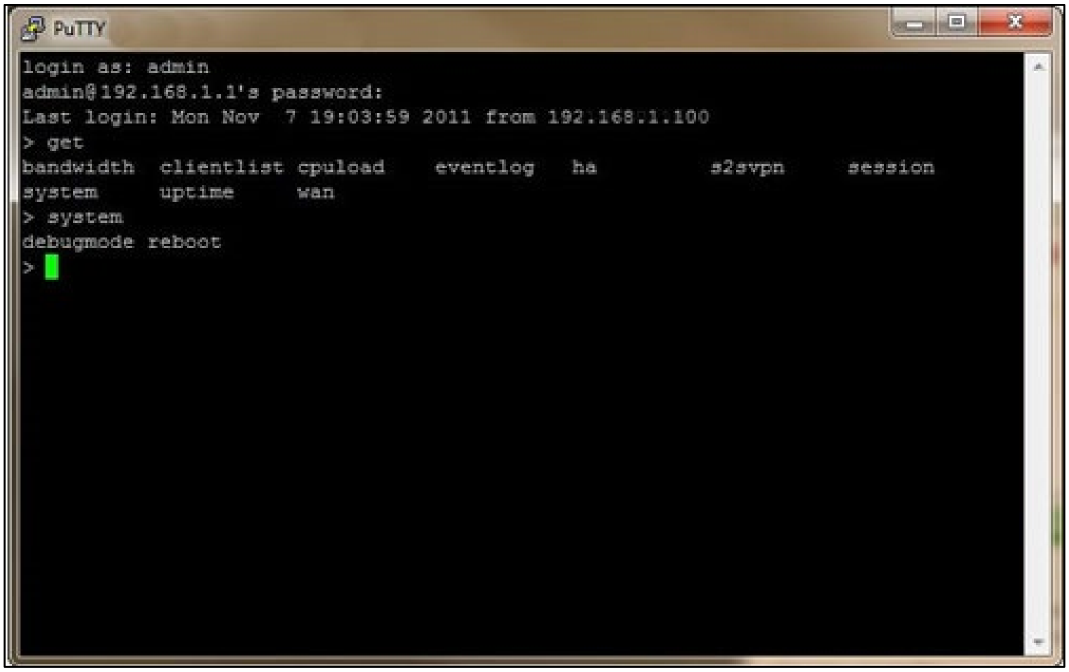
```
    1.0s:    15.7284 Mbps       0 retrans /    146 KB cwnd
    2.0s:    16.2527 Mbps       0 retrans /    245 KB cwnd
    3.0s:    16.7775 Mbps       0 retrans /    342 KB cwnd
    4.0s:    16.2528 Mbps       0 retrans /    451 KB cwnd
    5.0s:    16.2530 Mbps       0 retrans /    557 KB cwnd
    6.0s:    15.7287 Mbps       0 retrans /    634 KB cwnd
--
 Overall:    16.1172 Mbps       0 retrans /    707 KB cwnd
--
```

The test can be run again once it’s complete by clicking the **Start** button or you can click **Close** and change the parameters for the test.

16.7 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*.



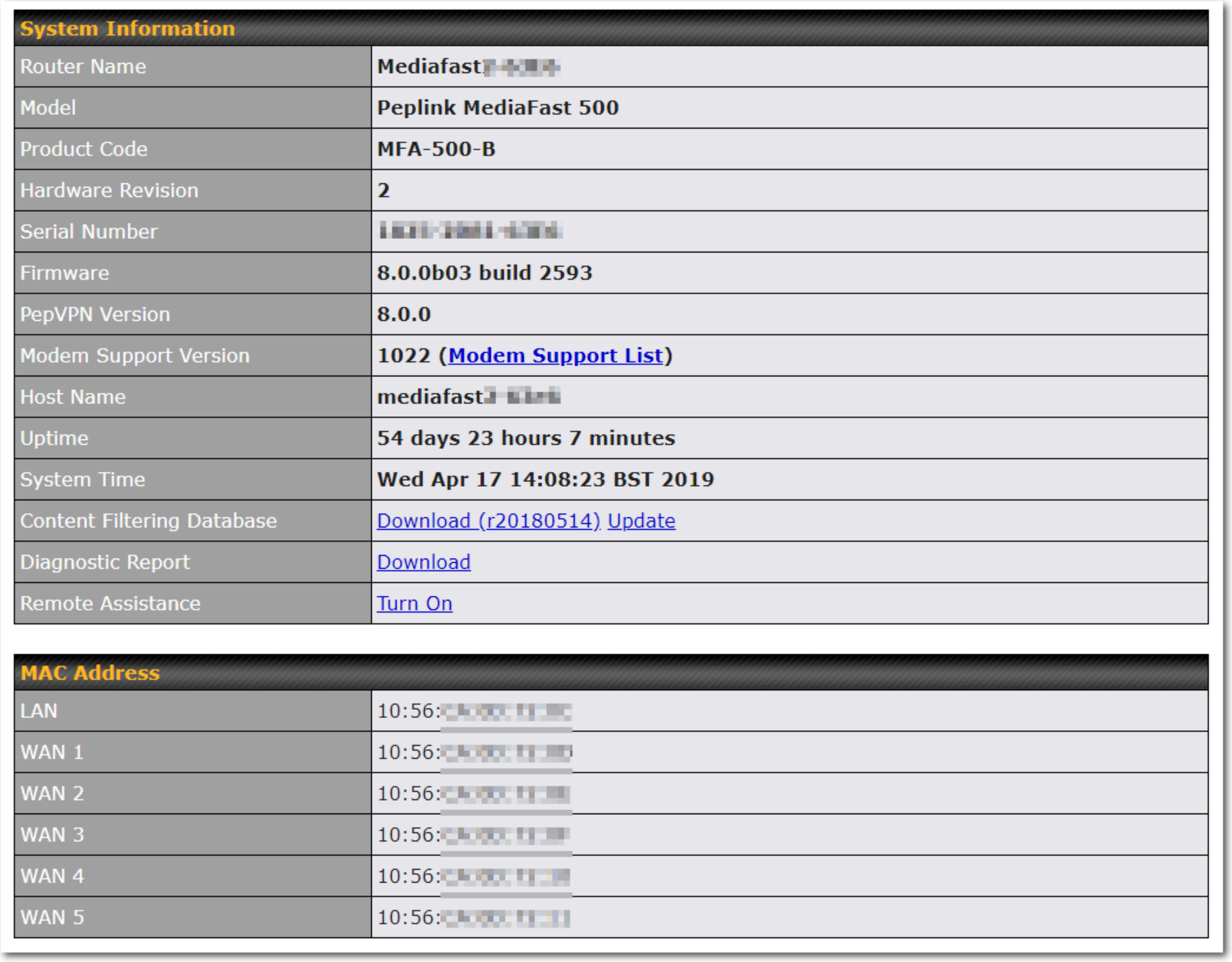
```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist cpuload    eventlog   ha         s2svpn     session
system     uptime     wan
> system
debugmode reboot
> 
```

17 Status Tab

17.1 Status

17.1.1 Device

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



System Information	
Router Name	Mediafast[redacted]
Model	Peplink MediaFast 500
Product Code	MFA-500-B
Hardware Revision	2
Serial Number	[redacted]
Firmware	8.0.0b03 build 2593
PepVPN Version	8.0.0
Modem Support Version	1022 (Modem Support List)
Host Name	mediafast[redacted]
Uptime	54 days 23 hours 7 minutes
System Time	Wed Apr 17 14:08:23 BST 2019
Content Filtering Database	Download (r20180514) Update
Diagnostic Report	Download
Remote Assistance	Turn On

MAC Address	
LAN	10:56:[redacted]
WAN 1	10:56:[redacted]
WAN 2	10:56:[redacted]
WAN 3	10:56:[redacted]
WAN 4	10:56:[redacted]
WAN 5	10:56:[redacted]

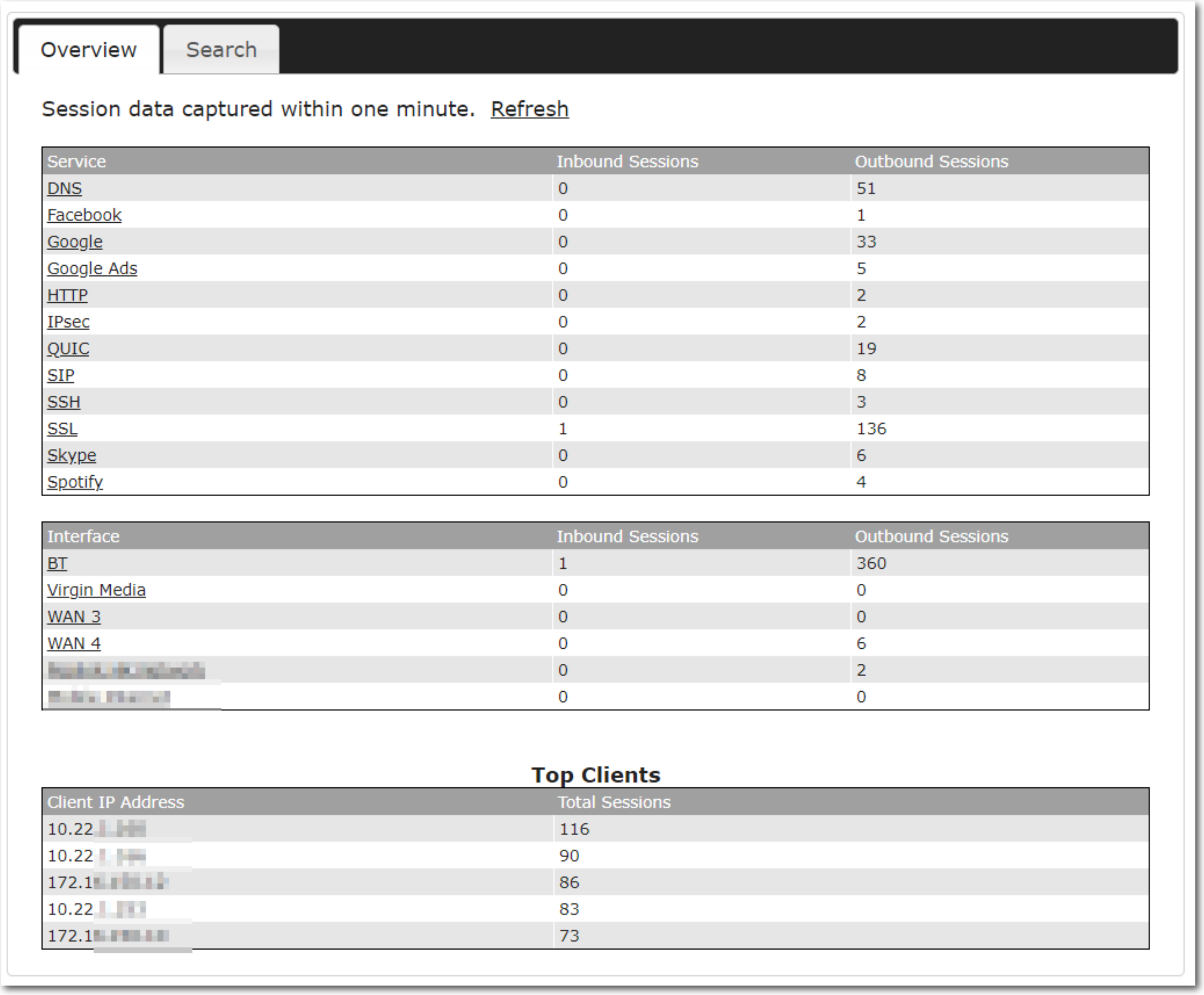
System Information	
Router Name	This is the name specified in the **Router Name** field located at **System>Admin Security**.
Model	This shows the model name and number of this device.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this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

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

Important Note
If you encounter issues and would like to contact the Peplink Support Team (http://www.peplink.com/contact/), please download the diagnostic report file and attach it along with a description of your issue.

17.1.2 Active Sessions

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



Session data captured within one minute. Refresh

Service	Inbound Sessions	Outbound Sessions
DNS	0	51
Facebook	0	1
Google	0	33
Google Ads	0	5
HTTP	0	2
IPsec	0	2
QUIC	0	19
SIP	0	8
SSH	0	3
SSL	1	136
Skype	0	6
Spotify	0	4

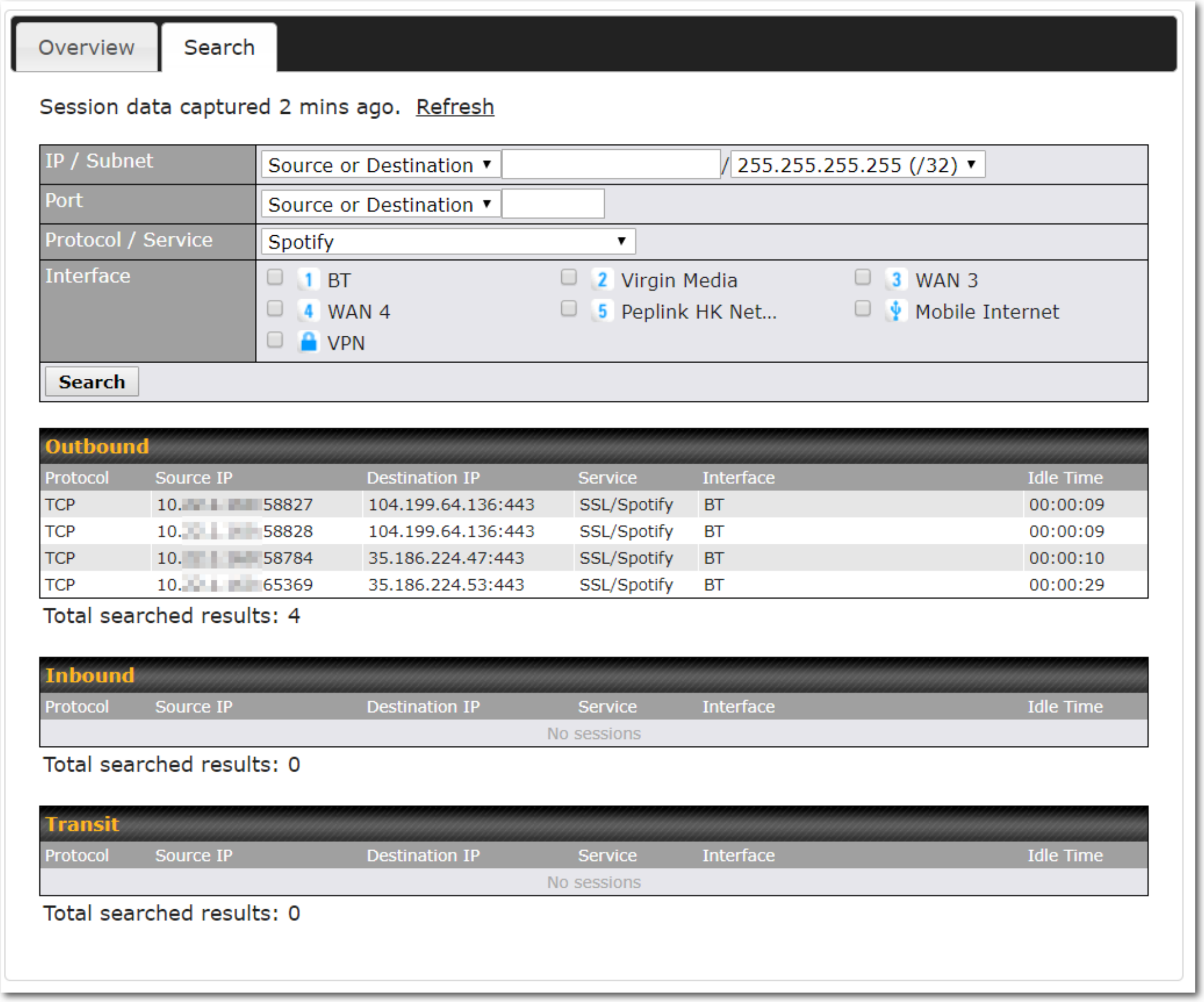
Interface	Inbound Sessions	Outbound Sessions
BT	1	360
Virgin Media	0	0
WAN 3	0	0
WAN 4	0	6
[redacted]	0	2
[redacted]	0	0

Top Clients

Client IP Address	Total Sessions
10.22[redacted]	116
10.22[redacted]	90
172.1[redacted]	86
10.22[redacted]	83
172.1[redacted]	73

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**.



Session data captured 2 mins ago. Refresh

IP / Subnet	Source or Destination ▾ / 255.255.255.255 (/32) ▾
Port	Source or Destination ▾
Protocol / Service	Spotify ▾
Interface	□ 1 BT □ 2 Virgin Media □ 3 WAN 3 □ 4 WAN 4 □ 5 Peplink HK Net... □ Mobile Internet □ VPN

Search

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
TCP	10.[redacted]58827	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.[redacted]58828	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.[redacted]58784	35.186.224.47:443	SSL/Spotify	BT	00:00:10
TCP	10.[redacted]65369	35.186.224.53:443	SSL/Spotify	BT	00:00:29

Total searched results: 4

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					

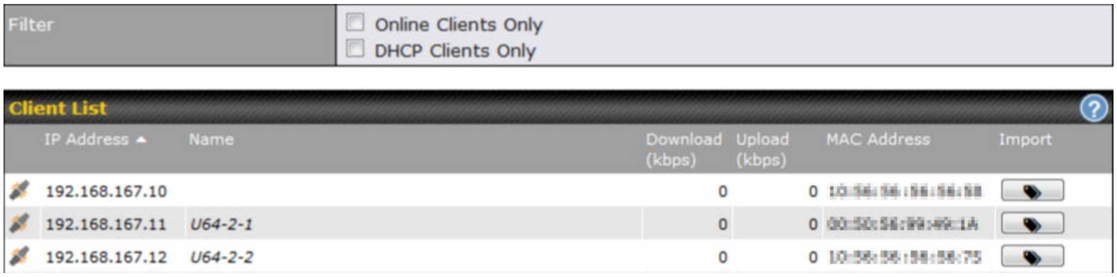
Total searched results: 0

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.

17.1.3 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	□ Online Clients Only □ DHCP Clients Only

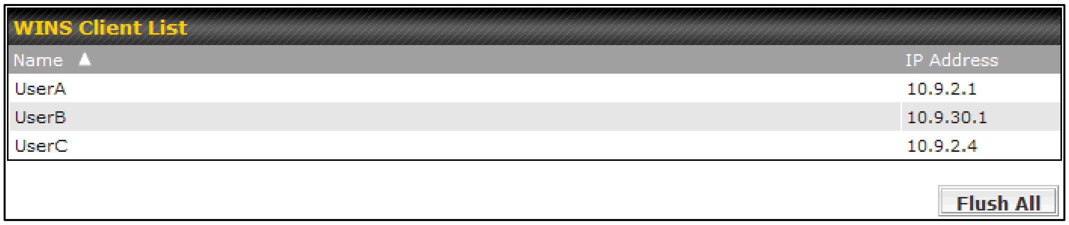
Client List

IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
192.168.167.10		0	0	[redacted]	
192.168.167.11	*U64-2-1*	0	0	[redacted]	
192.168.167.12	*U64-2-2*	0	0	[redacted]	

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

17.1.4 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

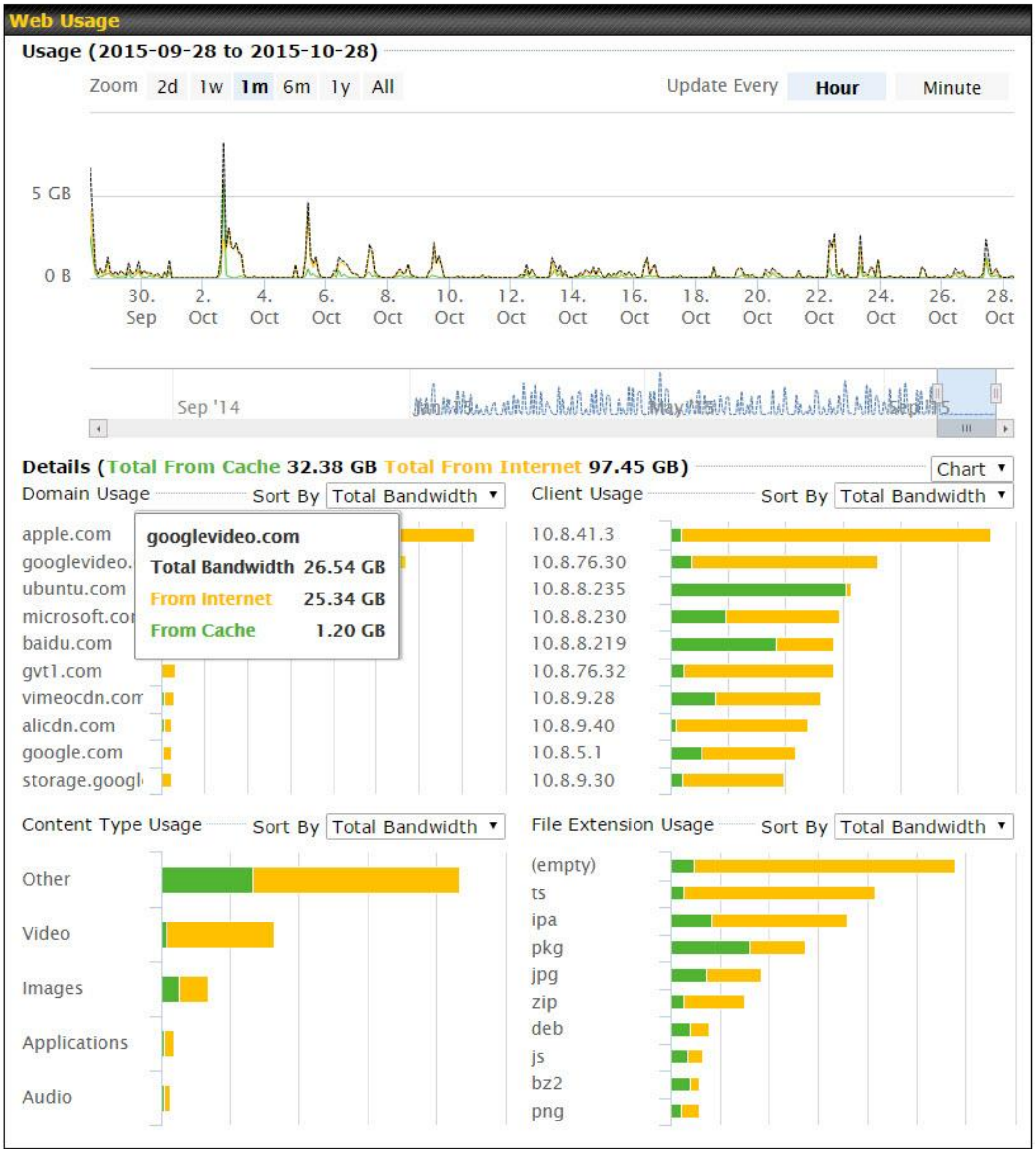
The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush All** to flush all WINS client records.

17.1.5 OSPF & RIPv2

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

17.1.6 MediaFast

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



Web Usage

Usage (2015-09-28 to 2015-10-28)

Details (Total From Cache 32.38 GB Total From Internet 97.45 GB)

Domain Usage — Sort By: Total Bandwidth

Client Usage — Sort By: Total Bandwidth

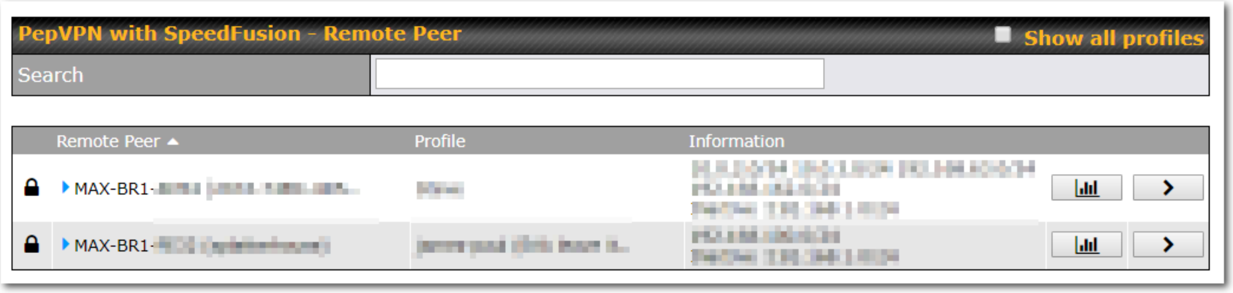
Content Type Usage — Sort By: Total Bandwidth

File Extension Usage — Sort By: Total Bandwidth

googlevideo.com	
Total Bandwidth	26.54 GB
From Internet	25.34 GB
From Cache	1.20 GB

17.1.7 SpeedFusion Status

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



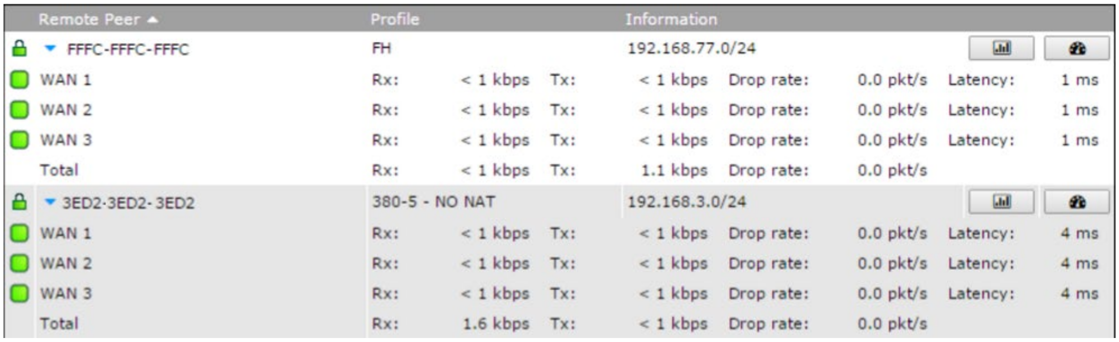
PepVPN with SpeedFusion - Remote Peer

□ Show all profiles

Search

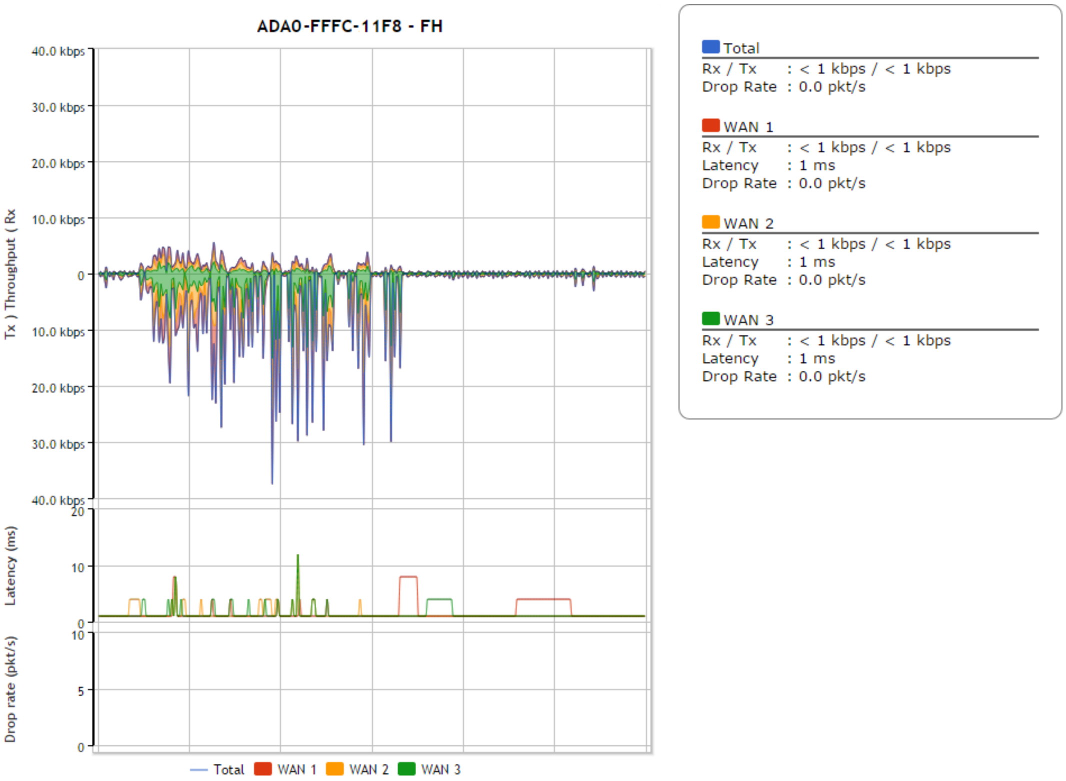
	Remote Peer ▲	Profile	Information
🔒	▶ MAX-BR1-[redacted]	[redacted]	[redacted]
🔒	▶ MAX-BR1-[redacted]	[redacted]	[redacted]

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				
🟩	WAN 1	Rx:	< 1 kbps	Tx:	< 1 kbps	Drop rate:	0.0 pkt/s	Latency:	1 ms
🟩	WAN 2	Rx:	< 1 kbps	Tx:	< 1 kbps	Drop rate:	0.0 pkt/s	Latency:	1 ms
🟩	WAN 3	Rx:	< 1 kbps	Tx:	< 1 kbps	Drop rate:	0.0 pkt/s	Latency:	1 ms
	Total	Rx:	< 1 kbps	Tx:	1.1 kbps	Drop rate:	0.0 pkt/s		
🔒	▼ 3ED2-3ED2-3ED2	380-5 - NO NAT			192.168.3.0/24				
🟩	WAN 1	Rx:	< 1 kbps	Tx:	< 1 kbps	Drop rate:	0.0 pkt/s	Latency:	4 ms
🟩	WAN 2	Rx:	< 1 kbps	Tx:	< 1 kbps	Drop rate:	0.0 pkt/s	Latency:	4 ms
🟩	WAN 3	Rx:	< 1 kbps	Tx:	< 1 kbps	Drop rate:	0.0 pkt/s	Latency:	4 ms
	Total	Rx:	1.6 kbps	Tx:	< 1 kbps	Drop rate:	0.0 pkt/s		

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



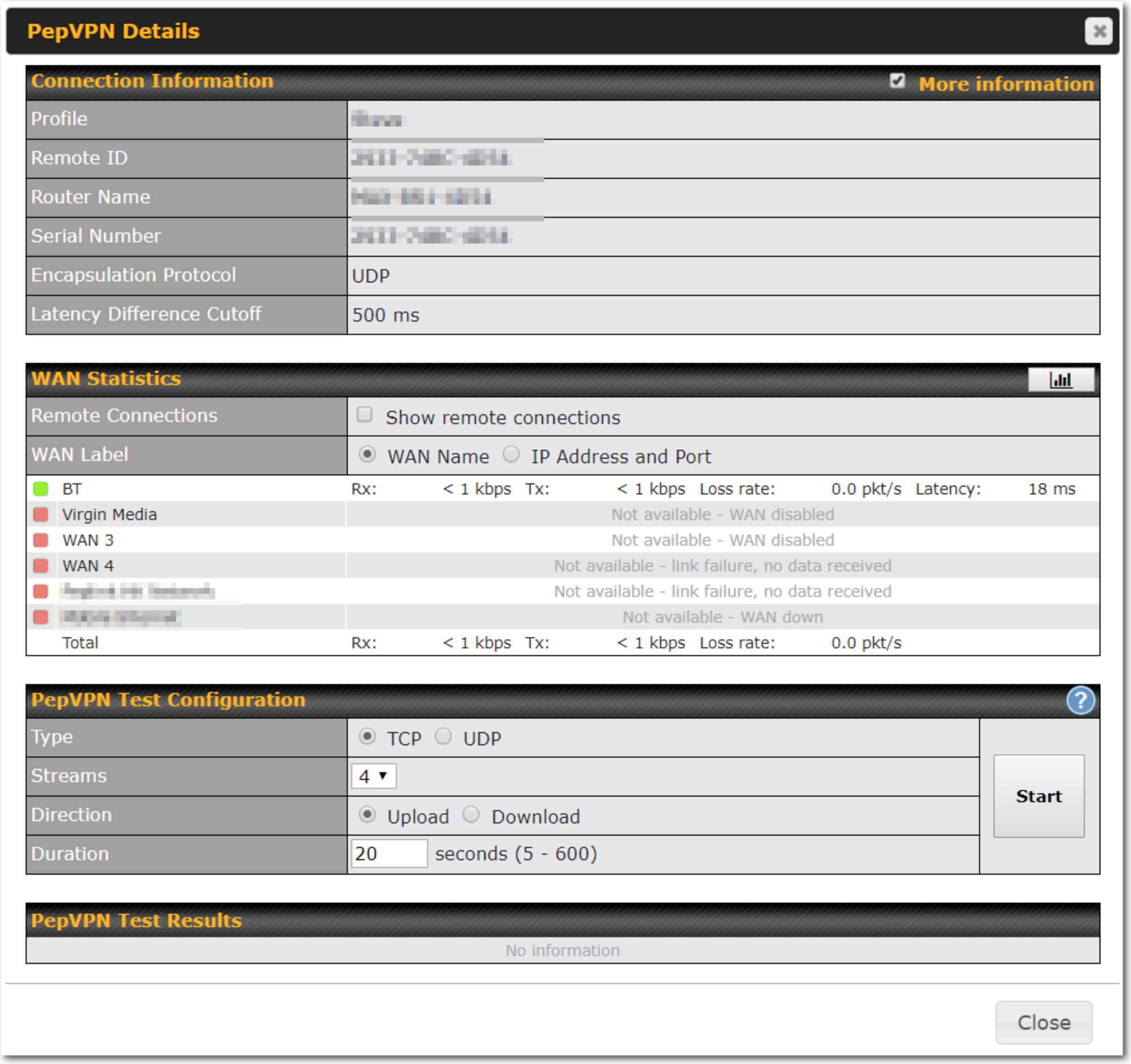
🟦 Total
Rx / Tx : < 1 kbps / < 1 kbps
Drop Rate : 0.0 pkt/s

🟥 WAN 1
Rx / Tx : < 1 kbps / < 1 kbps
Latency : 1 ms
Drop Rate : 0.0 pkt/s

🟧 WAN 2
Rx / Tx : < 1 kbps / < 1 kbps
Latency : 1 ms
Drop Rate : 0.0 pkt/s

🟩 WAN 3
Rx / Tx : < 1 kbps / < 1 kbps
Latency : 1 ms
Drop Rate : 0.0 pkt/s

When pressing the > button, the following menu will appear:



Connection Information ☑ More information

Profile	[redacted]
Remote ID	[redacted]
Router Name	[redacted]
Serial Number	[redacted]
Encapsulation Protocol	UDP
Latency Difference Cutoff	500 ms

WAN Statistics

Remote Connections	□ Show remote connections
WAN Label	● WAN Name ○ IP Address and Port

🟩	BT	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s	Latency:	18 ms
🟥	Virgin Media	Not available - WAN disabled							
🟥	WAN 3	Not available - WAN disabled							
🟥	WAN 4	Not available - link failure, no data received							
🟥	[redacted]	Not available - link failure, no data received							
🟥	[redacted]	Not available - WAN down							
	Total	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s		

PepVPN Test Configuration

Type	● TCP ○ UDP
Streams	4 ▾
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

PepVPN Test Results

No information

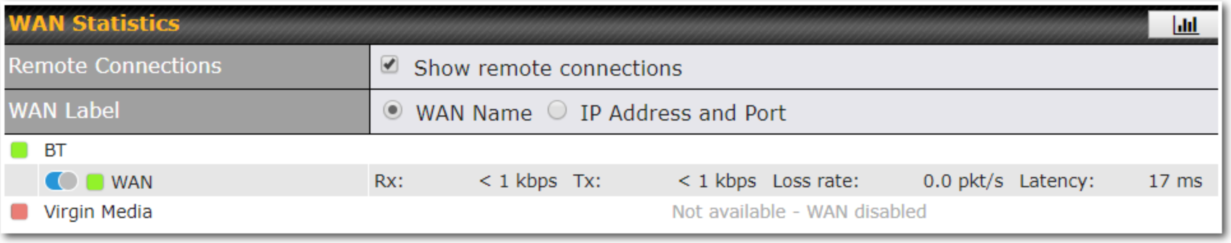
The **connection information** shows the details of the selected PepVPN profile, consisting of the Profile name, **Router ID**, **Router Nam**e and **Serial Number** of the remote router

Advanced features for the PepVPN profile will also be shown when the **More Information** checkbox is selected.

The **WAN statistics** show information about the local and remote WAN connections (when **show Remote**

connections) is selected.

The available details are **WAN Name, IP address** and **port** used for the Speedfusion connection. **Rx and Tx rates, Loss rate and Latency**.
Connections can be temporarily disabled by sliding the switch button next to a WAN connection to the left. The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15 minutes without any action.
This can be used when testing the PepVPN speed between two locations to see if there is interference or network congestion between certain WAN connections.



WAN Statistics

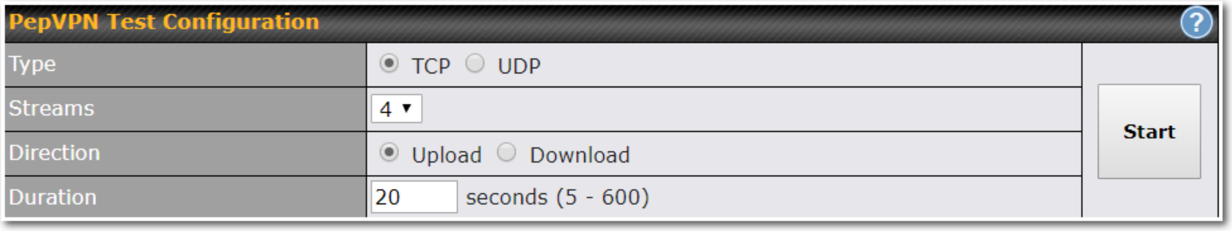
Remote Connections	☑ Show remote connections
WAN Label	● WAN Name ○ IP Address and Port

🟩 BT

🟩 WAN — Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 17 ms

🟥 Virgin Media — Not available - WAN disabled

The PepVPN test configuration allows to configure and perform throughput tests. THis is usually done after the initial installation of the routers and in case there are problems with aggregation.

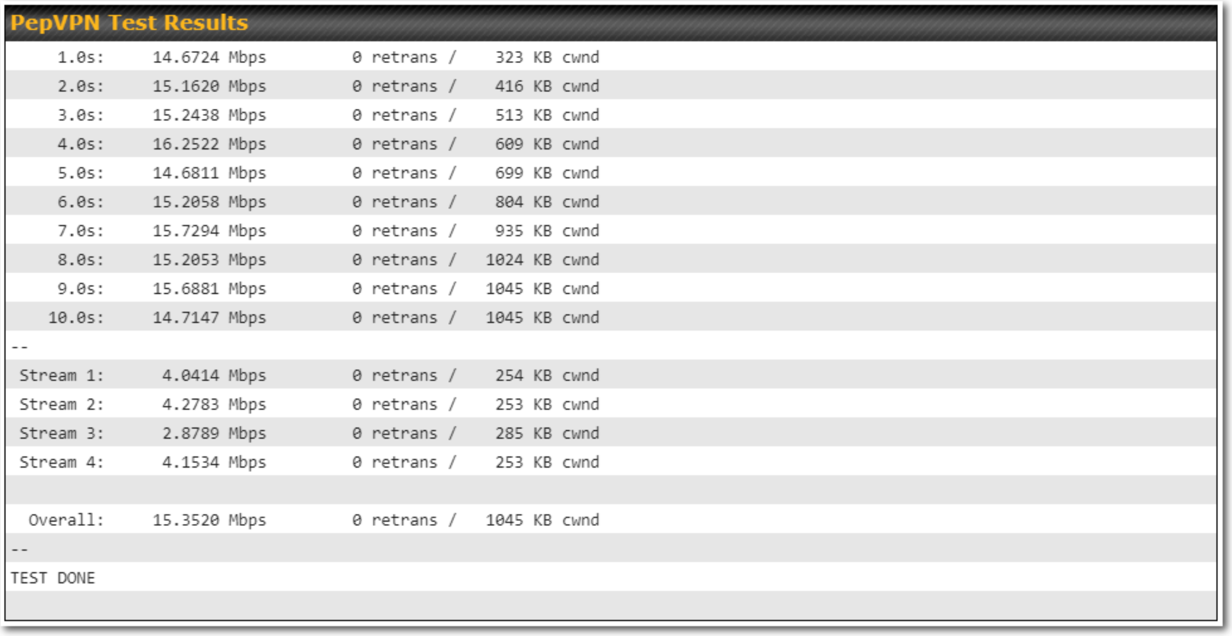


PepVPN Test Configuration

Type	● TCP ○ UDP
Streams	4 ▾
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

Press the Start button to perform throughput test according to the configured options.

If TCP is selected, 4 parallel streams will be generated to get the optimal results by default. This can be customized by selecting a different value of streams.
Using more streams will typically get better results if the latency of the tunnel is high.



PepVPN Test Results

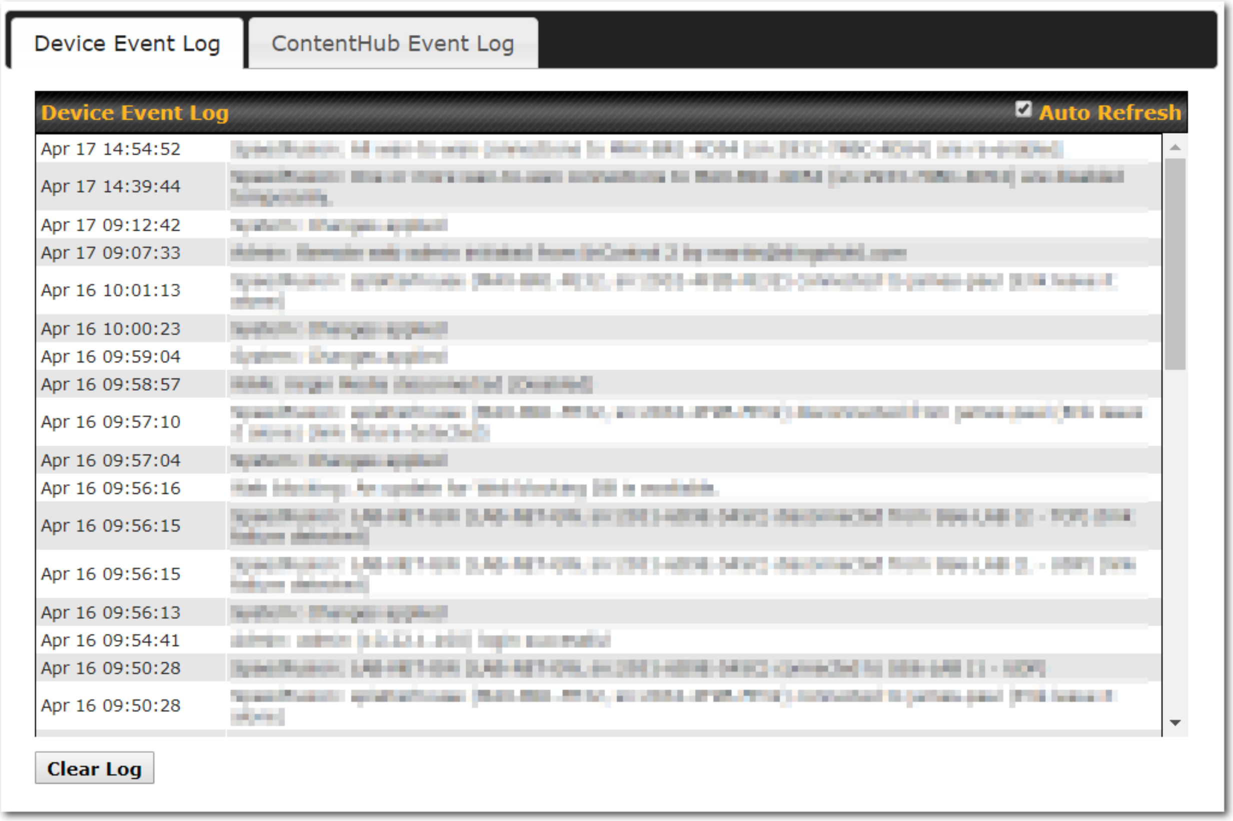
```
    1.0s:     14.6724 Mbps         0 retrans /    323 KB cwnd
    2.0s:     15.1620 Mbps         0 retrans /    416 KB cwnd
    3.0s:     15.2438 Mbps         0 retrans /    513 KB cwnd
    4.0s:     16.2522 Mbps         0 retrans /    609 KB cwnd
    5.0s:     14.6811 Mbps         0 retrans /    699 KB cwnd
    6.0s:     15.2058 Mbps         0 retrans /    804 KB cwnd
    7.0s:     15.7294 Mbps         0 retrans /    935 KB cwnd
    8.0s:     15.2053 Mbps         0 retrans /   1024 KB cwnd
    9.0s:     15.6881 Mbps         0 retrans /   1045 KB cwnd
   10.0s:     14.7147 Mbps         0 retrans /   1045 KB cwnd
--
 Stream 1:     4.0414 Mbps         0 retrans /    254 KB cwnd
 Stream 2:     4.2783 Mbps         0 retrans /    253 KB cwnd
 Stream 3:     2.8789 Mbps         0 retrans /    285 KB cwnd
 Stream 4:     4.1534 Mbps         0 retrans /    253 KB cwnd

  Overall:    15.3520 Mbps         0 retrans /   1045 KB cwnd
--
TEST DONE
```

17.1.8 Event Log

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

Device Event Log

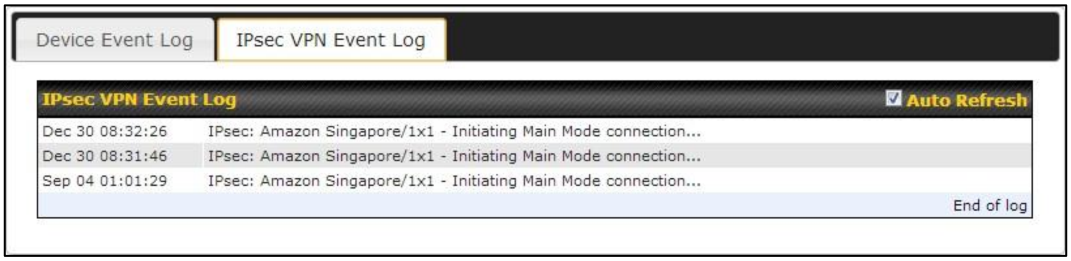


Device Event Log ☑ Auto Refresh

```
Apr 17 14:54:52   [redacted]
Apr 17 14:39:44   [redacted]
Apr 17 09:12:42   [redacted]
Apr 17 09:07:33   [redacted]
Apr 16 10:01:13   [redacted]
Apr 16 10:00:23   [redacted]
Apr 16 09:59:04   [redacted]
Apr 16 09:58:57   [redacted]
Apr 16 09:57:10   [redacted]
Apr 16 09:57:04   [redacted]
Apr 16 09:56:16   [redacted]
Apr 16 09:56:15   [redacted]
Apr 16 09:56:15   [redacted]
Apr 16 09:56:13   [redacted]
Apr 16 09:54:41   [redacted]
Apr 16 09:50:28   [redacted]
Apr 16 09:50:28   [redacted]
```

The log section displays a list of events that have 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 ☑ 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
```

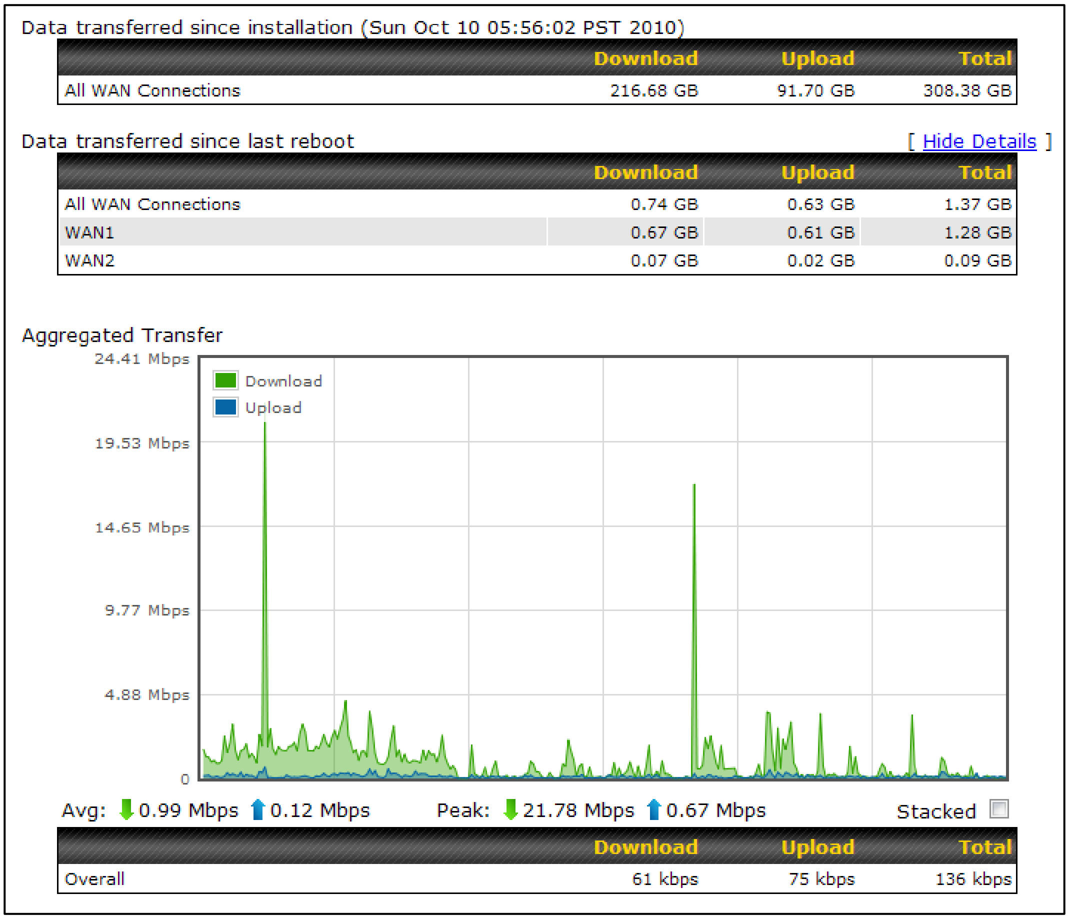
This section displays a list of events that have taken place within an IPsec VPN connection. Check the box next to **Auto Refresh** and the log will be refreshed automatically. For an AP event log, navigate to **AP>Info**.

17.2 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.

17.2.1 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.



Data transferred since installation (Sun Oct 10 05:56:02 PST 2010)

	Download	Upload	Total
All WAN Connections	216.68 GB	91.70 GB	308.38 GB

Data transferred since last reboot [Hide Details]

	Download	Upload	Total
All WAN Connections	0.74 GB	0.63 GB	1.37 GB
WAN1	0.67 GB	0.61 GB	1.28 GB
WAN2	0.07 GB	0.02 GB	0.09 GB

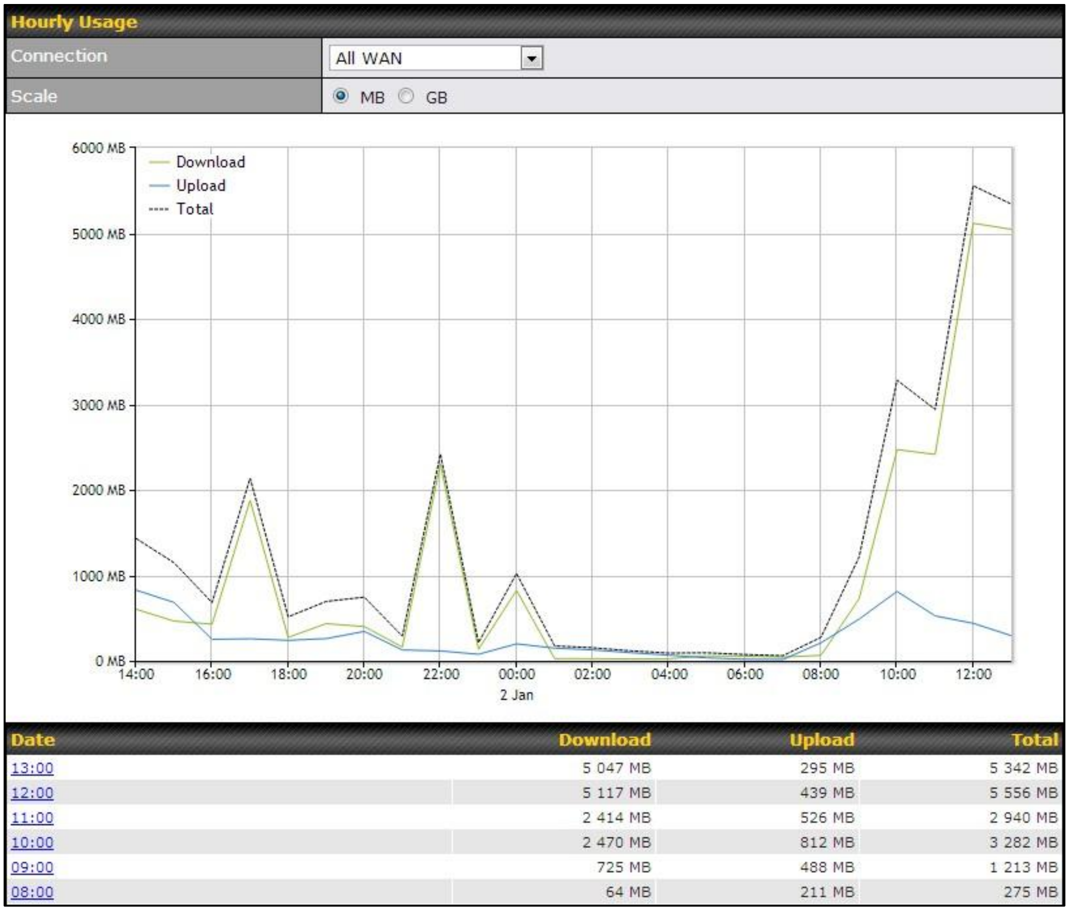
Aggregated Transfer

Avg: ⬇0.99 Mbps ⬆0.12 Mbps Peak: ⬇21.78 Mbps ⬆0.67 Mbps Stacked □

	Download	Upload	Total
Overall	61 kbps	75 kbps	136 kbps

17.2.2 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.



Hourly Usage

Connection	All WAN ▾
Scale	● MB ○ GB

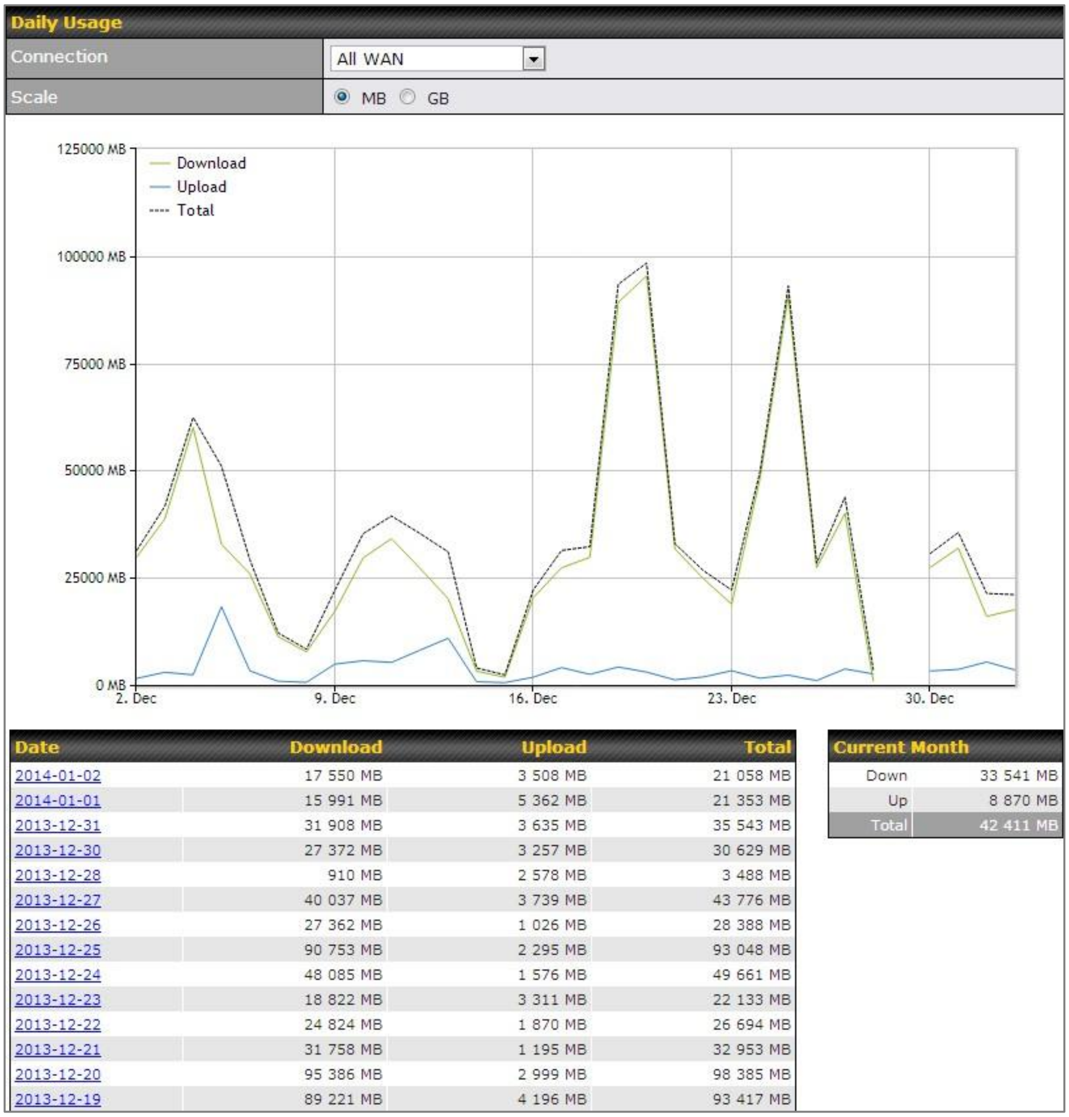
Date	Download	Upload	Total
13:00	5 047 MB	295 MB	5 342 MB
12:00	5 117 MB	439 MB	5 556 MB
11:00	2 414 MB	526 MB	2 940 MB
10:00	2 470 MB	812 MB	3 282 MB
09:00	725 MB	488 MB	1 213 MB
08:00	64 MB	211 MB	275 MB

17.2.3 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**).



Daily Usage

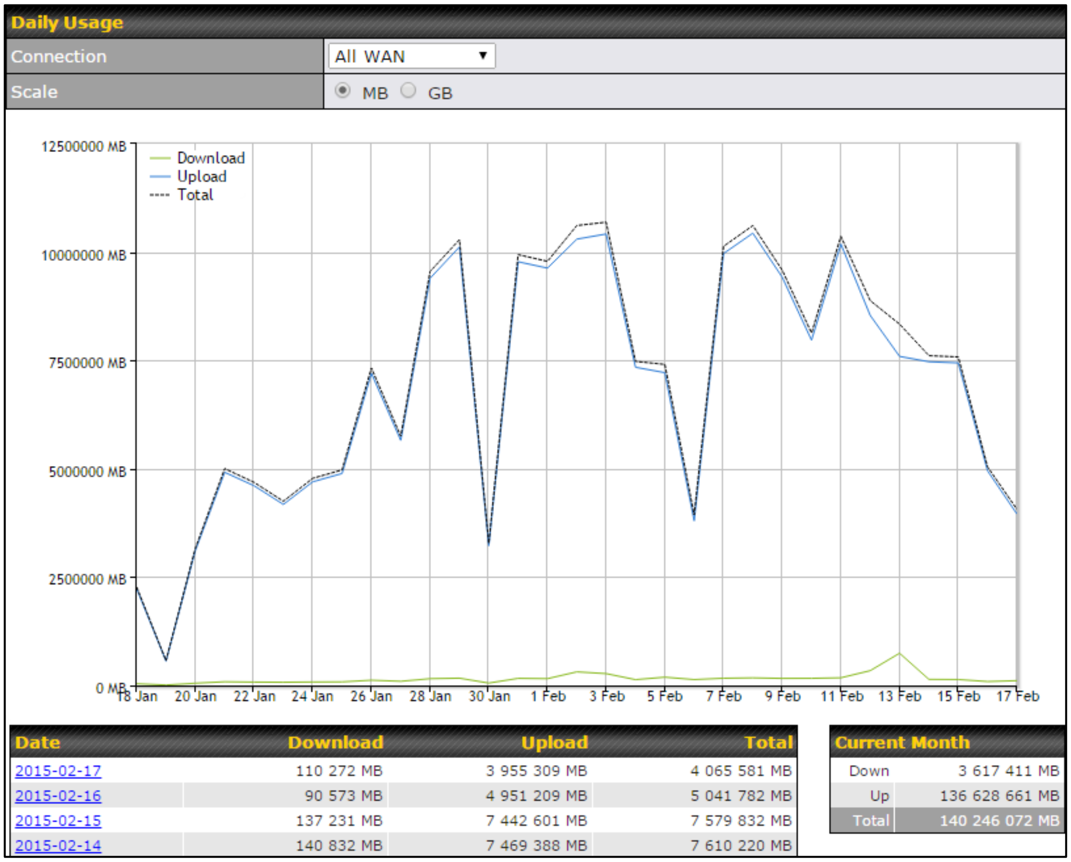
Connection: All WAN

Scale: ● MB ○ GB

Date	Download	Upload	Total
2014-01-02	17 550 MB	3 508 MB	21 058 MB
2014-01-01	15 991 MB	5 362 MB	21 353 MB
2013-12-31	31 908 MB	3 635 MB	35 543 MB
2013-12-30	27 372 MB	3 257 MB	30 629 MB
2013-12-28	910 MB	2 578 MB	3 488 MB
2013-12-27	40 037 MB	3 739 MB	43 776 MB
2013-12-26	27 362 MB	1 026 MB	28 388 MB
2013-12-25	90 753 MB	2 295 MB	93 048 MB
2013-12-24	48 085 MB	1 576 MB	49 661 MB
2013-12-23	18 822 MB	3 311 MB	22 133 MB
2013-12-22	24 824 MB	1 870 MB	26 694 MB
2013-12-21	31 758 MB	1 195 MB	32 953 MB
2013-12-20	95 386 MB	2 999 MB	98 385 MB
2013-12-19	89 221 MB	4 196 MB	93 417 MB

Current Month	
Down	33 541 MB
Up	8 870 MB
Total	42 411 MB

Status



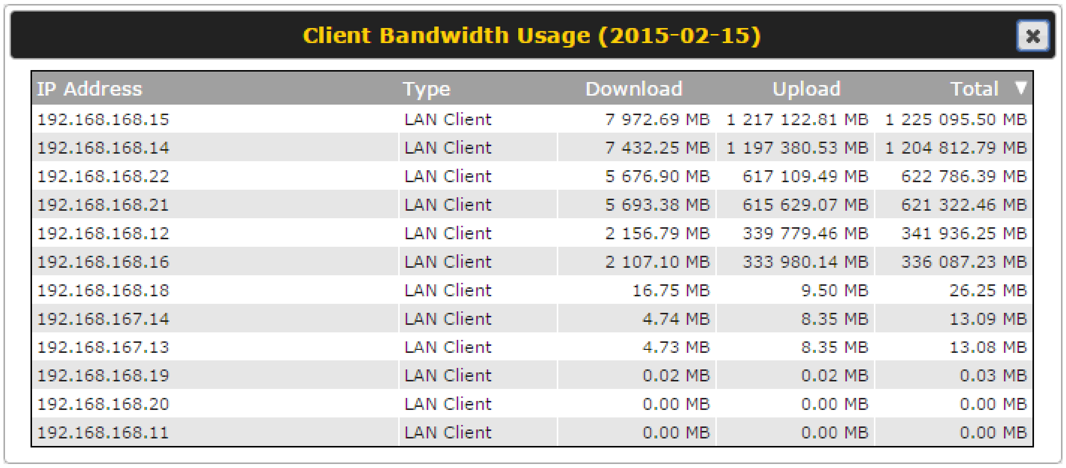
Daily Usage

Connection	All WAN ▾
Scale	● MB ○ GB

Date	Download	Upload	Total
2015-02-17	110 272 MB	3 955 309 MB	4 065 581 MB
2015-02-16	90 573 MB	4 951 209 MB	5 041 782 MB
2015-02-15	137 231 MB	7 442 601 MB	7 579 832 MB
2015-02-14	140 832 MB	7 469 388 MB	7 610 220 MB

Current Month	
Down	3 617 411 MB
Up	136 628 661 MB
Total	140 246 072 MB

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



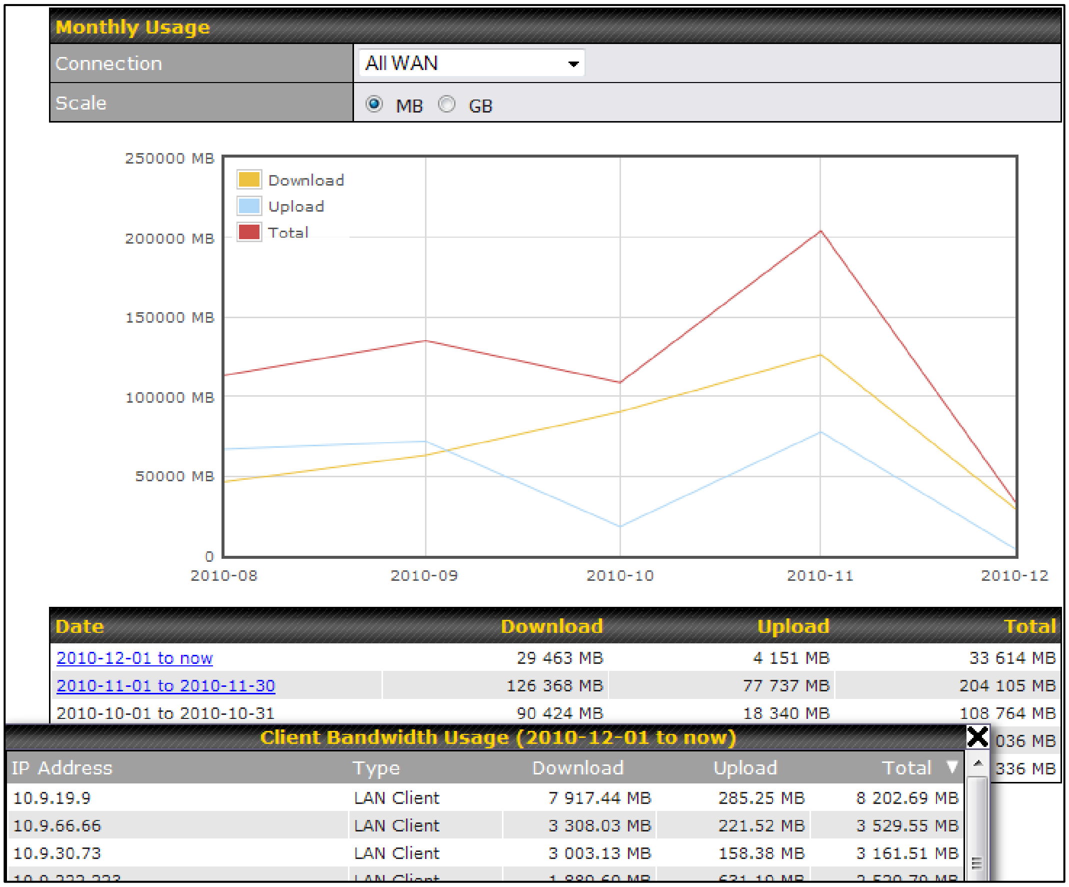
Client Bandwidth Usage (2015-02-15)

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

17.2.4 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**).



Monthly Usage

Connection	All WAN
Scale	● MB ○ GB

Date	Download	Upload	Total
2010-12-01 to now	29 463 MB	4 151 MB	33 614 MB
2010-11-01 to 2010-11-30	126 368 MB	77 737 MB	204 105 MB
2010-10-01 to 2010-10-31	90 424 MB	18 340 MB	108 764 MB
			036 MB
			336 MB

Client Bandwidth Usage (2010-12-01 to now)

IP Address	Type	Download	Upload	Total ▼
10.9.19.9	LAN Client	7 917.44 MB	285.25 MB	8 202.69 MB
10.9.66.66	LAN Client	3 308.03 MB	221.52 MB	3 529.55 MB
10.9.30.73	LAN Client	3 003.13 MB	158.38 MB	3 161.51 MB
10.9.222.223	LAN Client	1 889.60 MB	631.10 MB	2 520.70 MB

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 paperclip, press and keep the reset button pressed.

Note: There is a dual function to the reset button.

Hold for 5-10 seconds for admin password reset (green status light starts blinking)

Hold for more than 10 seconds for a factory reset (until all WAN/LAN port lights start blinking).

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**

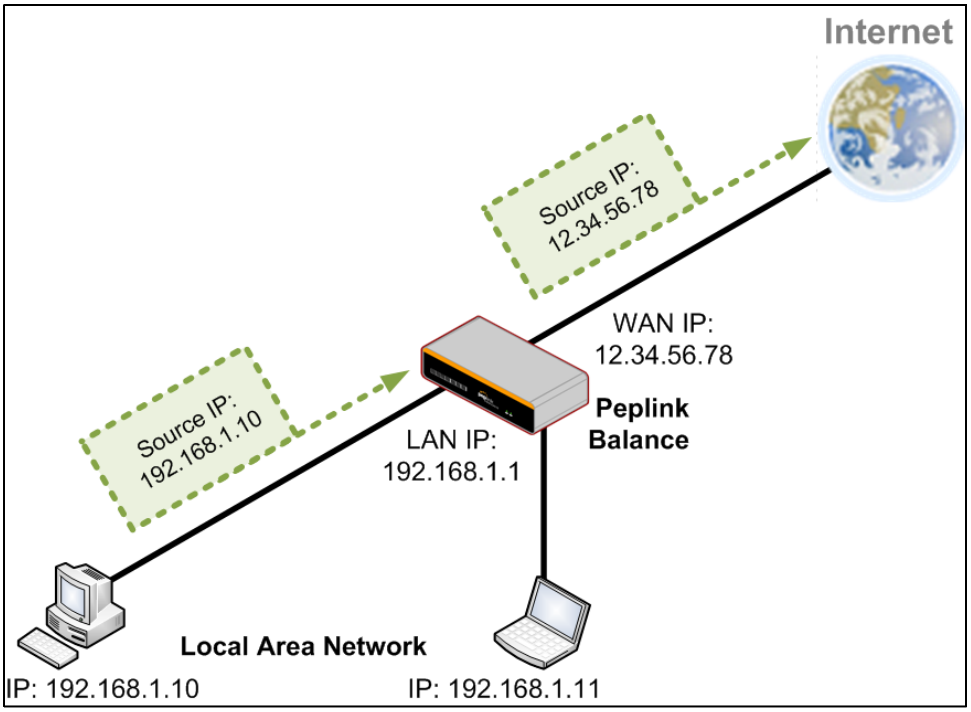
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

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.

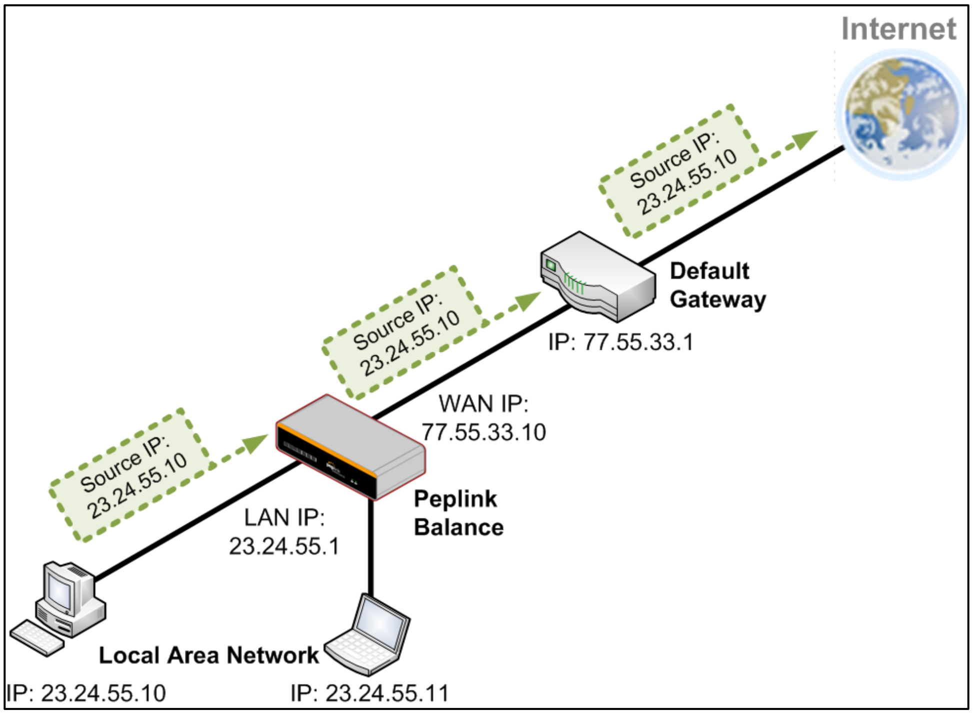
The following figure shows the packet flow in NAT mode:



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

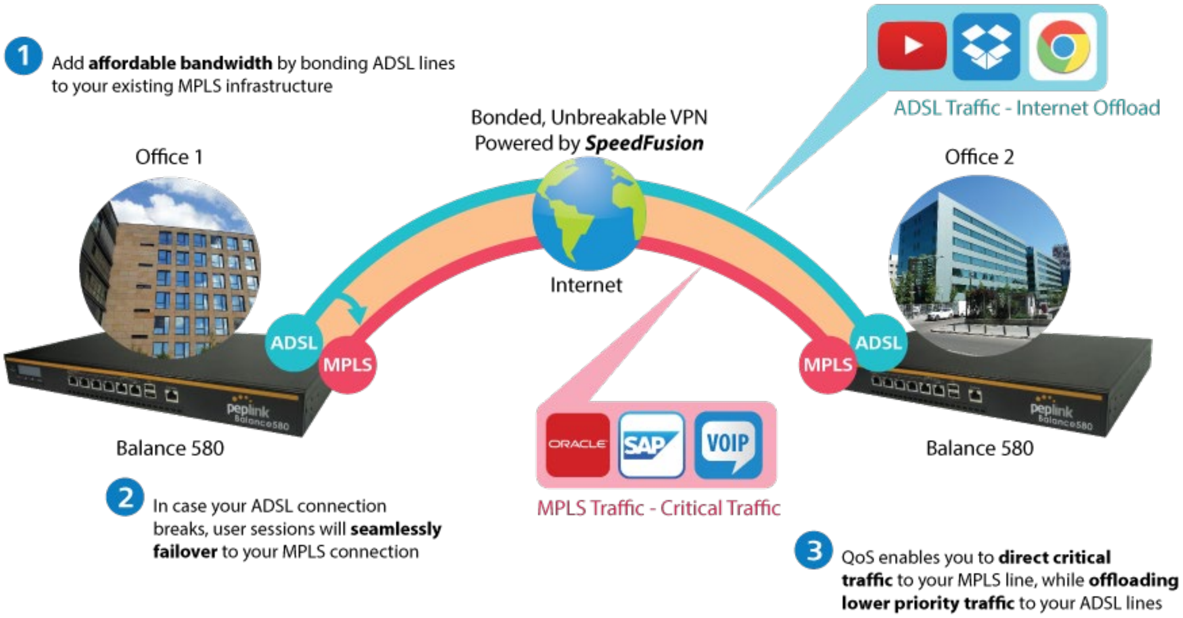
Special features of Balance 2500: have high availability capability and capable of connecting to optical fiber based LAN through SFP+ connector

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.

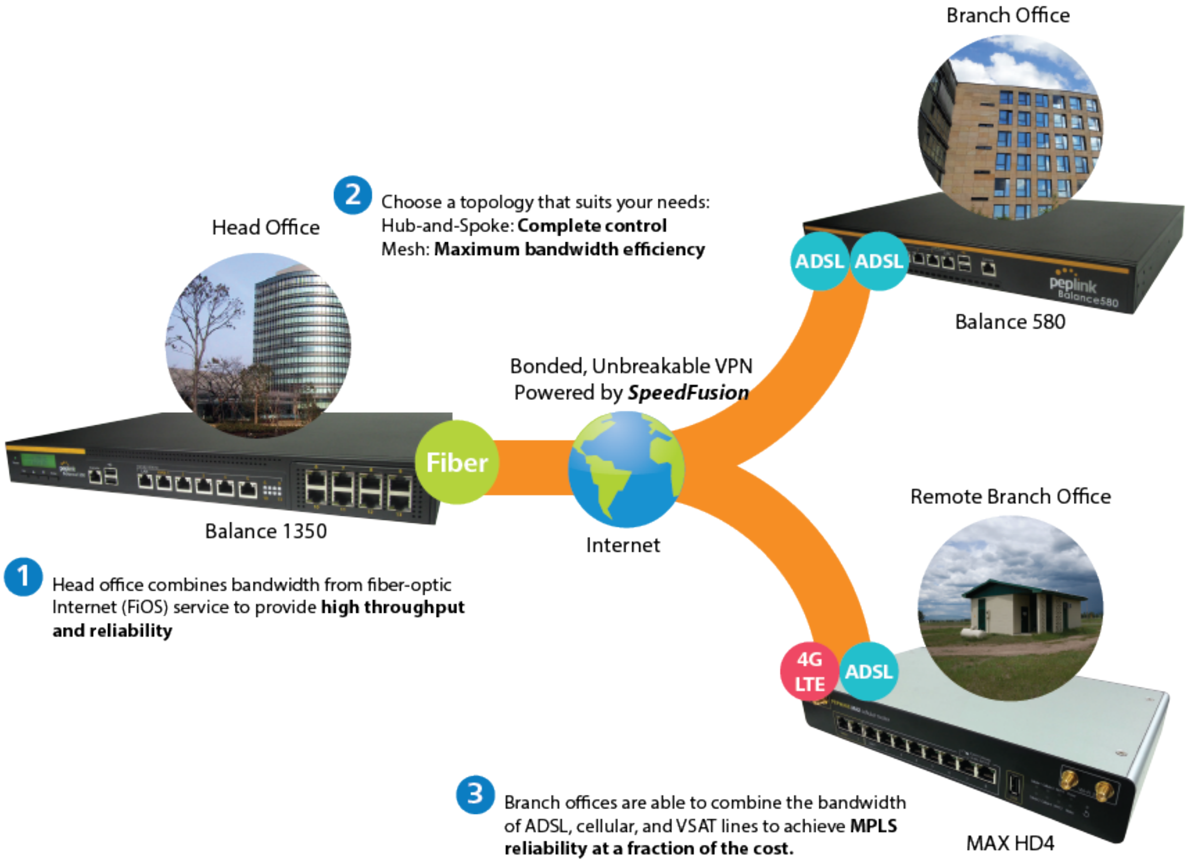
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement


1 Add **affordable bandwidth** by bonding ADSL lines to your existing MPLS infrastructure
Bonded, Unbreakable VPN
Powered by ***SpeedFusion***
ADSL Traffic - Internet Offload
Office 1
Office 2
Internet
ADSL
MPLS
ADSL
MPLS
ORACLE
SAP
VOIP
Balance 580
Balance 580
MPLS Traffic - Critical Traffic
2 In case your ADSL connection breaks, user sessions will **seamlessly failover** to your MPLS connection
3 QoS enables you to **direct critical traffic** to your MPLS line, while **offloading lower priority traffic** to your ADSL lines

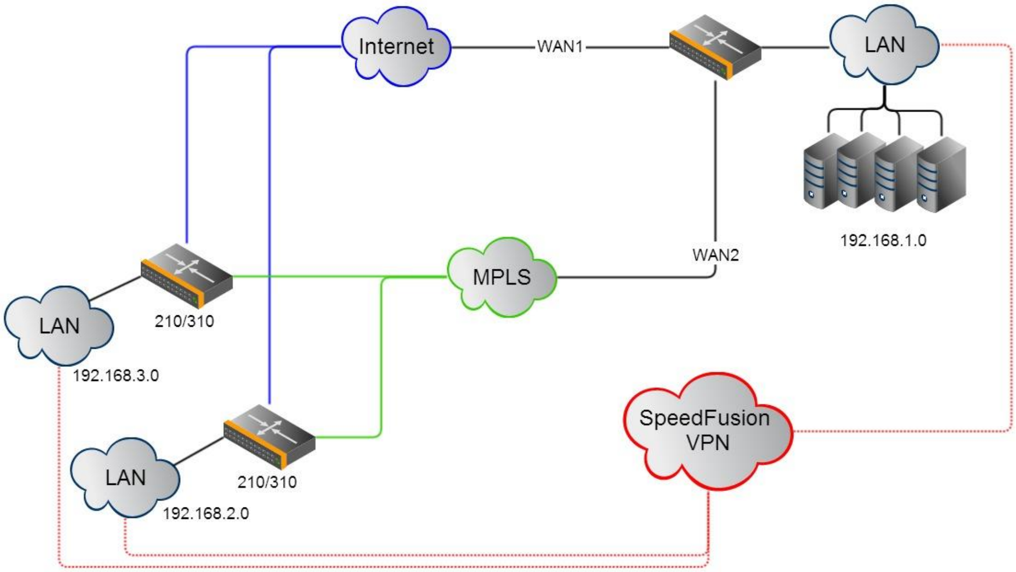
Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your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

Option 2: MPLS Alternative


Branch Office
Head Office
2 Choose a topology that suits your needs:
Hub-and-Spoke: **Complete control**
Mesh: **Maximum bandwidth efficiency**
ADSL
ADSL
Balance 580
Bonded, Unbreakable VPN
Powered by ***SpeedFusion***
Fiber
Balance 1350
Internet
Remote Branch Office
1 Head office combines bandwidth from fiber-optic Internet (FiOS) service to provide **high throughput and reliability**
4G LTE
ADSL
3 Branch offices are able to combine the bandwidth of ADSL, cellular, and VSAT lines to achieve **MPLS reliability at a fraction of the cost.**
MAX HD4

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 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

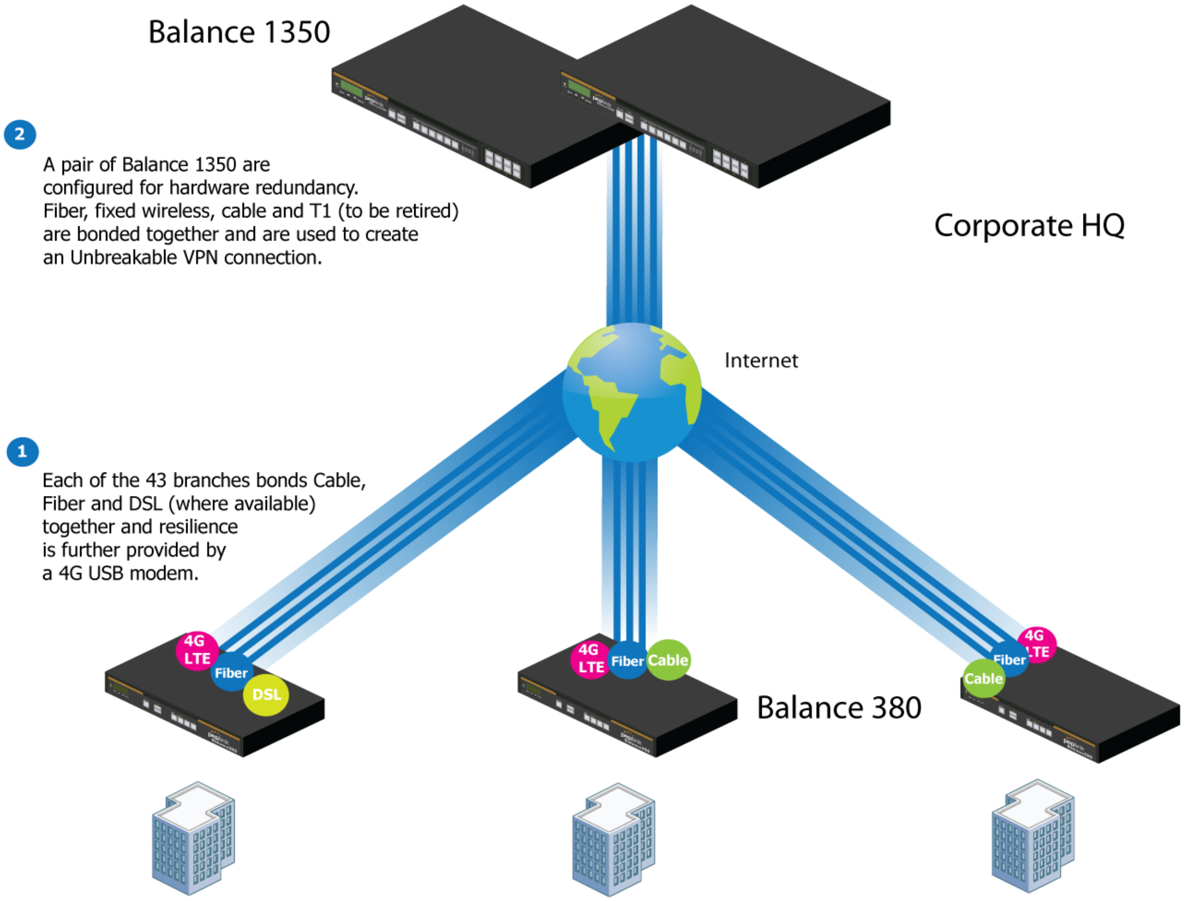
- Extreme savings of $100,000 per year
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

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

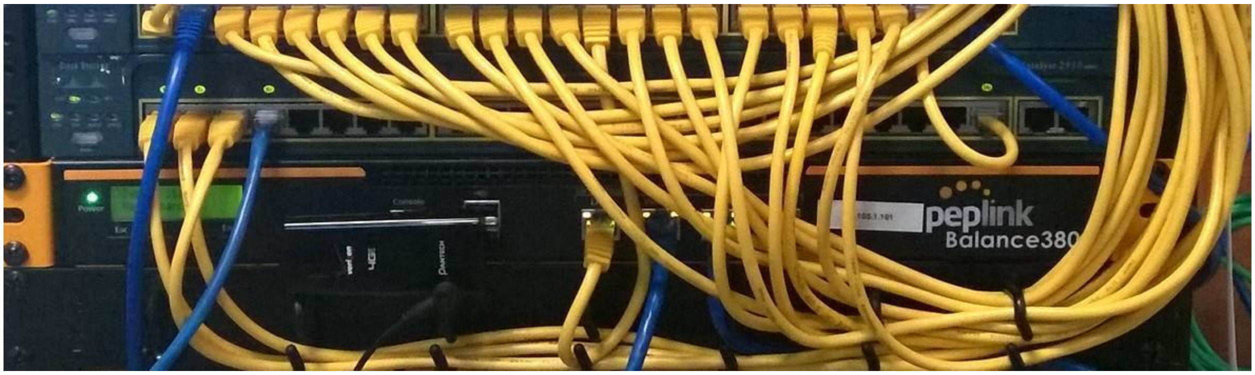
In evaluating an upgrade to its network infrastructure, it was only natural that Harrington settled on the best in the industry — Peplink. Peplink partner Frontier Computer Corporation was chosen to help design and deploy the solution. Since Peplink gear is so easy to configure and install, Harrington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


Balance 1350
2
A pair of Balance 1350 are configured for hardware redundancy. Fiber, fixed wireless, cable and T1 (to be retired) are bonded together and are used to create an Unbreakable VPN connection.
Corporate HQ
Internet
1
Each of the 43 branches bonds Cable, Fiber and DSL (where available) together and resilience is further provided by a 4G USB modem.
4G LTE
Fiber
DSL
4G LTE
Fiber
Cable
Balance 380
4G LTE
Fiber
Cable

43x branches

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

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



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

PLUSS

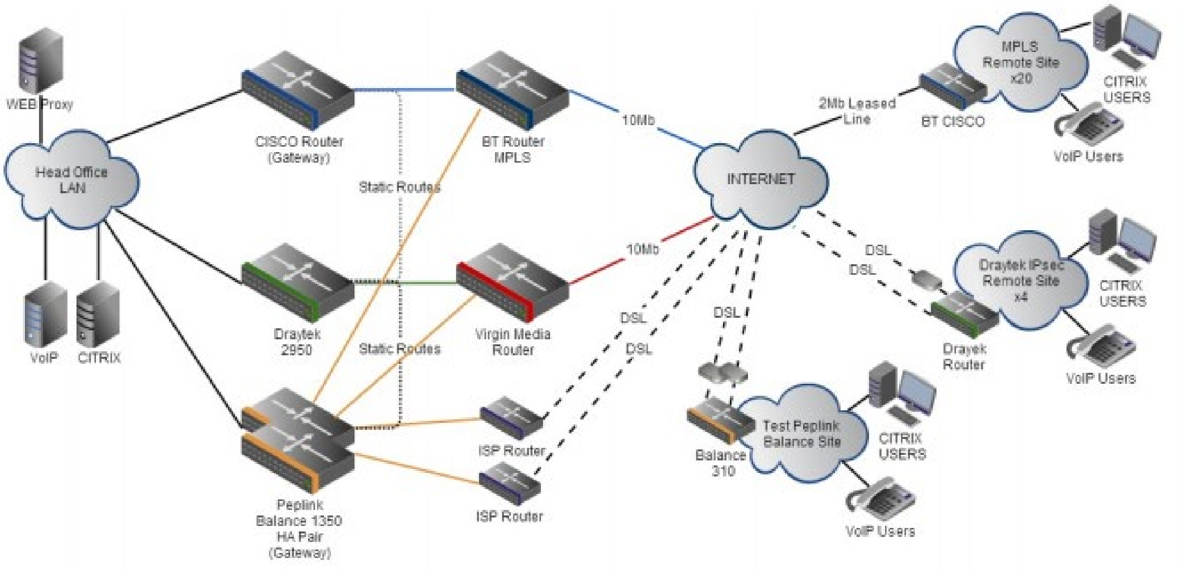
Peplink + Citrix + VoIP Adds Up to Fast, Cost-Effective WAN for Pluss

Adding to Life
pluss
400
USERS
VoIP 290
EndPoints
30+
SITES
"It saves us money, is easy to manage and grows with us effortlessly."
Steve Taylor - Pluss

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

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

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



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

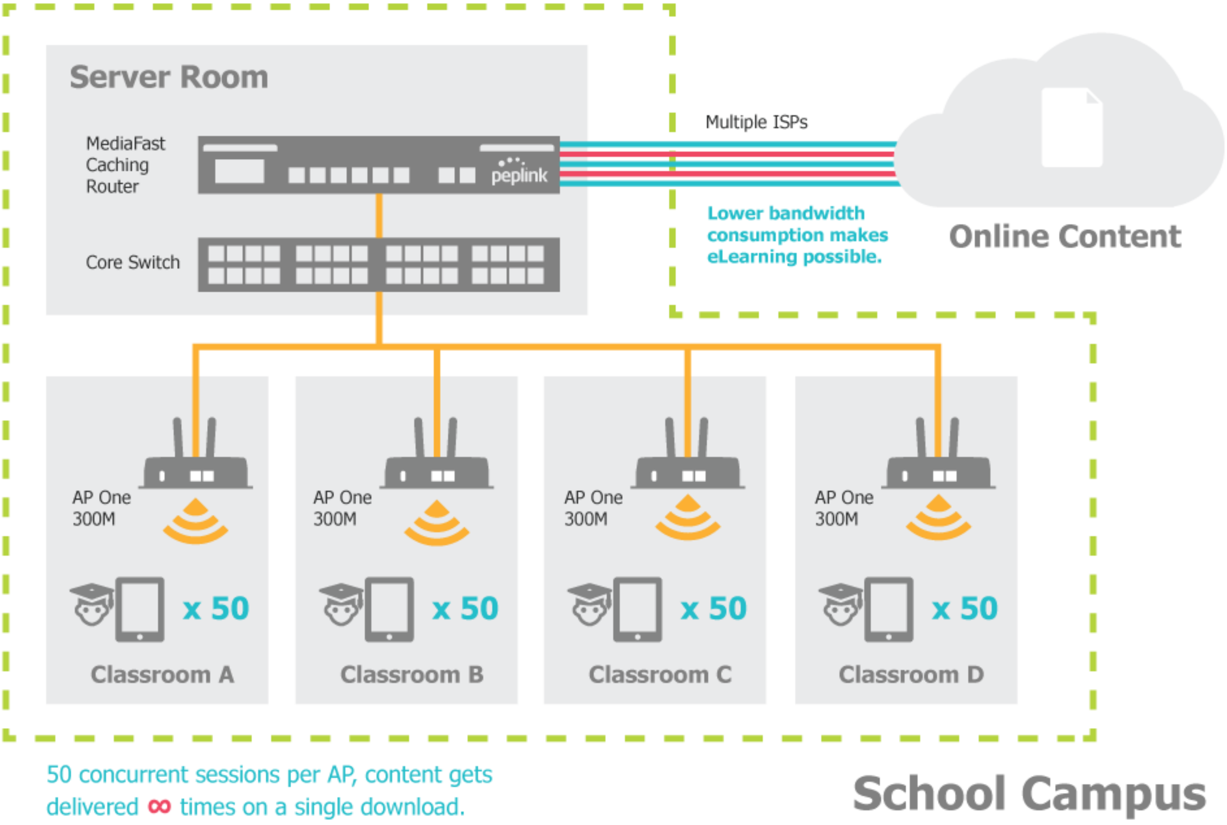
Solution

- 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


Server Room
MediaFast Caching Router
peplink
Core Switch
Multiple ISPs
Lower bandwidth consumption makes eLearning possible.
Online Content
AP One 300M
x 50
Classroom A
AP One 300M
x 50
Classroom B
AP One 300M
x 50
Classroom C
AP One 300M
x 50
Classroom D
50 concurrent sessions per AP, content gets delivered ∞ times on a single download.
School Campus

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 30M/2M and 50M/50M, 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

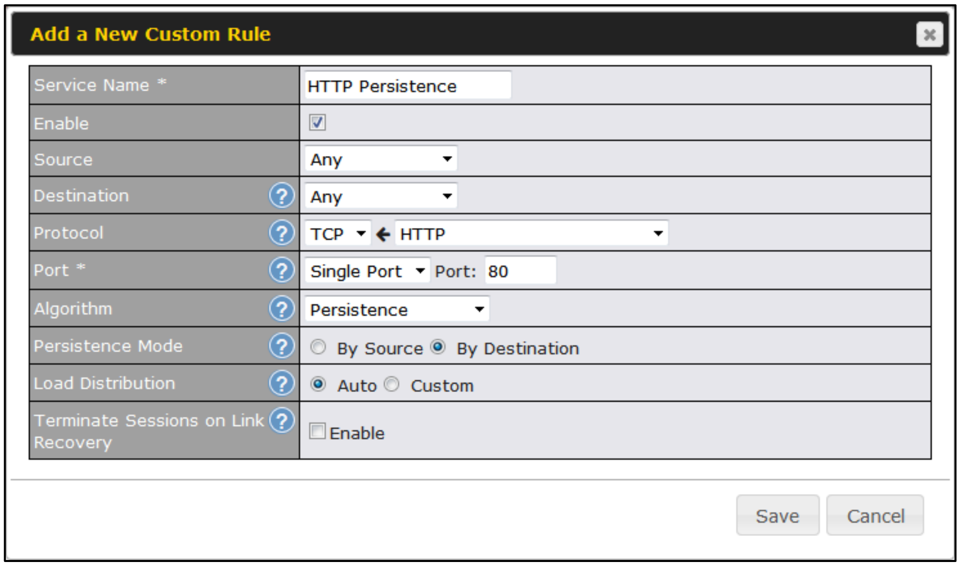
Make use of the persistence functionality of the Peplink Balance. With persistence configured and the **By Destination** option selected, the Peplink Balance will use a consistent WAN connection for source-destination pairs of IP addresses, preventing sessions from being dropped.

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	☑
Source	Any
Destination	Any
Protocol	TCP ← HTTP
Port *	Single Port Port: 80
Algorithm	Persistence
Persistence Mode	○ By Source ● By Destination
Load Distribution	● Auto ○ Custom
Terminate Sessions on Link Recovery	□ Enable

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

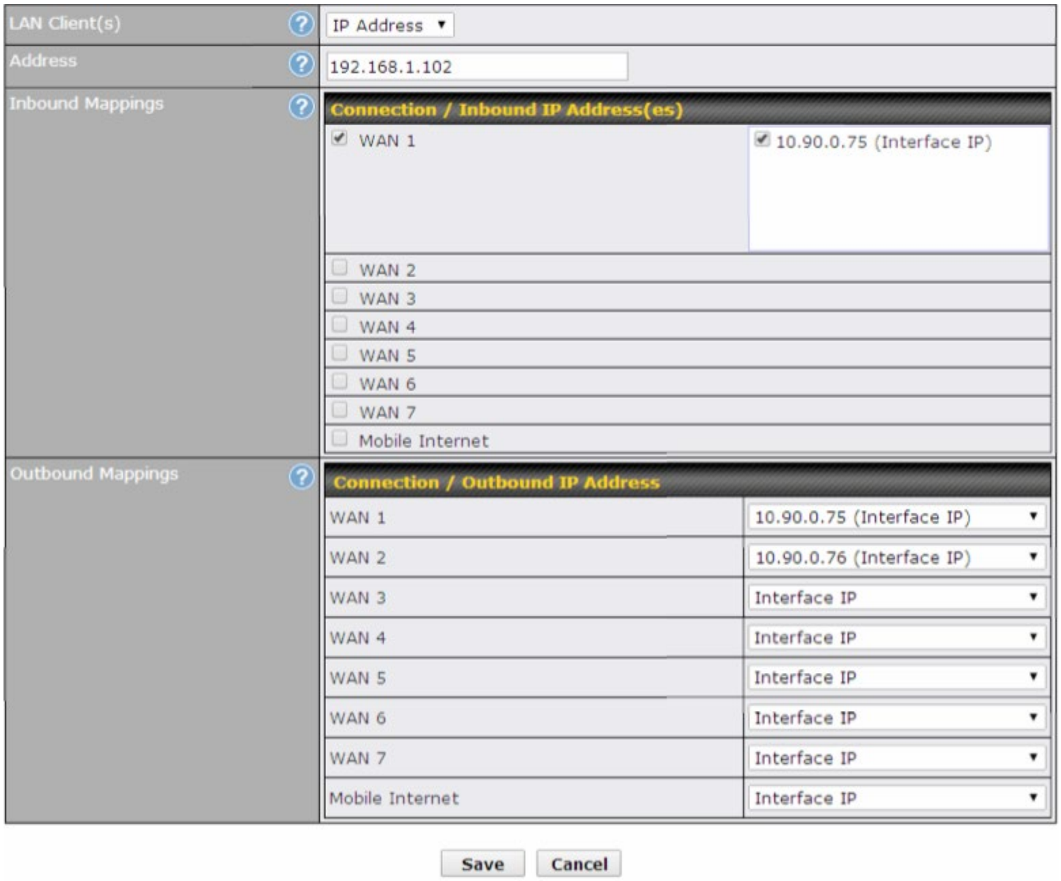
Scenario

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

Connection / Inbound IP Address(es)	
☑ WAN 1	☑ 10.90.0.75 (Interface IP)
☐ WAN 2	
☐ WAN 3	
☐ WAN 4	
☐ WAN 5	
☐ WAN 6	
☐ WAN 7	
☐ Mobile Internet	

Outbound Mappings

Connection / Outbound IP Address	
WAN 1	10.90.0.75 (Interface IP) ▾
WAN 2	10.90.0.76 (Interface IP) ▾
WAN 3	Interface IP ▾
WAN 4	Interface IP ▾
WAN 5	Interface IP ▾
WAN 6	Interface IP ▾
WAN 7	Interface IP ▾
Mobile Internet	Interface IP ▾

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

Inbound Access Restriction

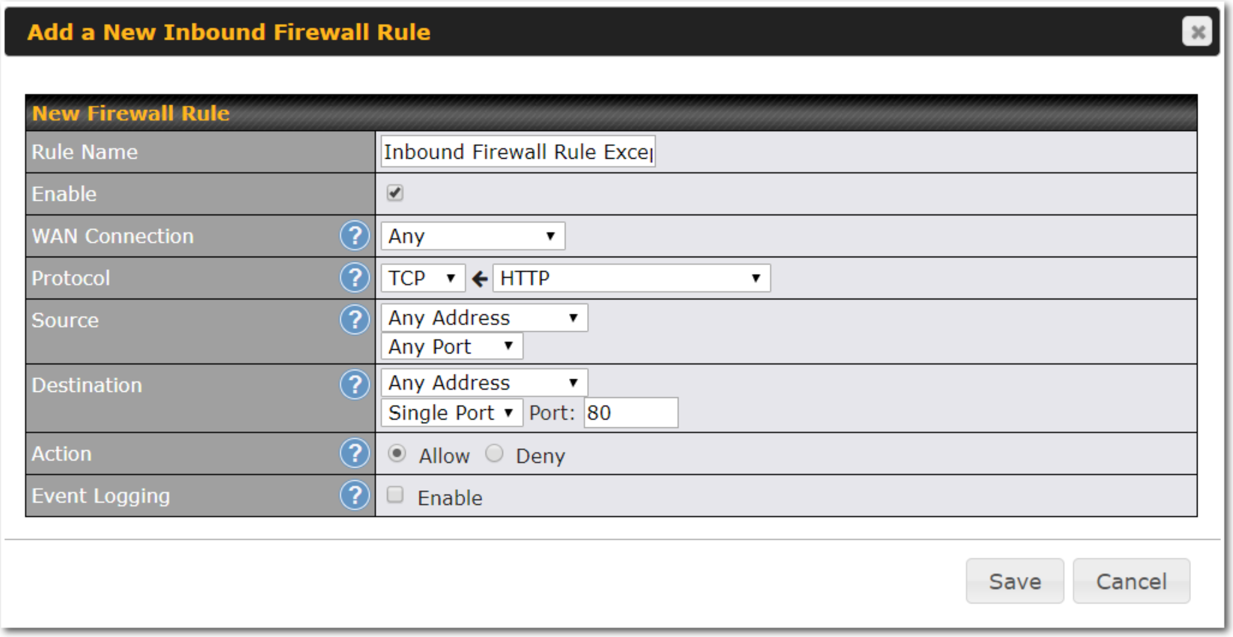
Scenario

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 **Network>Firewall>Access Rules**. Then click the **Add Rule** button in the **Inbound Firewall Rules** table and change the settings according to the following screenshot:



Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	Inbound Firewall Rule Excep
Enable	☑
WAN Connection	Any
Protocol	TCP ← HTTP
Source	Any Address Any Port
Destination	Any Address Single Port Port: 80
Action	● Allow ○ Deny
Event Logging	□ 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.

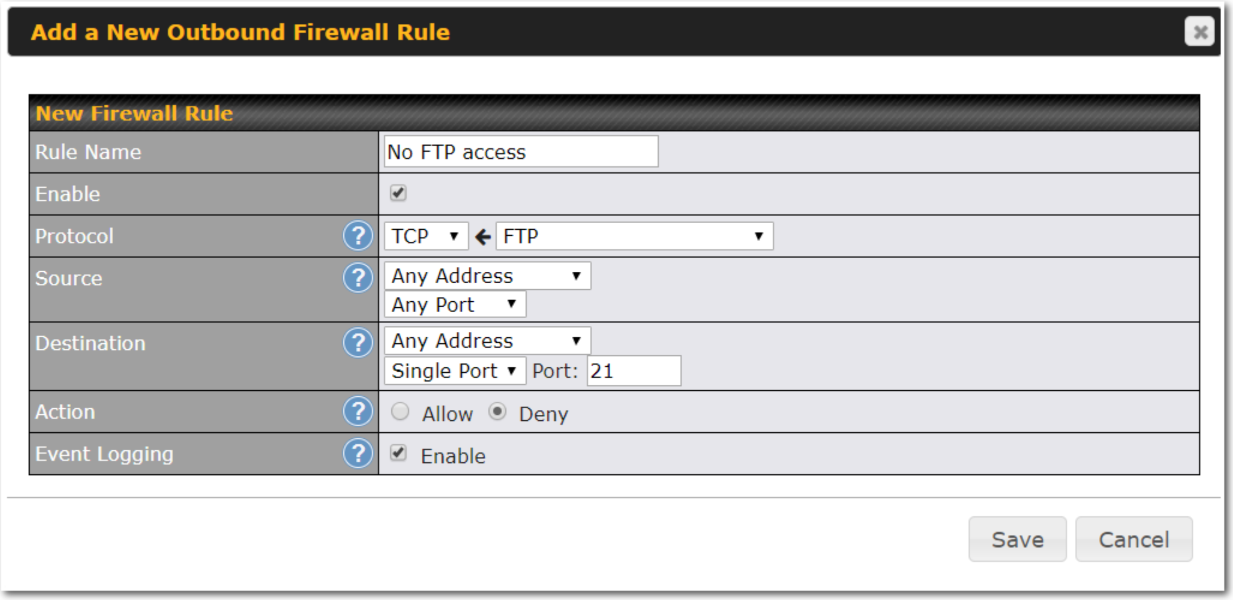
Outbound Access Restriction

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 the Internet and private network for outbound access, navigate to **Network>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	☑
Protocol	TCP ▾ ← FTP ▾
Source	Any Address ▾ Any Port ▾
Destination	Any Address ▾ Single Port ▾ Port: 21
Action	○ Allow ● Deny
Event Logging	☑ 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^{TM} 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:

https://forum.peplink.com/t/speed-test-tool-for-combined-download-speed-in-multi-wan-environment/8457

Problem 2

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

Solution

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

Problem 3

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

Solution

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

Problem 4

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

Solution

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

Problem 5

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

Solution

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

Problem 6

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

Solution

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

Additional troubleshooting resources:

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

Appendix E.

CE Declaration of Conformity (for Balance 30 Pro series model)

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer: PISMO LABS TECHNOLOGY LIMITED

Description of the appliance: PEPWAVE / PEPLINK Wireless Product

Model name of the appliance:

- Balance 20X
- B20X
- Surf SOHO
- Surf SOHO LTE
- Surf SOHO LTEA
- Balance 20X LTE
- Balance 20X LTEA
- PismoAC8E
- BPL-021X-LTE-E-T
- BPL-021X-LTEA-W-T
- EXM-MINI-1LTEA-W
- EXM-MINI-1LTEA-P
- PismoAC8P
- PismoAC8

Trade name of the appliance: PEPWAVE / PEPLINK

The construction of the appliance is in accordance with the following standards:

- EN 300 328 V2.1.1
- EN 301 893 V2.1.1
- EN 303 413 V1.1.1
- EN 301 908-1 V11.1.1
- Draft EN 301 489-1 V2.2.1
- Draft EN 301 489-17 V3.2.0
- Draft EN 301 489-19 V2.1.1
- Draft EN 301 489-52 V1.1.0
- EN 55032: 2015 + AC:2016
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013
- EN 55035: 2017
- EN 62311: 2008
- EN 62368-1:2014/A11:2017

PISMO LABS TECHNOLOGY LIMITED

Anthony Chong
Director of Hardware Engineering
Pismo Labs Technology Limited
Hong Kong, September 24, 2019

Caution:
The 5150 to 5350 MHz frequency range is restricted to indoor use only,

⚠	AT	BE	BG	HR	CY	CZ	DK
	EE	FI	FR	DE	EL	HU	IE
	IT	LV	LT	LU	MT	NL	PL
	PT	RO	SK	SI	ES	SE	UK

Frequency band and maximum power table:

Frequency Band	**Maximum RF Power transmitted (dBm)**
WCDMA Band I	23
WCDMA Band II	23
WCDMA Band VIII	23
LTE Band 1	23
LTE Band 3	23
LTE Band 7	22
LTE Band 8	23
LTE Band 20	23

Frequency Band	**Maximum EIRP**
WLAN 2412-2472 MHz	19.84
WLAN 5180-5240 MHz	22.89

CE Radiation Exposure Statement

This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Appendix F.

Federal Communication Commission Interference Statement

(for Balance 30 Pro series model)

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.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.
Note: The country code selection is for non-US models only and is not available to all US models. Per FCC regulation, all WiFi products marketed in US must fixed to US operation channels only.

Appendix G.

ISED Canada Warning Statement (for Balance 30 Pro series model)

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:(1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :(1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

La bande 5150-5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Caution

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and

(iii) where applicable, antenna type(s), antenna model(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.

Mise en garde

(i) Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement à une utilisation en intérieur afin de réduire les risques d'interférence préjudiciables aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) pour les dispositifs avec antenne(s) détachable(s), le gain d'antenne maximal autorisé pour les dispositifs dans la bande 5725-5850 MHz doit être tel que l'équipement soit toujours conforme à la norme e.i.r.p. limites, le cas échéant; et

(iii) le cas échéant, type(s) d'antenne, modèle(s) d'antenne et angle(s) d'inclinaison dans le cas le plus défavorable nécessaire pour rester conforme à l'e.i.r.p. L'exigence de masque d'altitude énoncée à la section 6.2.2.3 doit être clairement indiquée.

IC Radiation Exposure Statement

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

Déclaration d'exposition aux radiations:

Cet équipement respecte les limites d’exposition aux rayonnements IC définies pour un environnement non contrôlé. Cet équipement doit être installé et mis en marche à une distance minimale de 20 cm qui sépare l’élément rayonnant de votre corps.

This radio transmitter IC: 20682-P1AC8E has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio IC: 20682-P1AC8E a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

WLAN Antenna type: Replacement Antenna
WLAN Antenna gain: 2412~2462 GHz / 2.44 dBi
5150~5250 GHz / 4.10 dBi
5725~5850 GHz / 4.73 dBi