



Peplink Balance and MediaFast

User Manual

Peplink Products:

One/One Core/Two/20/20X/30 LTE/30 Pro/210/310/310X/310 5G/310 Fiber 5G/
305/380/380X/580/580X/710/1350/2500/EPX/SDX/SDX Pro/
MediaFast 200/500/750

Peplink Balance Firmware 8.1.3
August 2021

Table of Contents

Introduction and Scope	8
Glossary	9
Product Comparison Charts	11
Balance Routers (for Small Office / Branch)	11
Balance Routers (for for Enterprise / Headquarters)	12
MediaFast Routers	13
Product Features	14
Advanced Feature Summary	18
Drop-in Mode and LAN Bypass: Transparent Deployment	18
QoS: Clearer VoIP	18
Per-User Bandwidth Control	19
High Availability via VRRP	19
USB Modem and Android Tethering	20
Built-In Remote User VPN Support	20
LACP NIC Bonding	21
KVM Virtualization	21
DPI Engine	22
NetFlow	22
Wi-Fi Air Monitoring	22
SP Default Configuration	22
Package Contents	23
Peplink Balance One/Two	23
Peplink Balance 20/30/30 LTE/30 Pro/50	23
Peplink Balance 20X	23
Peplink Balance 210/310	23
Peplink Balance 310X	23
Peplink Balance 310 5G	24
Peplink Balance 310 Fiber 5G	24
Peplink Balance 305/380/580/710/1350/2500	24
Peplink Balance 380X/580X	24
Peplink MediaFast 200	24
Peplink MediaFast 500	25
Peplink EPX	25

Peplink SDX	25
Peplink SDX Pro	25
Peplink Balance Overview	26
Peplink Balance One	26
Peplink Balance Two	28
Peplink Balance 20	30
Peplink Balance 20X	31
Peplink Balance 30 LTE	35
Peplink Balance 30 Pro	37
Peplink Balance 50	39
Peplink Balance 210	40
Peplink Balance 305	42
Peplink Balance 310	43
Peplink Balance 310X	45
Peplink Balance 310 5G	47
Peplink Balance 310 Fiber 5G	49
Peplink Balance 380	51
Peplink Balance 380X	52
Peplink Balance 580	55
Peplink Balance 580X	56
Peplink Balance 710	59
Peplink Balance 1350	60
Peplink Balance 2500	62
Peplink MediaFast Overview	64
Peplink MediaFast 200	64
Peplink MediaFast 500	65
Peplink MediaFast 750	67
Peplink Flex-Module Supported Models	69
Peplink EPX	69
Peplink SDX	72
Peplink SDX Pro	75
Flex Module Expansion Modules	77
LCD Display Menu	80
Installation	81

Preparation	81
Constructing the Network	81
Basic Configuration	82
Connecting to the Web Admin Interface	82
Configuration with the Setup Wizard	83
SpeedFusion Cloud	88
Activate SpeedFusion Cloud Service	88
Enable SpeedFusion Cloud	90
Connect Clients to Cloud	98
Link Wi-Fi to Cloud	99
Optimize Cloud Application	101
Network Tab	102
WAN	102
Health Check Settings	115
Bandwidth Allowance Monitor Settings	118
Additional Public IP Settings	118
Dynamic DNS Settings	119
LAN	120
Network Settings	121
Network Settings (Common Settings)	125
Port Settings	130
VPN	130
SpeedFusion	131
IPsec VPN	137
GRE Tunnel	141
Outbound Policy	143
Inbound Access	154
Servers	154
Services	156
DNS Settings	158
NAT Mappings	176
MediaFast	178
Setting Up MediaFast Content Caching	178
Viewing MediaFast Statistics	180
Prefetch Schedule	181

ContentHub	183
Configure a website to be published from the ContentHub	183
Configure an application to be published from the ContentHub	185
MDM Settings	188
Docker	188
KVM	189
Captive Portal	190
QoS	192
User Groups	193
Bandwidth Control	194
Application	195
Prioritization for Custom Application	196
DSL/Cable Optimization	196
Firewall	196
Access Rules	197
Intrusion Detection and DoS Prevention	202
Content Blocking	203
Application Blocking	203
Web Blocking	204
Customized Domains	204
Exempted User Groups	204
Exempted Subnets	204
URL Logging	204
Routing Protocols	205
OSPF & RIPv2	205
BGP	207
Remote User Access	212
L2TP with IPsec	212
OpenVPN	212
PPTP	213
Authentication Methods	213
Misc. Settings	215
High Availability	215
Certificate Manager	219
Service Forwarding	220
SMTP Forwarding	221

Web Proxy Forwarding	222
DNS Forwarding	222
Custom Service Forwarding	222
Service Passthrough	223
NTP Server	224
Grouped Networks	224
Remote SIM Management	226
SIM Toolkit	228
AP Tab	230
AP	230
AP Controller	230
Wireless SSID	231
Wireless Mesh	235
AP > Profiles	236
AP Controller Status	240
Info	240
Access Points (Usage)	241
Wireless SSID	244
Wireless Client	245
Mesh / WDS	247
Nearby Device	248
Event Log	248
Toolbox	249
System Tab	250
System	250
Admin Security	250
Firmware	254
Time	256
Schedule	257
Email Notification	258
Event Log	261
SNMP	262
SMS Control	264
InControl	265
Configuration	266
Feature Add-ons	267

Reboot	267
Tools	268
Ping	268
Traceroute	269
Wake-on-LAN	269
WAN Analysis	270
CLI (Command Line) Support	274
Status Tab	275
Status	275
Device	275
Active Sessions	277
Client List	279
WINS Clients	280
OSPF & RIPv2	280
MediaFast	281
PepVPN / SpeedFusion Status	282
Event Log	287
Device Event Log	287
IPsec Event Log	288
WAN Quality	288
Usage Reports	289
Real-Time	289
Hourly	290
Daily	290
Monthly	293
Appendix	294
Restoration of Factory Defaults	294
Routing under DHCP, Static IP, and PPPoE	294
FusionSIM Manual	297
Case Studies	309
Harrington Industrial Plastics	313
PLUSS	316
Troubleshooting	325

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 20X
- Peplink Balance 30 LTE/Pro
- Peplink Balance 210
- Peplink Balance 310
- Peplink Balance 310X
- Peplink Balance 310 5G
- Peplink Balance 310 Fiber 5G
- Peplink Balance 380
- Peplink Balance 380X
- Peplink Balance 580
- Peplink Balance 580X
- Peplink Balance 710
- Peplink Balance 1350
- Peplink Balance 2500
- Peplink MediaFast 200/500/750
- Peplink EPX
- Peplink SDX
- Peplink SDX Pro

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 (for Small Office / Branch)

	20	20X	30 LTE	30 PRO	ONE	TWO	210	310X
Product Code	BPL-021	BPL-021X-LTE	BPL-031-LTE	BPL-031-LT EA	BPL-ONE	BPL-TWO	BPL-210	BPL-310X
Capacity								
Ethernet WAN Ports	2 (GE) +	1 (GE)	2 (GE)	2 (GE)	2/5 (GE) #	2 (GE)	2 (GE) +	2 (GE)
LAN Ports	4 (GE)	4 (GE)	4 (GE)	4 (GE)	8/5 (GE) #	4 (GE)	7 (GE)	9 (GE)
Simultaneous Dual-Band 802.11ac/a/b/g/n Wi-Fi AP	No	Yes	No	Yes	Yes	No	No	No
Embedded 4G LTE	No	Yes	Yes	Yes	No	No	No	Yes
SIM Card Size	No	Mini-SIM (2FF)	Mini-SIM (2FF)	Mini-SIM (2FF)	No	No	No	Mini-SIM (2FF)
USB WAN Modem Port	1	1	1	1	1	1	1	2
Recommended Users	1-60	1-60	1-60	1-60	1-60	25-150	25-150	50-500
Stateful Firewall Throughput	150Mbps	900Mbps	200Mbps	400Mbps	600Mbps/ 400Mbps #	1Gbps	350Mbps	2.5Gbps

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

2.2 Balance Routers (for for Enterprise / Headquarters)

	305	310X	380	380X	580	580X	710	1350	2500
Product Code	BPL-305	BPL-310X	BPL-380	BPL-380X	BPL-580	BPL-580X	BPL-710	BPL-135	BPL-2500 *
Capacity									
Ethernet WAN Ports	3 (GE)	2 (GE)	3 (GE)	3 (GE)	5 (GE)	5 (GE)	<u>7 (GE)</u>	13 (GE)	12 (GE)/4 (GE) & 2 (10G SFP+) *
LAN Ports	3 (GE)	9 (GE)	3 (GE)	3 (GE)	3 (GE)	3 (GE)	3 (GE)	3 (GE)	8 (GE)/2 (10G SFP+) *
Simultaneous Dual-Band 802.11ac/a/b/g/n Wi-Fi AP	No	No	No	No	No	No	No	No	No
Embedded 4G LTE	No	Yes	No	No	No	No	No	No	No
SIM Card Size	No	Yes	No	No	No	No	No	No	No
USB WAN Modem Port	1	2	1	1	1	1	1	1	1
Recommended Users	50-500	50-500	50-500	50-500	300-1000	300-1000	500-2000	1000-5000	5000-20000+
Stateful Firewall Throughput	1Gbps	2.5Gbps	1Gbps	3Gbps	1.5Gbps	4Gbps1	2.5Gbps	5Gbps	8Gbps

A full product comparison for Balance routers is available at:

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

2.3 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; 802.3at 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 802.3at (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
- USB Ethernet Adapter support

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 SpeedFusion™
- 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
- SpeedFusion™ 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



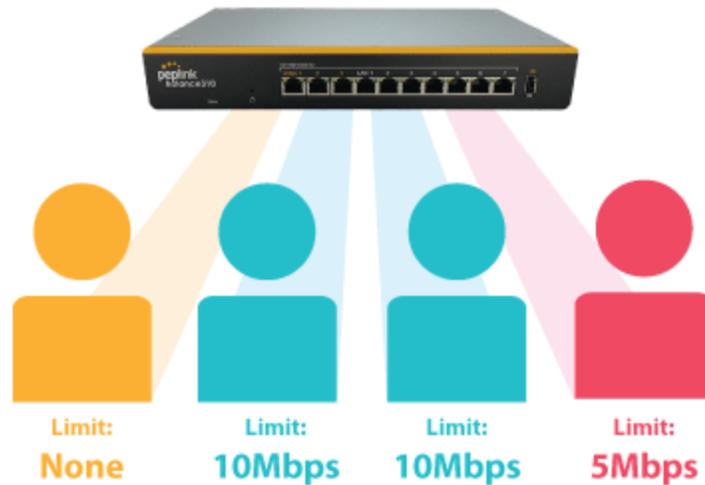
As your organization grows, it may require more bandwidth, but modifying your network can be tedious. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. For any reason your Peplink router loses power, the **LAN Bypass** will safely and automatically 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.

By default, the USB port is “USB Modem” mode. If you need to use it to connect to USB Ethernet Adapter, you need to change it to “USB Ethernet” mode,

<https://forum.peplink.com/t/can-i-use-ethernet-adapters-on-the-usb-wan/8327>

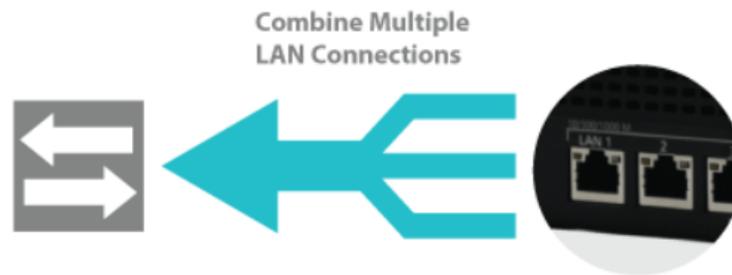
4.6 Built-In Remote User VPN Support



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.

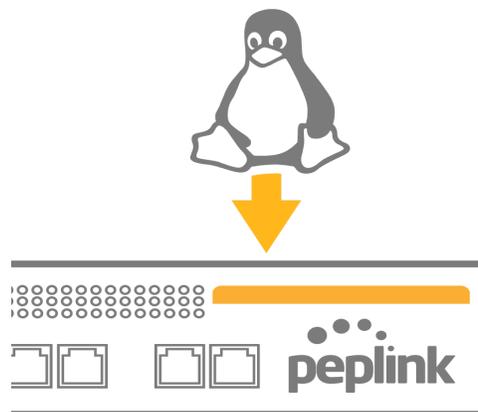
[Click here for the full instructions on setting up L2TP with IPsec.](#)
[Click here for the full instructions on setting up OpenVPN connections](#)

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.

4.8 KVM Virtualization



KVM is a virtualisation module that allows administrators using our routers to host a large range of virtual machines. KVM is now supported by some of the Mediafast models.

[Click here for the full instructions to set up KVM](#)

4.9 DPI Engine

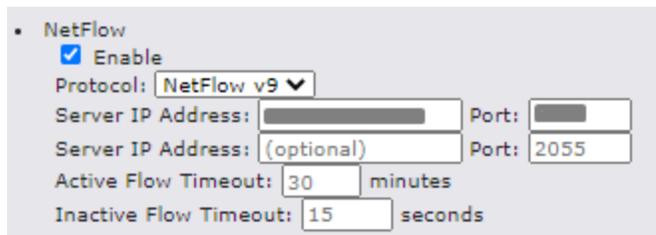
The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.

<https://forum.peplink.com/t/updated-ic2-deep-packet-inspection-dpi-reports-and-everything-you-need-to-know-about-it/29658>

4.10 NetFlow

NetFlow protocol is used to track network traffic. Tracking information from NetFlow can be sent to the NetFlow collector, which analyzes data and generates reports for review.

Note: To enable this feature, go to <https://<Device's IP>/cgi-bin/MANGA/support.cgi>



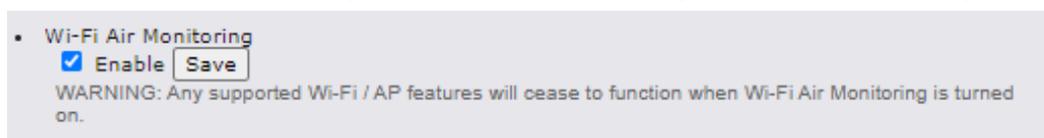
• NetFlow

- Enable
- Protocol:
- Server IP Address: Port:
- Server IP Address: Port:
- Active Flow Timeout: minutes
- Inactive Flow Timeout: seconds

4.11 Wi-Fi Air Monitoring

Peplink routers support Wi-Fi “Air Monitoring Mode” which is used to troubleshoot remotely and proactively monitor Wi-Fi and WAN performance. After enabling Wi-Fi Air Monitoring, reports can be viewed under **InControl 2 > Reports > AirProbe Reports**.

Note: To enable this feature, go to <https://<Device's IP>/cgi-bin/MANGA/support.cgi>



• Wi-Fi Air Monitoring

- Enable
- WARNING: Any supported Wi-Fi / AP features will cease to function when Wi-Fi Air Monitoring is turned on.

4.12 SP Default Configuration

The SP Default Configuration feature written in the updated KB article allows for the provisioning of custom made settings (a.k.a. InControl2 configuration) via the Ethernet LAN port and is ideal for those wanting to do a bulk deployment of many Peplink devices.

Note: If you would like to use this feature, please contact your purchase point (Eg.VAD).

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/30 Pro/50

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

5.3 Peplink Balance 20X

- Peplink Balance 20X
- 2x LTE Antenna, 1x GPS Antenna, 2x Wi-Fi Antenna
- Power adapter
- Information slip

5.4 Peplink Balance 210/310

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

5.5 Peplink Balance 310X

- Peplink Balance 310X
- 2x LTE Antenna, 1x GPS Antenna
- Power adapter
- Ear L-Mounts kit
- Power cord

5.6 Peplink Balance 310 5G

- Balance 310 5G
- Power adapter
- Power cord
- 4x Rubber foot
- 6x Cellular Antenna

5.7 Peplink Balance 310 Fiber 5G

- Balance 310 Fiber 5G
- Power adapter
- Power cord
- 4x Rubber foot
- 4x Cellular Antenna
- 4x Wi-Fi Antenna

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

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

5.9 Peplink Balance 380X/580X

- Peplink 380X/580X
- Power cord
- 1 Pair of Mounting Brackets

5.10 Peplink MediaFast 200

- Peplink MediaFast 200
- Power adapter
- Information slip

5.11 Peplink MediaFast 500

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

5.12 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

5.13 Peplink SDX

- SDX Base Chassis
- 1U 19" Rackmount Chassis

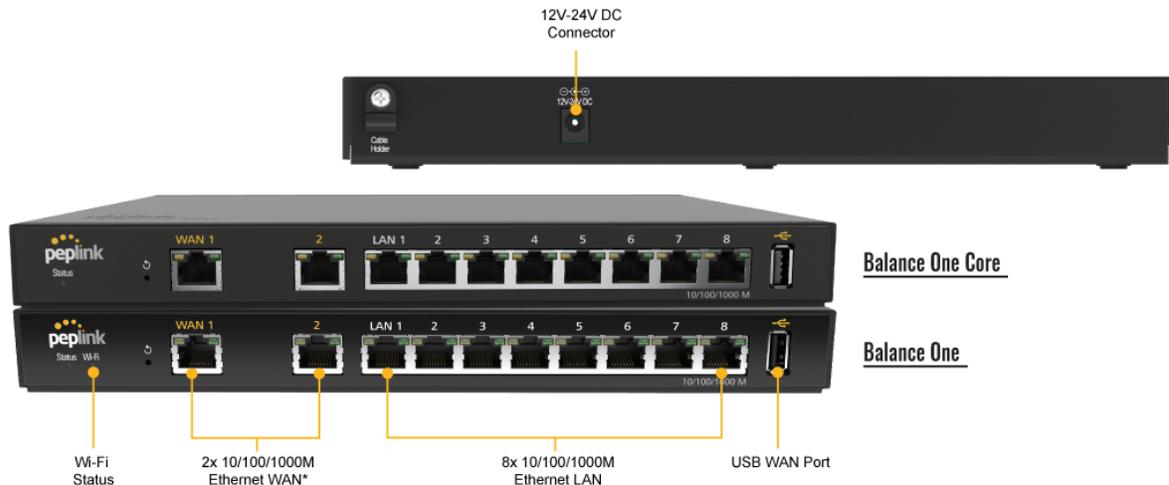
5.14 Peplink SDX Pro

- SDX Pro Base Chassis
- 1U 19" Rack-mount Chassis
- 1x Rubber Foot Pack
- 2x Power Cords
- 1x L-mount Set

6 Peplink Balance Overview

6.1 Peplink Balance One

6.1.1 Panel Appearance



*If the WAN Activation License (BPL-ONE-LC-5WAN) is activated, router throughput will be changed to 400Mbps, both number of WAN and LAN will become 5.

6.1.2 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 – 1000 Mbps OFF – 10 / 100 Mbps or port is not connected
Orange LED	Blinking – Data is transferring

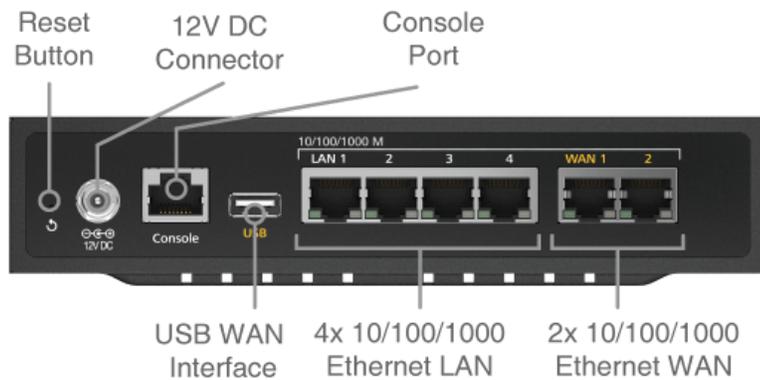
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

Wi-Fi Indicators		
Wi-Fi	OFF	Disabled
	Green	Ready

USB Port	
USB Ports	For future functionality

6.2 Peplink Balance Two

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

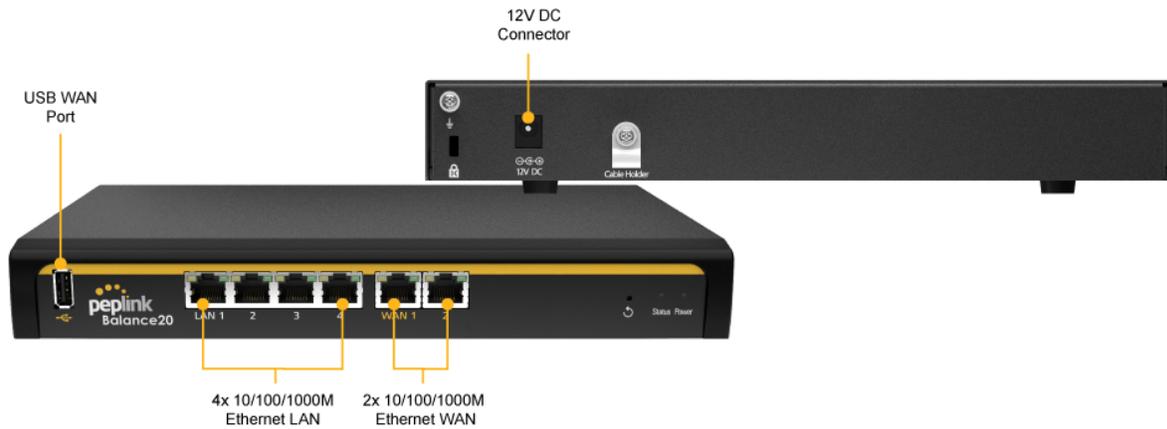
Red – Booting up or busy
Blinking red – Boot up error
Green – Ready

LAN and WAN Ports	
Green LED	ON – 1000 Mbps OFF – 10 / 100 Mbps or port is not connected
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 20

6.3.1 Panel Appearance



6.3.2 LED Indicators

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

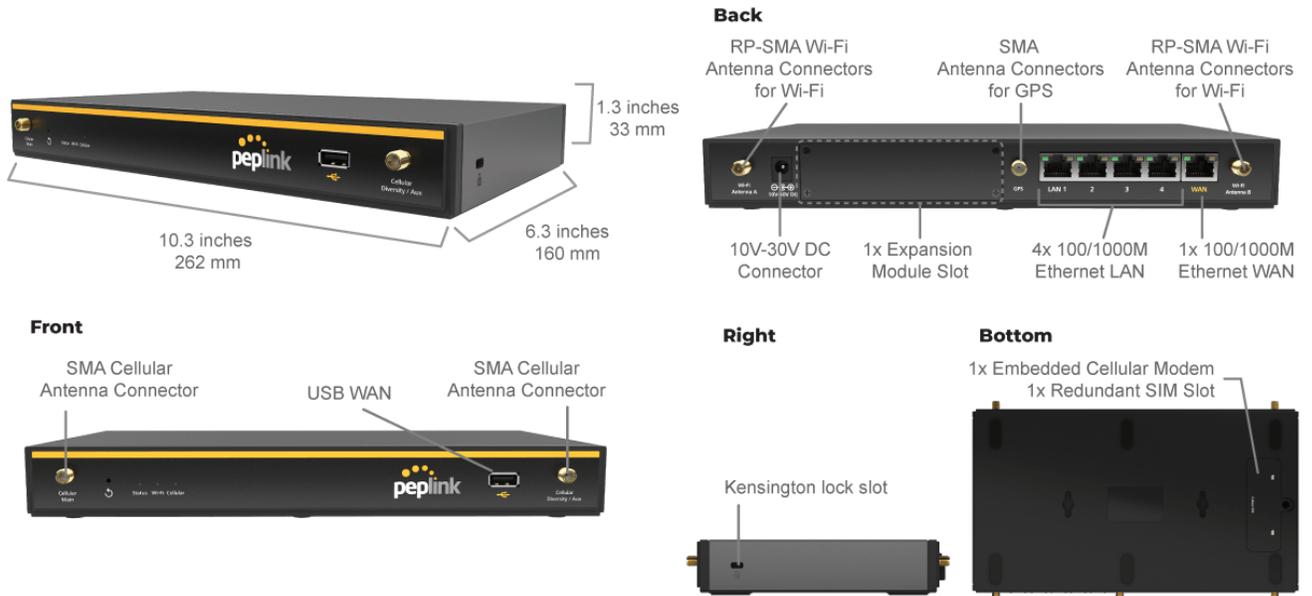
Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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 20X

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

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

Wi-Fi AP Indicators		
Wi-Fi AP	OFF	Disabled
	ON	Enabled

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

6.4.3 Flex Module Mini

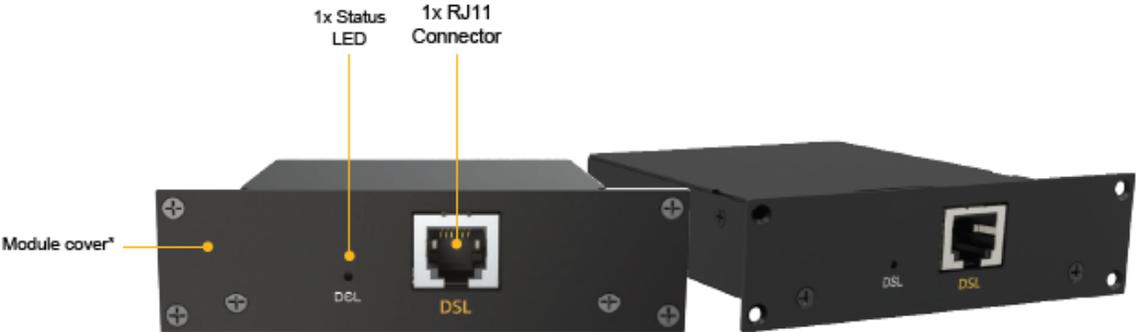


1x LTE-A Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots
Antenna Connectors	2x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	300Mbps/50Mbps (CAT-6) 600Mbps/150Mbps (CAT-12)
Power	10W

Consumption	
Weight	0.83 pounds 375 grams



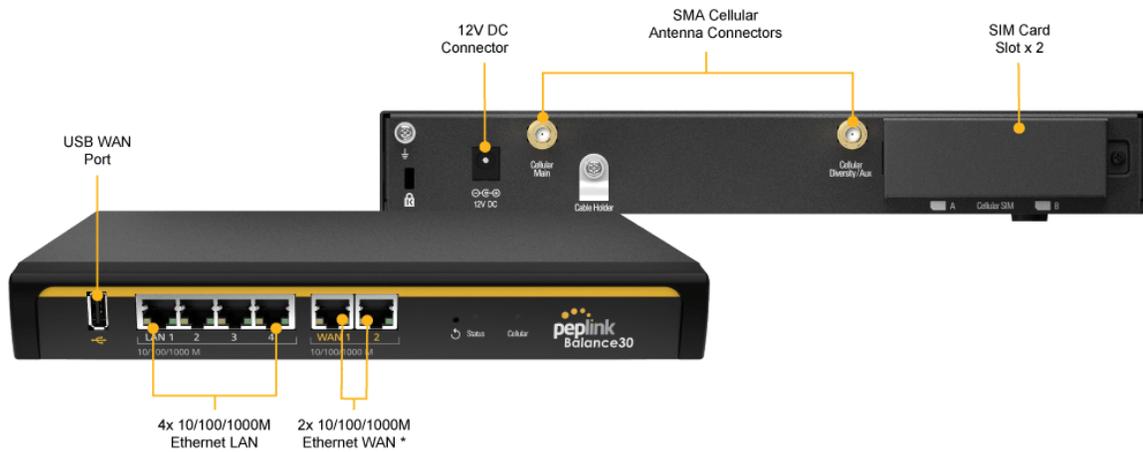
1xLTE-A Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots
Antenna Connectors	4x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	1.2 Gbps/150 Mbps (CAT-18)
Power Consumption	10W
Weight	0.83 pounds 375 grams



1x VDSL Module	
Interface	1x RJ11 Connector, 1x Status LED
Power Consumption	9W
Weight	0.44 pounds 200 grams

6.5 Peplink Balance 30 LTE

6.5.1 Panel Appearance



* WAN ports can act as a LAN port if needed.

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

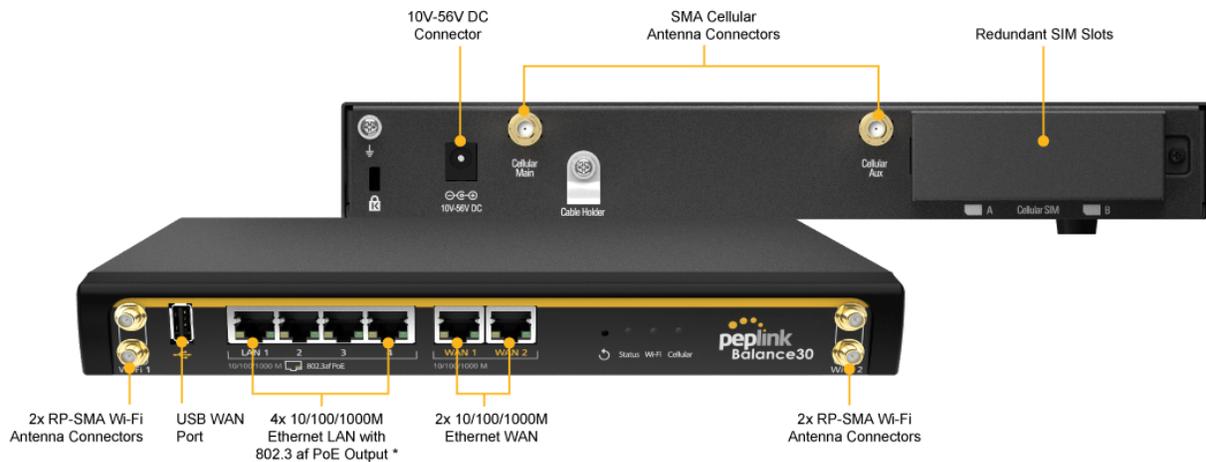
Cellular WAN Indicators		
Cellular	OFF	Disabled
	Blinking slowly	Connecting to wireless network
	ON	Connected to wireless network

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

6.6 Peplink Balance 30 Pro

For certification information, please refer to Appendix F (page 327 ~ 330)

6.6.1 Panel Appearance



* PoE Activation Kit is available separately, needs at least 48V of input for PoE output

6.6.2 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

WAN Ports

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

LAN Ports	
Green LED	ON – POE Enabled OFF - POE Disabled
Orange LED	Blinking – 10 / 100 / 1000 Mbps with activity OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

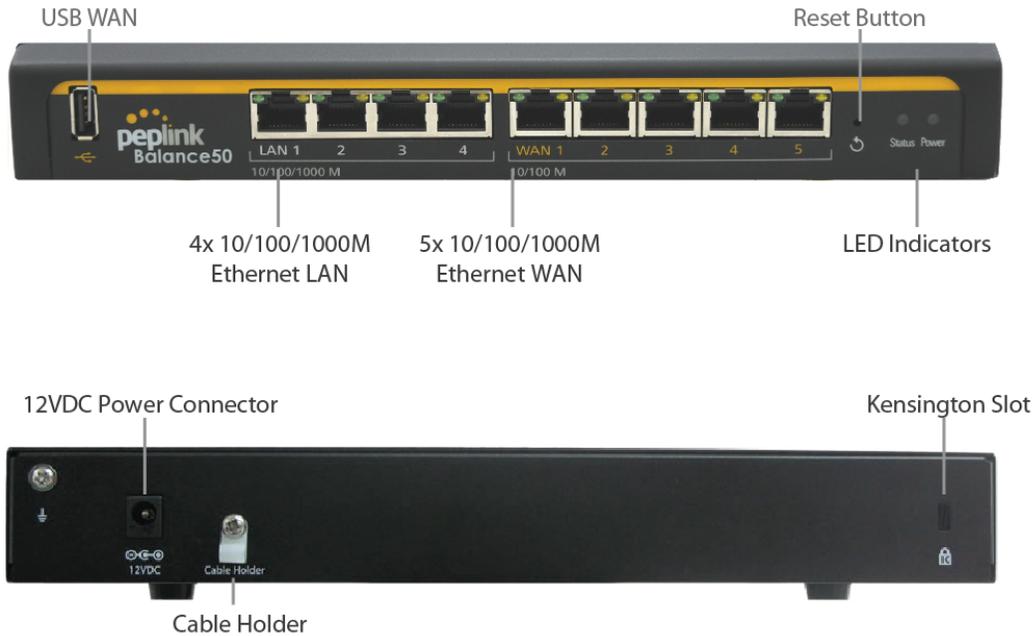
Wi-Fi AP Indicators		
Wi-Fi AP	OFF	Disabled
	ON	Enabled

Cellular WAN Indicators		
Cellular	OFF	Disabled
	Blinking slowly	Connecting to wireless network
	ON	Connected to wireless network

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

6.7 Peplink Balance 50

6.7.1 Front Panel Appearance



6.7.2 LED Indicators

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

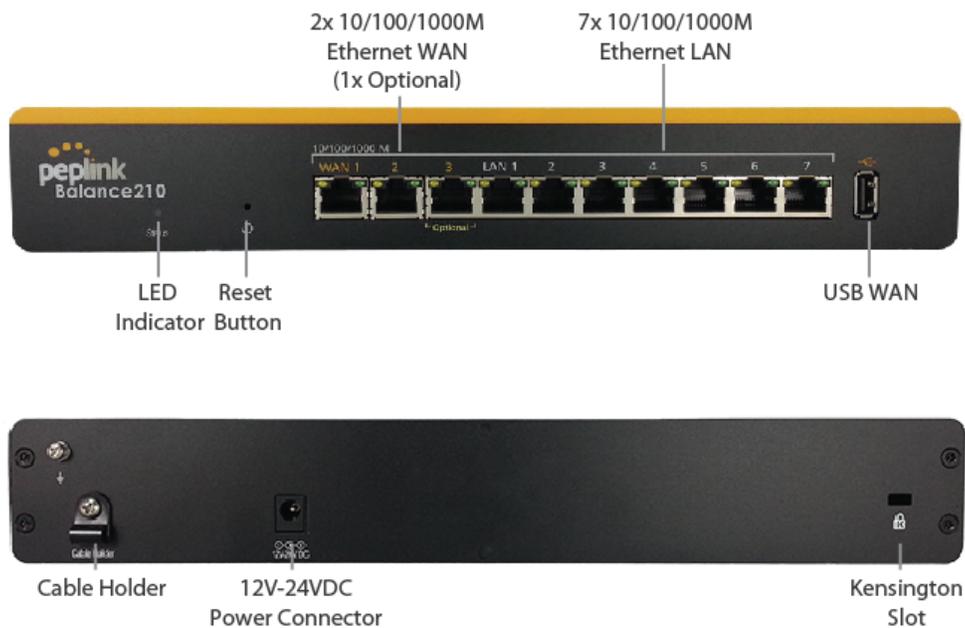
Power and Status Indicators	
Power	OFF – Power off
	Green – Power on
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

6.8 Peplink Balance 210

6.8.1 Front Panel Appearance



6.8.2 LED Indicators

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

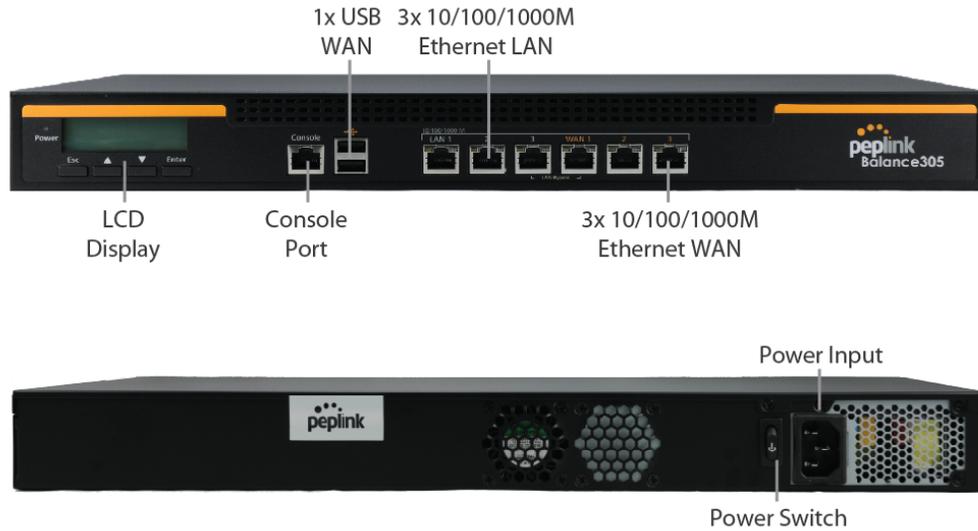
Power and Status Indicators	
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

6.9 Peplink Balance 305

6.9.1 Front Panel Appearance



6.9.2 LED Indicators

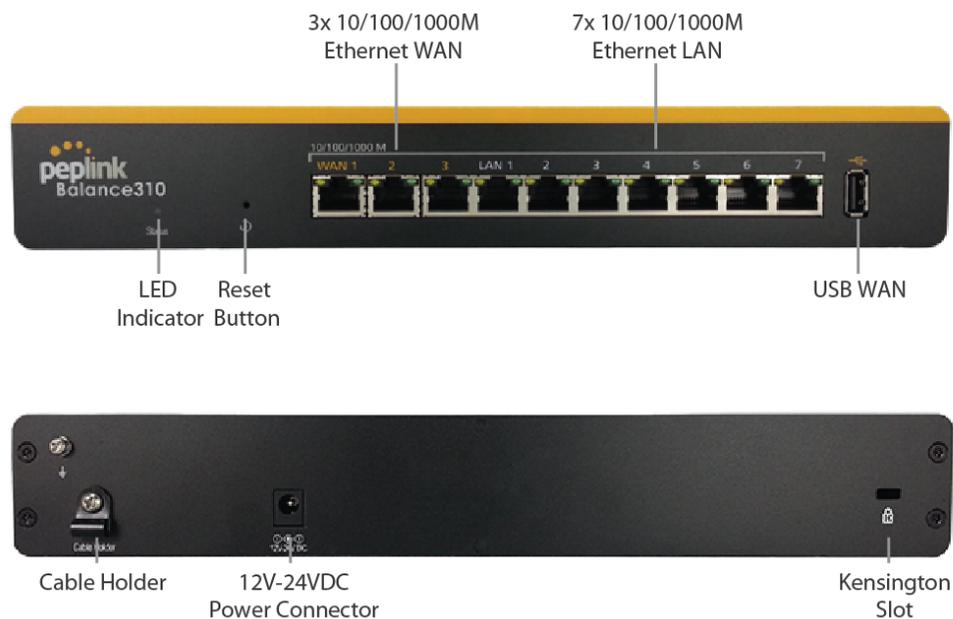
The statuses indicated by the front panel LEDs are as follows:

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 310

6.10.1 Front Panel Appearance



6.10.2 LED Indicators

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

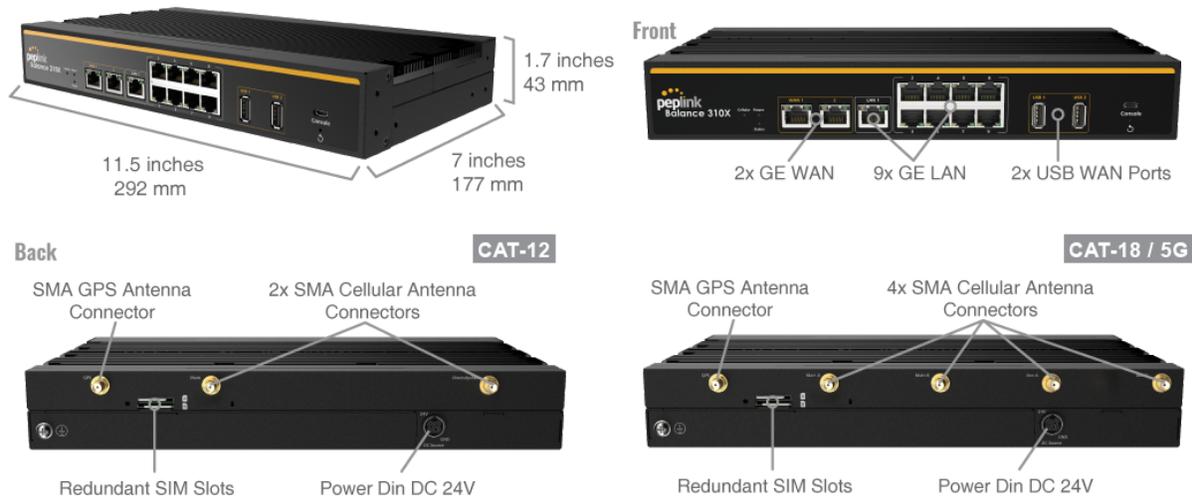
Power and Status Indicators	
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

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

6.11 Peplink Balance 310X

6.11.1 Front Panel Appearance



6.11.2 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

WAN Ports

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

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

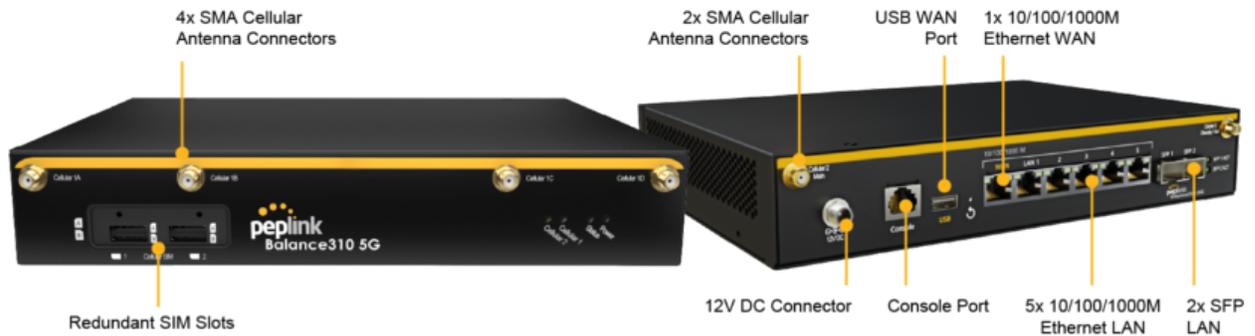
Cellular WAN Indicators		
Cellular	OFF	Disabled
	Blinking slowly	Connecting to wireless network
	ON	Connected to wireless network

Wi-Fi AP Indicators		
Wi-Fi AP	OFF	Disabled
	ON	Enabled

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

6.12 Peplink Balance 310 5G

6.12.1 Front Panel Appearance



6.12.2 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

WAN Port	
Right LED	GREEN - 1000 Mbps
	ORANGE - 100 Mbps
	OFF – 10 Mbps or port is not connected
Left LED	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

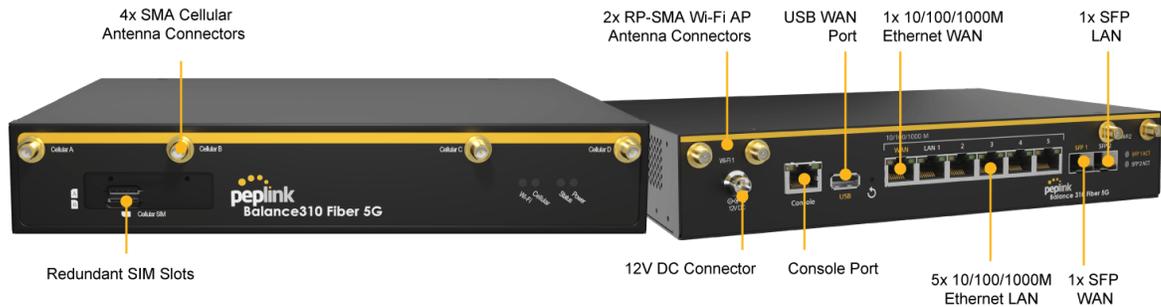
LAN Ports	
Right LED	<p>GREEN – 1000 Mbps</p> <p>ORANGE - 100 Mbps</p> <p>OFF – 10 Mbps or port is not connected</p>
Left LED	<p>Blinking – Data is transferring</p> <p>OFF – Port is not connected</p>
Port Type	Auto MDI/MDI-X ports

Cellular WAN Indicators		
Cellular	OFF	Disabled
	Blinking slowly	Connecting to wireless network
	ON	Connected to wireless network

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

6.13 Peplink Balance 310 Fiber 5G

6.13.1 Front Panel Appearance



6.13.2 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

WAN Port	
Right LED	GREEN - 1000 Mbps ORANGE - 100 Mbps OFF – 10 Mbps or port is not connected
Left LED	Blinking – Data is transferring OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

LAN Ports	
Right LED	GREEN – 1000 Mbps ORANGE - 100 Mbps OFF – 10 Mbps or port is not connected
Left LED	Blinking – Data is transferring OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

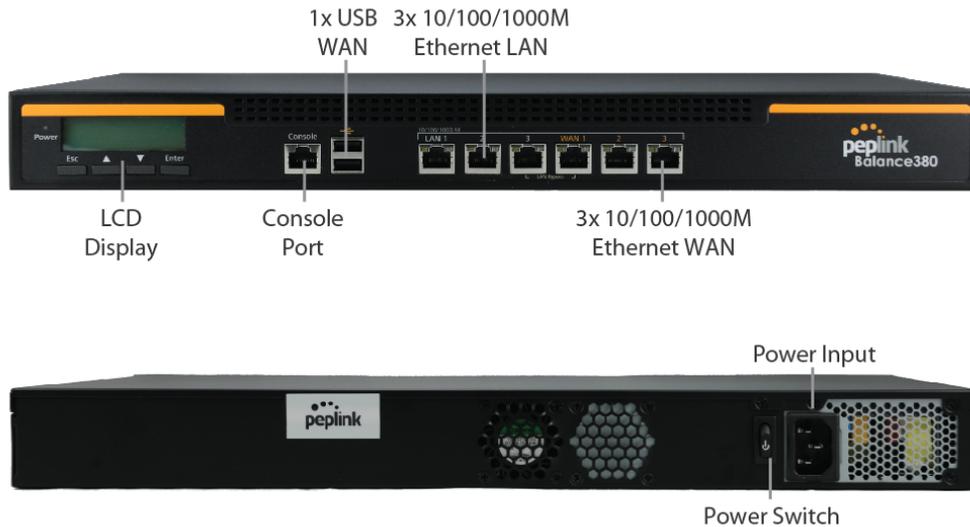
Cellular WAN Indicators		
Cellular	OFF	Disabled
	Blinking slowly	Connecting to wireless network
	ON	Connected to wireless network

Wi-Fi AP Indicators		
Wi-Fi AP	OFF	Disabled
	ON	Enabled

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

6.14 Peplink Balance 380

6.14.1 Panel Appearance



6.14.2 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

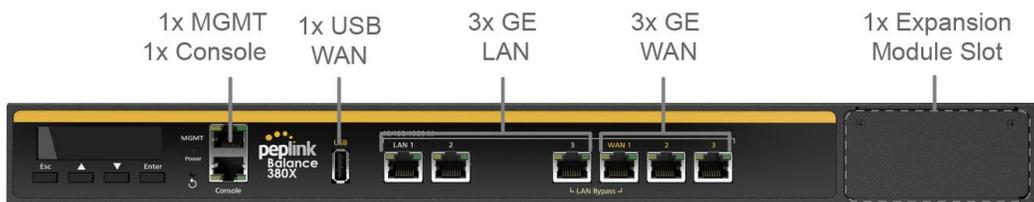
Console Port	Reserved for engineering use
USB Ports	For connecting a 4G/3G USB modem

6.15 Peplink Balance 380X

6.15.1 Panel Appearance



Front



Back



6.15.2 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	GREEN – 1000 Mbps
	OFF – 10 / 100 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

6.15.3 Flex Module Mini



1x LTE-A Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots

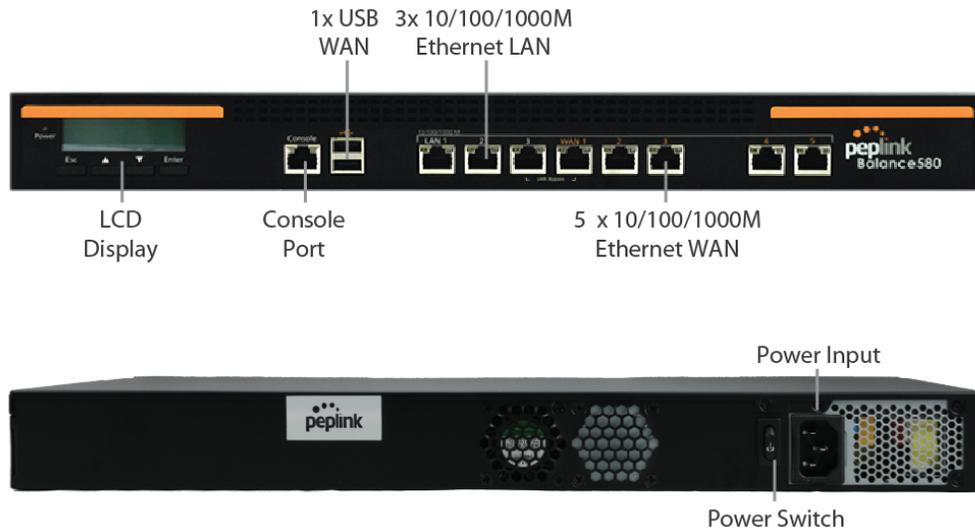
Antenna Connectors	2x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	300Mbps/50Mbps (CAT-6) 600Mbps/150Mbps (CAT-12)
Power Consumption	10W
Weight	0.83 pounds 375 grams



1xLTE-A Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots
Antenna Connectors	4x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	1.2 Gbps/150 Mbps (CAT-18)
Power Consumption	10W
Weight	0.83 pounds 375 grams

6.16 Peplink Balance 580

6.16.1 Panel Appearance



6.16.2 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
---------------------	------------------------------

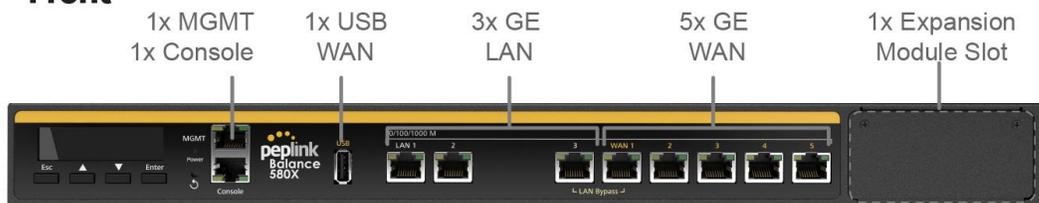
USB Ports	For connecting a 4G/3G USB modem
------------------	----------------------------------

6.17 Peplink Balance 580X

6.17.1 Panel Appearance



Front



Back



6.17.2 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	GREEN – 1000 Mbps
	OFF – 10 / 100 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

6.17.3 Flex Module Mini



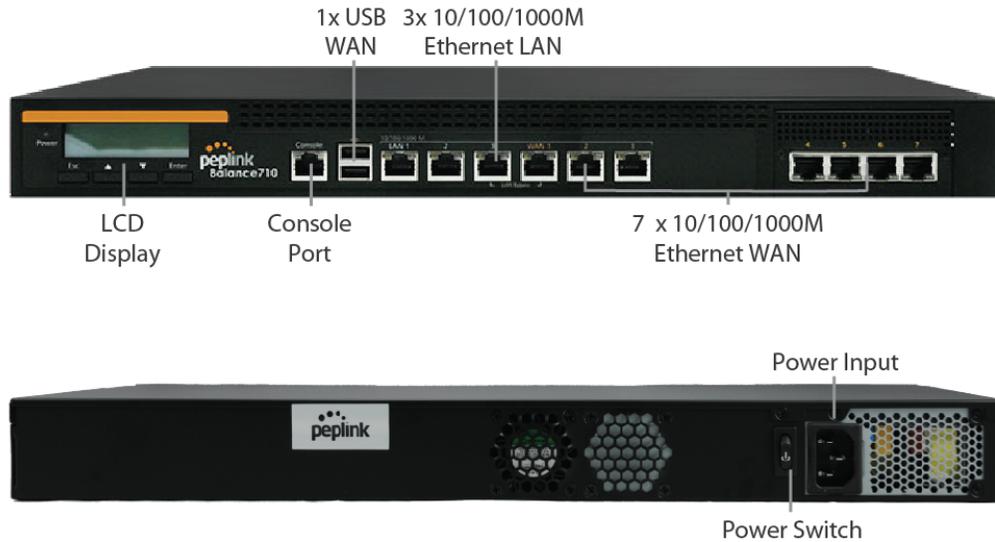
1x LTEA Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots
Antenna Connectors	2x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	300Mbps/50Mbps (CAT-6) 600Mbps/150Mbps (CAT-12)
Power Consumption	10W
Weight	0.83 pounds 375 grams



1xLTEA Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots
Antenna Connectors	4x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	1.2 Gbps/150 Mbps (CAT-18)
Power Consumption	10W
Weight	0.83 pounds 375 grams

6.18 Peplink Balance 710

6.18.1 Front Panel Appearance



6.18.2 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	ORANGE – 1000 Mbps
	GREEN – 100 Mbps
	OFF – 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
------------------	----------------------

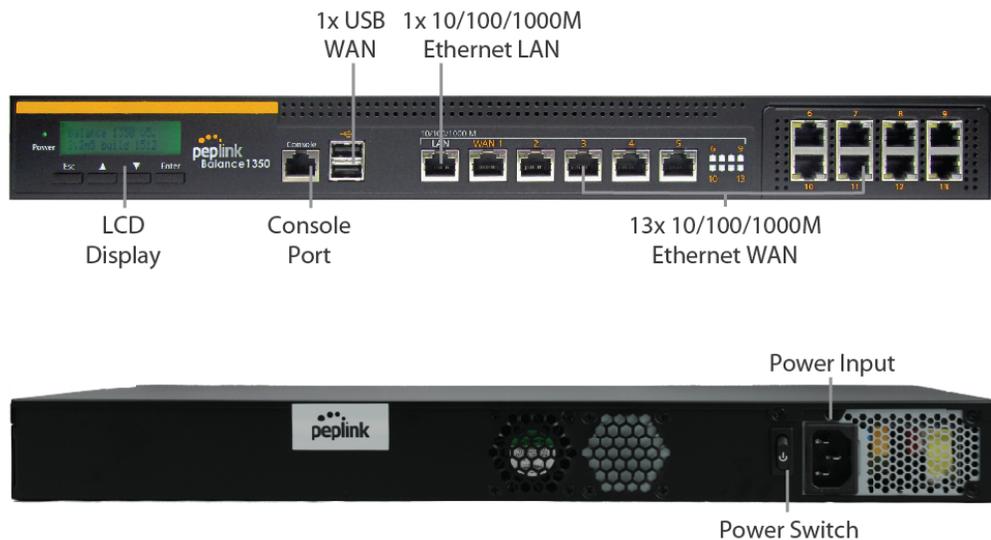
Console & USB Ports

Console Port	Reserved for engineering use
---------------------	------------------------------

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

6.19 Peplink Balance 1350

6.19.1 Panel Appearance



6.19.2 LED Indicators

Status indicated in the front panel is as follows:

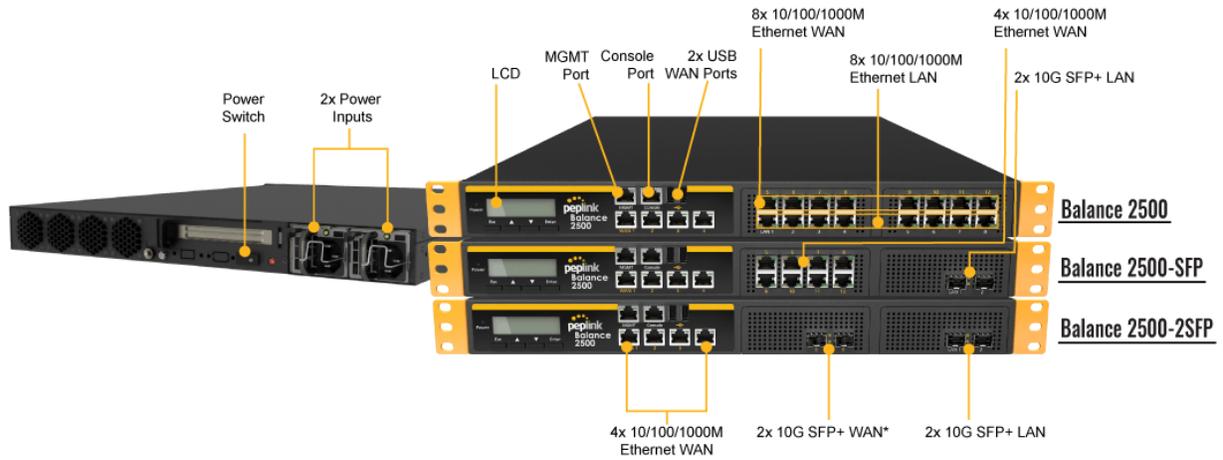
LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

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

6.20 Peplink Balance 2500

6.20.1 Panel Appearance



*Balance 2500 is available in two configurations with different LAN interfaces.

6.20.2 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

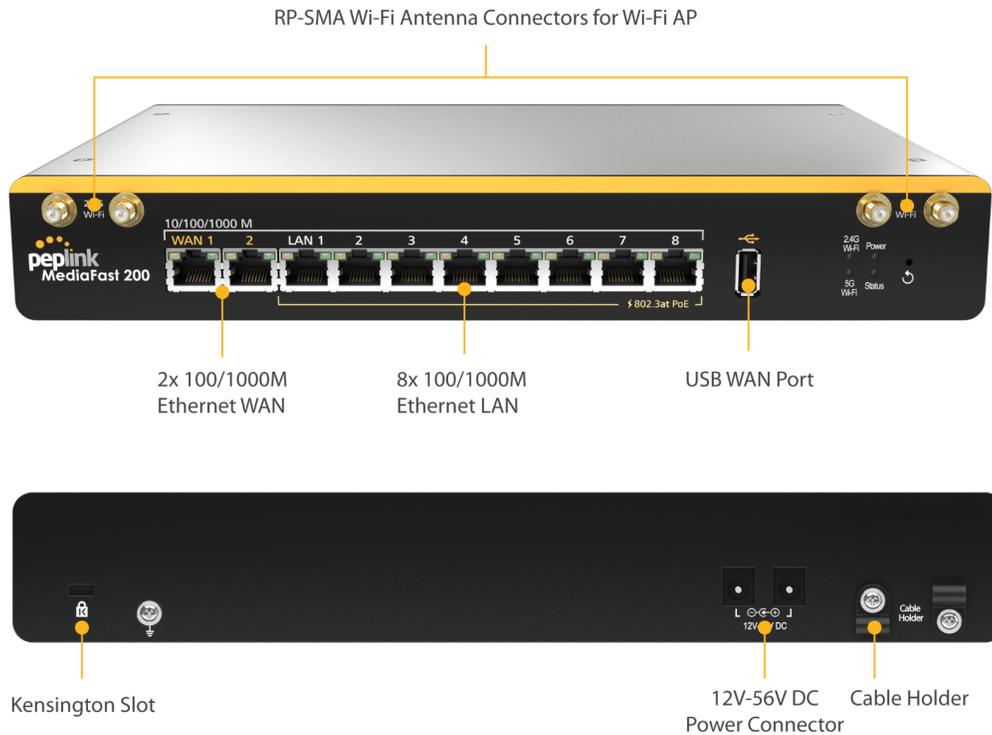
Console Port Reserved for engineering use

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

7 Peplink MediaFast Overview

7.1 Peplink MediaFast 200

7.1.1 Panel Appearance



7.1.2 LED Indicators

Status indicated in the front panel is as follows:

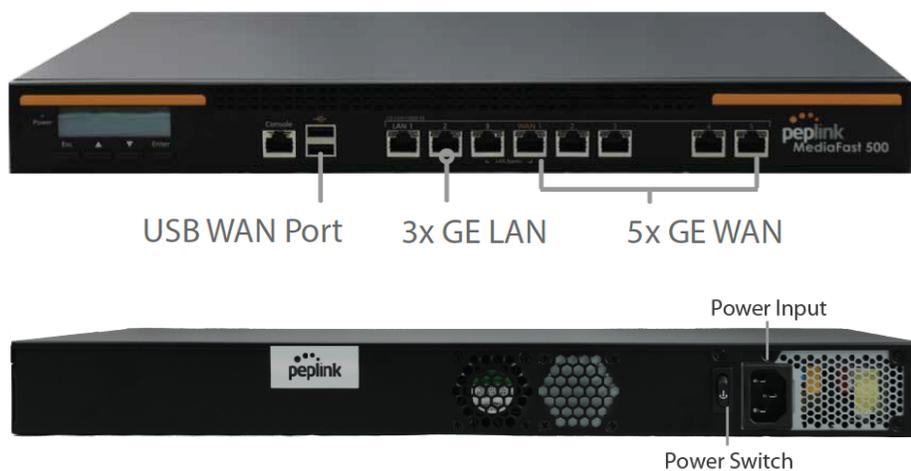
LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

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:

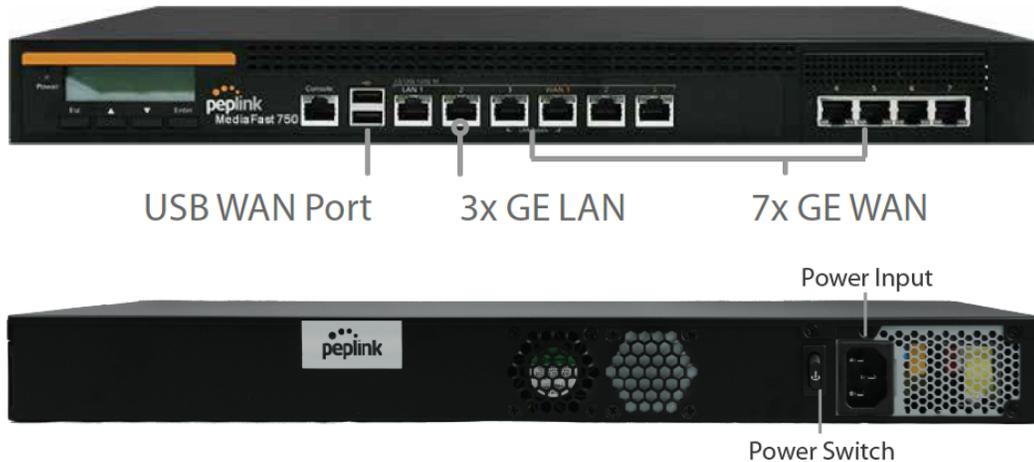
LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

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 this can be used simultaneously to allow bonding using our SpeedFusion technology.

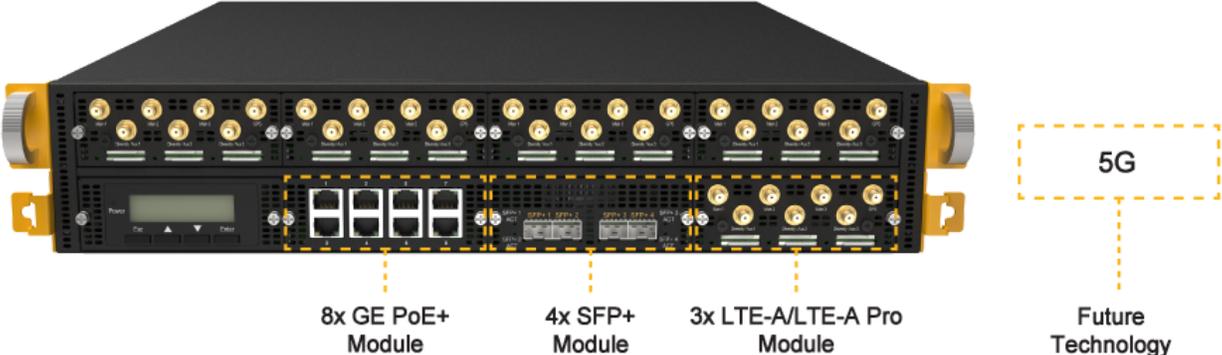
With its modular construction, the EPX is suitable for any deployment.

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

Front



Back



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 – PoE is disabled
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.

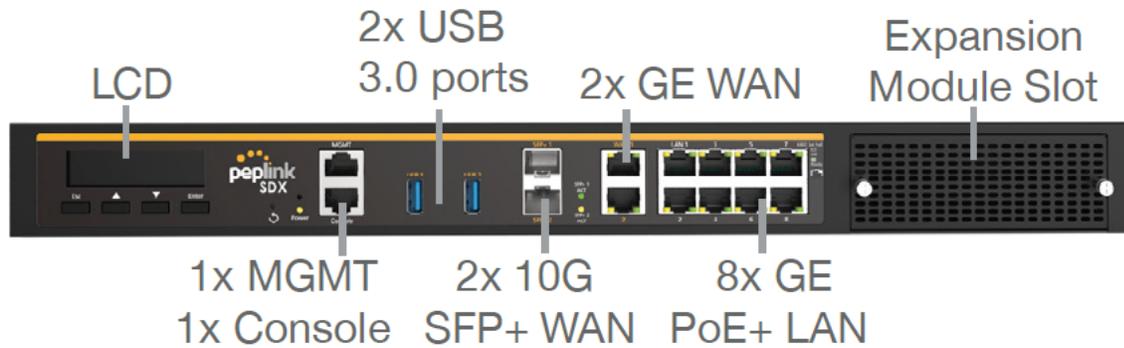
8.2.1 Main Chassis

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

WAN Ports	
Right LED	GREEN – 1000 Mbps
	OFF – 10 Mbps / 100 Mbps or the 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

LAN Ports	
Right LED	GREEN – PoE enabled
	OFF – PoE is disabled
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 Port	CLI console connection
USB Ports	For connecting 4G/3G USB modems for additional WAN connections
MGMT Port	Management port

8.3 Peplink SDX Pro

In addition to the power of the SDX, the SDX Pro offers greater flexibility and functionality. It has two FlexModule slots, enabling you to customize the device with different modules to suit any deployment. It supports edge computing so it can deliver websites, applications, and docker containers to connected devices.

8.3.1 Main Chassis

SDX Pro Main Chassis	
Power Input	AC Input 100V - 240V
Power Consumption	140W System* , 420W PoE+ Power Budget
Throughput	24 Gbps
PepVPN/SpeedFusion Throughput	No Encryption: 1 Gbps 256-bit AES: 600 Mbps
Dimensions	17.2 x 13.8 x 1.7 inches - 438 x 350 x 44 mm
Weight (No Modules)	15.9 pounds - 7.2 kilograms
Operating Temperature	32° – 104°F (0° – 40°C)
Humidity	10% – 85% (non-condensing)
Certifications	FCC, IC, CE

* 140W consumption for the main chassis, 20W consumption for the optional module.

8.3.2 Panel Appearance



* WAN ports are configured as a LAN ports by default, configuration is changeable on the Web Admin

8.3.3 LED Indicators

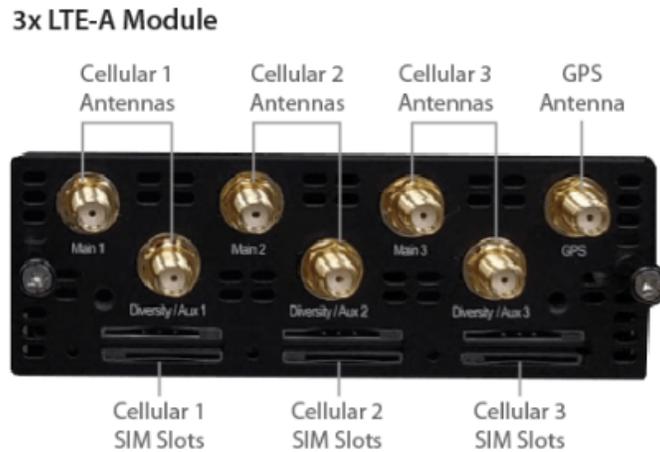
LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

WAN Ports	
Right LED	GREEN – 1000 Mbps
	OFF – 10 Mbps / 100 Mbps or 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 Port	CLI console connection
USB Ports	For connecting 4G/3G USB modems for additional WAN connections
MGMT Port	Management port

8.4 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

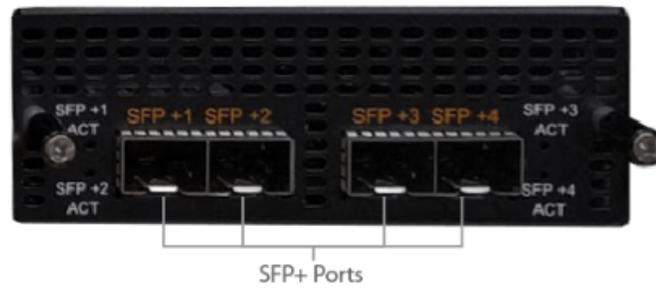
8x GE PoE Module



GE PoE+ Enabled
Ethernet Ports

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



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.
- > Serial number
- > System time
- > System uptime
- > CPU load
- > LAN
 - > Status
 - > IP address
 - > Subnet mask

- > Link status

- > WAN1
- > WAN2
- > WAN3*

- > VPN status

- >VPN Profile 1
- >VPN Profile 2
- >...
- >VPN Profile n

- > Link usage

- > Throughput in
 - > WAN1
 - > WAN2
 - > WAN3*
- > Throughput out
 - > WAN1
 - > WAN2
 - > WAN3*

- > Data Transferred

- > WAN1
- > WAN2
- > WAN3*

- > Maintenance



(shows firmware version)

(shows serial number)

(shows current time)

(shows system uptime since last reboot)

(shows current CPU loading, 0-100%)

(shows LAN port physical status)

(shows LAN IP address)

(shows LAN subnet mask)

(shows Connected/Disconnected, IP address list)

(shows Connected/Disconnected)

(shows transfer rate in Kbps)

(shows transfer rate in Kbps)

(shows volume transferred since last reboot in MB)

```

> 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,
    > LAN                                100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
    > 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 connect up to 4 computers.
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.

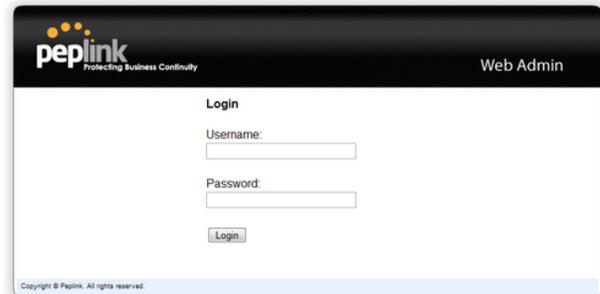
To connect to the web admin of the Peplink Balance, enter the following LAN IP address in the address field of the web browser:

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

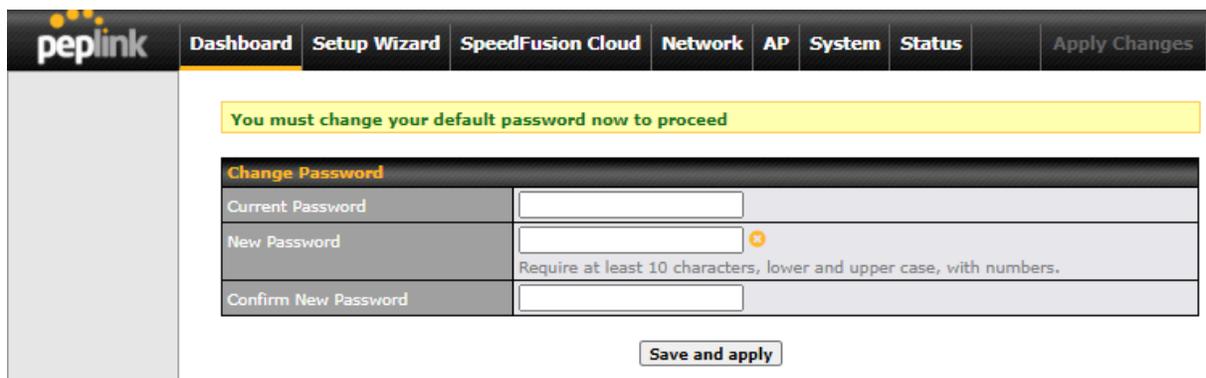


(This is the default admin user login of the Peplink Balance.)

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.



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.

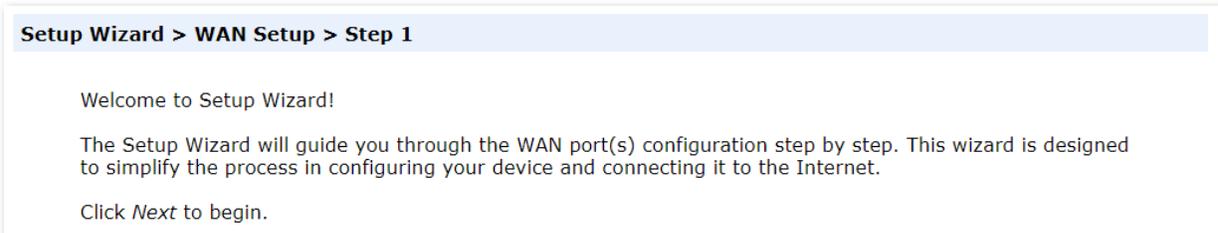
11.2 Configuration with the Setup Wizard

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

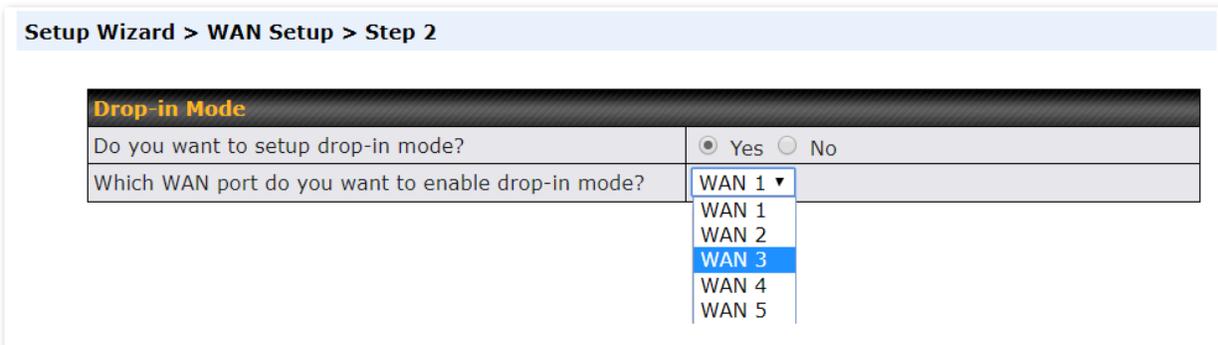
To begin, click **Setup Wizard** after connecting to the web admin interface.



Click **Next >>** to begin.



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



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

Setup Wizard > WAN Setup > Step 3

Choose the WAN port(s) to be configured.

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

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

Setup Wizard > WAN Setup > Step 4

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

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

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

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

Setup Wizard > WAN Setup > Step 4

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

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

If **Custom Mobile Operator Settings** is selected, APN parameters are required. Some service providers may charge a fee for connecting to a different APN. Please consult your service provider for the correct settings.

Setup Wizard > WAN Setup > Step 5

Enter the parameters of Mobile Operator Settings for Mobile Internet.

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

Click on the appropriate check box(es) to select the preferred WAN connection(s). Connection(s) not selected in this step will be used as 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	<input checked="" type="checkbox"/>
WAN 2	<input checked="" type="checkbox"/>

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

Setup Wizard > WAN Setup > Step 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 SpeedFusion Cloud

With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*



*SpeedFusion Cloud is supported in firmware version 8.1.0 and above. SpeedFusion Cloud is a subscription basis. SpeedFusion Cloud license can be purchased at <https://store.peplink.com/> > **Cloud Solutions > SpeedFusion Cloud Service.**

12.1 Activate SpeedFusion Cloud Service

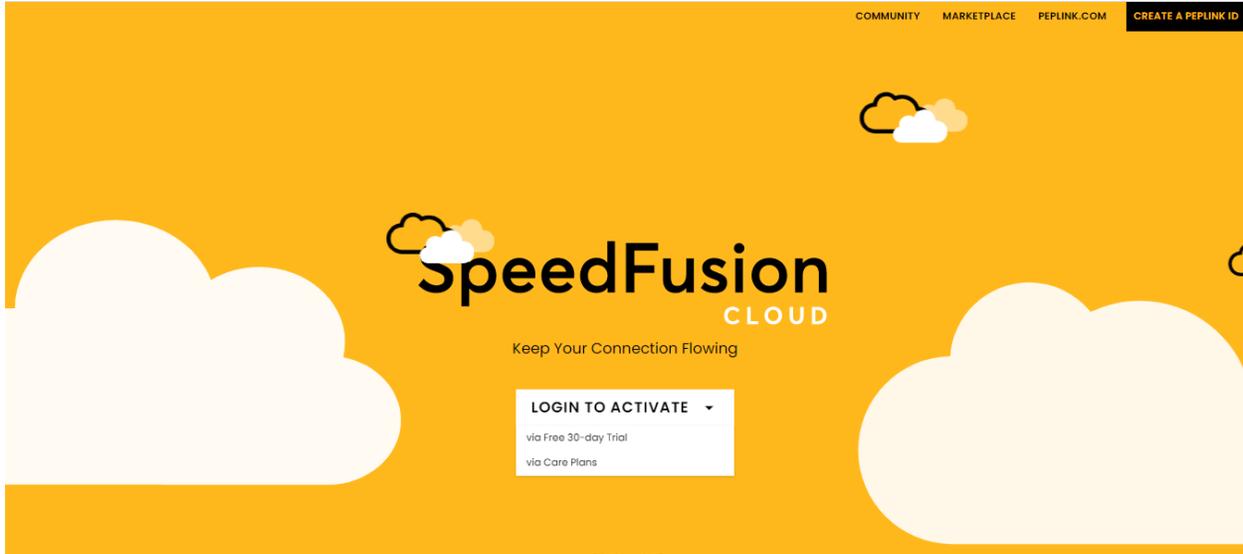
You are entitled to a 30-day free period with 100GB of SpeedFusion usage upon activation of the SpeedFusion Cloud service. This offer is limited to once per device. To get your activation key please visit SpeedFusion Cloud.

The screenshot shows the Peplink web interface for SpeedFusion Cloud. The navigation menu includes Dashboard, Setup Wizard, SpeedFusion Cloud (highlighted), Network, AP, System, Status, and Apply Changes. The main content area is titled 'SpeedFusion Cloud' and includes the following options:

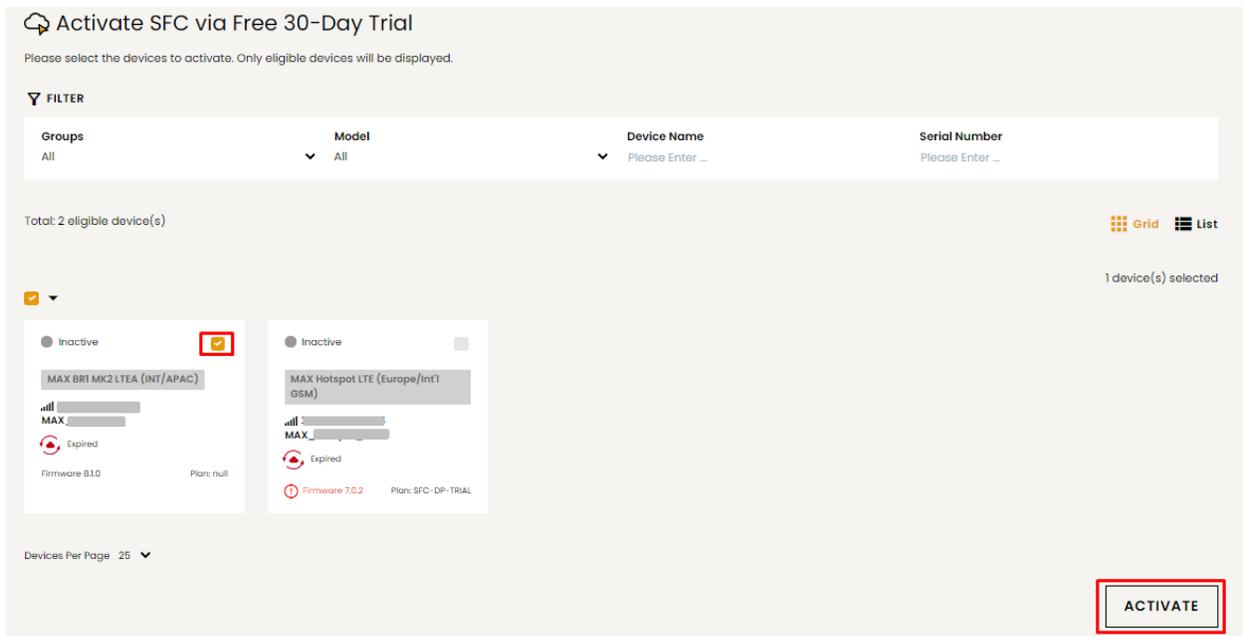
- Get your activation key now**: Enjoy all the delicious features powered by SpeedFusion. (This option is highlighted with a red box in the original image.)
- Choose Cloud Location**: Which cloud you'd like to connect?
- Connect Clients to Cloud**: Select a cloud for your laptops, phones, or other devices.
- Link Wi-Fi to Cloud**: Create a Wi-Fi SSID that is dedicated for the cloud.

A 'Logout' button is visible in the bottom left corner of the interface.

Go to activate.speedfusion.com and select the type of SpeedFusion Cloud service, “Via Free 30-days Trial” or “Via Care Plans”, that you would like to activate. Next, register or login to your account.



Select the devices that you wish to activate SpeedFusion Cloud on and click **ACTIVATE**.



From **System > Features Add-ons**, paste the license key into the window and click on **Activate** once you have received the license key.

The screenshot shows the PEPWAVE web interface. The top navigation bar includes: Dashboard, SpeedFusion Cloud, Network, Advanced, AP, System (selected), Status, and Apply Changes. The left sidebar lists System and Tools categories. Under System, 'Feature Add-ons' is selected. The main content area displays the 'Feature Activation' window with the following details:

Feature Activation	
Activation Key	9629a523e54fe148f876e75cf95df776f248e248b618b618a6199b23e54fe148f876e75cf95df776f351e640e450b618b618a310ae10a711a219a6249c5af05ef747c958e346e248c95bf75df309a709a3199c7ae64cf34dd05ce540f947b66afa46e34db668f55dff5ff75dff46f809dd4cef09be18a619d16bbfa96c3083b48a7d337ade187a5ce2e4e1

Below the license key is an **Activate** button.

12.2 Enable SpeedFusion Cloud

Enable SpeedFusion Cloud from **SpeedFusion Cloud > Choose Cloud Location**.

The screenshot shows the SpeedFusion Cloud configuration page. The top navigation bar includes: Dashboard, SpeedFusion Cloud (selected), Network, AP, System, Status, and Apply Changes. The main content area features the SpeedFusion Cloud logo and the following text:

Aggregate your bandwidth, connect you to different geo-location, and more.

- Choose Cloud Location**
Which cloud you'd like to connect?
- Connect Clients to Cloud**
Select a cloud for your laptops, phones, or other devices.

Choose **Automatic** > Click on the green tick button to confirm the change.

PEPWAVE Dashboard **SpeedFusion Cloud** Network Advanced AP System Status Apply Changes

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location
	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">--- Automatic ---</div> <div style="background-color: #e0e0e0; padding: 2px;">---</div> <div style="background-color: #007bff; color: white; padding: 2px;">--- Automatic ---</div> <div style="padding: 2px;">Australia (SYD)</div> <div style="padding: 2px;">Germany (FRA)</div> <div style="padding: 2px;">Japan (TYO)</div> <div style="padding: 2px;">Singapore (SIN)</div> <div style="padding: 2px;">United Kingdom (LON)</div> <div style="padding: 2px;">United States (NYC)</div> <div style="padding: 2px;">United States (SFO)</div> </div>

Click on **Apply Changes** to save the change.

PEPWAVE Dashboard **SpeedFusion Cloud** Network Advanced AP System Status **Apply Changes**

Saved! Changes will be effective after clicking the 'Apply Changes' button.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location
SEC	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">--- Automatic ---</div> </div>

Changes applied successfully.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	
SEC	--- Automatic ---	

By default, the router will build a SpeedFusion tunnel to the SpeedFusion Cloud

PEPWAVE | Dashboard | **SpeedFusion Cloud** | Network | Advanced | AP | System | Status | Apply Changes

WAN Connection Status ?

Priority 1 (Highest) Drag desired (Priority 1) connections here

Priority 2

1 Cellular 1	Connected to MY MAXIS LTE-A	Details
2 Cellular 2	Connected to MY MAXIS LTE-A	Details

Priority 3 Drag desired (Priority 3) connections here

Disabled

1 WAN 1	<input type="checkbox"/> Disabled	Details
2 WAN 2	<input type="checkbox"/> Disabled	Details
3 Cellular 3	<input type="checkbox"/> Disabled	Details
4 Cellular 4	<input type="checkbox"/> Disabled	Details
Wi-Fi WAN	<input type="checkbox"/> Disabled	Details
3 LAN 1 as WAN	<input type="checkbox"/> Disabled	Details
4 LAN 2 as WAN	<input type="checkbox"/> Disabled	Details
5 LAN 3 as WAN	<input type="checkbox"/> Disabled	Details

LAN Interface

Router IP Address: 192.168.50.1

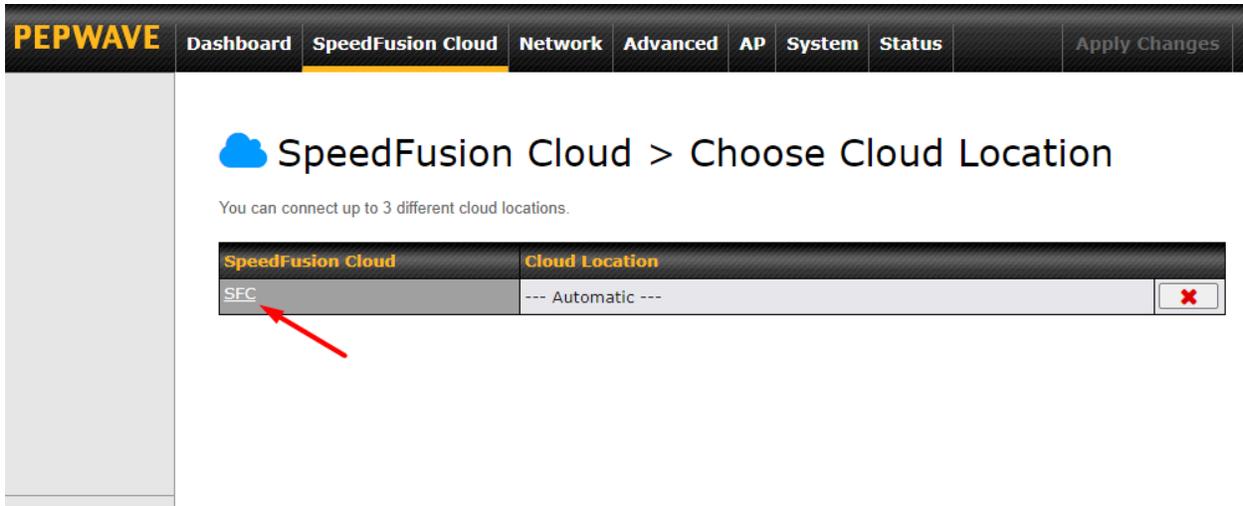
Wi-Fi AP ON [Details](#)

PEPWAVE_EBB4

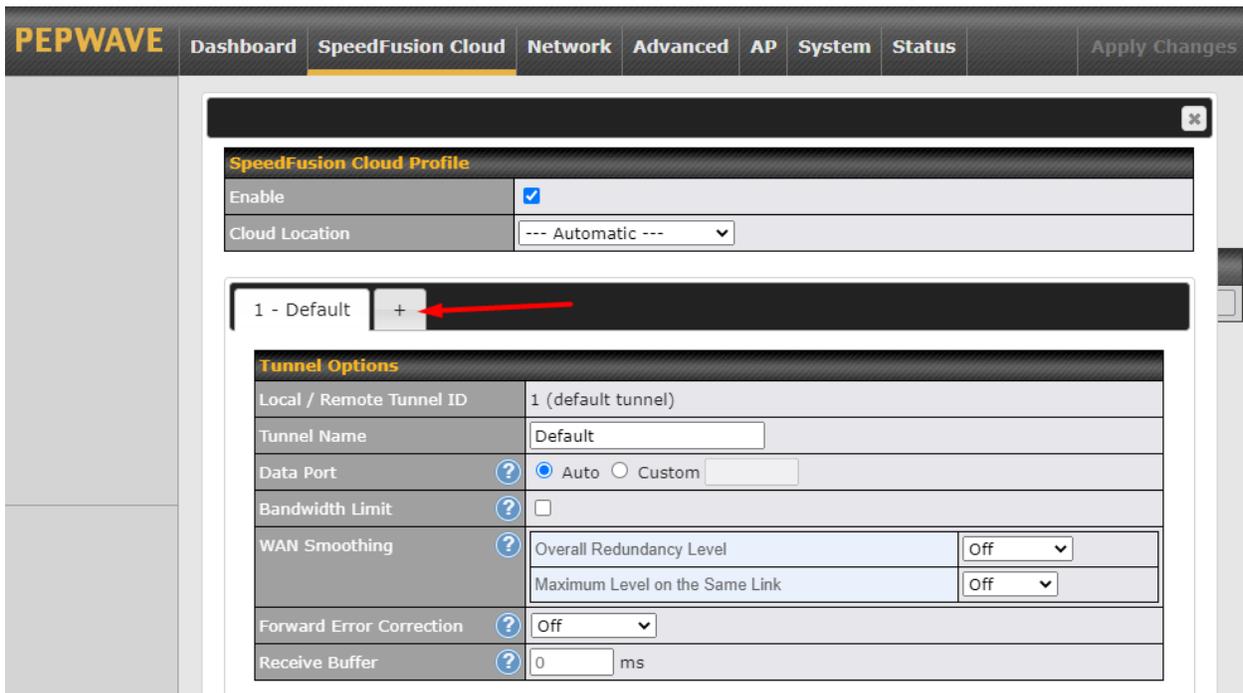
SpeedFusion Cloud

SFC	Established
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)	

If you are running a latency sensitive service like video streaming or VOIP, a WAN Smoothing sub-tunnel can be created. Navigate to **Speedfusion Cloud > Choose a cloud location > SFC**.



A Speedfusion tunnel configuration window will pop out. Click on the + sign to create the WAN Smoothing sub-tunnel.



PEPWAVE Dashboard **SpeedFusion Cloud** Network Advanced AP System Status Apply Changes

SpeedFusion Cloud Profile

Enable	<input checked="" type="checkbox"/>
Cloud Location	--- Automatic ---

1 - Default 2 - WAN Smoo... +

Tunnel Options

Local / Remote Tunnel ID	2	
Tunnel Name	WAN Smoothing 	
Data Port	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>	
Bandwidth Limit	<input type="checkbox"/>	
WAN Smoothing	Overall Redundancy Level	Normal <input type="text"/>
	Maximum Level on the Same Link	Normal <input type="text"/>
Forward Error Correction	Off <input type="text"/>	
Receive Buffer	0 <input type="text"/> ms	

Click on **Save** and **Apply Changes** to save the configuration. Now, the router has 2 Speedfusion tunnels to the Speedfusion Cloud.

PEPWAVE | Dashboard | **SpeedFusion Cloud** | Network | Advanced | AP | System | Status | Apply Changes

WAN Connection Status ?

Priority 1 (Highest)
Drag desired (Priority 1) connections here

Priority 2

1 Cellular 1	Connected to MY MAXIS LTE-A	Details
2 Cellular 2	Connected to MY MAXIS LTE-A	Details

Priority 3
Drag desired (Priority 3) connections here

Disabled

1 WAN 1	<input type="checkbox"/> Disabled	Details
2 WAN 2	<input type="checkbox"/> Disabled	Details
3 Cellular 3	<input type="checkbox"/> Disabled	Details
4 Cellular 4	<input type="checkbox"/> Disabled	Details
Wi-Fi WAN	<input type="checkbox"/> Disabled	Details
3 LAN 1 as WAN	<input type="checkbox"/> Disabled	Details
4 LAN 2 as WAN	<input type="checkbox"/> Disabled	Details
5 LAN 3 as WAN	<input type="checkbox"/> Disabled	Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP ON [Details](#)

PEPWAVE_EBB4

SpeedFusion Cloud

SFC (1 - Default)	Established
SFC (2 - WAN Smoothing)	Established
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)	

Create an outbound policy to steer the internet traffic to go into Speedfusion Cloud. Please go to **Advanced > Outbound Policy**, click on **Add Rule** to create a new outbound policy.

The screenshot shows the Peplink PEPWAVE web interface. The top navigation bar includes: Dashboard, SpeedFusion Cloud, Network, **Advanced**, AP, System, Status, and Apply Changes. The left sidebar lists various configuration categories: Advanced (SpeedFusion, IPsec VPN, GRE Tunnel, **Outbound Policy**, Port Forwarding), NAT Mappings, QoS (User Groups, Bandwidth Control, Application), Firewall (Access Rules, Content Blocking), Routing Protocols (OSPF & RIPv2, BGP), Remote User Access, and Misc. Settings (High Availability, RADIUS Server, Certificate Manager, Service Forwarding, Service Passthrough, GPS Forwarding, NTP Server, Grouped Networks).

The main content area displays the **Outbound Policy** configuration page. A modal window titled **Add a New Custom Rule** is open, showing the following configuration details:

- Service Name:** to_internet
- Enable:**
- Source:** IP Address, 192.168.50.10
- Destination:** Any
- Protocol:** Any, Protocol Selection ::
- Algorithm:** Priority
- Priority Order:**

Priority Order	Not In Use
Highest Priority	
Cloud: SFC (1 - Defau...	
Cloud: SFC (2 - WAN ...	
WAN: WAN 1	
WAN: WAN 2	
WAN: Cellular 1	
WAN: Cellular 2	
WAN: Cellular 3	
WAN: Cellular 4	
WAN: USB	
WAN: Wi-Fi WAN	
WAN: LAN 1 as WAN	
WAN: LAN 2 as WAN	
WAN: LAN 3 as WAN	
Lowest Priority	
- When No Connections are Available:** Drop the Traffic
- Terminate Sessions on Connection Recovery:** Enable

Buttons for **Save** and **Cancel** are located at the bottom right of the modal.

Outbound Policy ?

Custom ✎

Rules 👉 Drag and drop rows by the left to change rule order ?

Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes SpeedFusion Cloud Routes					
to internet	Priority VPN: SFC (1 - Def...	IP Address 192.168.50.10	Any	Any	✖
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				
Add Rule					

Expert Mode ?

Enabled ✎

12.3 Connect Clients to Cloud

SpeedFusion Cloud provides a convenient way to route the LAN client to the cloud. From **SpeedFusion Cloud > Connect Clients to Cloud**.

peplink **Dashboard** **SpeedFusion Cloud** Network AP System Status Apply Changes

 **SpeedFusion Cloud**

Aggregate your bandwidth, connect you to different geo-location, and more.



Choose Cloud Location

Which cloud you'd like to connect?



Connect Clients to Cloud

Select a cloud for your laptops, phones, or other devices.

Choose a client from the drop down list > Click + > Save > Apply Changes.

SpeedFusion Cloud > Connect Clients to Cloud

Traffic from the selected clients will be redirected to the assigned cloud.

SpeedFusion Cloud			
Automatic	Client	IP Address	
	MY-Room-A-DellPC (40:23:43:26:F7:93)	192.168.52.179	✖
	---		+

Save

12.4 Link Wi-Fi to Cloud

SpeedFusion Cloud provides a convenient way to route the Wi-Fi client to the cloud from **SpeedFusion Cloud > Link Wi-Fi to Cloud**. This option is available for **Balance 20X, Balance 30 Pro, and Balance One**.

SpeedFusion Cloud

Aggregate your bandwidth, connect you to different geo-location, and more.

- Choose Cloud Location**
 Which cloud you'd like to connect?
- Connect Clients to Cloud**
 Select a cloud for your laptops, phones, or other devices.
- Link Wi-Fi to Cloud**
 Create a Wi-Fi SSID that is dedicated for the cloud.

Create a new SSID for SpeedFusion Cloud. The new SSID will inherit all settings from one of the existing SSIDs including the Security Policy. Then click **Save** follow by **Apply Changes**.

SpeedFusion Cloud > Link Wi-Fi to Cloud

The new SSID will inherit all settings from the existing SSID including the Security Policy.

SpeedFusion Cloud			
Automatic	Reference SSID	SSID for Cloud	
	Home	Home_SFC	

Save

SpeedFusion Cloud SSID will be shown on **Dashboard**.

LAN Interface

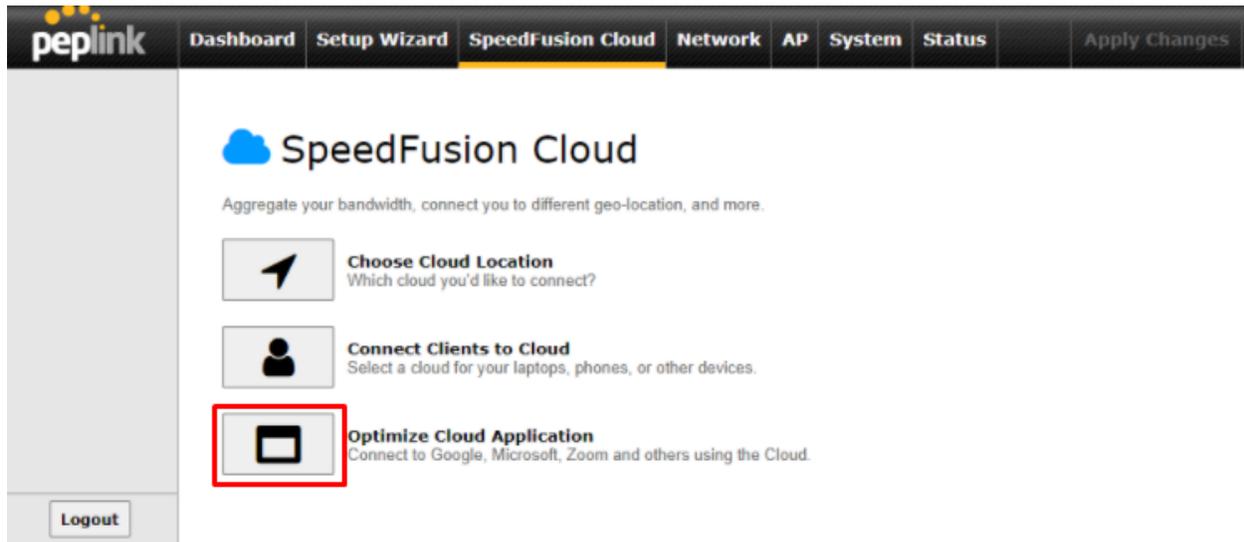
Router IP Address: 192.168.54.1

Wi-Fi AP ON **Details**

HomeBunker	Home	Home_SFC	
------------	------	----------	--

12.5 Optimize Cloud Application

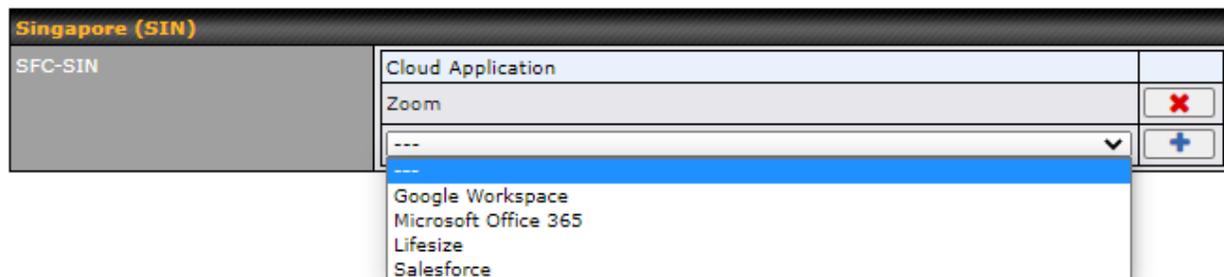
Optimize Cloud Application allows you to route Internet traffic through SpeedFusion Cloud based on the application. Go to **SpeedFusion Cloud > Optimize Cloud Application**.



Select a Cloud application to route through SpeedFusion Cloud from the drop down list > Click  > Save > Apply Changes. Click the  to remove a selected Cloud application from routing through SpeedFusion Cloud.

SpeedFusion Cloud > Optimize Cloud Application

Traffic of the selected cloud application will be redirected to the assigned cloud.



13 Network Tab

13.1 WAN

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

WAN Connection Settings ?	
WAN Connection Name	WAN
Enable	<input type="checkbox"/>
Connection Method ?	DHCP ▼
Routing Mode ?	<input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
Hostname (Optional) ?	<input type="text"/> <input type="checkbox"/> Use custom hostname
Management IP Address	<input type="text"/> 255.255.255.0 (/24) ▼
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
Connection Priority	<input checked="" type="radio"/> Always-on (Priority 1) <input type="radio"/> Backup
Independent from Backup WANs ?	<input type="checkbox"/>
Reply to ICMP Ping ?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Upload Bandwidth ?	<input type="text" value="100"/> Mbps ▼
Download Bandwidth ?	<input type="text" value="100"/> Mbps ▼

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:

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:																	
	<ul style="list-style-type: none"> DHCP <table border="1"> <tr> <td>Connection Method</td> <td><input type="text" value="DHCP"/></td> </tr> <tr> <td>Routing Mode</td> <td><input checked="" type="radio"/> NAT</td> </tr> <tr> <td>Hostname (Optional)</td> <td><input type="text"/> <input type="checkbox"/> Use custom hostname</td> </tr> </table>	Connection Method	<input type="text" value="DHCP"/>	Routing Mode	<input checked="" type="radio"/> NAT	Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname											
	Connection Method	<input type="text" value="DHCP"/>																
	Routing Mode	<input checked="" type="radio"/> NAT																
	Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname																
	<ul style="list-style-type: none"> Static IP <table border="1"> <tr> <td>Connection Method</td> <td><input type="text" value="Static IP"/></td> </tr> <tr> <td>Routing Mode</td> <td><input checked="" type="radio"/> NAT</td> </tr> <tr> <td>IP Address</td> <td><input type="text"/></td> </tr> <tr> <td>Subnet Mask</td> <td><input type="text" value="255.255.255.0 (/24)"/></td> </tr> <tr> <td>Default Gateway</td> <td><input type="text"/></td> </tr> </table>	Connection Method	<input type="text" value="Static IP"/>	Routing Mode	<input checked="" type="radio"/> NAT	IP Address	<input type="text"/>	Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>	Default Gateway	<input type="text"/>							
	Connection Method	<input type="text" value="Static IP"/>																
	Routing Mode	<input checked="" type="radio"/> NAT																
	IP Address	<input type="text"/>																
	Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>																
Default Gateway	<input type="text"/>																	
<ul style="list-style-type: none"> PPPoE <table border="1"> <tr> <td>Connection Method</td> <td><input type="text" value="PPPoE"/></td> </tr> <tr> <td>Routing Mode</td> <td><input checked="" type="radio"/> NAT</td> </tr> <tr> <td>PPPoE User Name</td> <td><input type="text"/></td> </tr> <tr> <td>PPPoE Password</td> <td><input type="text"/></td> </tr> <tr> <td>Confirm PPPoE Password</td> <td><input type="text"/></td> </tr> <tr> <td>Service Name (Optional)</td> <td><input type="text"/> <small>Leave it blank unless it is provided by ISP</small></td> </tr> <tr> <td>IP Address (Optional)</td> <td><input type="text"/> <small>Leave it blank unless it is provided by ISP</small></td> </tr> <tr> <td>Keep-Alive Interval</td> <td><input type="text" value="6"/> seconds(s)</td> </tr> <tr> <td>Keep-Alive Retry</td> <td><input type="text" value="6"/></td> </tr> </table>	Connection Method	<input type="text" value="PPPoE"/>	Routing Mode	<input checked="" type="radio"/> NAT	PPPoE User Name	<input type="text"/>	PPPoE Password	<input type="text"/>	Confirm PPPoE Password	<input type="text"/>	Service Name (Optional)	<input type="text"/> <small>Leave it blank unless it is provided by ISP</small>	IP Address (Optional)	<input type="text"/> <small>Leave it blank unless it is provided by ISP</small>	Keep-Alive Interval	<input type="text" value="6"/> seconds(s)	Keep-Alive Retry	<input type="text" value="6"/>
Connection Method	<input type="text" value="PPPoE"/>																	
Routing Mode	<input checked="" type="radio"/> NAT																	
PPPoE User Name	<input type="text"/>																	
PPPoE Password	<input type="text"/>																	
Confirm PPPoE Password	<input type="text"/>																	
Service Name (Optional)	<input type="text"/> <small>Leave it blank unless it is provided by ISP</small>																	
IP Address (Optional)	<input type="text"/> <small>Leave it blank unless it is provided by ISP</small>																	
Keep-Alive Interval	<input type="text" value="6"/> seconds(s)																	
Keep-Alive Retry	<input type="text" value="6"/>																	
<ul style="list-style-type: none"> L2TP 																		

Connection Method	L2TP
Routing Mode	<input checked="" type="radio"/> NAT
L2TP User Name	<input type="text"/>
L2TP Password	<input type="text"/>
Confirm L2TP Password	<input type="text"/>
Server IP Address / Host	<input type="text"/>
Address Type	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP

- **GRE**

Connection Method	GRE
Routing Mode	<input checked="" type="radio"/> NAT
WAN IP Address	<input type="text"/>
WAN Subnet Mask	255.255.255.0 (/24)
WAN Default Gateway	<input type="text"/>
Remote GRE Host	<input type="text"/>
Tunnel Local IP Address	<input type="text"/>
Tunnel Remote IP Address	<input type="text"/>
Outgoing NAT IP Address	<input type="text"/>

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 icon.

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.

Management IP Address

Management IP Address is available for configuration when you click the link in the help icon via the Hostname.

This option allows you to configure the management IP address for the DHCP WAN connection.

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 the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.

<p>Connection Priority</p>	<p>This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only.</p> <p>If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections.</p> <p>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.</p>
<p>Independent from Backup WANs</p>	<p>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.</p>
<p>Reply to ICMP PING</p>	<p>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.</p> <p>Default: ticked (Yes)</p>
<p>Upload Bandwidth</p>	<p>This field refers to the maximum upload speed.</p> <p>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.</p>
<p>Download Bandwidth</p>	<p>This field refers to the maximum download speed.</p> <p>Default weight control for outbound traffic will be adjusted according to this value.</p>

WAN Connection Settings (Cellular)

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

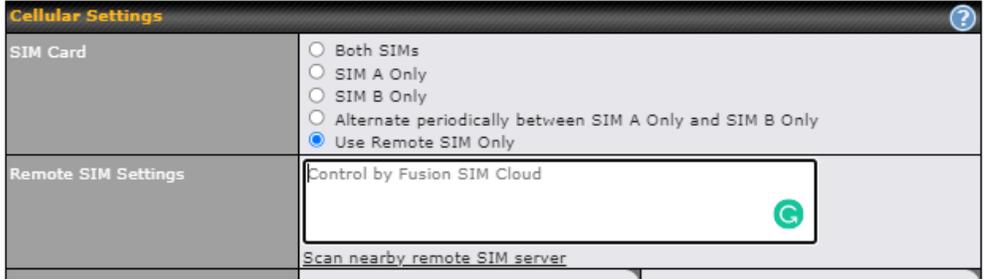
WAN Connection Settings ?	
WAN Connection Name	<input type="text" value="Cellular 1"/>
Enable	<input checked="" type="checkbox"/>
Routing Mode ?	<input checked="" type="radio"/> NAT
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
Connection Priority	<input checked="" type="radio"/> Always-on (Priority 1) <input type="radio"/> Backup
Independent from Backup WANs ?	<input type="checkbox"/>
Standby State ?	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Idle Disconnect	<input type="checkbox"/>
Reply to ICMP Ping ?	<input checked="" type="radio"/> Yes <input type="radio"/> No

WAN 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	<p>This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding.</p> <p>In the case if you need to choose IP Forwarding for your scenario. Click the ? button to enable IP Forwarding.</p>
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>
Connection	This option allows you to configure the WAN connection whether for normal daily usage or as

<p>Priority</p>	<p>a backup connection only.</p> <p>If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections.</p> <p>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.</p>
<p>Independent from Backup WANs</p>	<p>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.</p>
<p>Idle Disconnect</p>	<p>If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default.</p>
<p>Reply to ICMP PING</p>	<p>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.</p> <p>Default: ticked (Yes)</p>

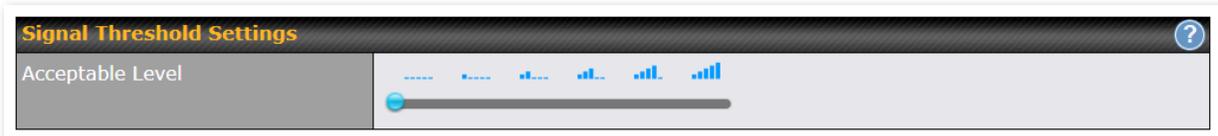
Cellular Settings ?		
SIM Card	<input checked="" type="radio"/> Both SIMs <input type="radio"/> SIM A Only <input type="radio"/> SIM B Only <input type="radio"/> Alternate periodically between SIM A Only and SIM B Only <input type="radio"/> Use Remote SIM Only	
Preferred SIM Card	<input checked="" type="radio"/> No preference <input type="radio"/> SIM A <input type="radio"/> SIM B	
	SIM Card A	SIM Card B
Carrier Selection ?	<input checked="" type="radio"/> Auto	<input checked="" type="radio"/> Auto
LTE/3G ?	Auto ▾	Auto ▾
Optimal Network Discovery ?	<input type="checkbox"/>	<input type="checkbox"/>
Band Selection	Auto ▾	Auto ▾
Data Roaming	<input type="checkbox"/>	<input type="checkbox"/>
Authentication	Auto ▾	Auto ▾
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	<input type="text"/>	<input type="text"/>
Username	<input type="text"/>	<input type="text"/>
Password	<input type="text"/>	<input type="text"/>
Confirm Password	<input type="text"/>	<input type="text"/>
SIM PIN (Optional) ?	<input type="text"/> <input type="text"/> (Confirm)	<input type="text"/> <input type="text"/> (Confirm)
Bandwidth Allowance Monitor ?	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
Action ?	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day ?	On <input type="text" value="1st"/> of each month at 00:00 midnight	On <input type="text" value="1st"/> of each month at 00:00 midnight
Monthly Allowance ?	<input type="text"/> GB ▾	<input type="text"/> GB ▾

Cellular Settings	
SIM Card	Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards. For routers that support the SIM Injector, you may select the "Use Remote SIM Only" to provision a SIM from a SIM Injector. Further details on the SIM Injector found is available here: https://www.peplink.com/products/sim-injector/ .
Preferred SIM	If "Both SIMs" were selected on the above field, then you can designate the priority of the

Card	SIM card slots here.
Remote SIM Settings	<p>If “Use Remote SIM Only” is selected in the SIM card section, the Remote SIM Settings will be shown.</p>  <p>You may need to enable the remote SIM Host settings in the Remote SIM management, see the section 13.14.7 or Appendix C for more details on FusionSIM. After that, click on “Scan nearby remote SIM server” to show the serial number(s) of the connected SIM Injector(s).</p> <p>If you want to select a specific SIM, in the Cellular Settings, type “:” and then the number of the SIM slot, eg.1111-2222-3333:7.</p>
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



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 / RSRP	-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:	<input type="text" value="n/a"/>	dBm (Recovery: <input type="text" value="n/a"/> dBm)
	SINR:	<input type="text" value="n/a"/>	dB (Recovery: <input type="text" value="n/a"/> dB)
3G	RSSI:	<input type="text" value="n/a"/>	dBm (Recovery: <input type="text" value="n/a"/> dBm)

WAN Connection Settings (USB)

WAN Connection Settings	
WAN Connection Name	<input type="text" value="Mobile Internet"/>
Enable	<input checked="" type="checkbox"/> Always on
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
Connection Priority	<input type="radio"/> Always-on (Priority 1) <input checked="" type="radio"/> Backup <input type="text" value="Priority 2"/>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Idle Disconnect	<input type="checkbox"/>
Reply to ICMP Ping	<input checked="" type="radio"/> Yes <input type="radio"/> No

WAN Connection Settings	
WAN Connection Name	Indicate a name you wish to give 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.
DNS Server	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.
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

	<p>priority of other WAN connections.</p> <p>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.</p>
Standby State	This option allows you to choose whether to remain the connection connected or disconnect it when this WAN connection is no longer in the highest priority and has entered the standby state.
Idle Disconnect	If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default.
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 (Yes)

By default, the USB port is “USB Modem” mode. If you need to use it to connect to USB Ethernet Adapter, you need to change it to “USB Ethernet” mode, by enabling the hidden feature . Once this feature is enabled, the interface will behave as normal Ethernet WAN. The options that are the same as the ethernet WAN connection configuration are shown in the Ethernet WAN section.

Modem Settings	
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Dial Number	<input type="text"/>
SIM PIN (Optional)	<input type="text"/> <input type="text"/> (Confirm)

ModemSettings	
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.

WAN Connection Settings (Common)

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

Physical Interface Settings	
Port Speed	<input type="text" value="Auto"/>
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="1440"/>
MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
MAC Address Clone	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="10:56:CA:15:92:5D"/>
VLAN	<input type="checkbox"/>

Physical Interface Settings	
Speed	<p>This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems.</p> <p>When a static speed is set, you may choose whether to advertise its speed to the peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device.</p> <p>Default: Auto</p>
MTU	<p>This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value. Default value is 1440.</p>
MSS	<p>This field is for specifying the Maximum Segment Size of the WAN connection.</p> <p>When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections.</p> <p>Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections.</p> <p>Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size.</p> <p>Default: Auto</p>
MAC Address Clone	<p>Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.</p>
VLAN	<p>Check the box to assign a VLAN to the interface.</p>

DHCP Settings	
Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text" value="1.1.1.1"/> DNS Server 2: <input type="text" value="8.8.8.8"/>

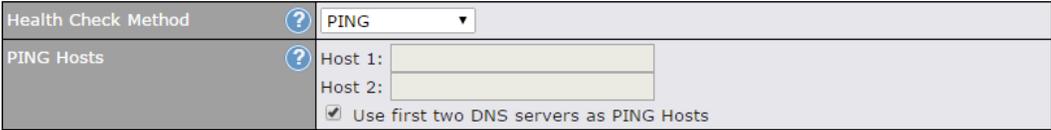
DHCP Settings	
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with a hostname, you can safely bypass this option.
DNS Servers	<p>Each ISP may provide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

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	
 <p>The screenshot shows the 'Health Check Method' dropdown menu set to 'Disabled'. Below the dropdown, a red error message reads: 'Health Check disabled. Network problem cannot be detected.'</p>	
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	
 <p>The screenshot shows the 'Health Check Method' dropdown menu set to 'PING'. Below it, there are two input fields for 'Host 1' and 'Host 2'. A checkbox labeled 'Use first two DNS servers as PING Hosts' is checked.</p>	
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: <input type="text"/> ? Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers

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

Health Check DNS Servers

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

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

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

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

Health Check Method: HTTP

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

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

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

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

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

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

Other Health Check Settings

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

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

Note

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

For example, if WAN1, WAN2, and WAN3 have connection types of **Always-on**, **Backup Priority Group 1**, and **Backup Priority Group 2**, respectively, when WAN1 goes down, WAN2 and WAN3 will try to connect. If WAN3 is connected first, WAN2 will still be kept connecting. If WAN2 is connected, WAN3 will disconnect or 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	<input checked="" type="checkbox"/> Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On <input type="text" value="1st"/> of each month at 00:00 midnight
Monthly Allowance	<input type="text"/> GB

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

Disclaimer

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	<div style="border: 1px solid #ccc; padding: 5px;"> IP Address <input type="text"/> Subnet Mask <input type="text" value="255.255.255.255 (/32)"/> </div> <div style="text-align: center; margin: 5px 0;">↓</div> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right; margin-top: 5px;"><input type="button" value="X"/></div> <p style="font-size: small; margin-top: 5px;">Those settings will not be saved until the save button below has been pressed.</p>

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**.

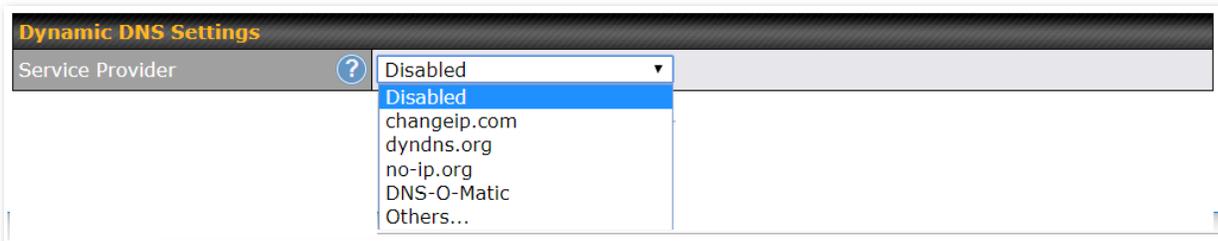
Dynamic DNS Settings

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**.



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

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

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

Important Note

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

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

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

13.2 LAN

13.2.1 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 (/24) ▼

IP Settings

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

Network Settings ? [Close](#)

Name	<input type="text"/>	Help To define a layer-2 bridging based PepVPN, please click here .
VLAN ID	<input type="text"/>	
Inter-VLAN routing	<input checked="" type="checkbox"/>	

Network Settings

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	<input type="checkbox"/> No profile is available	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.
Spanning Tree Protocol	<input type="checkbox"/>	
Override IP Address when bridge connected	<input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None	
DHCP Server		

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	<input checked="" type="checkbox"/>	Enable	
DHCP Server Logging	<input type="checkbox"/>		
IP Range	<input type="text"/> - <input type="text"/>	255.255.255.0 (/24) ▾	
Lease Time	1	Days 0	Hours 0 Mins
DNS Servers	<input checked="" type="checkbox"/>	Assign DNS server automatically	
WINS Servers	<input type="checkbox"/>	Assign WINS server	
BOOTP	<input type="checkbox"/>		
Extended DHCP Option	Option	Value	
	<i>No Extended DHCP Option</i>		
	Add		
DHCP Reservation	<input checked="" type="checkbox"/>	Name	MAC Address
			00:00:00:00:00:00
		Static IP	+

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

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

13.2.2 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.

[^] - Advanced feature, please click the ? button on the top right hand corner of the Static Route session to activate and configure Virtual Network Mapping to resolve network address conflict with remote peers.

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 networks.

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	<input type="checkbox"/>

WINS Server Settings

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

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

DNS Proxy Settings																			
Enable	<input checked="" type="checkbox"/>																		
DNS Caching	<input type="checkbox"/>																		
Include Google Public DNS Servers	<input type="checkbox"/>																		
Local DNS Records	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td style="text-align: center;">+</td> </tr> </tbody> </table>	Host Name	IP Address				+												
Host Name	IP Address																		
		+																	
Domain Lookup Policy	<table border="1"> <thead> <tr> <th>Domain</th> <th>Connection</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td style="text-align: center;">+</td> </tr> </tbody> </table>	Domain	Connection				+												
Domain	Connection																		
		+																	
DNS Resolvers	<table border="1"> <thead> <tr> <th>WAN Connection</th> <th>DNS Servers</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> WAN 1</td> <td>1.1.1.1 1.0.0.1</td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 3</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 4</td> <td>8.8.8.8 8.8.4.4</td> </tr> <tr> <td><input type="checkbox"/> WAN 5</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Mobile Internet</td> <td></td> </tr> <tr> <th>LAN Connection</th> <th>DNS Servers</th> </tr> <tr> <td><input type="checkbox"/> Untagged LAN</td> <td></td> </tr> </tbody> </table> <p>Preferred connections are shown with <input checked="" type="checkbox"/></p>	WAN Connection	DNS Servers	<input type="checkbox"/> WAN 1	1.1.1.1 1.0.0.1	<input type="checkbox"/> WAN 2		<input type="checkbox"/> WAN 3		<input type="checkbox"/> WAN 4	8.8.8.8 8.8.4.4	<input type="checkbox"/> WAN 5		<input type="checkbox"/> Mobile Internet		LAN Connection	DNS Servers	<input type="checkbox"/> Untagged LAN	
WAN Connection	DNS Servers																		
<input type="checkbox"/> WAN 1	1.1.1.1 1.0.0.1																		
<input type="checkbox"/> WAN 2																			
<input type="checkbox"/> WAN 3																			
<input type="checkbox"/> WAN 4	8.8.8.8 8.8.4.4																		
<input type="checkbox"/> WAN 5																			
<input type="checkbox"/> Mobile Internet																			
LAN Connection	DNS Servers																		
<input type="checkbox"/> Untagged LAN																			

DNS Proxy Settings

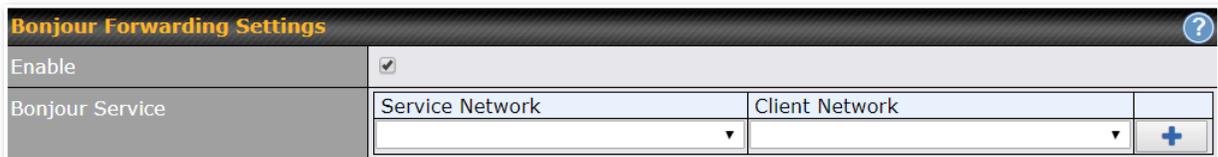
Enable To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**.
A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN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

DNS Caching This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This

	feature can improve DNS response time by storing all received DNS results for faster DNS lookup. However, it cannot return the most updated result for frequently updated DNS records. By default, DNS Caching is disabled.
Include Google Public DNS Servers	When this option is enabled, the DNS proxy server will forward DNS requests to Google's public DNS servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Peplink Balance, the corresponding IP address will be returned. To display the option to set TTL manually, click  . Click  to create a new record. Click  to remove a record.
Domain Lookup Policy	DNS proxy will look up the domain names defined here using only the specified connections.
DNS Resolvers^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.

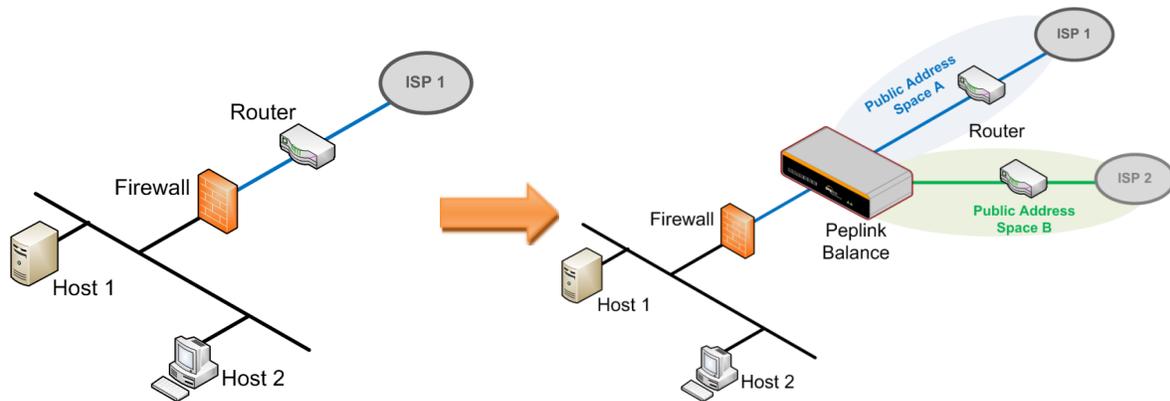


Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	Choose Service and Client networks from the drop-down menus, and then click  to add the networks. To delete an existing Bonjour listing, click  . Bonjour Forwarding is supported on All Balance models, MAX 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	<input checked="" type="checkbox"/>
WAN for Drop-In Mode ?	WAN 1 ▾
Share Drop-In IP ?	<input checked="" type="checkbox"/>
Shared IP Address ?	<input type="text"/> 255.255.255.0 (/24) ▾
WAN Default Gateway ?	<input type="text"/> <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) <input type="text"/> - <input type="text"/> <input type="button" value="↓"/> <input type="text"/> <input type="button" value="Delete"/>
WAN DNS Servers ?	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
<p>NOTE: The DHCP Server Settings will be overwritten.</p> <p>The following WAN 1 settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.</p> <p>The PPTP Server will be disabled.</p> <p>Tip: please review the DNS Forwarding setting under the Service Forwarding section.</p>	

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

WAN Default Gateway

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.

13.2.3 Port Settings

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

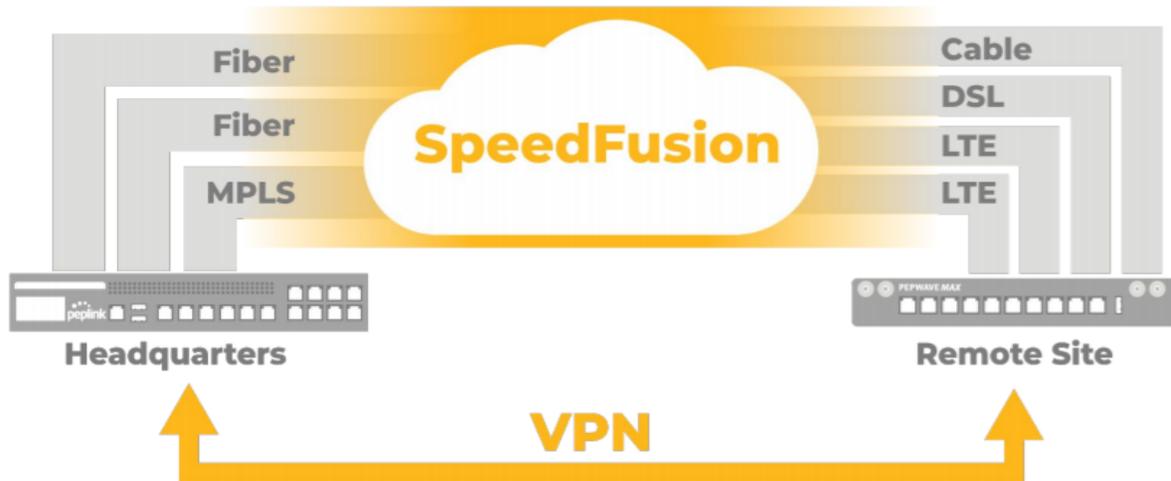
Port Settings						
	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port 1 	<input checked="" type="checkbox"/>			Trunk ▼	Any ▼
2	LAN Port 2	<input type="checkbox"/>	Auto ▼	<input checked="" type="checkbox"/>	Trunk ▼	Any ▼
3	LAN Port 3	<input checked="" type="checkbox"/>			Trunk ▼	Any ▼

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)

13.3 VPN

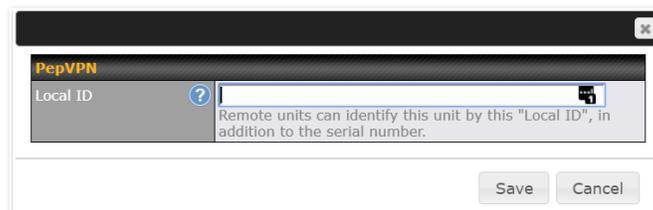
13.3.1 SpeedFusion



Peplink Balance SpeedFusion™ Bandwidth Bonding is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion securely connects one or more branch offices to your company's main headquarters or to other branches. The data, voice, and video communications between these locations are kept confidential across the public Internet.

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

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



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

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

SpeedFusion Profiles

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

The local LAN subnet and subnets behind the LAN (defined under Static Route on the LAN Settings page) will be advertised to the VPN. All VPN members will be able to route to local subnets.

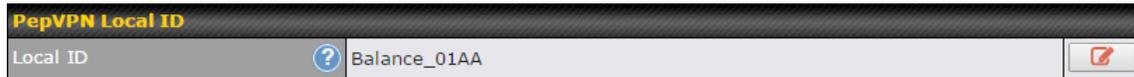
Send All Traffic To	?
No PepVPN profile selected	
<input type="button" value="↗"/>	

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:

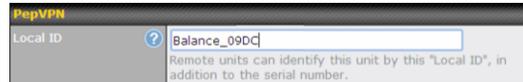
Send All Traffic	
Send All Traffic To	<input checked="" type="checkbox"/> Balance 2929-2929-2929 ▼ DNS Server: <input type="text" value="8.8.8.8"/> <input type="text" value="8.8.4.4"/>
	<input checked="" type="checkbox"/> Backup Site Balance-4848-4848-4848 ▼ DNS Server: <input type="text" value="8.8.8.8"/> <input type="text" value="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.

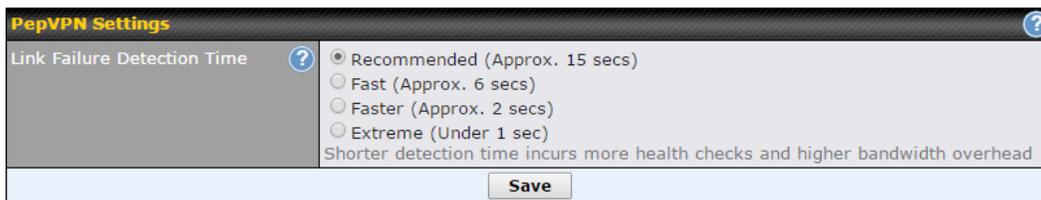


PepVPN Local ID

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



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



Link Failure Detection

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

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

Link Failure Detection Time

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

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

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

Important Note

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

SpeedFusion: Profile Configuration

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

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

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

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

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

Limit	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	<p>While using PepVPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN's available bandwidth.</p> <p>Off - Disable WAN Smoothing.</p> <p>Normal - The total bandwidth consumption will be at most 2x of the original data traffic.</p> <p>Medium - The total bandwidth consumption will be at most 3x of the original data traffic.</p> <p>High - The total bandwidth consumption depends on the number of connected active tunnels.</p>

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

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

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

WAN Connection Priority	
WAN Connection Priority	<p>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.</p> <p>To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the  button.</p>

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>

13.3.2 IPsec VPN

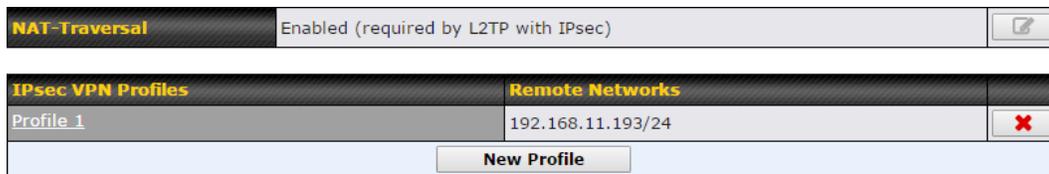
Peplink Balance IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

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 > VPN > IPsec VPN**.



A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown.

NAT-Traversal should be enabled if your system is behind a NAT router.

Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Peplink Balance, Cisco, or Juniper Routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.

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

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

Encapsulation	
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 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

WAN Connection Priority	
Priority	WAN Selection
1	WAN <input type="text"/>
2	----- <input type="text"/>

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

13.3.3 GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. A GRE tunnel is similar to IPsec or PepVPN.

To configure a GRE Tunnel, navigate to **Network > VPN > GRE Tunnel**.

GRE Tunnel Profiles	Remote Networks
No GRE profile defined	
<input type="button" value="New Profile"/>	

Click the **New Profile** button to create new GRE tunnel profiles that establish tunnel connections to remote tunnel endpoints via available WAN connections. To edit the profiles, click on its associated connection name in the leftmost column.

GRE Tunnel Profile ✕

Name	<input type="text"/>		
Active	<input checked="" type="checkbox"/>		
Remote GRE IP Address	<input type="text"/>		
Tunnel Local IP Address	<input type="text"/>		
Tunnel Remote IP Address	<input type="text"/>		
Tunnel Subnet Mask	<input checked="" type="radio"/> Auto <input type="radio"/> <input type="text" value="255.255.255.0 (/24)"/>		
Connection	WAN ▼		
Remote Networks	Network	Subnet Mask	
	<input type="text"/>	<input type="text" value="255.255.255.0 (/24)"/>	+

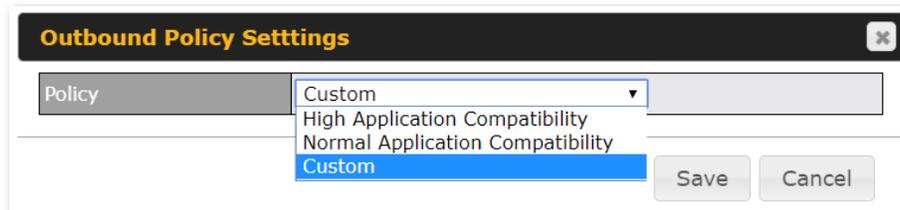
GRE Tunnel Profile Settings

Name	This field is for specifying a name to represent this GRE Tunnel connection profile.
Active	When this box is checked, this GRE Tunnel connection profile will be enabled. Otherwise, it will be disabled.
Remote GRE IP Address	This field is for entering the remote GRE's IP address
Tunnel Local IP Address	This field is for specifying the tunnel source IP address.
Tunnel Remote IP Address	This field is for specifying the tunnel destination IP address
Tunnel Subnet Mask	This field is to select the subnet mask that is to be used for the GRE tunnel.
Connection	Select the appropriate WAN connection from the drop-down menu.
Remote Networks	Input the LAN and subnets that are located at the remote site here.

13.4 Outbound Policy

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

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



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

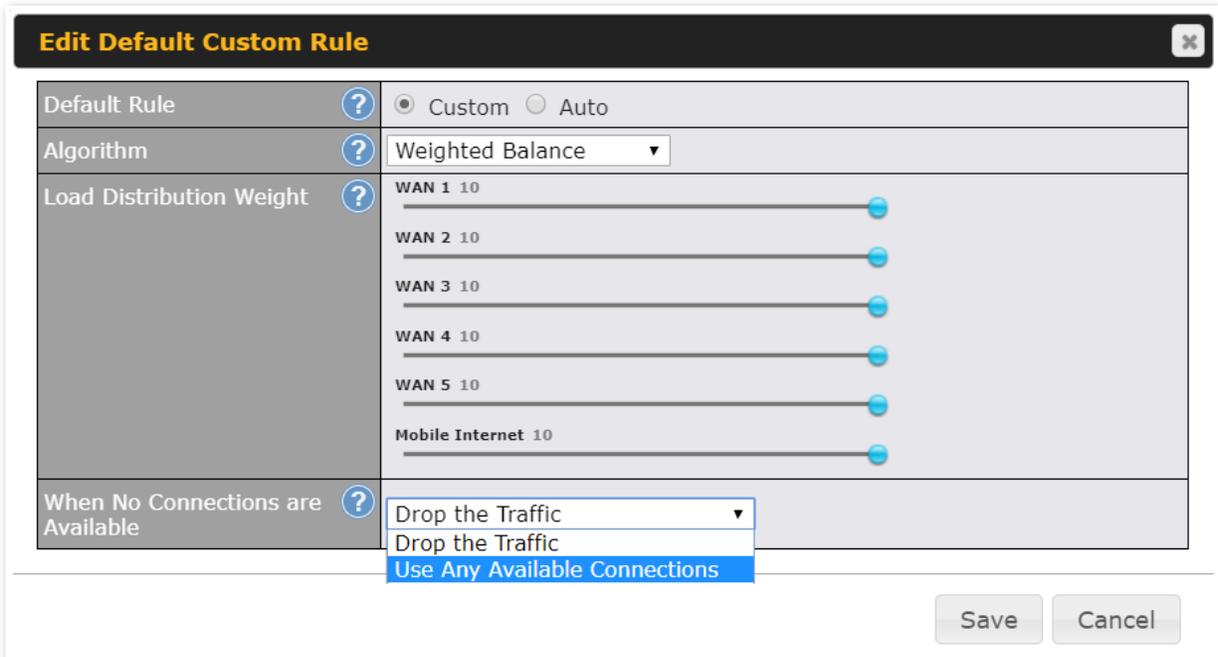
Outbound Policy Settings	
High Application Compatibility	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the highest application compatibility.
Normal Application Compatibility	Outbound 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:



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

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



Edit Default Custom Rule	
Default Rule	<input checked="" type="radio"/> Custom <input type="radio"/> Auto
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic Drop the Traffic Use Any Available Connections

Save Cancel

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

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

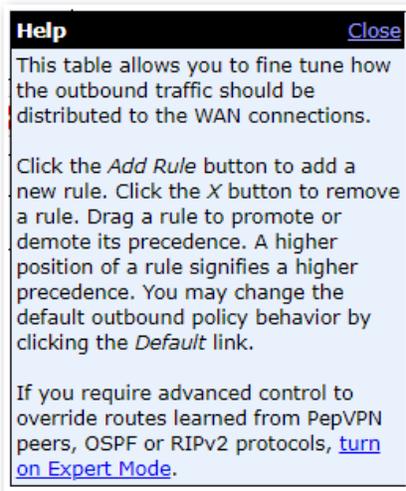
Add a New Custom Rule
✕

Service Name	<input style="width: 90%;" type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Source	Any ▾
Destination	? IP Network ▾ <input style="width: 80px;" type="text"/> Mask: 255.255.255.0 (/24) ▾
Protocol	? Any ▾ ← :: Protocol Selection :: ▾
Algorithm	? Weighted Balance ▾
Load Distribution Weight	? <div style="margin-top: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 2px;"> WAN 1 10 <input style="width: 80%; border: none; border-bottom: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 2px;"> WAN 2 10 <input style="width: 80%; border: none; border-bottom: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 2px;"> WAN 3 10 <input style="width: 80%; border: none; border-bottom: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 2px;"> WAN 4 10 <input style="width: 80%; border: none; border-bottom: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 2px;"> WAN 5 10 <input style="width: 80%; border: none; border-bottom: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; align-items: center;"> Mobile Internet 10 <input style="width: 80%; border: none; border-bottom: 1px solid #ccc;" type="text"/> </div> </div>
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	<p>This setting specifies whether the outbound traffic rule takes effect. When Enable is checked, the rule takes effect: traffic is matched and actions are taken by the 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.</p> <p>Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.</p>
Source	This setting specifies the source IP address, IP network, MAC address or Grouped network for traffic that matches the rule.

	
<p>Destination</p>	<p>This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, PepVPN Profile or Grouped network for traffic that matches the rule.</p>  <p>If Domain Name is chosen and a domain name, such as <i>foobar.com</i>, is entered, any outgoing accesses to <i>foobar.com</i> and <i>*.foobar.com</i> will match this criterion. You may enter a wildcard (.) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter <i>foobar.*</i>, for example, <i>www.foobar.com</i>, <i>www.foobar.co.jp</i>, or <i>foobar.co.uk</i> will also match. Placing wildcards in any other position is not supported.</p> <p>NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, access to any one of the server names will also match this rule.</p>
<p>Protocol and Port</p>	<p>This setting specifies the IP protocol and port of traffic that matches this rule. Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> • Any • TCP • UDP • IP • DSCP <p>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.</p>
<p>Algorithm</p>	<p>This setting specifies the behavior of the Pepwave router for the custom rule.</p> <p>One of the following values can be selected (note that some Pepwave routers provide only some of these options):</p> <ul style="list-style-type: none"> • Weighted Balance • Persistence • Enforced • Priority • Overflow • Least Used • Lowest Latency

	<ul style="list-style-type: none"> • Fastest Response Time <p>For a full explanation of each Algorithm, please see the following article: https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithms-work/8059</p>
Load Distribution Weight	This is to define the outbound traffic weight ratio for each WAN connection.
When No connections are available	<p>This field allows you to configure the default action when all the selected Connections are not available.</p> <p>Drop the Traffic - Traffic will be discarded.</p> <p>Use Any Available Connections - Traffic will be routed to any available Connection, even it is not selected in the list.</p> <p>Fall-through to Next Rule - Traffic will continue to match next Outbound Policy rule just like this rule is inactive.</p>
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 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.



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**.

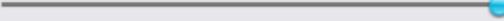
In Expert Mode, a new special rule, **SpeedFusion™ Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion™ routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets will be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

above the bar to override the SpeedFusion™ routes.

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

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	<input type="text" value="Weighted Balance"/>
Load Distribution Weight	<p>WAN 1 10 </p> <p>WAN 2 10 </p> <p>WAN 3 10 </p> <p>WAN 4 10 </p> <p>WAN 5 10 </p> <p>Mobile Internet 10 </p>

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	 <input checked="" type="radio"/> By Source <input type="radio"/> 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	? <ul style="list-style-type: none"> WAN: WAN 1 <li style="background-color: #0070C0; color: white;">WAN: WAN 1 WAN: WAN 2 WAN: WAN 3 WAN: WAN 4 WAN: WAN 5 WAN: Mobile Internet
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

Priority Order	?	Highest Priority	Not In Use
		WAN: WAN	
		WAN: Cellular 1	
		WAN: Cellular 2	
		WAN: USB	
		WAN: LAN 1 as WAN	
		WAN: GRE WAN 1	
		WAN: GRE WAN 2	
		WAN: OpenVPN WAN 1	
		Lowest Priority	
When No Connections are Available	?	Drop the Traffic	
Terminate Sessions on Connection Recovery	?	<input type="checkbox"/> 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	? <table border="1"> <tr> <td>Highest Priority</td> </tr> <tr> <td>WAN: WAN 1</td> </tr> <tr> <td>WAN: WAN 2</td> </tr> <tr> <td>WAN: Wi-Fi WAN</td> </tr> <tr> <td>WAN: Cellular 1</td> </tr> <tr> <td>WAN: Cellular 2</td> </tr> <tr> <td>WAN: USB</td> </tr> <tr> <td>Lowest Priority</td> </tr> </table>	Highest Priority	WAN: WAN 1	WAN: WAN 2	WAN: Wi-Fi WAN	WAN: Cellular 1	WAN: Cellular 2	WAN: USB	Lowest Priority
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	<input style="width: 90%;" type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Source	Any ▾
Destination	? IP Network ▾ <input style="width: 100px;" type="text"/> Mask: 255.255.255.0 (/24) ▾
Protocol	? Any ▾ ← :: Protocol Selection :: ▾
Algorithm	? Least Used ▾
Connection	<input type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> 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	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Source	Any ▾
Destination	<input type="text" value="IP Network"/> ▾ <input type="text" value="Mask: 255.255.255.0 (/24)"/> ▾
Protocol	Any ▾ ◀ :: Protocol Selection :: ▾
Algorithm	<input type="text" value="Lowest Latency"/> ▾ <small>Note: Use of Lowest Latency will incur additional network usage.</small>
Connection	<input type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input type="checkbox"/> Mobile Internet
When No Connections are Available	<input type="text" value="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

Add a New Custom Rule
✕

Service Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Source	Any ▾
Destination	<input type="text" value="IP Network"/> ▾ <input style="width: 100px; margin-left: 10px;" type="text"/> Mask: <input type="text" value="255.255.255.0 (/24)"/> ▾
Protocol	<input type="text" value="Any"/> ▾ ← <input type="text" value=":: Protocol Selection ::"/> ▾
Algorithm	Fastest Response Time ▾
Connection	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input type="checkbox"/> Mobile Internet
When No Connections are Available	<input type="text" value="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.

13.5 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.

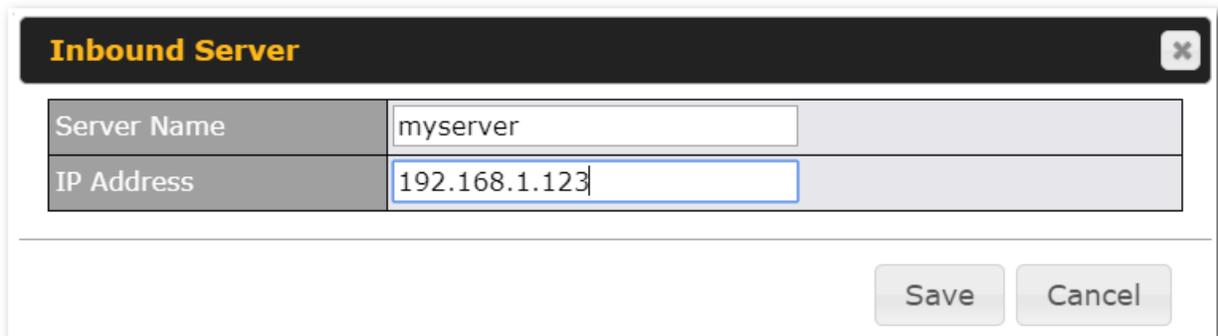
13.5.1 Servers

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.



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



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



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

13.5.2 Services

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

Service	IP Address(es)	Server	Protocol
No Services Defined			
<input type="button" value="Add Service"/>			

Tip

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

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

Inbound Service ✕

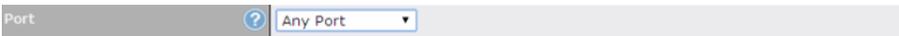
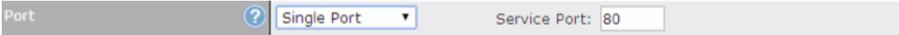
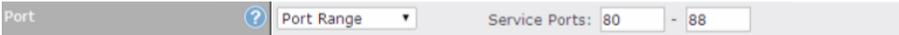
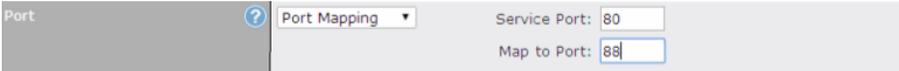
Enable	<input checked="" type="checkbox"/>
Service Name	<input type="text"/>
Protocol	TCP ▾ ◀ :: Protocol Selection :: ▾
Port	Any Port ▾
Inbound IP Address(es) (Require at least one IP address)	<div style="background-color: #1a3d54; color: white; padding: 2px;"> Connection / IP Address(es) All Clear </div> <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input type="checkbox"/> Mobile Internet <input type="checkbox"/> PepVPN
Included Server(s) (Require at least one IP address)	<div style="background-color: #1a3d54; color: white; padding: 2px;"> Server </div> <input type="checkbox"/> 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	<p>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.</p> <p>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.).</p> <p>After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and the port number will remain manually modifiable.</p>
Port	<p>The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p> <p>Any Port, Single Port, Port Range, Port Map, and Range Mapping</p> <div data-bbox="440 751 1339 787" data-label="Form">  </div> <p>Any Port: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP and Port is set to Any Port, then all TCP traffic will be forwarded to the configured servers.</p> <div data-bbox="440 928 1339 963" data-label="Form">  </div> <p>Single Port: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP, Port is set to Single Port, and Service Port is set to 80, then TCP traffic received on Port 80 will be forwarded to the configured servers via port 80.</p> <div data-bbox="440 1136 1339 1171" data-label="Form">  </div> <p>Port Range: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP, Port is set to Port Range, and Service Port set to 80-88, then TCP traffic received on ports 80 through 88 will be forwarded to the configured servers via the respective ports.</p> <div data-bbox="440 1373 1339 1444" data-label="Form">  </div> <p>Port Mapping: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the Servers setting.</p> <p>For example, if IP Protocol is set to TCP, Port is set to Port Mapping, Service Port is set to 80, and Map to Port is set to 88, then TCP traffic on port 80 is forwarded to the configured servers via port 88.</p> <p>(Please see below for details on the Servers setting.)</p> <div data-bbox="440 1646 1339 1717" data-label="Form">  </div>

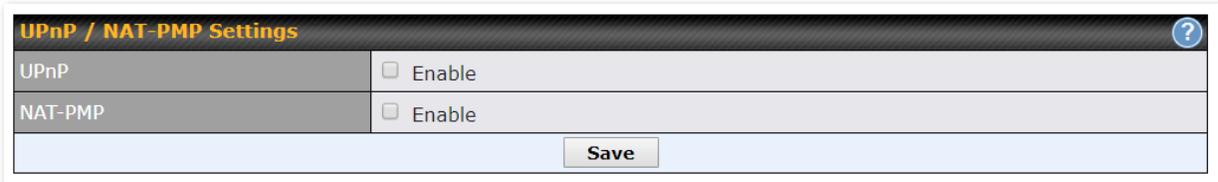
	Range Mapping: traffic that is received by Peplink Balance via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the Servers setting.
Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Included Server(s)	<p>This setting specifies the LAN servers that handle requests for the service, and the relative weight values. The amount of traffic that is distributed to a server is proportional to the weight value assigned to the server relative to the total weight.</p> <p>Example:</p> <p>With the following weight settings on a Peplink Balance:</p> <ul style="list-style-type: none"> demo_server_1: 10 demo_server_2: 5 <p>The total weight is 15 = (10 + 5)</p> <p>Matching traffic distributed to demo_server_1: 67% = (10 / 15) x 100%</p> <p>Matching traffic distributed to demo_server_2: 33% = (5 / 15) x 100%</p>

UPnP / NAT-PMP Settings

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

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

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



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

13.5.3 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

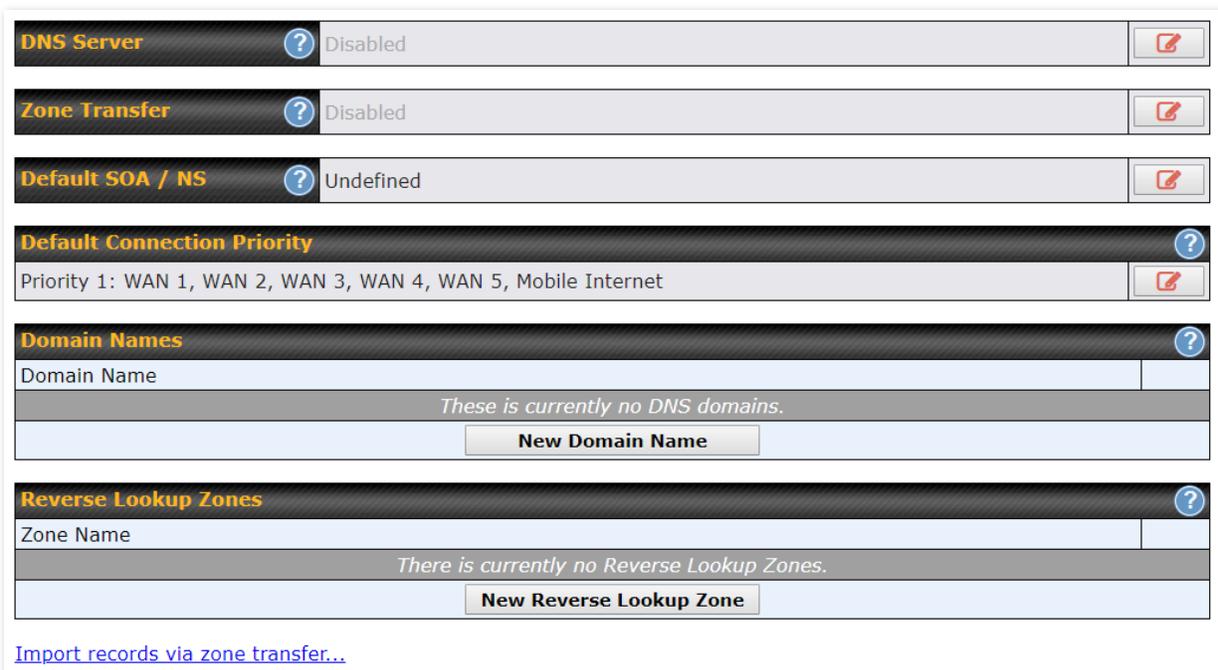
IP address for the domain name on the most appropriate healthy WAN connection. It can also act as a generic DNS server for hosting “A”, “CNAME”, “MX”, “TXT” and “NS” records.

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

Note: DNS names may only contain alphanumeric characters (A-Z and 0-9), hyphens (-), and periods (.). The period is only allowed when it is used to delimit the components of domain style names.

For more information, see the following websites:

- rfc952
- rfc1123



The screenshot shows the DNS Settings configuration page. It includes several sections:

- DNS Server:** Disabled (with a help icon and edit button).
- Zone Transfer:** Disabled (with a help icon and edit button).
- Default SOA / NS:** Undefined (with a help icon and edit button).
- Default Connection Priority:** Priority 1: WAN 1, WAN 2, WAN 3, WAN 4, WAN 5, Mobile Internet (with a help icon and edit button).
- Domain Names:** A table with a header 'Domain Name' and a 'New Domain Name' button. Below the table, it says 'These is currently no DNS domains.'
- Reverse Lookup Zones:** A table with a header 'Zone Name' and a 'New Reverse Lookup Zone' button. Below the table, it says 'There is currently no Reverse Lookup Zones.'

At the bottom of the form, there is a link: [Import records via zone transfer...](#)

DNS Settings	
DNS Servers	<p>This setting specifies the WAN IP addresses on which the DNS server of the Peplink Balance should listen.</p> <p>If no addresses are selected, the inbound link load balancing feature will be disabled and the Peplink Balance will not respond to DNS requests.</p> <p>To specify and/or modify the IP addresses on which the DNS server should listen, click the button that corresponds to DNS Server, and a selection screen will be displayed:</p>

	<p>To specify the Internet IP addresses on which the DNS server should listen, select the desired WAN connection then select the desired associated IP addresses. (Multiple items in the list can be selected by holding CTRL and clicking on the items.)</p> <p>Click Save to save the settings when configuration is complete.</p>
Zone Transfer	<p>This setting specifies the IP address(es) of the secondary DNS server(s) authorized to retrieve zone records from the DNS server of the Peplink Balance.</p> <p>The zone transfer server of the Peplink Balance listens on TCP port 53.</p> <p>The Peplink Balance serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing its LAN interface.</p>
Routing Control by Subnet Database	<p>When this function is enabled, the system will check to see if an incoming DNS client is within any WAN's ISP subnet. Only the matched WAN(s)'s IP addresses will be returned. Note that this feature is available only when a subnet database has been defined.</p>
Default SOA / NS	<p>Click the <input type="button" value="Define"/> button to define a default SOA / NS record for all domain names.</p> <p>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.</p> <p>For defining default NS records, the host <i>[domain]</i> indicates that this record is for the domain name itself without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the Host field left empty. When the entered name server is a fully qualified domain name (FQDN), the IP Address field will be disabled.</p>
Default Connection Priority	<p>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.</p> <p>The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable.</p> <p>To specify the primary and backup connections, click the <input type="button" value="Define"/> button that corresponds to Default Connection Priority. A selection screen will appear.</p> <p>Each WAN connection is associated with a priority number. Click Save to save the settings when configuration is complete.</p>
Domain name	<p>This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its "NS", "MX" and "TXT" records, and its sub-domains' "A" and "CNAME" records. Add a new record by clicking the New Domain Name button. Click on a domain name to edit. Press the red X to remove a domain name.</p>

New Domain Name

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

SOA Record ?						
Use Default SOA and NS Records						

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

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

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

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

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

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

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

SOA Records

Default / Custom SOA Record
✕

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

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

SOA Record
✕

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

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**.

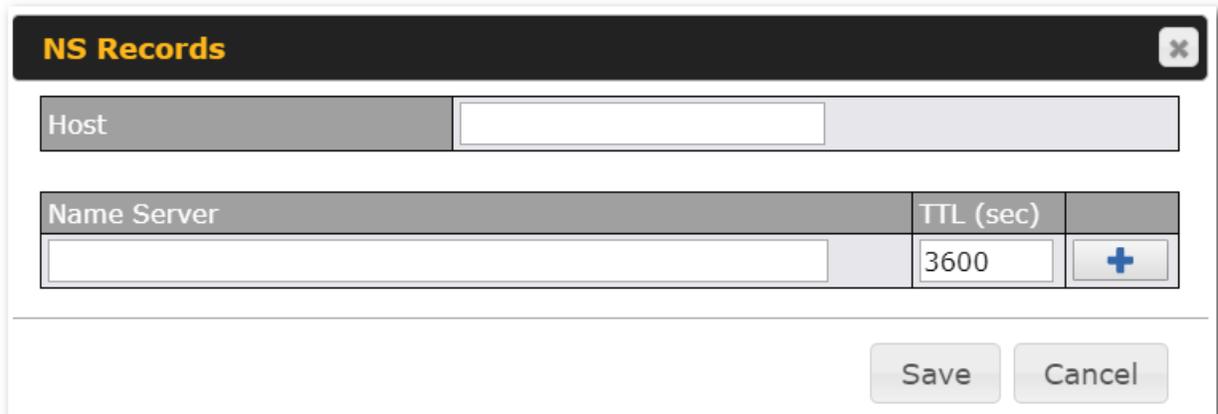
Default values are set for SOA and NS records,

- **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:



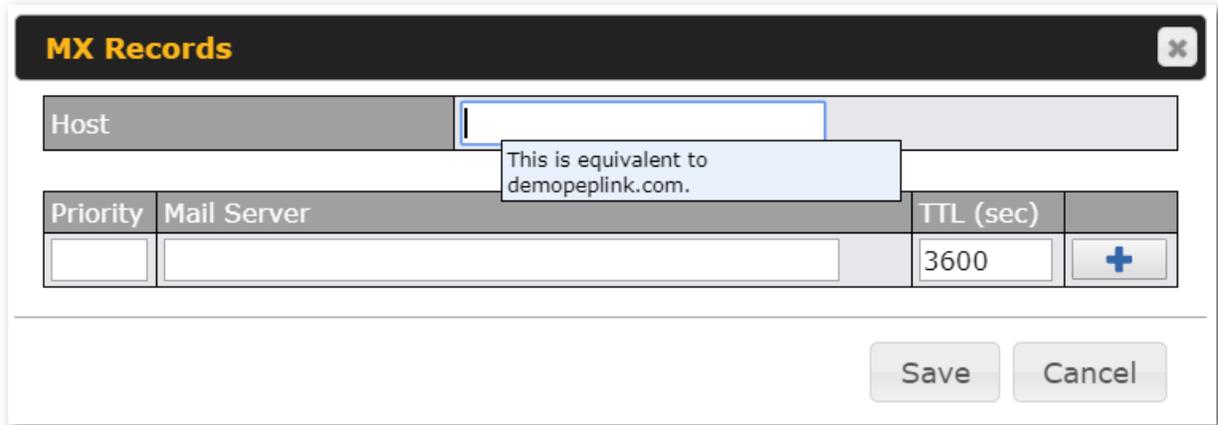
The screenshot shows a window titled "NS Records" with a close button (X) in the top right corner. Below the title bar, there is a "Host" label followed by an empty text input field. Underneath, there is a table with two columns: "Name Server" and "TTL (sec)". The "Name Server" column contains an empty text input field. The "TTL (sec)" column contains the value "3600" and a blue "+" button to its right. At the bottom of the window, there are two buttons: "Save" and "Cancel".

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:

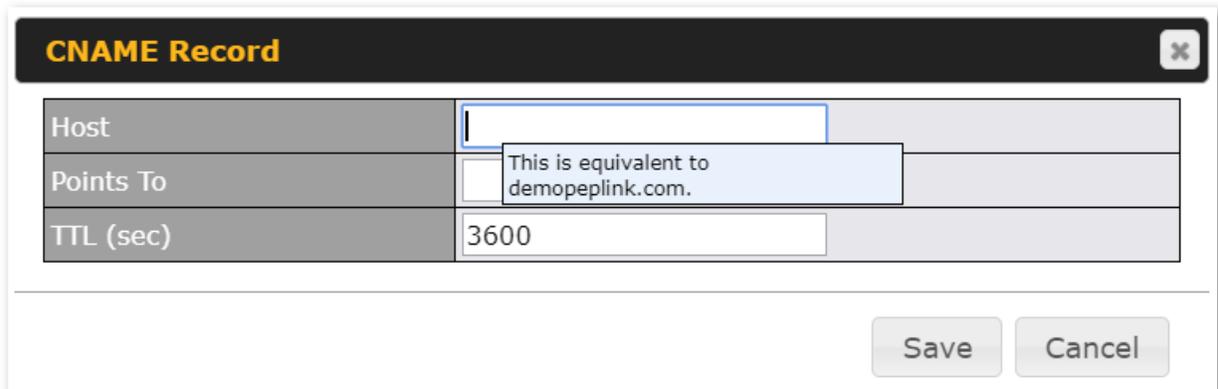


Priority	Mail Server	TTL (sec)	
<input type="text"/>	<input type="text"/>	3600	<input type="button" value="+"/>

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:



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

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	<input style="width: 90%;" type="text"/>
TTL (sec)	<input style="width: 20px;" type="text" value="5"/> <div style="border: 1px solid #ccc; padding: 2px; font-size: 0.8em; margin-left: 5px;">This is equivalent to demopeplink.com.</div>
Priority	<input checked="" type="radio"/> Default <input type="radio"/> Custom

Included IP Address(es)
<input type="checkbox"/> WAN 1
<input type="checkbox"/> WAN 2
<input type="checkbox"/> WAN 3
<input type="checkbox"/> WAN 4
<input type="checkbox"/> WAN 5
<input type="checkbox"/> Mobile Internet
<input type="checkbox"/> Custom IP Address

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

A Record	
Host Name	This field specifies the A record of this sub-domain to be served by the Peplink Balance. The wildcard character "*" is supported. The IP addresses of "*.domain.name" will be returned for every name ending with ".domain.name" except names that have their own records.
TTL	This setting specifies the time to live of this record in external DNS caches. In order to reflect any dynamic changes on the IP addresses in case of link failure and recovery, this value should be set to a smaller value, e.g., 5 secs, 60 secs, etc.

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

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	<input style="width: 90%;" type="text"/>
TXT Value	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"> <p>This is equivalent to demopeplink.com.</p> </div>
TTL (sec)	<input style="width: 90%;" type="text" value="3600"/>

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

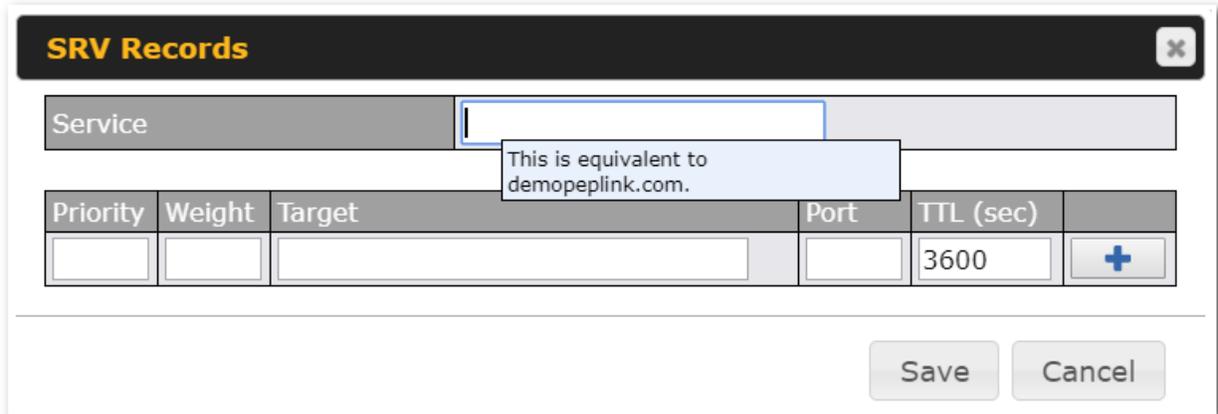
When creating a TXT record for the domain itself (not a sub-domain), the **Host** field should be left blank.

The maximum size of the TXT Value is 255 bytes.

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

SRV Records

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

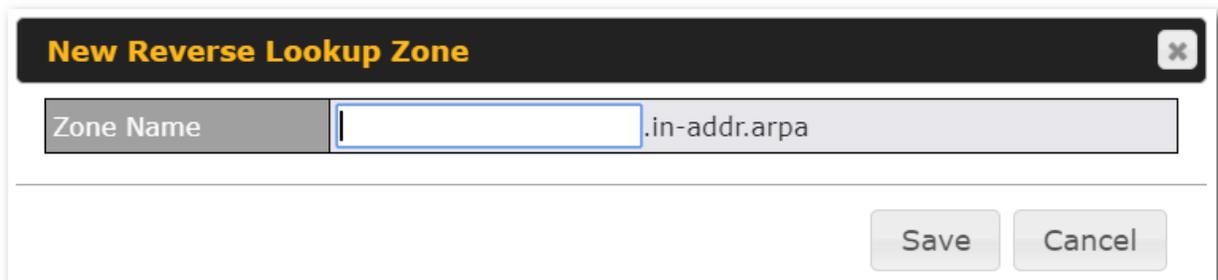


Priority	Weight	Target	Port	TTL (sec)	
				3600	+

- **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**.



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

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

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

- Create a reverse lookup zone that corresponds to the subnet network address of the host.
In the reverse lookup zone, add a pointer (PTR) resource record that maps the host IP address to

the host name.

- Click the **New Reverse Lookup Zone** button and enter a reverse lookup zone name. If you are delegated the subnet *11.22.33.0/24*, the **Zone Name** should be *33.22.11.in-addr.addr*. PTR records for *11.22.33.1*, *11.22.33.2*, ... *11.22.33.254* should be defined in this zone where the host IP numbers are *1*, *2*, ... *254*, respectively.

33.22.11.in-addr.arpa
✕

SOA Record
?

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

NS Records
?

Host	Name Server	TTL (sec)	
WARNING: You should define NS records in your zone!			
<input type="button" value="New NS Records"/>			

CNAME Records
?

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

PTR Records
?

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

SOA Record

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

SOA Record
✕

Name Server	?	<input style="width: 95%;" type="text"/>
Email	?	<input style="width: 95%;" type="text" value="webmaster"/>
Refresh (sec)	?	<input style="width: 95%;" type="text" value="14400"/>
Retry (sec)	?	<input style="width: 95%;" type="text" value="900"/>
Expire (sec)	?	<input style="width: 95%;" type="text" value="1209600"/>
Min Time (sec)	?	<input style="width: 95%;" type="text" value="3600"/>
TTL (sec)	?	<input style="width: 95%;" type="text" value="3600"/>

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

For example:

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

"ns2.mydomain.com."

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

NS Records

NS Records ✕

Host			
		This is equivalent to 33.22.11.in-addr.arpa.	
Name Server		TTL (sec)	
		3600	+

Save
Cancel

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

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

CNAME Records

CNAME Record ✕

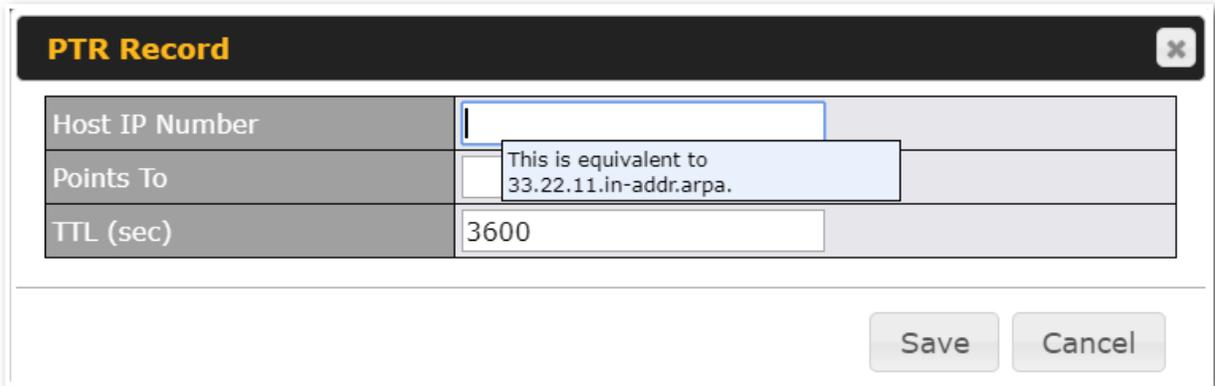
Host			
Points To		This is equivalent to 33.22.11.in-addr.arpa.	
TTL (sec)			
		3600	

Save
Cancel

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

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

PTR Records



PTR Record	
Host IP Number	<input type="text"/>
Points To	<input type="text"/> This is equivalent to 33.22.11.in-addr.arpa.
TTL (sec)	<input type="text" value="3600"/>

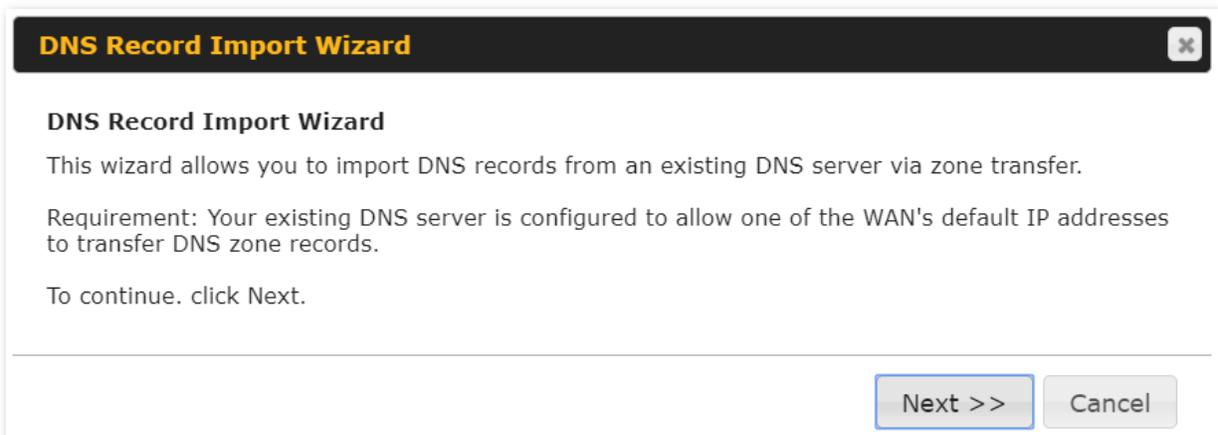
To create a new PTR record, click the **New PTR Record** button.

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

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
▼

<< Back
Next >>
Cancel

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

DNS Record Import Wizard
✕

Step 2 of 3

Domain Names (Zones):

mycompany.com
 peplink.com

(One domain name per line)

<< Back
Next >>
Cancel

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

Important Note

If you have entered domain(s) which already exist in your settings, a warning message will appear. Select **Next >>**

to overwrite the existing record or << **Back** to go back to the previous step.

DNS Record Import Wizard
✕

Step 2 of 3 (Continue)

WARNING: The following domain(s) already exist:

peplink.com

The existing records of these domains will be overwritten.

<< Back
Next >>
Cancel

DNS Record Import Wizard
✕

Fetching zone records...

Abort

DNS Record Import Wizard
✕

Step 3 of 3

Fetch Results

Domain	Result	Details
peplink.com	Ok	
mycompany.com	Ok	

Cancel

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

Zone: mytest.com

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

13.6 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**.



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 ?	<div style="background-color: #333; color: white; padding: 2px;">Connection / Inbound IP Address(es)</div> <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input type="checkbox"/> Mobile Internet <input type="checkbox"/> PepVPN													
Outbound Mappings ?	<div style="background-color: #333; color: white; padding: 2px;">Connection / Outbound IP Address</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>WAN 1</td> <td>10.22.1.182 (Interface IP) ▼</td> </tr> <tr> <td>WAN 2</td> <td>Interface IP ▼</td> </tr> <tr> <td>WAN 3</td> <td>Interface IP ▼</td> </tr> <tr> <td>WAN 4</td> <td>192.168.254.10 (Interface IP) ▼</td> </tr> <tr> <td>WAN 5</td> <td>Interface IP ▼</td> </tr> <tr> <td>Mobile Internet</td> <td>Interface IP ▼</td> </tr> </table>		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 ▼
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	<p>This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when IP Address is selected in the LAN Client(s) field.</p> <p>Note 1: Inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode.</p> <p>Note 2: Each WAN IP address can be associated to one NAT mapping only.</p>
Outbound Mappings	<p>This setting specifies the WAN IP addresses should be used when an IP connection is made from a LAN host to the Internet.</p> <p>Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility).</p> <p>Note 1: If you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the Outbound Policy section.</p> <p>Note 2: WAN connections in drop-in mode or IP forwarding mode are not shown here.</p>

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

Important Note

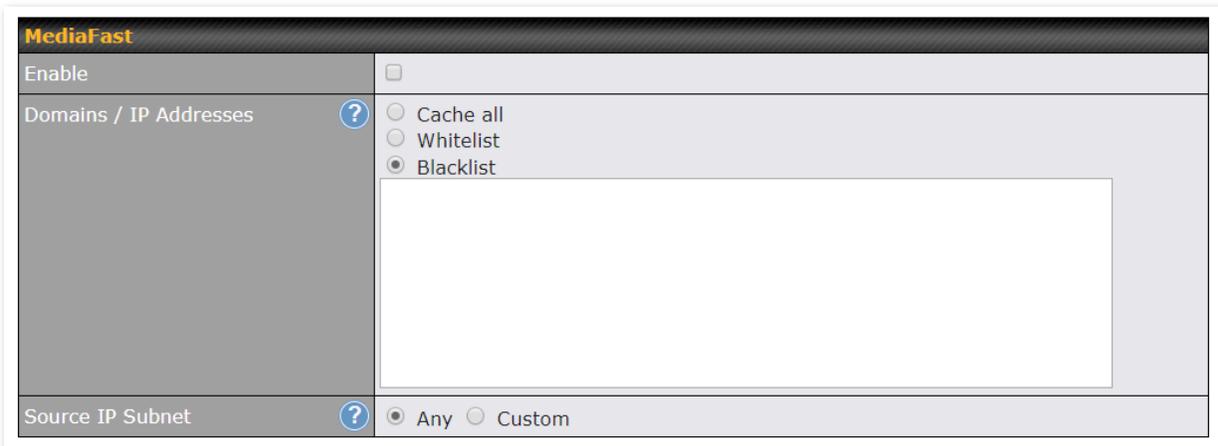
Inbound firewall rules override inbound mapping settings.

13.7 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	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.

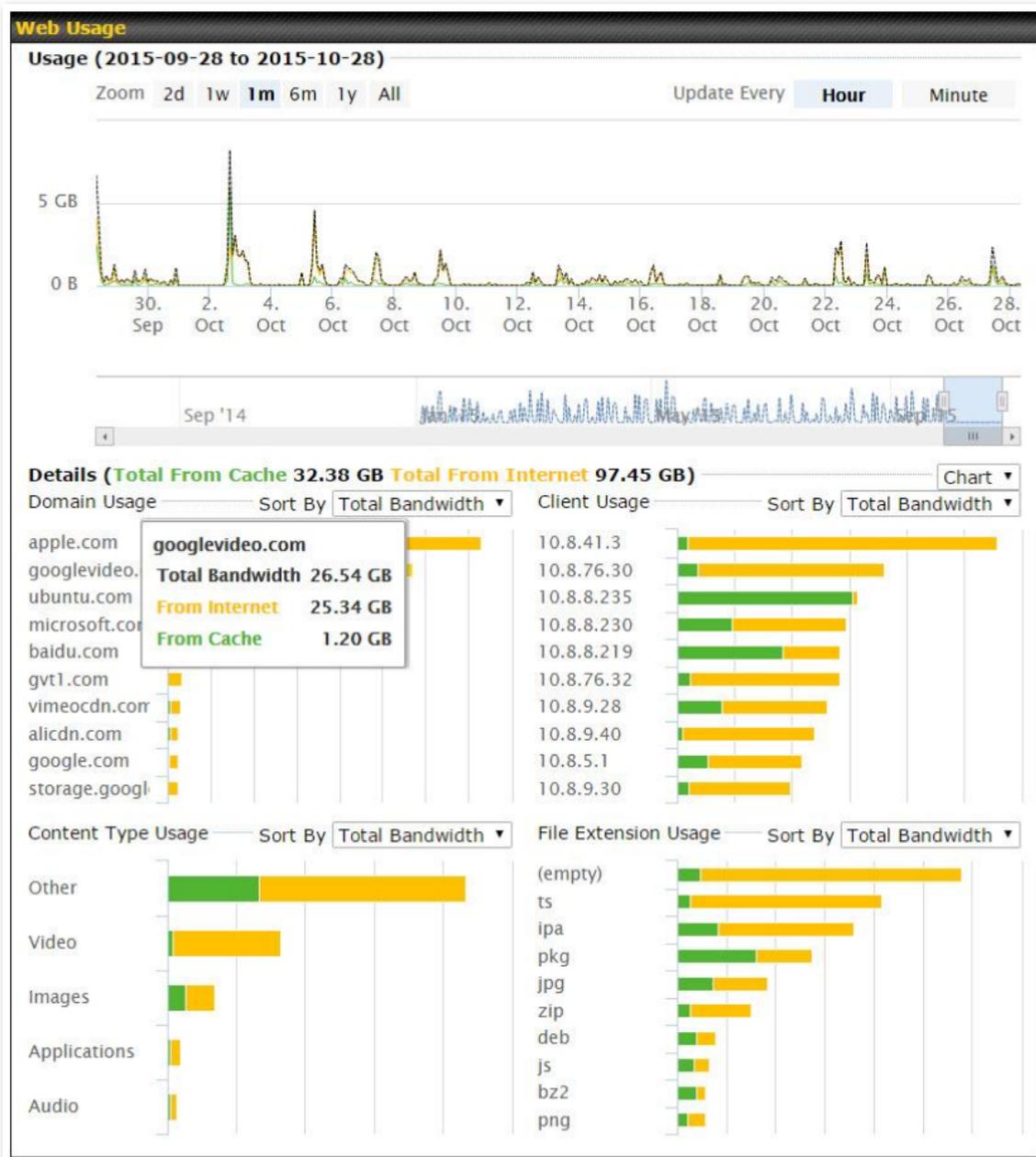
The **Secure Content Caching** menu operates identically to the **MediaFast** menu, except it is for secure content caching accessible through https://. In order for Mediafast devices to cache and deliver HTTPS content, every client needs to have the necessary certificates installed*.

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

Cache Control	
Content Type	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**.



Prefetch Schedule

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

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

Tools	
Clear Web Cache	Clear Statistics

Prefetch Schedule Settings	
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  .

Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:

New Schedule

MediaFast Schedule
✕

Name (optional)	<input style="width: 90%;" type="text"/>	
Active	<input checked="" type="checkbox"/>	
URL	<input style="width: 70%;" type="text"/>	<input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="button" value="+"/>
Depth	2 ▾ levels Default	
Time Period	From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾	
Repeat	Everyday ▾	
Bandwidth Limit	0 <input style="width: 40px;" type="text"/> Gbps ▾ (0: Unlimited)	

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.

13.8 ContentHub

Integrated into MediaFast-enabled routers, ContentHub allows you to deliver webpages and applications using the local storage on your router.

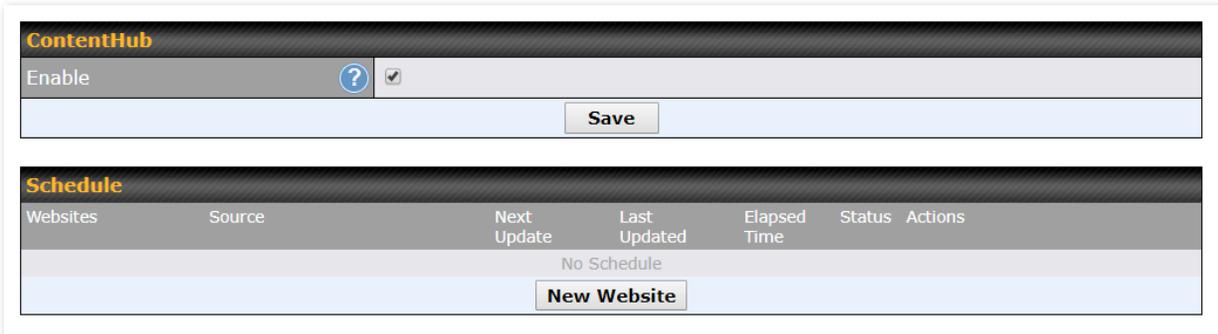
Users will be able to access news, articles, videos, and access your web app, without the need for internet access.

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		<input checked="" type="checkbox"/>				
<input type="button" value="Save"/>						
Schedule						
Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
No Schedule						
<input type="button" value="New Website"/>						

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.

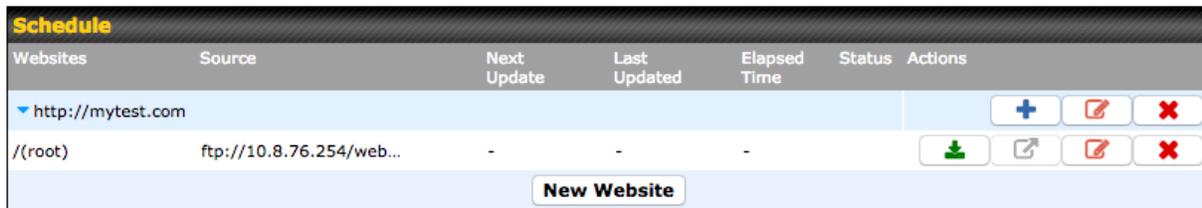
Click **New Website**, and the following configuration options will appear:

Schedule
✕

Active	<input checked="" type="checkbox"/>
Type	<input checked="" type="radio"/> Website <input type="radio"/> Application
Protocol	HTTP ▾
Domain/Path	? http:// <input style="width: 150px;" type="text"/>
Source	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> ftp ▾ :// Username: Password: </div> <div style="border: 1px solid #ccc; padding: 2px;"> <input style="width: 100%; height: 15px;" type="text"/> <input style="width: 100%; height: 15px;" type="text"/> <input style="width: 100%; height: 15px;" type="text"/> </div> </div>
Period	Everyday ▾ From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾
Bandwidth Limit	0 <input style="width: 40px;" type="text"/> Gbps ▾ (0: Unlimited)

Schedule	
Active	Checkbox toggles the activation of the content.
Type	This option allows you to select Website or Application
Protocol	HTTP,HTTPS or both
Domain/Path	The contenthub uses this as the domain name for client access (such as http://mytest.com).
Method	Only applicable for Application type: Choose between sync or file upload
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.
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:



Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▼ http://mytest.com						+ [edit] [delete]
/(root)	ftp://10.8.76.254/web...	-	-	-		↓ [refresh] [edit] [delete]

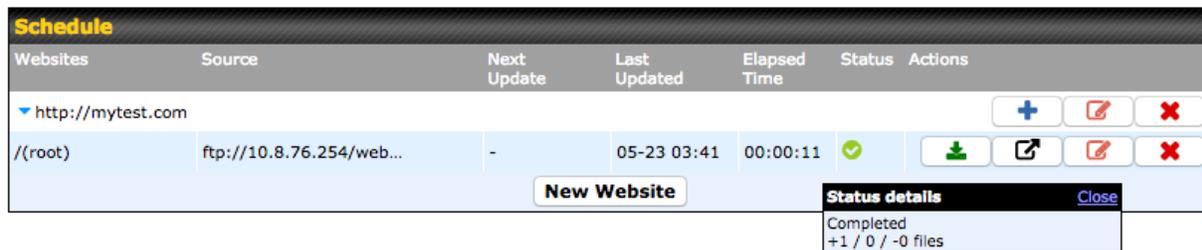
[New Website](#)

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:



Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▼ http://mytest.com						+ [edit] [delete]
/(root)	ftp://10.8.76.254/web...	-	05-23 03:41	00:00:11	✓	↓ [refresh] [edit] [delete]

[New Website](#)

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:

peplink

[Dashboard](#)
[Setup Wizard](#)
[Network](#)
[AP](#)
[System](#)
[Status](#)
Apply Changes

System

- Admin Security
- Firmware
- Time
- Schedule
- Email Notification
- Event Log
- SNMP
- InControl
- Configuration
- Feature Add-ons
- Reboot

Tools

- Ping
- Traceroute
- Wake-on-LAN
- Storage Manager
- Package Manager

Logout

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

Package List	Update All
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	<input checked="" type="checkbox"/>
Type	<input type="radio"/> Website <input checked="" type="radio"/> Application
Protocol	HTTP
Domain	http:// <input type="text"/>
Method	<input checked="" type="radio"/> Sync <input type="radio"/> File Upload
Source	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">ftp</div> <div style="border-bottom: 1px solid #ccc; flex-grow: 1;"></div> <div style="margin-right: 10px;">://</div> <div style="border-bottom: 1px solid #ccc; flex-grow: 1;"></div> </div> <div style="margin-top: 5px;">Username: <input style="width: 100%;" type="text"/></div> <div style="margin-top: 5px;">Password: <input style="width: 100%;" type="text"/></div>
Period	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">Everyday</div> <div style="margin-left: 10px;">⌵</div> </div> <div style="margin-top: 5px;"> From <input style="width: 30px;" type="text"/> : <input style="width: 30px;" type="text"/> to <input style="width: 30px;" type="text"/> : <input style="width: 30px;" type="text"/> </div>
Bandwidth Limit	<input style="width: 50px;" type="text"/> 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	<input checked="" type="checkbox"/>
Account Settings	<input type="radio"/> Follow Web Admin Account <input checked="" type="radio"/> Custom
Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

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

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).

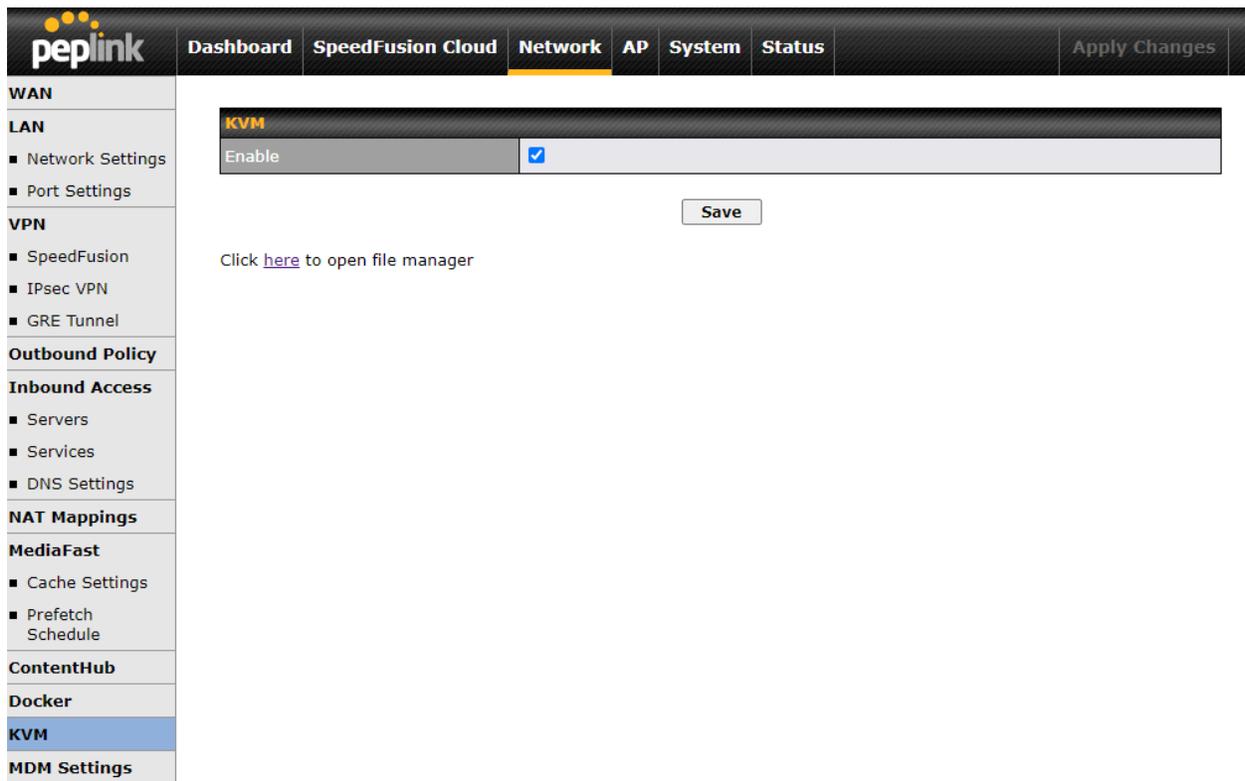
The Peplink router will search through the Docker Hub repository when creating a new Docker Container. <https://hub.docker.com/explore/> 7

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>

KVM

Mediafast enabled routers now support KVM. Users will have to download and install Virtual Machine Manager to manage the KVM virtual machines, through this users are able to virtualise the linux environment.

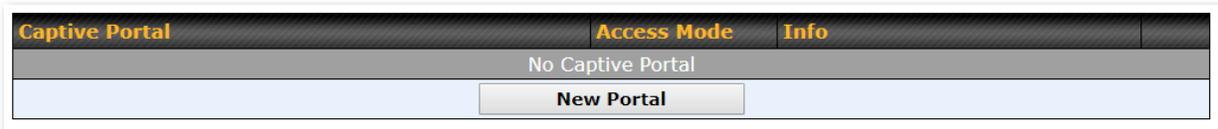


The screenshot displays the Peplink web management interface. At the top, there is a navigation bar with tabs for Dashboard, SpeedFusion Cloud, Network (selected), AP, System, and Status, along with an Apply Changes button. On the left, a sidebar menu lists various configuration categories: WAN, LAN (with sub-items Network Settings and Port Settings), VPN (with sub-items SpeedFusion, IPsec VPN, and GRE Tunnel), Outbound Policy, Inbound Access (with sub-items Servers, Services, and DNS Settings), NAT Mappings, MediaFast (with sub-items Cache Settings and Prefetch Schedule), ContentHub, Docker, KVM (highlighted in blue), and MDM Settings. The main content area shows the KVM configuration page. It features a 'KVM' header, an 'Enable' checkbox which is checked, and a 'Save' button. Below this, there is a text link: 'Click [here](#) to open file manager'.

For detailed configuration instructions please refer to our knowledge base:

<https://forum.peplink.com/t/how-to-install-virtual-machine-into-peplink-routers/29269>

13.9 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	<input type="text" value="demoportal"/>	
Enable	<input type="checkbox"/>	
Hostname	<input type="text" value="captive-portal.peplink.com"/> Default	
Access Mode	<input checked="" type="radio"/> Open Access <input type="radio"/> User Authentication <input type="radio"/> External Server	

Portal Access Settings

Access Quota	<input type="text" value="30"/> mins (0: Unlimited)
	<input type="text" value="0"/> MB (0: Unlimited)
Quota Reset Time	<input checked="" type="radio"/> Daily at <input type="text" value="00"/> :00 <input type="radio"/> 1440 minutes after quota reached
Inactive Timeout	<input type="text" value="0"/> minutes (0: No Timeout)
Allowed Networks	<input type="text" value="Domain Name / IP Address / Network"/> +
Allowed Clients	<input type="text" value="MAC / IP Address"/> +
Splash Page	<input checked="" type="radio"/> Built-in <input type="radio"/> External, URL: <input type="text" value="http://"/>
Popup Handling	<input type="checkbox"/> Bypass Popup (Redirection only takes place on normal browser) <input type="checkbox"/> Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	<input type="text" value="(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	<p>This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:</p> <table border="1" data-bbox="553 779 1382 976"> <tr> <td>Authentication</td> <td colspan="2">RADIUS Server ▾</td> </tr> <tr> <td>Auth Server</td> <td><input type="text"/></td> <td>Port 1812 Default</td> </tr> <tr> <td>Auth Server Secret</td> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>CoA-DM</td> <td colspan="2"><input type="checkbox"/></td> </tr> <tr> <td>Accounting Server</td> <td><input type="text"/></td> <td>Port 1813 Default</td> </tr> <tr> <td>Accounting Server Secret</td> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Accounting Interim Interval</td> <td><input type="text"/></td> <td>seconds</td> </tr> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	RADIUS Server ▾		Auth Server	<input type="text"/>	Port 1812 Default	Auth Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters	CoA-DM	<input type="checkbox"/>		Accounting Server	<input type="text"/>	Port 1813 Default	Accounting Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters	Accounting Interim Interval	<input type="text"/>	seconds
Authentication	RADIUS Server ▾																					
Auth Server	<input type="text"/>	Port 1812 Default																				
Auth Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters																				
CoA-DM	<input type="checkbox"/>																					
Accounting Server	<input type="text"/>	Port 1813 Default																				
Accounting Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters																				
Accounting Interim Interval	<input type="text"/>	seconds																				
LDAP Server	<p>This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:</p> <table border="1" data-bbox="553 1199 1377 1352"> <tr> <td>Authentication</td> <td colspan="2">LDAP Server ▾</td> </tr> <tr> <td>LDAP Server</td> <td><input type="text"/></td> <td>Port 389 Default</td> </tr> <tr> <td></td> <td colspan="2"><input type="checkbox"/> Use DN/Password to bind to LDAP Server</td> </tr> <tr> <td>Base DN</td> <td colspan="2"><input type="text"/></td> </tr> <tr> <td>Base Filter</td> <td colspan="2"><input type="text"/></td> </tr> </table> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>	Authentication	LDAP Server ▾		LDAP Server	<input type="text"/>	Port 389 Default		<input type="checkbox"/> Use DN/Password to bind to LDAP Server		Base DN	<input type="text"/>		Base Filter	<input type="text"/>							
Authentication	LDAP Server ▾																					
LDAP Server	<input type="text"/>	Port 389 Default																				
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server																					
Base DN	<input type="text"/>																					
Base Filter	<input type="text"/>																					
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	<p>Clients will get disconnected when the inactive the configured time is reached. Default 0: no timeout</p>
Allowed Networks	<p>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.</p>
Allowed Clients	<p>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.</p>
Splash Page	<p>Here, you can choose between using the Balance's built-in captive portal and redirecting clients to a URL you define.</p>
Popup Handling	<p>Configurable options for popup handling:</p> <ul style="list-style-type: none"> - Bypass Popup (Redirection only takes place on normal browser) - Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	<p>A hostname that can be used to logout captive portal when being accessed on browser.</p>
Customize splash page	<p>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.</p>

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	<input checked="" type="checkbox"/>
Custom Landing Page	<input type="checkbox"/>

Page: Login Edit mode ON ?

Login
TNC
Success
Quota reached

Save

13.10 QoS

13.10.1 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 ▾ <input style="width: 100%;" type="text"/>
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.

13.10.2 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	<input checked="" type="checkbox"/>		
	↕	↕	
Bandwidth %	Manager	Staff	Guest
	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	<input checked="" type="checkbox"/>				
User Bandwidth Limit	Download		Upload		
	Manager: Unlimited		Unlimited		
	Staff:	0 Mbps	0 Mbps	(0: unlimited)	
	Guest:	0 Mbps	0 Mbps	(0: unlimited)	

13.10.3 Application

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

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

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

Application	Priority			
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High	— Normal	↑ High	✘
All Email Protocols	↑ High	↑ High	↑ High	✘
MySQL	↑ High	— Normal	↓ Low	✘
SIP	↑ High	↓ Low	↓ Low	✘
<input type="button" value="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.

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.

13.11 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)

Internal Network (VLAN to VLAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

13.11.1 Access Rules

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

Outbound Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any		
Default	Any	Any	Any		

Add Rule

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

Add a New Outbound Firewall Rule ✕

New Firewall Rule

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

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

Inbound Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Protocol	WAN	Source	Destination	Action
test	Any	Any	Any	Any	
Default	Any	Any	Any	Any	

Add Rule

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

Add a New Inbound Firewall Rule
✕

New Firewall Rule

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

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

Internal Network Firewall Rules (👤 Drag and drop rows by the left to change rule order) ?					
Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	📄	✖
Default	Any	Any	Any	✔	
<input type="button" value="Add Rule"/>					

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

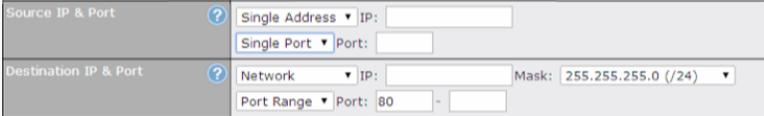
Add a New Internal Network Firewall Rule

New Firewall Rule	
Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Protocol	<input type="text" value="Any"/> ← :: Protocol Selection :: ▾
Source	<input type="text" value="Any Address"/> ▾
Destination	<input type="text" value="Any Address"/> ▾
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save Cancel

Inbound / Outbound / Internal Network Firewall Settings

Rule Name	This setting specifies a name for the firewall rule.
Enable	<p>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.</p> <p>If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.

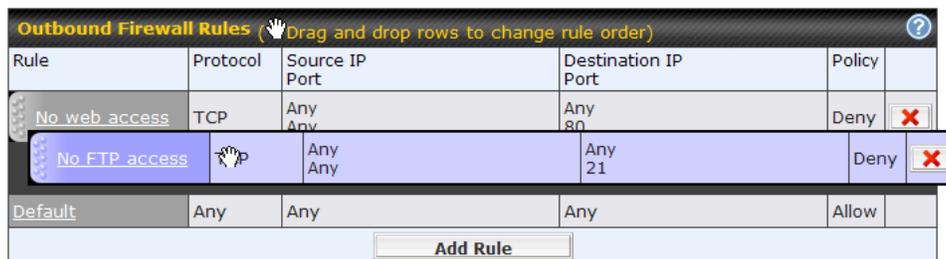
<p>Protocol</p>	<p>This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> • Any • TCP • UDP • ICMP • DSCP • IP <p>Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill 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.</p>
<p>Source and Port</p>	<p>This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the Source IP & Port setting, as indicated with the following screenshots:</p>  <p>In addition, a single port, or a range of ports, can be specified for the Source settings.</p>
<p>Destination and Port</p>	<p>This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the Destination IP & Port setting, as indicated with the following screenshots:</p>  <p>In addition, a single port, or a range of ports, can be specified for the settings.</p>
<p>Action</p>	<p>This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:</p> <ul style="list-style-type: none"> • Source IP & port • Destination IP & port <p>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).</p>
<p>Event Logging</p>	<p>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</p> <ul style="list-style-type: none"> • 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.



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

To remove a rule, click the  button.

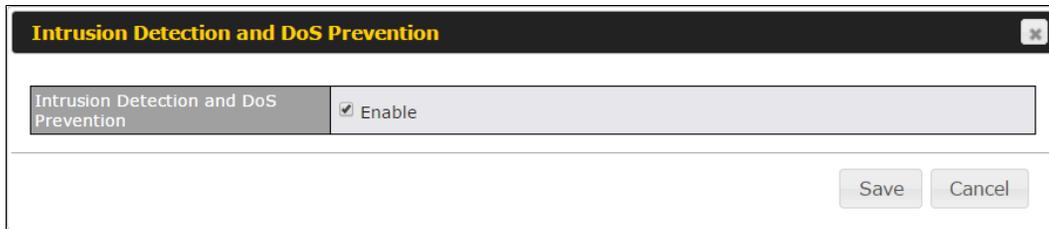
Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default** rule will be applied.

The **Default** rule is **Allow** for Outbound, Inbound and Internal Network access.

Tip

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

Intrusion Detection and DoS Prevention



The screenshot shows a configuration window titled "Intrusion Detection and DoS Prevention". Inside the window, there is a section with the label "Intrusion Detection and DoS Prevention" and a checked checkbox labeled "Enable". At the bottom right of the window, there are two buttons: "Save" and "Cancel".

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

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

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

13.11.2 Content Blocking

Application Blocking ?

Please Select Application... +

Web Blocking ?

Preset Category

<input type="radio"/> High <input type="radio"/> Moderate <input type="radio"/> Low <input checked="" type="radio"/> Custom	<input type="checkbox"/> Adware <input type="checkbox"/> Dating <input type="checkbox"/> P2P/File sharing <input type="checkbox"/> Malware <input type="checkbox"/> Social Networking <input type="checkbox"/> Violence	<input type="checkbox"/> Aggressive <input type="checkbox"/> Drugs <input type="checkbox"/> Gambling <input checked="" type="checkbox"/> Pornography <input type="checkbox"/> Contraband <input type="checkbox"/> Weapons	<input type="checkbox"/> Audio-Video <input type="checkbox"/> File Hosting <input type="checkbox"/> Games <input checked="" type="checkbox"/> Proxy/Anonymizer <input type="checkbox"/> Update Sites
--	--	--	--

Content Filtering Database Auto Update ?

Customized Domains ?
 +

Exempted Domains from Web Blocking ?
 +

Exempted User Groups ?

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

Exempted Subnets ?

Network	Subnet Mask	
<input style="width: 100%;" type="text"/>	255.255.255.0 (/24)	+

URL Logging

Enable	<input type="checkbox"/>
Log Server Host	<input style="width: 80%;" type="text"/> 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™ peer clients to access these websites. Exceptions can be added using the instructions in **Sections 21.2.1.4** and **21.2.1.5**.

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

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

Exempted User Groups

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

Exempted Subnets

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

URL Logging

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

13.12 Routing Protocols

13.12.1 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		
0.0.0.0	Untagged LAN (192.168.112.1/24), WAN 4 (192.168.254.10/24)	
<input type="button" value="Add"/>		
RIPv2		
No RIPv2 Defined.		
OSPF & RIPv2 Route Advertisement		
PepVPN Route Isolation	<input type="checkbox"/> Enable	
Network Advertising	--- <input type="button" value="+"/>	All LAN/VLAN networks will be advertised when no network advertising is chosen.
Static Route Advertising	<input checked="" type="checkbox"/> Enable	
	Excluded Networks	Subnet Mask
	<input type="text"/>	255.255.255.0 (/24) <input type="button" value="+"/>
<input type="button" value="Save"/>		

OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the WAN IP address. If you want to specify your own ID, enter it into the Custom field.
Area	This is an overview of the OSPF areas that you have defined. Clicking on the name under Area allows you to configure the connection. To define a new area, click Add. To delete an existing area, click on the .

OSPF settings ✕

Area ID	<input type="text" value="0.0.0.0"/>
Link Type	<input checked="" type="radio"/> Broadcast <input type="radio"/> Point-to-Point
Authentication	None ▾
Interfaces ?	<input checked="" type="checkbox"/> Untagged LAN (192.168.112.1/24) <input type="checkbox"/> Management VLAN (10.0.2.1/24) <input type="checkbox"/> jamestest (10.22.37.1/24) <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input checked="" type="checkbox"/> WAN 4 (192.168.254.10/24) <input type="checkbox"/> WAN 5

OSPF Settings	
Area ID	Assign a name to be applied to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore them.
Link Type	Choose the type of network that this area will use.
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are MD5 and Text . Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver OSPF packets.

To access RIPv2 settings, click on  .

RIPv2 settings ✕

Authentication	None ▾
Interfaces	<input type="checkbox"/> Untagged LAN (192.168.112.1/24) <input type="checkbox"/> Management VLAN (10.0.2.1/24) <input type="checkbox"/> jamestest (10.22.37.1/24) <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 (192.168.254.10/24) <input type="checkbox"/> WAN 5

RIPv2 Settings	
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are MD5 and Text . Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver RIPv2 packets.

OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation	<input type="checkbox"/> Enable						
Network Advertising	<div style="display: flex; align-items: center;"> <input style="width: 80%;" type="text" value="---"/> ▾ <input style="margin-left: 10px;" type="button" value="+"/> </div> <small>All LAN/VLAN networks will be advertised when no network advertising is chosen.</small>						
Static Route Advertising	<input checked="" type="checkbox"/> Enable <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Excluded Networks</th> <th style="width: 30%;">Subnet Mask</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td><input style="width: 90%;" type="text"/></td> <td>255.255.255.0 (/24) ▾</td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Excluded Networks	Subnet Mask		<input style="width: 90%;" type="text"/>	255.255.255.0 (/24) ▾	<input type="button" value="+"/>
Excluded Networks	Subnet Mask						
<input style="width: 90%;" type="text"/>	255.255.255.0 (/24) ▾	<input type="button" value="+"/>					

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	Enabling OSPF & RIPv2 Route Advertising allows it to advertise LAN static routes over OSPF & RIPv2. Static routes on the Excluded Networks table will not be advertised.

13.12.2 BGP

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

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

Click the "**x**" to delete a BGP profile.

Click "**Add**" to create a new BGP profile.

BGP Profile ✕

BGP Profile						
Profile Name	<input type="text"/>					
Enable	<input checked="" type="checkbox"/>					
Interface	WAN ▼					
Router ID	<input checked="" type="radio"/> WAN IP Address <input type="radio"/> Custom: <input type="text"/>					
Autonomous System	<input type="text"/>					
Neighbor	?	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending
		<input type="text"/>	<input type="text"/>	disable	<input type="text"/>	<input type="text"/>
Hold Time	?	<input type="text" value="240"/>				
Next Hop Self	?	<input type="checkbox"/>				
iBGP Local Preference	?	<input type="text" value="100"/>				
BFD	?	<input type="checkbox"/> Enable				

BGP	
Name	This field specifies the name that represents this profile.
Enable	When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.
Interface	The interface in which the BGP neighbor is located.
Autonomous System	The Autonomous System Number (ASN) assigned to this profile.
Neighbor	BGP Neighbors and their details.

IP address	The IP address of the Neighbor.
Autonomous System	The Neighbor's ASN.
Multihop/TTL	This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255.
Password	(Optional) Assign a password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received routes.
Hold Time	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
Next Hop Self	Enable this option to advertise your own source address as the next hop when propagating routes.
iBGP Local Preference	This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100
BFD	Enable this option to add Bidirectional Forwarding Detection for path failure. All directly connected Neighbors that use the same physical interface share the same BFD settings. All multihop Neighbors share the same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.

Route Advertisement								
Network Advertising	<input type="text" value="---"/>	<input type="button" value="+"/>						
Static Route Advertising	<input checked="" type="checkbox"/> Enable							
	<table border="1"> <thead> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) <input type="button" value="v"/></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Excluded Networks	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) <input type="button" value="v"/>	<input type="button" value="+"/>	
Excluded Networks	Subnet Mask							
<input type="text"/>	255.255.255.0 (/24) <input type="button" value="v"/>	<input type="button" value="+"/>						
Custom Route Advertising	<table border="1"> <thead> <tr> <th>Networks</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) <input type="button" value="v"/></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Networks	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) <input type="button" value="v"/>	<input type="button" value="+"/>	
Networks	Subnet Mask							
<input type="text"/>	255.255.255.0 (/24) <input type="button" value="v"/>	<input type="button" value="+"/>						
Advertise OSPF Route	<input type="checkbox"/>							
Set Community	<table border="1"> <thead> <tr> <th>Community</th> <th>Route Prefix</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Community	Route Prefix		<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>	
Community	Route Prefix							
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>						

Route Advertisement	
Network Advertising	Select the Networks that will be advertised to the BGP Neighbor.
Static Route Advertising	Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised.
Custom Route Advertising	Additional routes to be advertised to the BGP Neighbor.
Advertise OSPF Route	When this box is checked, every learnt OSPF route will be advertised.
Set Community	<p>Assign a prefix to a Community</p> <p>Community: Two numbers in new-format. e.g. 65000:21344</p> <p>Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284</p> <p>Route Prefix: Comma separated networks. e.g. 172.168.1.0/24,192.168.1.0/28</p>

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

Route Import Settings	
Filter Mode	<p>This field allows for the selection of the filter mode for route import.</p> <p>None: All BGP routes will be accepted.</p> <p>Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p>Reject: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.</p>

Restricted Networks	<p>This field specifies the network(s) in the "route import" entry.</p> <p>Exact Match: When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.</p>
----------------------------	--

Route Export			
Filter Mode	<input type="text" value="Accept"/>		
Restricted Networks	Network	Subnet Mask	Exact Match
	<input type="text"/>	<input type="text" value="255.255.255.0 (/24)"/>	<input type="checkbox"/>
Export to other BGP Profile	<input type="checkbox"/>		
Export to OSPF	<input type="checkbox"/>		

Filter Mode	<p>This field allows for the selection of the filter mode for route export.</p> <p>None: All BGP routes will be accepted.</p> <p>Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p>Reject: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.</p>
Restricted Networks	<p>This field specifies the network(s) in the "route export" entry.</p> <p>Exact Match: When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.</p>
Export to other BGP Profile	<p>When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.</p>
Export to OSPF	<p>When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.</p>

13.13 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.

13.13.1 L2TP with IPsec

Remote User Access Settings	
Enable	<input checked="" type="checkbox"/>
VPN Type	<input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input type="radio"/> OpenVPN
Preshared Key	<input type="text"/> <input checked="" type="checkbox"/> 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.

13.13.2 OpenVPN

Remote User Access Settings	
Enable	<input checked="" type="checkbox"/>
VPN Type	<input type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input checked="" type="radio"/> 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:

Option 1: "Route all traffic" profile

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

Option 2: "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.

13.13.3 PPTP

Remote User Access Settings	
Enable	<input checked="" type="checkbox"/>
VPN Type	<input type="radio"/> L2TP with IPsec <input checked="" type="radio"/> PPTP <input type="radio"/> 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 methods.

13.13.4 Authentication Methods

Connect to Network	<input type="text" value="Untagged LAN"/>			
Authentication	<input type="text" value="Local User Accounts"/>			
User Accounts	<table border="1"> <tr> <td><input type="text" value="Username"/></td> <td><input type="text" value="Password"/></td> <td><input type="button" value="+"/></td> </tr> </table>	<input type="text" value="Username"/>	<input type="text" value="Password"/>	<input type="button" value="+"/>
<input type="text" value="Username"/>	<input type="text" value="Password"/>	<input type="button" value="+"/>		

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

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

Radius Server:

Authentication	RADIUS Server ▾
Auth Protocol	MS-CHAP v2 ▾
Auth Server	<input type="text"/> Port 1812 Default
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Accounting Server	<input type="text"/> Port 1813 Default
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> 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	<input type="text"/>
Domain	<input type="text"/>
Admin Username	<input type="text"/>
Admin Password	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

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

13.14 Misc. Settings

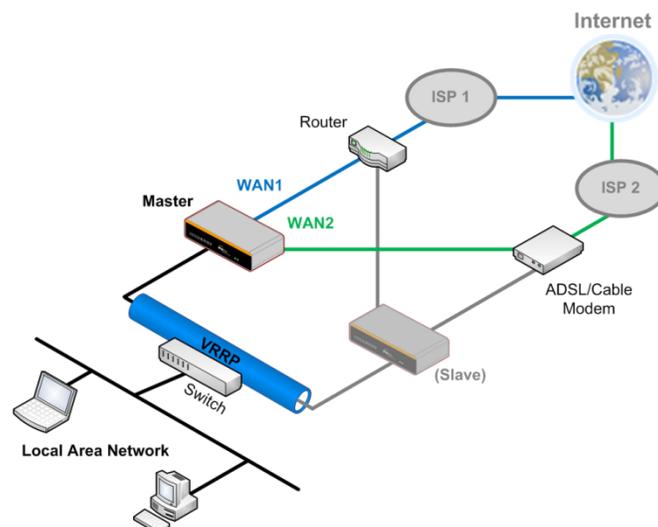
13.14.1 High Availability

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

Interface for Slave Router

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

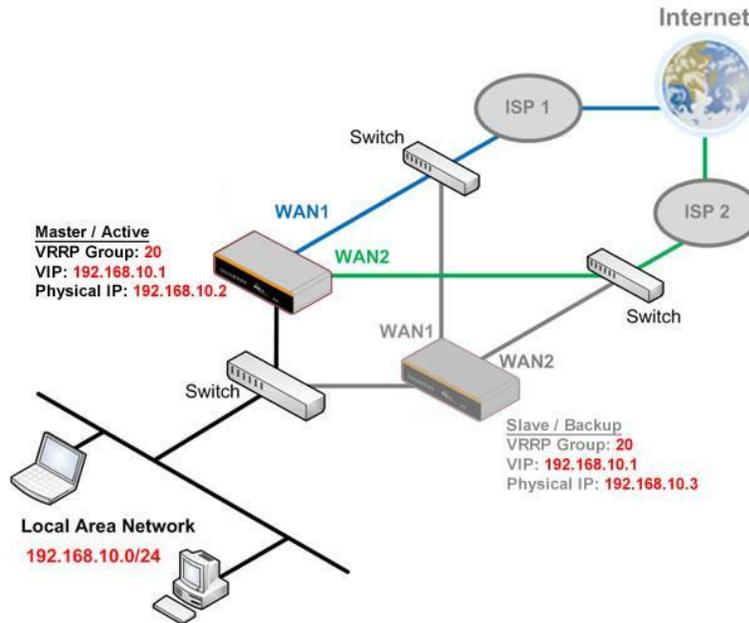
High Availability	
Enable	<input checked="" type="checkbox"/>
Group Number	5
Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/> Slave
Configuration Sync.	<input type="checkbox"/> Master Serial Number: 5454- 5454 - 5454
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask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

High Availability	
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.

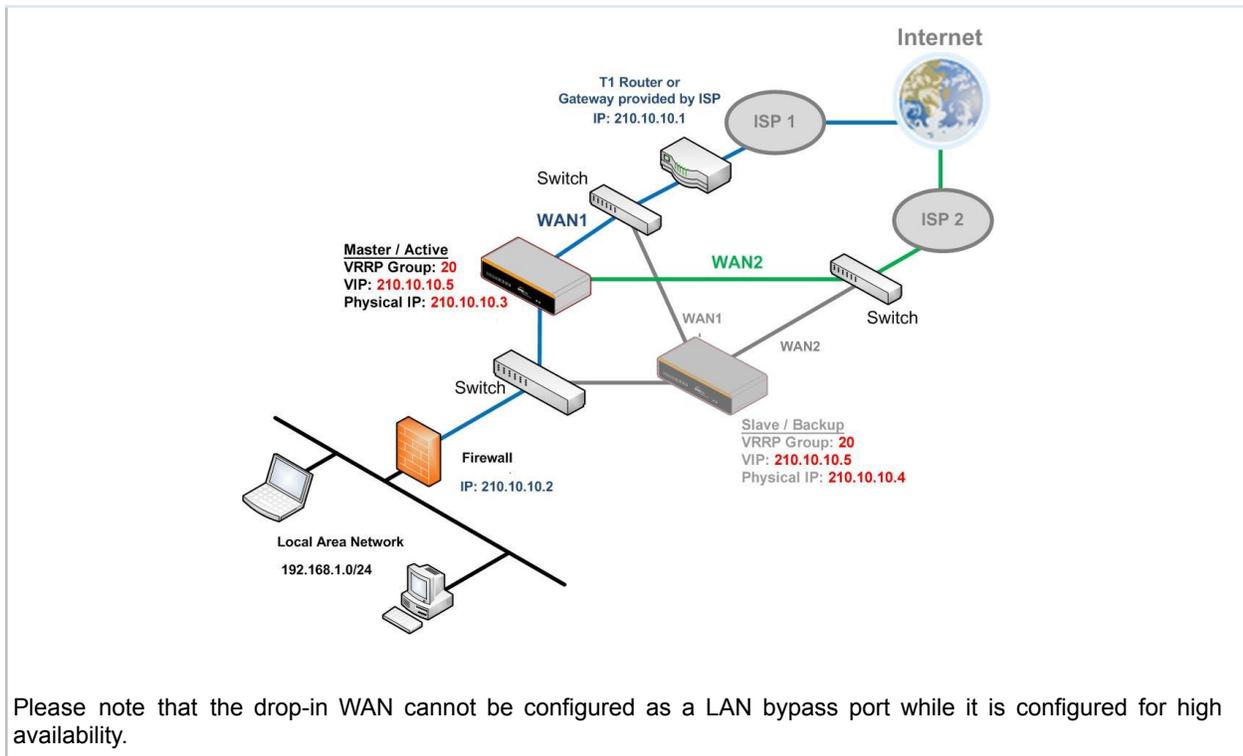
Subnet Mask This setting specifies the subnet mask of the LAN.

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.



13.14.2 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
<input type="button" value="Add Certificate"/>

Wi-Fi WAN Client Certificate
No Certificates defined
<input type="button" value="Add Certificate"/>

Wi-Fi WAN CA Certificate
No Certificates defined
<input type="button" value="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/>

13.14.3 Service Forwarding

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

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

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

SMTP Forwarding

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

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

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

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

Note

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

Web Proxy Forwarding

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

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

DNS Forwarding

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

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

Custom Service Forwarding

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

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

13.14.4 Service Passthrough

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

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

(Registered trademarks are copyrighted by their respective owner)

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

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

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.

13.14.5 NTP Server

Peplink routers can now serve as a local NTP server. Upon start up, it is now able to provide connected devices with the accurate time, precise UTC from either an external NTP server or via GPS and ensuring that connected devices always receive the correct time.

NTP Server setting can be found via: **Network>Misc. Settings>NTP Server**

NTP Server	
Enable	<input type="checkbox"/>
<input type="button" value="Save"/>	

Time Settings can be found at **System>Time>Time Settings**

Time Settings	
Time Zone	<div style="border: 1px solid #ccc; padding: 2px;">(GMT) Casablanca ▼</div> <input type="checkbox"/> Show all
Time Sync	<div style="border: 1px solid #ccc; padding: 2px;">Time Server ▼</div>
Time Server	<div style="border: 1px solid #ccc; padding: 2px;">0.peplink.pool.ntp.org</div>
<input type="button" value="Save"/>	

13.14.6 Grouped Networks

Grouped Networks	
Name	Networks
<input type="button" value="Add Group"/>	

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.

Grouped 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.

peplink

[Dashboard](#)
[Setup Wizard](#)
[Network](#)
[AP](#)
[System](#)
[Status](#)

WAN

LAN

- Network Settings
- Port Settings

VPN

- SpeedFusion
- IPsec VPN

Outbound Policy

Inbound Access

Outbound Policy

Custom

Add a New Custom Rule

Service Name	<input type="text"/>	
Enable	<input checked="" type="checkbox"/> Always on ▼	
Source	Grouped Networ ▼	Accounting ▼

13.14.7 Remote SIM Management

Remote SIM management is accessible via **Network > Misc Settings > Remote SIM Management**. By default, this feature is disabled.

Please note that a limited number of Pepwave routers support the SIM Injector, may refer to the link: <https://www.peplink.com/products/sim-injector/> or Appendix C for more details on FusionSIM Manual.

Remote SIM Host	
Remote SIM is disabled	

Remote SIM Host Settings

Remote SIM Host Settings	
Auto LAN Discovery	<input type="checkbox"/>
Remote SIM Host	<input type="text"/>

Remote SIM Host Settings	
Active LAN Discovery	Check this box to enable Auto LAN discovery of the remote SIM server.
Remote SIM Host	Enter the public IP address of the SIM Injector. If you enter IP addresses here, it is not necessary to tick the "Auto LAN Discovery" box above.

Remote SIM Host	
192.168.1.10	

Remote SIM Management	Server	Slot
No Remote SIM Defined.		
<input type="button" value="Add Remote SIM"/>		

You may define the Remote SIM information by clicking the “**Add Remote SIM**”. Here, you can enable **Data Roaming** and **custom APN** for your SIM cards.

Add Remote SIM ✕

Remote SIM	
SIM Server	<input type="text" value="New SIM Server..."/>
SIM Server - Serial Number	<input type="text"/>
SIM Server - Name	<input type="text" value="Optional"/>
SIM Slot	<input type="text" value="1"/>
SIM Slot - Name	<input type="text" value="Optional"/>
Data Roaming	<input type="checkbox"/>
Operator Settings (for LTE/HSPA/EDGE/GPRS only) ?	<input checked="" type="radio"/> Auto <input type="radio"/> Custom Mobile Operator Settings
SIM PIN (Optional)	<input type="text"/> <input type="text"/> (Confirm)

Add Remote SIM Settings	
SIM Server	Add a new SIM Server
SIM Server - Serial Number	Enter the serial number of SIM Server
SIM Server - Name	This optional field allows you define a name for the SIM Server
SIM Slot	Click the drop-down menu and choose which SIM slot you want to connect.
SIM Slot - Name	This optional field allows you define a name for the SIM slot.
Data Roaming	Enables data roaming on this particular SIM card.
Operator Settings (for LTE//HSPA/EDGE/GPRS Only)	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 a connection, you may select Custom to enter your carrier's APN, Username and Password settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto.

13.14.8 SIM Toolkit

The SIM Toolkit can be found via **Networks > Misc Settings > SIM Toolkit**. This 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	856195002108538
Tool	USSD

USSD	
USSD Code	<input type="text"/> <input type="button" value="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# <input type="button" value="Submit"/>
Receive SMS	<input type="button" value="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# <input type="button" value="Submit"/>
USSD Status	Request is sent successfully
Receive SMS	<input type="button" value="Get"/>

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

Received SMS	
May 27 20:02	<p>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)</p>
Aug 8 , 2013 14:51	<p>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)</p>

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	0734917100000000
Tool	SMS

SMS		Refresh
Jun 21, 2017 18:00	<p>Msg Thank you, your web password is verified - you can change this when you first login at thruon.com</p>	✖
May 06, 2017 12:23	<p>Message iPhone: Your new bill is ready to view. Go to your MyQ account on your desktop or on a mobile phone click here http://mobile.thruon.com/bills</p>	✖
Mar 15, 2017 10:03	<p>From Thruon Note: There is planned maintenance in the Eastern US on Wed, 3/15/17. If your service is affected, you can get updates here: http://bit.ly/1W47014</p>	✖
Mar 06, 2017 14:50	<p>Message iPhone: Your new bill is ready to view. Go to your MyQ account on your desktop or on a mobile phone click here http://mobile.thruon.com/bills</p>	✖
Dec 28, 2016 09:53	<p>From Thruon We are happy your registration is complete! As a special offer, we're sending you this offer applied to your first 30 days. Your monthly recurring charge will remain \$0 for the first 30 days.</p>	✖
Dec 06, 2016 13:09	<p>Message iPhone: Your new bill is ready to view. Go to your MyQ account on your desktop or on a mobile phone click here http://mobile.thruon.com/bills</p>	✖
Nov 08, 2016 11:29	<p>From Thruon Note: There is planned maintenance in the Eastern US on Wed, 11/9/16. If your service is affected, you can get updates here: http://bit.ly/1W47014</p>	✖
Sep 07, 2016 17:05	<p>From Thruon Need more details regarding our choice of streaming bandwidth? We can help. Call 1-888-488-01 or email your needs@thruon.com or support@peplink.com</p>	✖

14 AP Tab

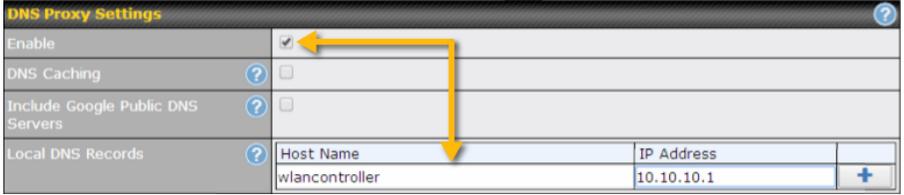
14.1 AP

14.1.1 AP Controller

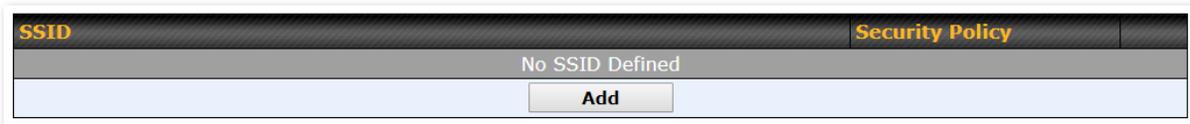
Clicking on the **AP** tab will default to this menu, where you can view basic AP management options:

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

AP Controller	
AP Management	<p>The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, 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.</p>
Support Remote AP	<p>The AP controller supports remote management of Pepwave APs. When this option is enabled, the AP controller will wait for management connections originating from remote APs over the WAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443.</p> <p>The DHCP server and/or local DNS server of the remote AP's network should be configured in the DNS Proxy Settings menu under Network>LAN. The procedure is as follows:</p> <ol style="list-style-type: none"> 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.

	
Sync. Method	<p>Select the required option to synchronize the managed AP's. Options are:</p> <ul style="list-style-type: none"> • As soon as possible (default) • Progressively (synchronize AP's in groups) • One at a time (synchronize one AP at a time)
Permitted AP	<p>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.</p>

14.1.2 Wireless SSID



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 show a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).



SSID	
SSID Settings	
SSID	PEPLINK_63E6
Enable	Always on ▾
VLAN	0 (0: Untagged) <input type="checkbox"/> Use VLAN Pool
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Multicast Filter	<input type="checkbox"/>
Multicast Rate	MCS0/6M ▾
IGMP Snooping	<input type="checkbox"/>
DHCP Relay	<input type="checkbox"/>
DHCP Option 82	<input type="checkbox"/>
Network Priority (QoS)	Gold ▾
Layer 2 Isolation	<input type="checkbox"/>
Maximum number of clients	2.4 GHz: 0 5 GHz: 0 (0: Unlimited)
Band Steering	<input type="checkbox"/> 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	<input type="password" value="••••••"/> <input checked="" type="checkbox"/> Hide Characters

Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options: <ul style="list-style-type: none"> • Open (No Encryption) • WPA3 -Personal (AES:CCMP) • WPA2/WPA3 -Personal (AES:CCMP) • 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.

NOTE:

When **WPA2/WPA3- Personal** is configured, if a managed AP which is NOT WPA3 PSK capable, the AP Controller will not push those WPA3 and WPA2/WPA3 SSID to that AP.

Access Control Settings	
Restricted Mode	Deny all except listed ▼
MAC Address List ?	<input type="text"/>

Access Control	
Restricted Mode	The settings allow the 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	<input type="text"/>	<input type="text"/>
Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Authentication Port	1812 <input type="text"/> Default	1812 <input type="text"/> Default
Accounting Port	1813 <input type="text"/> Default	1813 <input type="text"/> 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 the field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the Default button to enter 1812 .
Accounting Port	In the 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

14.1.3 Wireless Mesh

Wireless Mesh	Frequency Band
No Wireless Mesh Defined	
<input type="button" value="Add"/>	

Wireless Mesh Support is available on devices running 802.11ac (Wi-Fi 5) and above. Along with the AP Controller, mesh network extensions can be established, which can expand network coverage. Note that the Wireless Mesh settings need to match the Mesh ID and Shared Key of the other devices on the same selected frequency band.

To create a new Wireless Mesh profile, go to **AP > Wireless Mesh**, and click **Add**.

Wireless Mesh Settings
✕

Mesh ID	<input style="width: 90%;" type="text"/>
Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz
Shared Key	<input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters

Wireless Mesh Settings	
Mesh ID	Enter a name to represent the Mesh profile.
Frequency	Select the 2.4GHz or 5GHz frequency to be used.
Shared Key	Enter the shared key in the text field. Please note that it needs to match the shared keys of the other APs in the Wireless Mesh settings. Click Hide / Show Characters to toggle visibility.

14.1.4 AP > Profiles

AP Settings ?	
AP Profile Name	<input type="text"/>
SSID ?	<input type="checkbox"/> 2.4 GHz <input type="checkbox"/> 5 GHz <input type="checkbox"/> <input type="checkbox"/> PEPLINK_63E6
Operating Country	United States ▼
Preferred Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 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. <ul style="list-style-type: none"> • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). 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 <input type="button" value="Edit"/> Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto <input type="button" value="Edit"/> Channels: 36 40 44 48 149 153 157 161 165
Auto Channel Update	Daily at 03:00 <input checked="" type="checkbox"/> Wait until no active client associated	Daily at 03:00 <input checked="" type="checkbox"/> Wait until no active client associated
Output Power	Fixed: Max <input type="checkbox"/> Boost	Fixed: Max <input type="checkbox"/> Boost
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)	0 (0: Unlimited)

AP Settings (part 2)

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	<input type="text" value="0"/> (0: Untagged)
Operating Schedule	Always on ▾
Beacon Rate	<input type="text" value="1"/> Mbps ▾
Beacon Interval	<input type="text" value="100"/> ms ▾
DTIM	<input type="text" value="1"/> <input type="button" value="Default"/>
RTS Threshold	<input type="text" value="0"/> <input type="button" value="Default"/>
Fragmentation Threshold	<input type="text" value="0"/> (0: Disable) <input type="button" value="Default"/>
Distance / Time Converter	<input type="range"/> <input type="text" value="4050"/> m <small>Note: Input distance for recommended values</small>
Slot Time	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="9"/> μ s <input type="button" value="Default"/>
ACK Timeout	<input type="text" value="48"/> μ s <input type="button" value="Default"/>
Frame Aggregation	<input checked="" type="checkbox"/>
Aggregation Length	<input type="text" value="50000"/> <input type="button" value="Default"/>

Advanced AP Settings	
Management VLAN ID	<p>This field specifies the VLAN ID to tag to management traffic, such as communication traffic between the AP and the AP Controller. The value is zero by default, which means that no VLAN tagging will be applied.</p> <p>NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller.</p>
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 Converter	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.

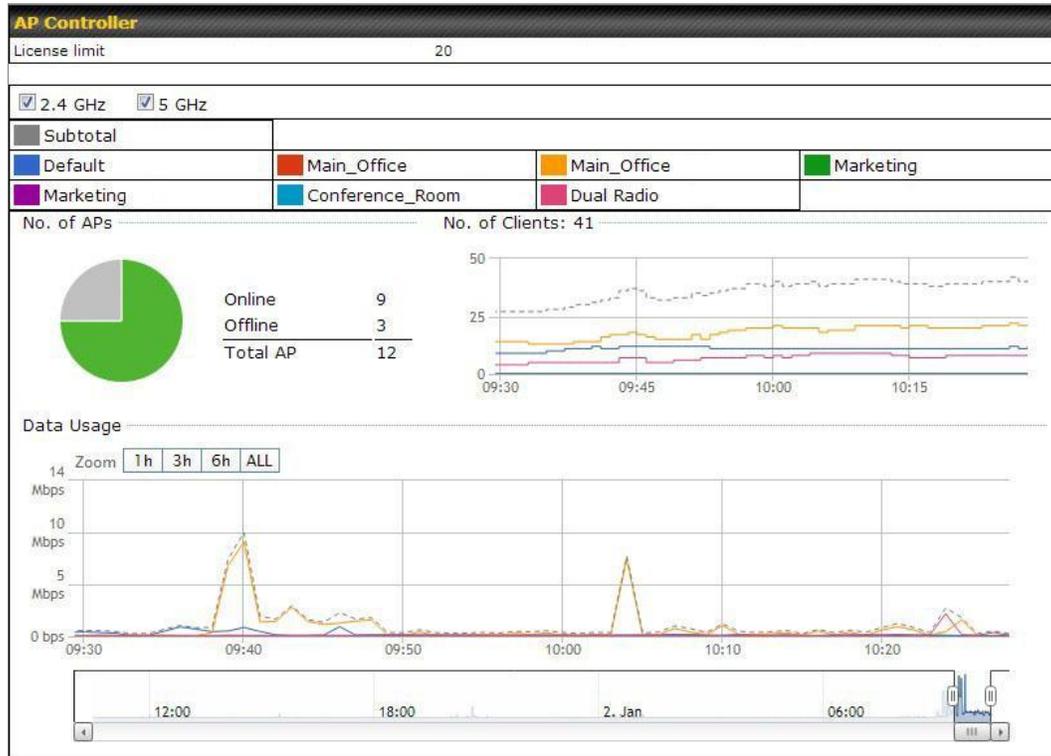
Web Administration Settings	
Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	<input type="text" value="443"/>
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username	<input type="text" value="admin"/>
Admin Password	<input type="password" value="....."/> <input type="button" value="Generate"/>
	<input checked="" type="checkbox"/> 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.

14.2 AP Controller Status

14.2.1 Info

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



AP Controller	
License Limit	This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage.
Frequency	Underneath, there are two check boxes labeled 2.4 Ghz and 5 Ghz . Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.
SSID	The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs.
No. of APs	This pie chart and table indicates how many APs are online and how many are offline.
No. of Clients	This graph displays the number of clients connected to each network at any given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time.

Data Usage

This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to **Zoom** to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

14.2.2 Access Points (Usage)

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

Search Filter

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

Managed APs Expand Collapse

Name	IP Address	MAC	Location	Firmware Pack ID	Configuration
▼ Default (8/9 online)					
<input type="checkbox"/> XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2 None ✓	🔍 📄 📊

Usage

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

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

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

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

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

Client List ✕

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

Close

Managed Wireless Devices

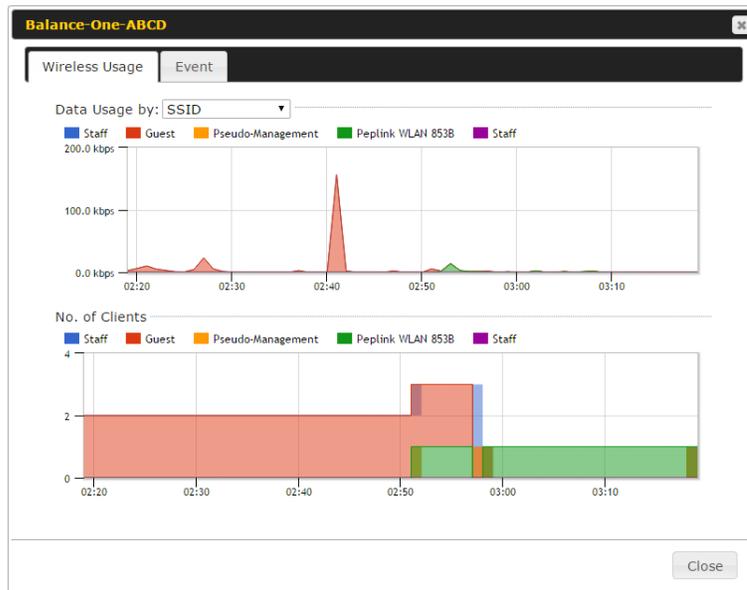
Click the  icon to configure each client

AP Details
✕

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

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

Click the  icon to see a graph displaying usage:



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

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

Event Information

Events

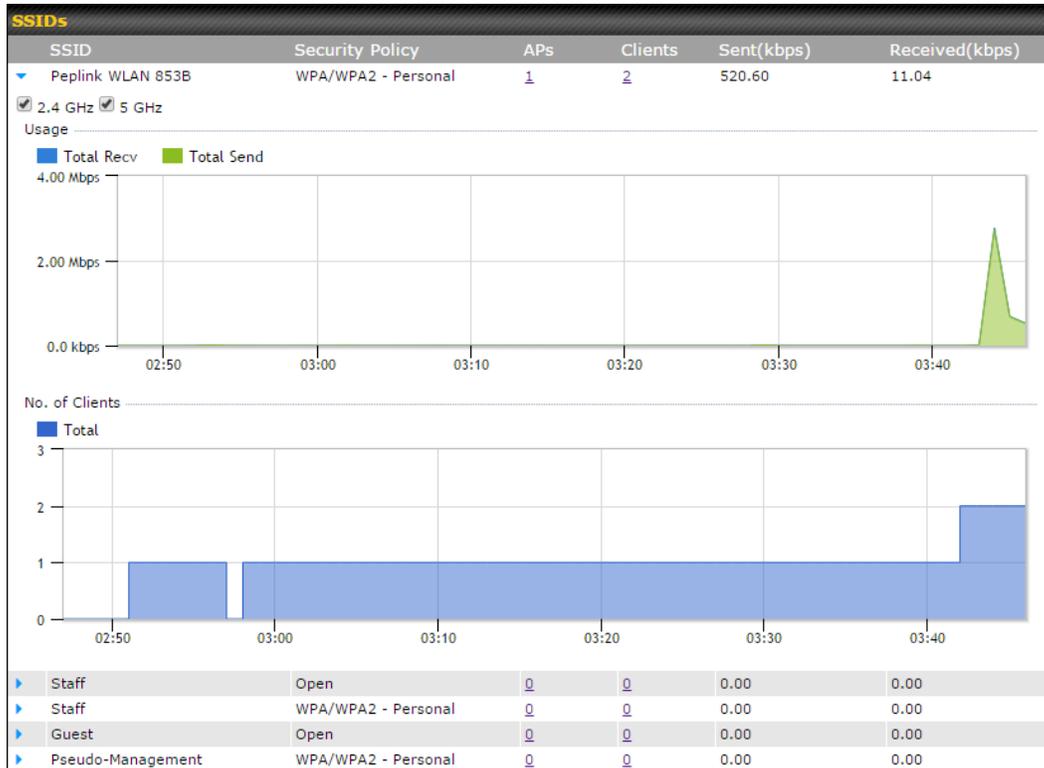
Jan 2 11:53:39	Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 11:39:31	Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:16:55	Client A8:BB:CF:E1:0F:1E disassociated from Balance_11a
Jan 2 11:11:54	Client A8:BB:CF:E1:0F:1E associated with Balance_11a
Jan 2 11:10:45	Client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

More...

Close

14.2.3 Wireless SSID

In-depth wireless SSID reports are available under **AP > Wireless SSID**.



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

14.2.4 Wireless Client

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

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

Top 10 Clients of last hour (Updated at 03:00)			
Client MAC Address	Upload	Download	
C0:EE:FB:20:13:36	53.5 KB	101.4 KB	☆ 

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

Client C0:EE:FB:20:13:36 ✕

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

■ Download
 ■ Upload

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

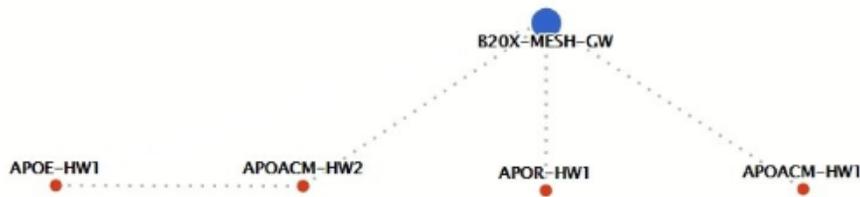
Close

14.2.5 Mesh / WDS

Mesh / WDS allows you to monitor the status of your wireless distribution system (WDS) or Mesh, and track activity by MAC address by navigating to **AP > Controller Status > Mesh / WDS**. This table shows the detailed information of each AP, including protocol, transmit rate (sent / received), signal strength, and duration.

Mesh / WDS						
Type	Peer MAC	Protocol	Rate (Send)	Rate (Receive)	Signal (dBm)	Duration
▼ APOACM-HW1/						
Mesh ()		802.11ac	325M	650M	-56	19:13:35
▼ APOACM-HW2/						
Mesh ()		802.11ac	650M	351M	-63	00:49:20
Mesh ()		802.11ac	390M	325M	-67	01:35:09
▼ APOE-HW1/						
Mesh ()		802.11ac	58.5M	130M	-69	00:45:22
▼ APOR-HW1/						
Mesh ()		802.11ac	325M	866.7M	-53	19:14:44
▼ B20X-MESH-GW/						
Mesh ()		802.11ac	433M	650M	-69	19:14:44
Mesh ()		802.11ac	325M	390M	-66	01:35:42
Mesh ()		802.11ac	351M	650M	-70	19:13:45
Mesh ()		802.11ac	130M	117M	-88	00:45:52

Network Graph



14.2.6 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.

14.2.7 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 <input type="text"/> hh:mm to <input type="text"/> hh:mm
Alerts only	<input type="checkbox"/>
<input type="button" value="Search"/>	

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client 54:EA:A0:3D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A0:3D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A0:3D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:11:6A:1E:09:A1 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 60:67:20:24:06:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A0:3D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:11:6A:1E:09:A1 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 10:00:3D:3D:A0:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 10:00:3D:3D:A0:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A0:3D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 30:8F:40:09:78:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A0:3D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A0:3D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A0:3D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A0:3D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A0:3D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:11:6A:1E:09:A1 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 9C:94:09:10:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A0:3D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A0:3D:A0:D5 associated with Marketing_11a	

More...

Events

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

14.3 Toolbox

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

Firmware Packs

Auto Power Adj.

Dynamic Channel Assignment

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

Check for Updates

Manual Upload

Default...

No default defined.

Firmware Packs

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

15 System Tab

15.1 System

15.1.1 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	<input type="text"/> hostname: <input type="text"/> ⚙️ This configuration is being managed by InControl.
Admin User Name	<input type="text" value="admin"/>
Admin Password	<input type="password" value="....."/>
Confirm Admin Password	<input type="password" value="....."/>
Read-only User Name	<input type="text" value="user"/>
User Password	<input type="password"/>
Confirm User Password	<input type="password"/>
Front Panel Passcode	<input type="checkbox"/>
Web Session Timeout	? <input type="text" value="4"/> Hours <input type="text" value="0"/> Minutes
Authentication by RADIUS	? <input type="checkbox"/> Enable
CLI SSH & Console	? <input type="checkbox"/> Enable
Security	HTTP / HTTPS ▾ <input checked="" type="checkbox"/> Redirect HTTP to HTTPS
Web Admin Access	HTTP: <input type="text" value="LAN Only"/> HTTPS: <input type="text" value="LAN Only"/> ▾
Web Admin Port	HTTP: <input type="text" value="80"/> HTTPS: <input type="text" value="443"/>
LAN Connection Access Settings	
Allowed LAN Networks	<input checked="" type="radio"/> Any <input type="radio"/> Allow this network only
<input type="button" value="Save"/>	

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 <i>admin</i> 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 <i>user</i> 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 15.3 .
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: <ul style="list-style-type: none"> • HTTP • HTTPS

	<ul style="list-style-type: none"> • HTTP/HTTPS <p>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.</p>
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
Web Admin Access	<p>This option is for specifying the network interfaces through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> • LAN only • LAN/WAN <p>If LAN/WAN is chosen, the WAN Connection Access Settings form will be displayed.</p>

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
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/>	10.88.3.158 (Interface IP)
<input type="checkbox"/> WAN 2	<input type="checkbox"/>	
<input type="checkbox"/> Wi-Fi WAN	<input type="checkbox"/>	
<input type="checkbox"/> Cellular 1	<input type="checkbox"/>	
<input type="checkbox"/> Cellular 2	<input type="checkbox"/>	
<input type="checkbox"/> USB	<input type="checkbox"/>	

WAN Connection Access Settings

Allowed Source IP Subnets	<p>This field allows you to restrict web admin access only from defined IP subnets.</p> <ul style="list-style-type: none"> • 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
----------------------------------	---

	<p>displayed beneath:</p> <p>The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of <i>w.x.y.z/m</i>, where <i>w.x.y.z</i> is an IP address (e.g., <i>192.168.0.0</i>), and <i>m</i> is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, <i>192.168.0.0/24</i>).</p> <p>To define multiple subnets, separate each IP subnet one in a line. For example:</p> <ul style="list-style-type: none"> • 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.

15.1.2 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**.

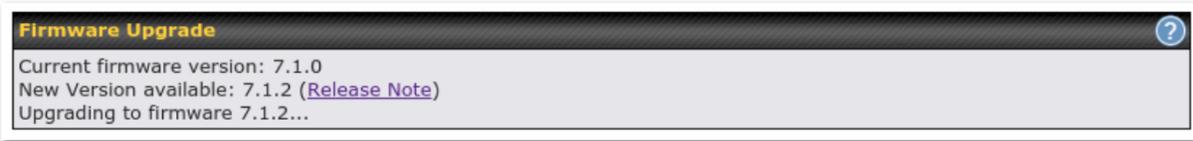


If an update is found the buttons will change to allow you to **Download and Update** the firmware.



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.



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.



*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.

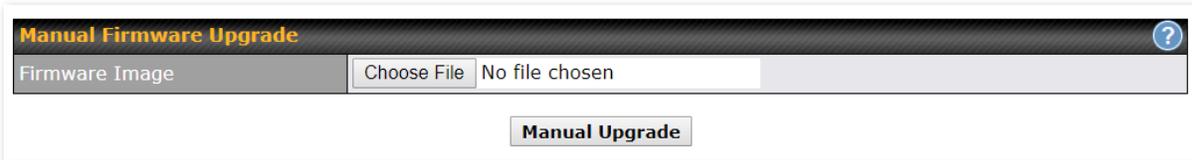
All of the Peplink/Pepwave GA firmware can be found [here](#). Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the Balance line.

Balance						
Product <input type="text"/>						
Search: <input type="text"/>						
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 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.



*Upgrading the firmware will cause the router to reboot.

The InControl method

[Described in this knowledgebase article on our forum.](#)

15.1.3 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 ▼ <input type="checkbox"/> Show all
Time Server	0.pepwave.pool.ntp.org <input type="button" value="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.

15.1.4 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	-	✖

New Schedule

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

Edit schedule profile ✕

Schedule Settings

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

Schedule Map

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

Save
Cancel

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.

15.1.5 Email Notification

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

Email Notification Setup ?	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	smtp.mycompany.com <input checked="" type="checkbox"/> Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	smtuser
SMTP Password	*****
Confirm SMTP Password	*****
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

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

SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check Require authentication .
Connection Security	This setting specifies via a drop-down menu one of the following valid Connection Security: <ul style="list-style-type: none"> • None • STARTTLS • SSL/TLS
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to 25 . If Connection Security is selected " STARTTLS ", the default port number will be set to 587 . If Connection Security is selected " SSL/TLS ", the default port number will be set to 465 . You may customize the port number by editing this field.
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.
 (NOTE: Settings are not saved. To confirm the update, click 'Save' button.)

Email Notification Setup ?	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	<input type="text"/> <input checked="" type="checkbox"/> Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Confirm SMTP Password	<input type="password"/>
Sender's Email Address	<input type="text"/>
Recipient's Email Address	<input type="text"/>

Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
<-> 220 smtp.gmail.com ESMTP h11sm3907691pjj.46 - gsmt
-> EHLO balance.peplink.com
<-> 250-smtp.gmail.com at your service, [14.192.209.255]
<-> 250-SIZE 35882577
<-> 250-8BITMIME
<-> 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
<-> 250-ENHANCEDSTATUSCODES
<-> 250-PIPELINING
<-> 250-CHUNKING
<-> 250 SMTPUTF8
-> AUTH PLAIN AGdwc2dhbjk0QGdtYVlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

15.1.6 Event Log

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

Send Events to Remote Syslog Server ?	
Remote Syslog	<input type="checkbox"/>
Remote Syslog Host	<input type="text"/>
Port:	<input type="text" value="514"/>

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

URL Logging	
Enable	<input checked="" type="checkbox"/>
Log Server Host	<input type="text"/>
Port:	<input type="text" value="514"/>

Session Logging	
Enable	<input checked="" type="checkbox"/>
Log Server Host	<input type="text"/>
Port:	<input type="text" value="514"/>

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.
URL Logging	This setting is to enable event logging at the specified log server.
URL Logging Host	This setting specifies the IP address or hostname of the URL log server.
Session Logging	This setting is to enable event logging at the specified log server.
Session	This setting specifies the IP address or hostname of the Session log server.

Logging Host



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

15.1.7 SNMP

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

SNMP Settings	
SNMP Device Name	Balance_0D84
SNMP Port	161 <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

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

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

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

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

The dialog box titled "SNMP Community" contains the following fields:

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

Buttons: Save, Cancel

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

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

The dialog box titled "SNMPv3 User" contains the following fields:

User Name	SNMPUser
Authentication	SHA password
Privacy	DES privacypassword

Buttons: Save, Cancel

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

15.1.8 SMS Control

SMS Control allows the user to control the device using SMS even if the modem does not have a data connection. The settings for configuring the SMS Control can be found at **System>SMS Control**.

Note: Supported Models

- **Balance/MAX:** *-LTE-E, *-LTEA-W, *-LTEA-P, *-LTE-MX
- **EPX:** *-LW*, *-LP*

The screenshot shows the 'SMS Control' configuration page. The 'Enable' checkbox is currently unchecked. There is a help icon (?) next to the checkbox.

When this box is checked, the device will be allowed to take actions according to received commands via SMS.

Make sure your mobile plan supports SMS, and note that some plans may incur additional charges for this.

SMS Control can reboot devices and configure cellular settings over signalling channels, even if the modem does not have an active data connection.

For details of supported SMS command sets, please refer to our [knowledge base](#).

The screenshot shows the 'SMS Control' configuration page with the 'Enable' checkbox checked. Below it is a 'Password' field with a 'Hide Characters' checkbox checked. At the bottom is a 'White List' table with one row containing 'Phone Number' and a '+' button to add more entries.

Save

SMS Control Settings	
Enable	Click the checkbox to enable the SMS Control.
Password	This setting sets the password for authentication - maximum of 32 characters, which cannot include semicolon (;).
White List	Optionally, you can add phone number(s) to the whitelist. Only matching phone numbers are allowed to issue SMS commands. Phone numbers must be in the E.164 International Phone Numbers format.

15.1.9 InControl

Controller Management Settings	
Controller	<input data-bbox="540 405 565 436" type="button" value="?"/> InControl ▾ <input type="checkbox"/> Restricted to Status Reporting Only
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/> <input type="text"/> <input type="checkbox"/> 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.

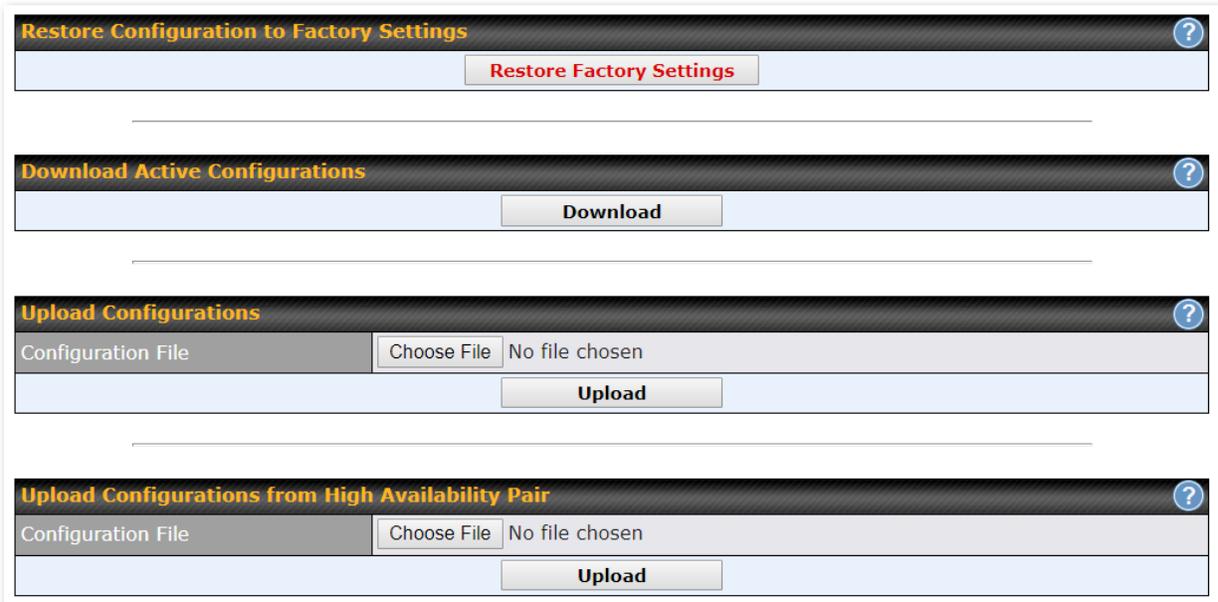
When the box **Restricted to Status Reporting Only** is ticked, the router will only report its status, but can't be managed or configured by InControl.

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.

15.1.10 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**.



The screenshot shows the Configuration page with the following sections:

- Restore Configuration to Factory Settings**: A button labeled "Restore Factory Settings".
- Download Active Configurations**: A button labeled "Download".
- Upload Configurations**: A file selection area with a "Choose File" button and "No file chosen" text, followed by an "Upload" button.
- Upload Configurations from High Availability Pair**: A file selection area with a "Choose File" button and "No file chosen" text, followed by an "Upload" button.

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.

15.1.11 Feature Add-ons

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



The image shows a web form titled "Feature Activation". It has a dark header with the title in orange. Below the header is a light gray area with the text "Activation Key" on the left and a large, empty white text input field on the right.

15.1.12 Reboot

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

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



The image shows a web form titled "Reboot System" with a help icon in the top right corner. The form contains the text "Select the firmware you want to use to start up this device:" followed by two radio button options: "Firmware 1: 8.0.1b01 build 2658 (Running)" and "Firmware 2: 8.0.0 build 2636". Below the options is a "Reboot" button.

15.2 Tools

15.2.1 Ping

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

Ping

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

Results

```

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.

15.2.2 Traceroute

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

Traceroute

Connection: WAN 1

Destination: 64.233.189.99

Start Stop

Results Clear Log

```

Traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 30 bytes packet
 0 10.86.137.254 (10.86.137.254) 0.708 ms 6.472 ms 6.267 ms
 1 10.86.86.254 (10.86.86.254) 0.819 ms 5.190 ms 5.446 ms
 2 10.86.86.1 (10.86.86.1) 1.070 ms 5.520 ms 5.960 ms
 3 10.86.3.2 (10.86.3.2) 0.182 ms 0.200 ms 0.196 ms
 4 118.183.88.254 (118.183.88.254) 0.264 ms 1.76.175.240.22 (118.175.240.22) 0.707 ms 118.183.88.254 (118.183.88.254) 0.472 ms
 5 192.75.46.128 (192.75.46.128) 0.488 ms 198.95.228.46 (198.95.228.46) 0.293 ms 0.293 ms
 6 200.128.1.128 (200.128.1.128) 0.301 ms 7.488 ms 7.488 ms
 7 198.176.86.184 (198.176.86.184) 4.811 ms 200.128.6.1 (200.128.6.1) 4.472 ms 192.75.108.128 (192.75.108.128) 4.241 ms
 8 200.128.6.220 (200.128.6.220) 0.228 ms 70.14.194.246 (70.14.194.246) 0.401 ms 200.128.6.220 (200.128.6.220) 4.478 ms
 9 70.14.233.20 (70.14.233.20) 0.842 ms 74.125.46.158 (74.125.46.158) 4.877 ms 70.14.233.20 (70.14.233.20) 0.884 ms
10 70.14.233.20 (70.14.233.20) 0.884 ms 209.85.252.161 (209.85.252.161) 7.315 ms 209.85.243.30 (209.85.243.30) 4.484 ms
11 209.85.252.213 (209.85.252.213) 4.872 ms 209.85.242.143 (209.85.242.143) 4.888 ms 0.888 ms
12 216.239.50.47 (216.239.50.47) 0.892 ms * 7.392 ms
13 64.233.189.99 (64.233.189.99) 0.176 ms 0.144 ms 0.832 ms
    
```

Tip

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

15.2.3 Wake-on-LAN

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

Wake-on-LAN

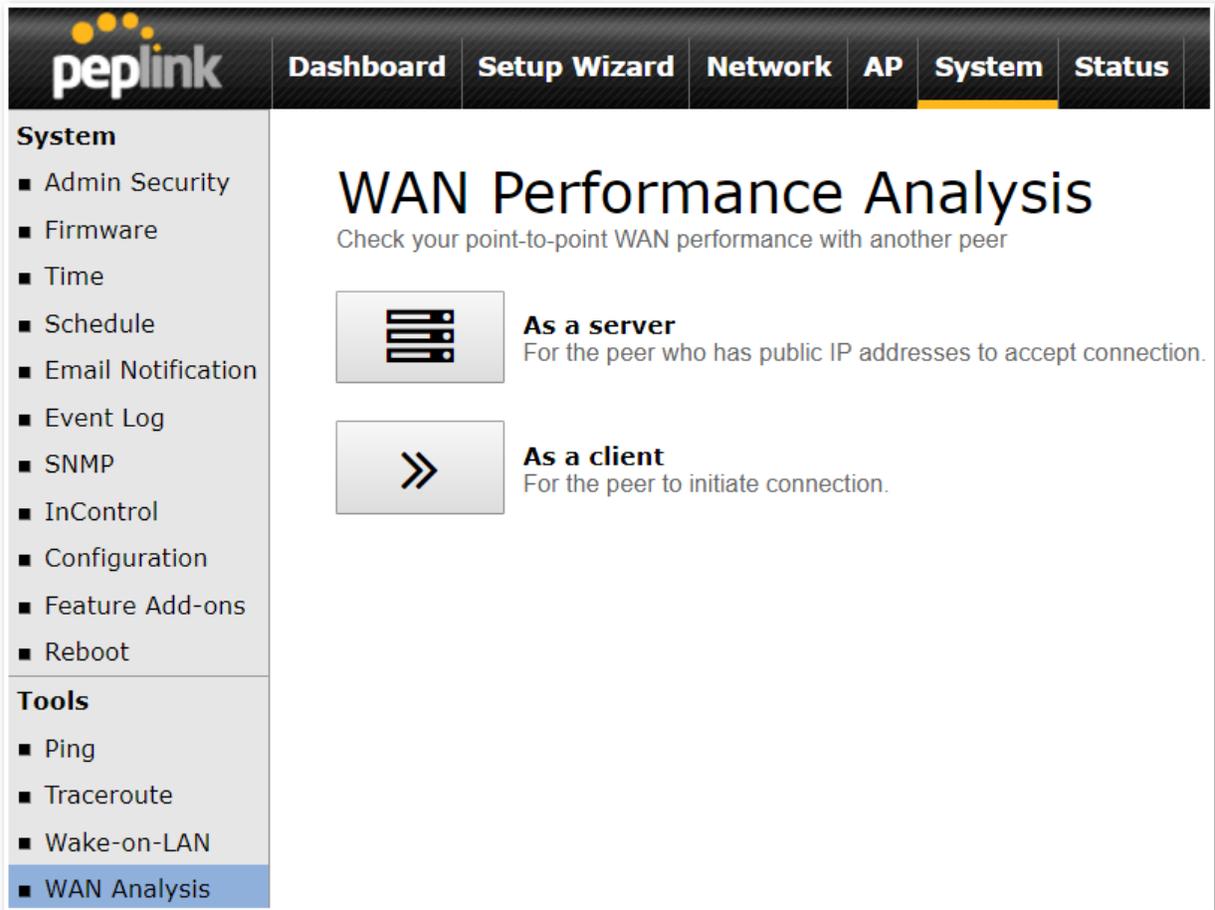
Wake-on-LAN Target: Custom MAC Address... 00:00:00:00:00:00 Send

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

15.2.4 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.



The screenshot shows the Peplink web interface. The top navigation bar includes: Dashboard, Setup Wizard, Network, AP, System (highlighted), and Status. The left sidebar menu is divided into 'System' and 'Tools' sections. Under 'System', there are items: Admin Security, Firmware, Time, Schedule, Email Notification, Event Log, SNMP, InControl, Configuration, Feature Add-ons, and Reboot. Under 'Tools', there are items: Ping, Traceroute, Wake-on-LAN, and WAN Analysis (highlighted in blue). The main content area is titled 'WAN Performance Analysis' with the subtitle 'Check your point-to-point WAN performance with another peer'. Below this, there are two options: 'As a server' (represented by a server rack icon) and 'As a client' (represented by a right-pointing arrow icon).

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.

The screenshot shows the Peplink web interface with the following elements:

- Navigation Bar:** Dashboard, Setup Wizard, Network, AP, System (selected), Status, Apply Changes
- System Menu:** Admin Security, Firmware, Time, Schedule, Email Notification, Event Log, SNMP, InControl, Configuration, Feature Add-ons, Reboot
- Tools Menu:** Ping, Traceroute, Wake-on-LAN, WAN Analysis (selected)
- WAN Performance Analysis Page:**
 - Server Settings:**

Status	<input checked="" type="checkbox"/> Listening (Control Port: 6000)
Control Port	<input type="text" value="6000"/>
<input type="button" value="Apply"/> <input type="button" value="Stop"/>	
 - WAN Connection Status:**

<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.22.1.182
<input type="checkbox"/> WAN 2	<input type="checkbox"/> Disabled
<input type="checkbox"/> WAN 3	<input type="checkbox"/> Disabled
<input type="checkbox"/> WAN 4	<input type="checkbox"/> Disabled
<input type="checkbox"/> WAN 5	<input type="checkbox"/> Disabled
<input type="checkbox"/> Mobile Internet	<input type="checkbox"/> 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.

System

- Admin Security
- Firmware
- Time
- Schedule
- Email Notification
- Event Log
- SNMP
- InControl
- Configuration
- Feature Add-ons
- Reboot

Tools

- Ping
- Traceroute
- Wake-on-LAN
- WAN Analysis**
- Storage Manager
- Package Manager

WAN Performance Analysis

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

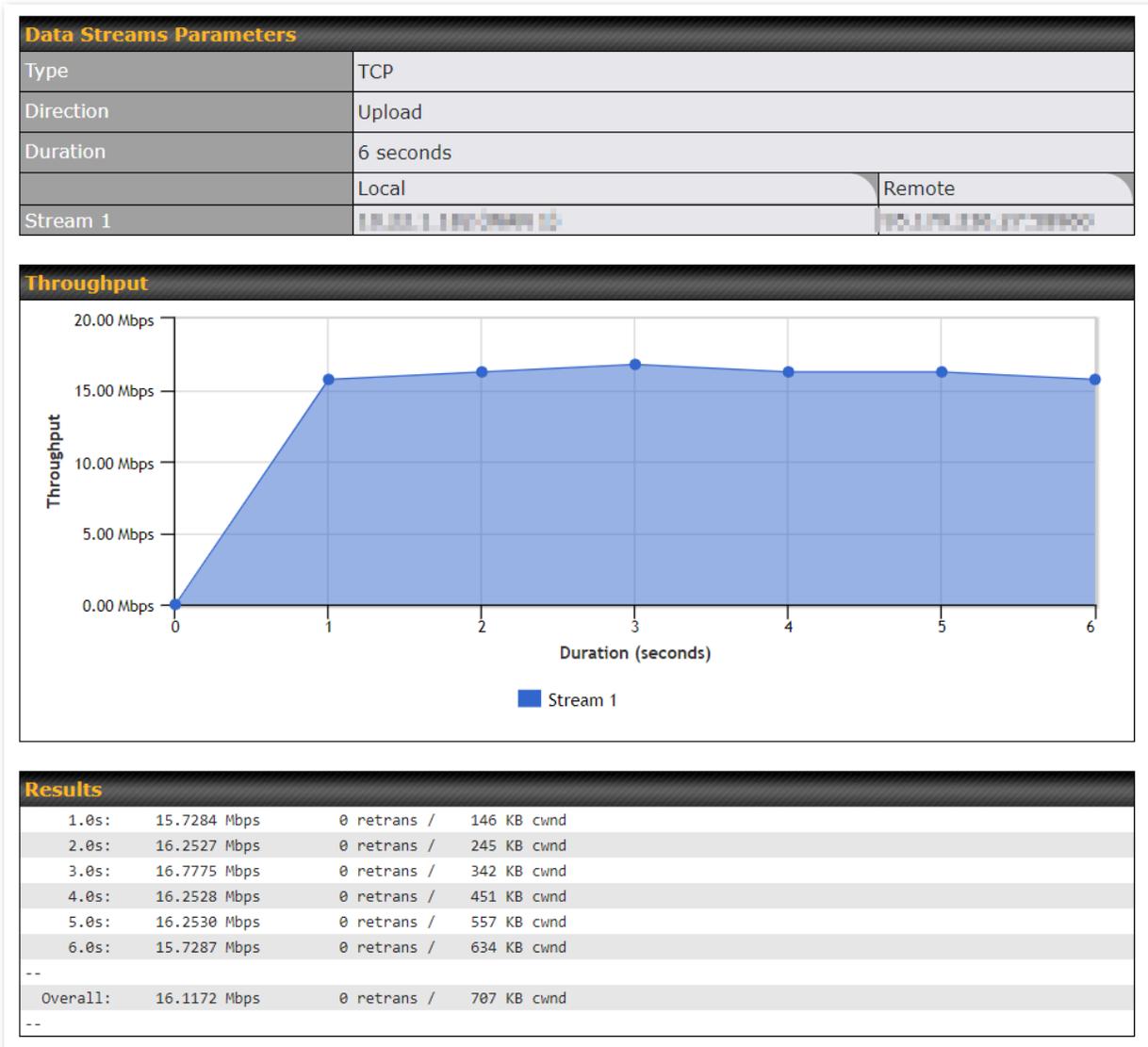
Client Settings

Control Port	6000
Data Port	57280 - 57287
Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download
Duration	20 seconds (5 - 600)

Data Streams

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**.

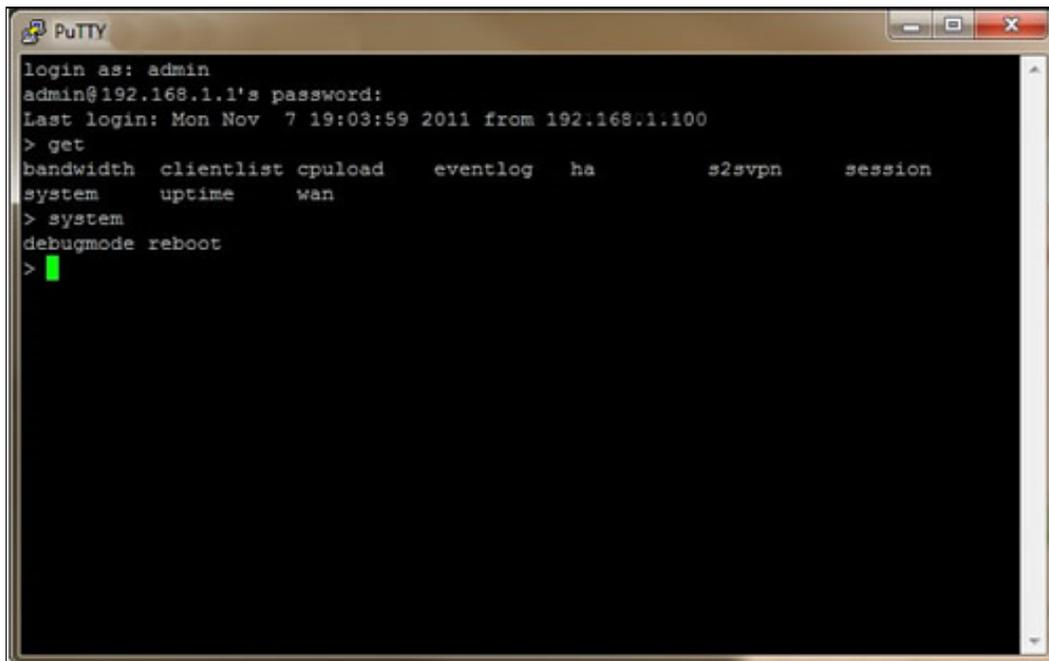


The test can be run again once it's complete by clicking the **Start** button or you can click **Close** and change the parameters for the test.

15.3 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
> get
bandwidth  clientlist  cpuload    eventlog  ha          s2svpn     session
system    uptime    wan
> system
debugmode  reboot
> █
```

16 Status Tab

16.1 Status

16.1.1 Device

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

System Information	
Router Name	Mediafast
Model	Peplink MediaFast 500
Product Code	MFA-500-B
Hardware Revision	2
Serial Number	
Firmware	8.0.0b03 build 2593
PepVPN Version	8.0.0
Modem Support Version	1022 (Modem Support List)
Host Name	mediafast
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	10:56:00:00:00:00
WAN 1	10:56:00:00:00:00
WAN 2	10:56:00:00:00:00
WAN 3	10:56:00:00:00:00
WAN 4	10:56:00:00:00:00
WAN 5	10:56:00:00:00:00

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.

16.1.2 Active Sessions

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

Overview
Search

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
WAN 5	0	2
WAN 6	0	0

Top Clients

Client IP Address	Total Sessions
10.22.1.100	116
10.22.1.101	90
172.16.17.100	86
10.22.1.102	83
172.16.17.101	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**.

Overview
Search

Session data captured 2 mins ago. [Refresh](#)

IP / Subnet	Source or Destination ▾ <input type="text" value="255.255.255.255 (/32) ▾"/>
Port	Source or Destination ▾ <input type="text"/>
Protocol / Service	Spotify ▾
Interface	<input type="checkbox"/> 1 BT <input type="checkbox"/> 2 Virgin Media <input type="checkbox"/> 3 WAN 3 <input type="checkbox"/> 4 WAN 4 <input type="checkbox"/> 5 Peplink HK Net... <input type="checkbox"/> Mobile Internet <input type="checkbox"/> VPN

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
TCP	10.0.0.1:58827	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.0.0.1:58828	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.0.0.1:58784	35.186.224.47:443	SSL/Spotify	BT	00:00:10
TCP	10.0.0.1:65369	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.

16.1.3 Client List

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

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

Filter		<input type="checkbox"/> Online Clients Only	<input type="checkbox"/> DHCP Clients Only		
Client List ?					
IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
192.168.167.10		0	0	10:56:56:56:56:56	
192.168.167.11	U64-2-1	0	0	00:50:56:56:49:1A	
192.168.167.12	U64-2-2	0	0	10:56:56:56:56:75	

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

In the client list table, there is a “Ban Client” feature which is used to disconnect the Wi-Fi and Remote User Access clients by clicking the button on the right.

Filter		<input type="checkbox"/> Online Clients Only	<input type="checkbox"/> DHCP Clients Only				
Client List ?							
IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)	
		0	0				
		0	0			-37	
		0	0				

There is a blocklist on the same page after you banned the Wi-Fi or Remote User Access clients.

Filter		<input type="checkbox"/> Online Clients Only	<input type="checkbox"/> DHCP Clients Only			
Access restriction in action, some clients are currently banned.						
Client List ?						
IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)

You may also unblock the Wi-Fi or Remote User Access clients when the client devices need to reconnect the network by clicking the button on the right.

Prohibited Client Access			
Service	Client	Blocked	
Wi-Fi	MAC address: B8:C3:85:41:	1 minute ago	

Close

16.1.4 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

Flush All

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.

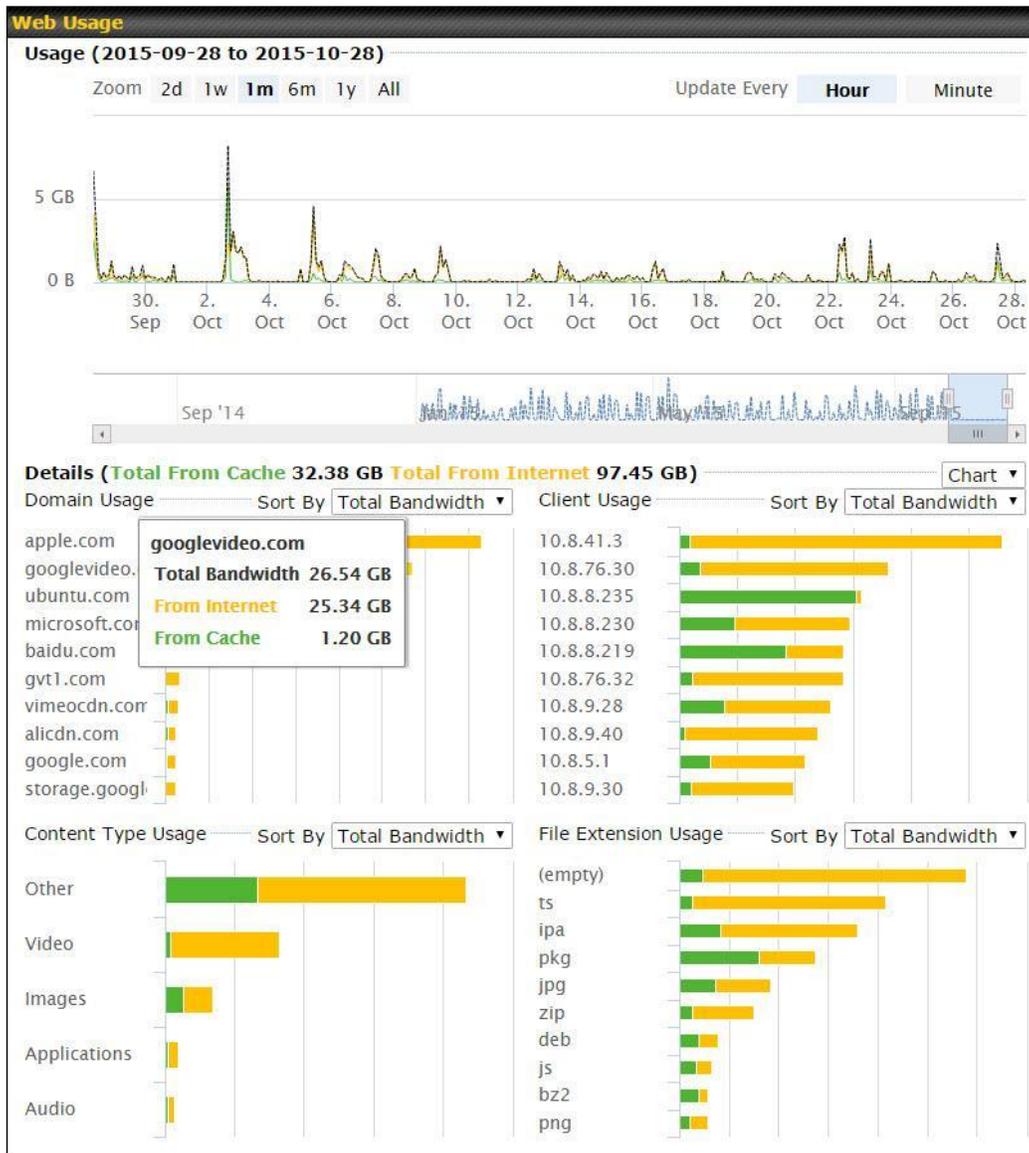
16.1.5 OSPF & RIPv2

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

peplink		Dashboard	Setup Wizard	Network	AP	System	Status	Apply Changes						
Status ■ Device ■ Active Sessions ■ Client List ■ OSPF & RIPv2 ■ BGP		OSPF & RIPv2 <table border="1"> <thead> <tr> <th>Area</th> <th>Remote Networks</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0</td> <td></td> </tr> <tr> <td>PepVPN</td> <td>10.0.2.0/24 10.0.3.0/24 192.168.63.0/24 10.0.100.0/24 192.168.100.0/24 192.168.162.0/24</td> </tr> </tbody> </table>							Area	Remote Networks	0.0.0.0		PepVPN	10.0.2.0/24 10.0.3.0/24 192.168.63.0/24 10.0.100.0/24 192.168.100.0/24 192.168.162.0/24
Area	Remote Networks													
0.0.0.0														
PepVPN	10.0.2.0/24 10.0.3.0/24 192.168.63.0/24 10.0.100.0/24 192.168.100.0/24 192.168.162.0/24													

16.1.6 MediaFast

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



16.1.7 PepVPN / SpeedFusion Status

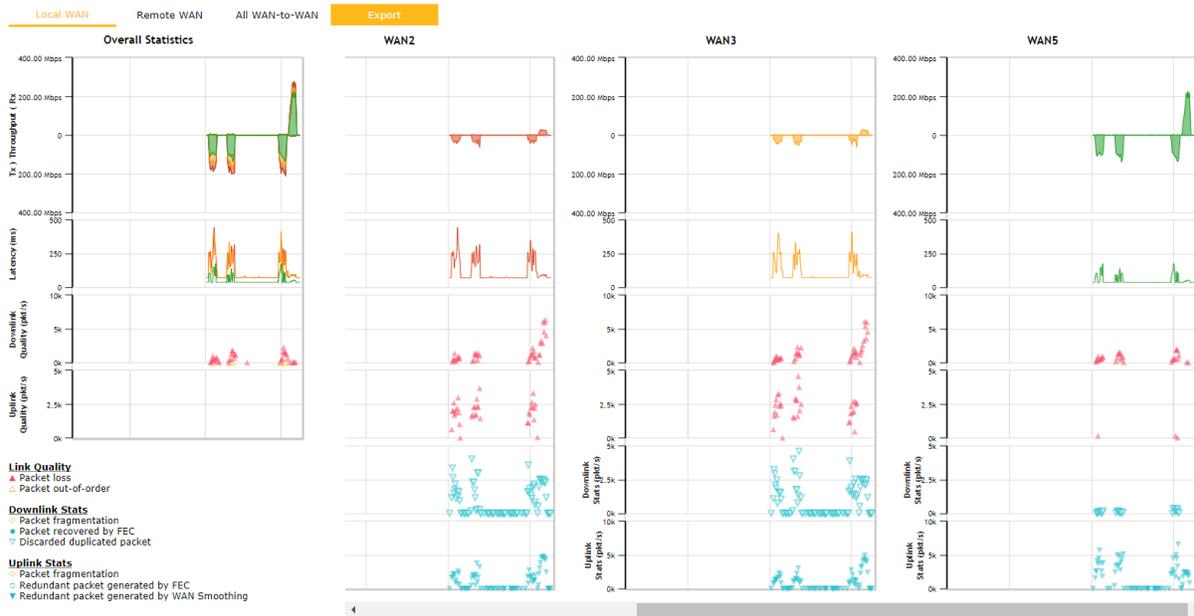
PepVPN/SpeedFusion Status shows the current connection status of each connection profile and is displayed at **Status> PepVPN/SpeedFusion**.

Remote Peer	Profile	Information
MAX-BR1-1000 (1000-1000-1000-1000)	1000	1000-1000-1000-1000 1000-1000-1000-1000 1000-1000-1000-1000
MAX-BR1-1000 (1000-1000-1000-1000)	1000	1000-1000-1000-1000 1000-1000-1000-1000 1000-1000-1000-1000

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

Remote Peer	Profile	Information
SFC-SIN-001 (SFC-SIN-001)	SFC	SpeedFusion Cloud
WAN1		Not available - WAN disabled
WAN2	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 42 ms
WAN3	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 42 ms
WAN4		Not available - WAN disabled
WAN5	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 10 ms
Mobile Internet	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 32 ms
Total	Rx: < 1 kbps Tx: 1.1 kbps	Loss rate: 0.0 pkt/s

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



When pressing the  button for a PepVPN/SpeedFusion Tunnel Bandwidth Test Tool, the following menu will appear:

PepVPN Details ✕

Connection Information More information

Profile	SFC
Remote ID	SFC-SIN-001
Device Name	SFC-SIN-001
Serial Number	1197-A047-2E3D

WAN Statistics 📊

Remote Connections	<input type="checkbox"/> Show remote connections					
WAN Label	<input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port					
<input type="checkbox"/> WAN1	Not available - WAN disabled					
<input checked="" type="checkbox"/> WAN2	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 43 ms
<input checked="" type="checkbox"/> WAN3	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 44 ms
<input type="checkbox"/> WAN4	Not available - WAN disabled					
<input checked="" type="checkbox"/> WAN5	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 10 ms
<input checked="" type="checkbox"/> Mobile Internet	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 42 ms
Total	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s

PepVPN Test Configuration ?

Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<div style="border: 1px solid #ccc; padding: 10px; width: 50px; margin: 0 auto;">Start</div>
Streams	4 ▼	
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download	
Duration	20 seconds (5 - 600)	

The **connection information** shows the details of the selected PepVPN profile, consisting of the Profile name, **Router ID**, **Router Name** 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	<input checked="" type="checkbox"/> Show remote connections
WAN Label	<input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port
■ BT	
<input checked="" type="checkbox"/> WAN	Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 17 ms
■ Virgin Media	Not available - WAN disabled

The PepVPN/SpeedFusion test configuration allows us to configure and perform thorough tests. This is usually done after the initial installation of the routers and in case there are problems with aggregation.

PepVPN Test Configuration 	
Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Streams	4 ▼
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download
Duration	20 seconds (5 - 600)
<input type="button" value="Start"/>	

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			

16.1.8 Event Log

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

Device Event Log

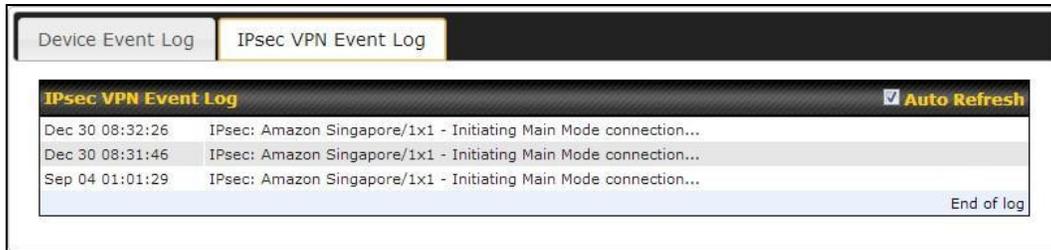
The screenshot shows the 'Device Event Log' interface. At the top, there are two tabs: 'Device Event Log' (selected) and 'ContentHub Event Log'. Below the tabs, the 'Device Event Log' section has a title bar with 'Auto Refresh' checked. The log contains the following entries:

Timestamp	Event Description
Apr 17 14:54:52	System: All user services (controlled by WAN 001-4034 [on 192.168.100.100]) are restarted
Apr 17 14:39:44	System: All user services (controlled by WAN 001-4034 [on 192.168.100.100]) are restarted temporarily.
Apr 17 09:12:42	System: Changes applied
Apr 17 09:07:33	Admin: Remote web admin initiated from IPControl 2 by user@2016peplink.com
Apr 16 10:01:13	System: System: WAN 001-4034 [on 192.168.100.100] connected to gateway [WAN leave it alone]
Apr 16 10:00:23	System: Changes applied
Apr 16 09:59:04	System: Changes applied
Apr 16 09:58:57	WAN: User Mode (connected) (Created)
Apr 16 09:57:10	System: System: WAN 001-4034 [on 192.168.100.100] disconnected to gateway [WAN leave it alone] (WAN leave it alone)
Apr 16 09:57:04	System: Changes applied
Apr 16 09:56:16	File sharing: An update for WebScheduling 2.0 is available.
Apr 16 09:56:15	System: LAN 001-001 [LAN 001-001 [on 192.168.100.100]] disconnected from WAN LAN 001-4034 [WAN leave it alone]
Apr 16 09:56:15	System: LAN 001-001 [LAN 001-001 [on 192.168.100.100]] disconnected from WAN LAN 001-4034 [WAN leave it alone]
Apr 16 09:56:13	System: Changes applied
Apr 16 09:54:41	Admin: admin (s.d.s.d.s) login successful
Apr 16 09:50:28	System: LAN 001-001 [LAN 001-001 [on 192.168.100.100]] connected to WAN LAN 001-4034
Apr 16 09:50:28	System: System: WAN 001-4034 [on 192.168.100.100] connected to gateway [WAN leave it alone]

At the bottom of the log, there is a 'Clear Log' button.

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.

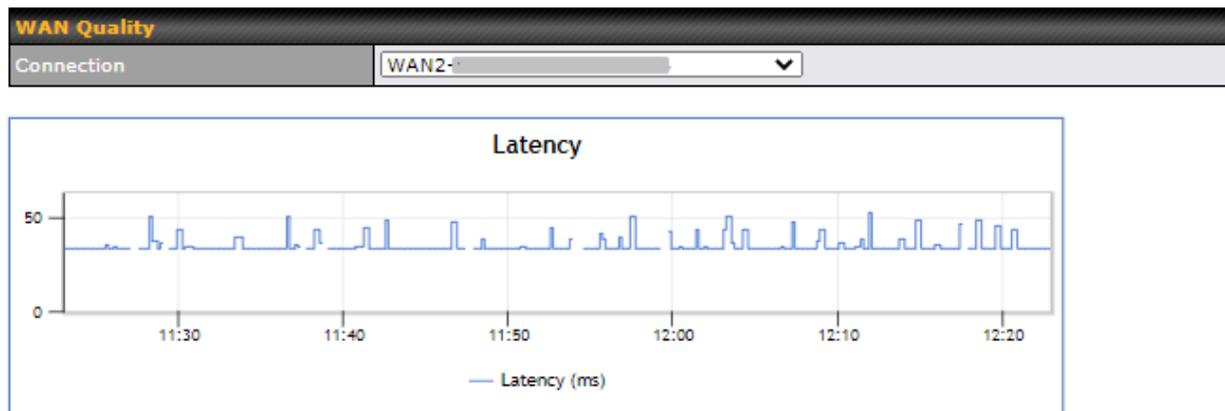
IPsec Event Log



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**.

16.2 WAN Quality



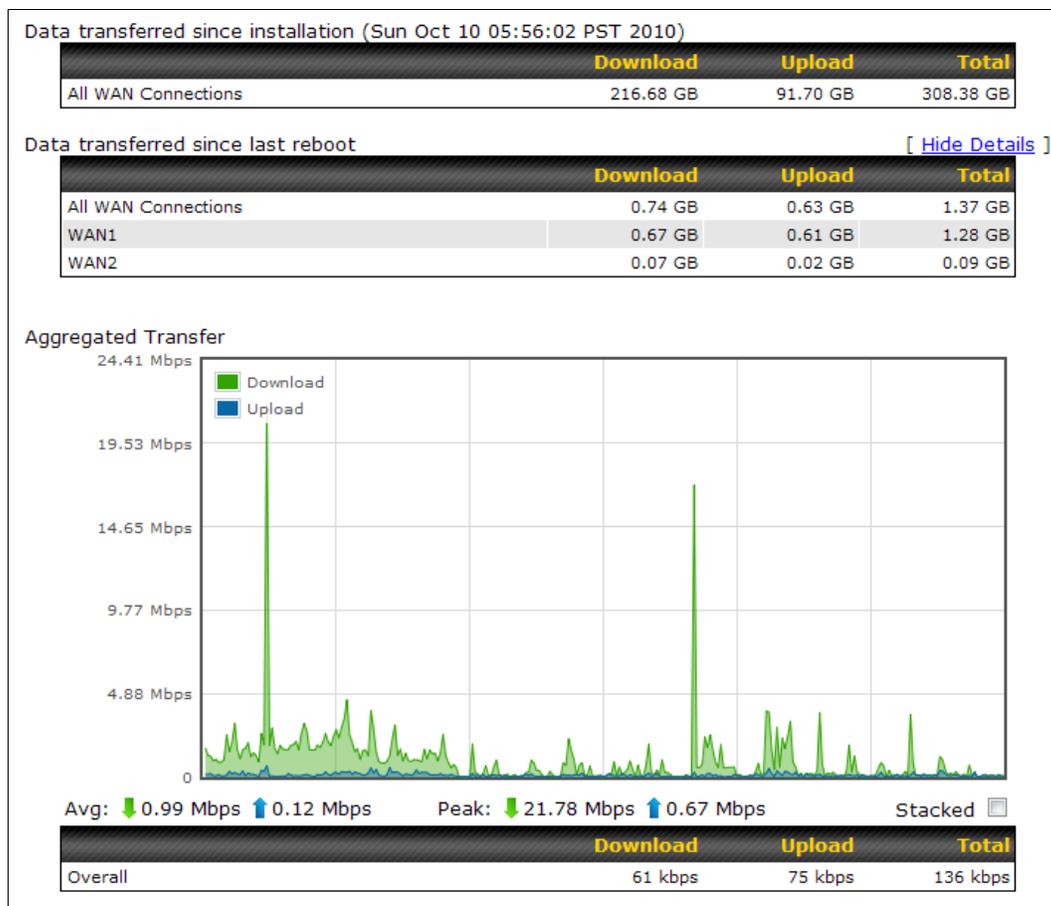
The **Status > WAN Quality** allows to show detailed information about each connected WAN connection.

16.3 Usage Reports

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.

16.3.1 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.



16.3.2 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.



16.3.3 Daily

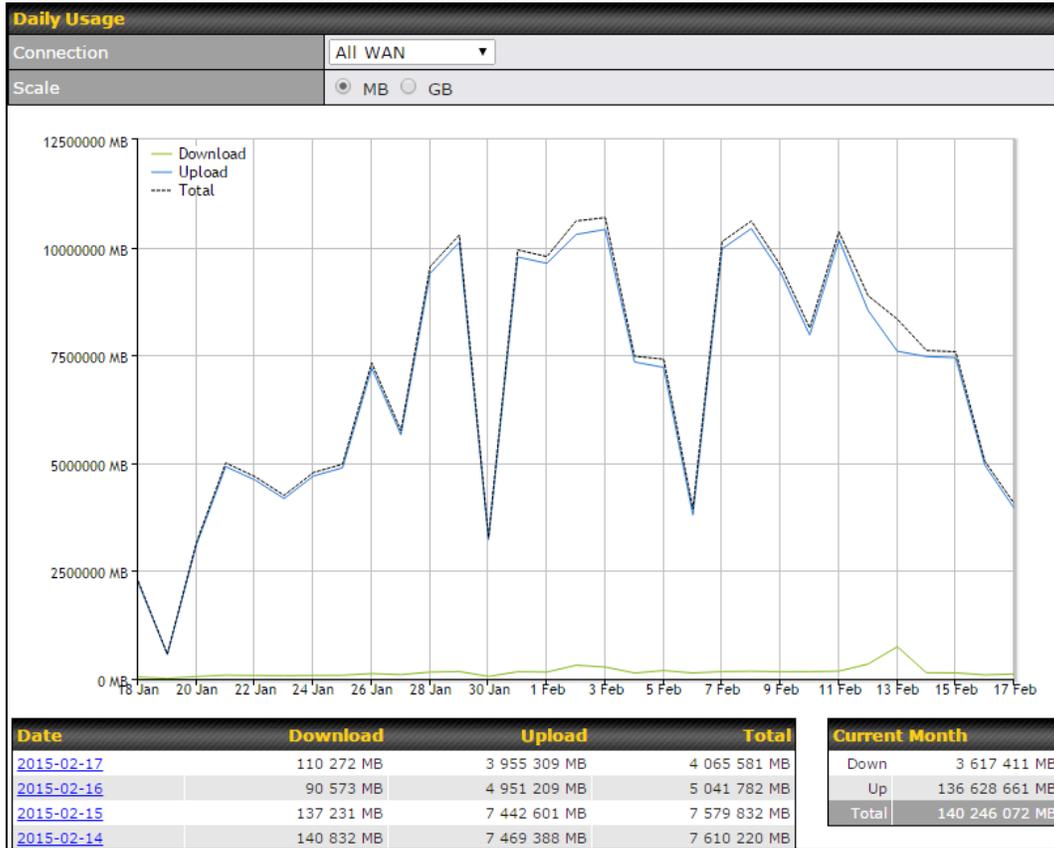
This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

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

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



Status



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

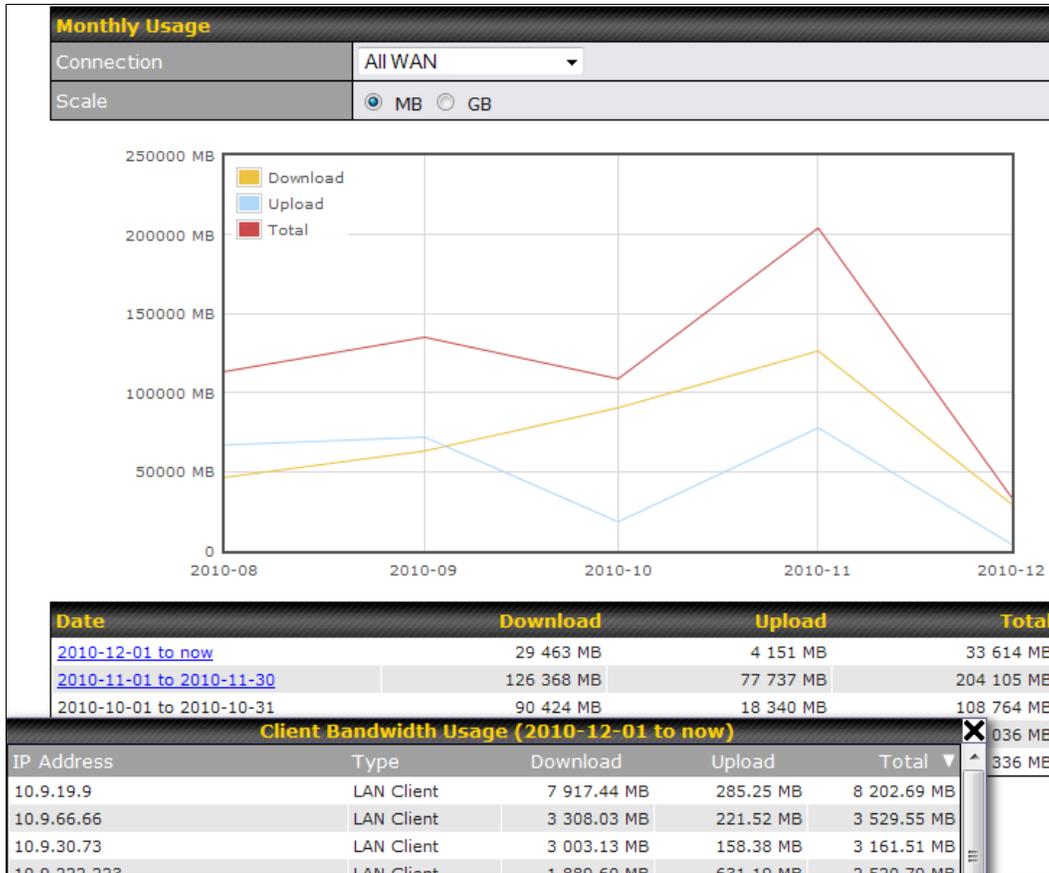
Client Bandwidth Usage (2015-02-15)

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

16.3.4 Monthly

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

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



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

Appendix

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.

Hold for 5-10 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

Hold for approximately 20 seconds for factory reset (Note: The LED status light blinks in RED 3 times and release the button, all WAN/LAN port lights start blinking)

After the Peplink Balance router finishes rebooting, the factory default settings will be restored.

For Balance/MediaFast models with an LCD menu:

- Use the buttons on the 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 previous configurations and bandwidth usage data will be lost after restoring factory default settings. Regular backup of configuration settings is strongly recommended.

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

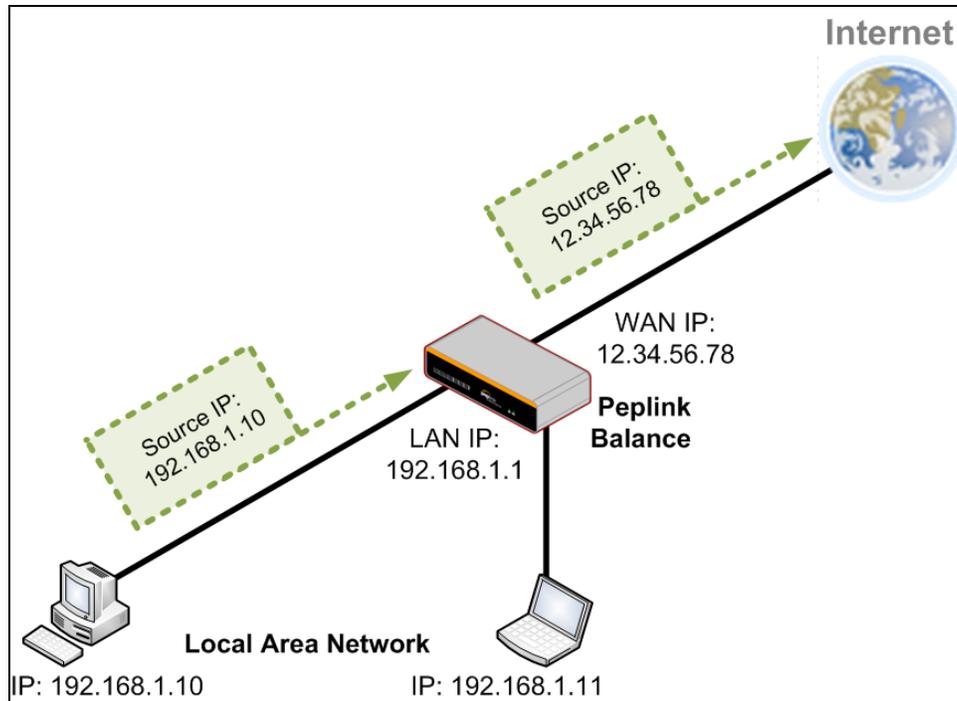
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

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

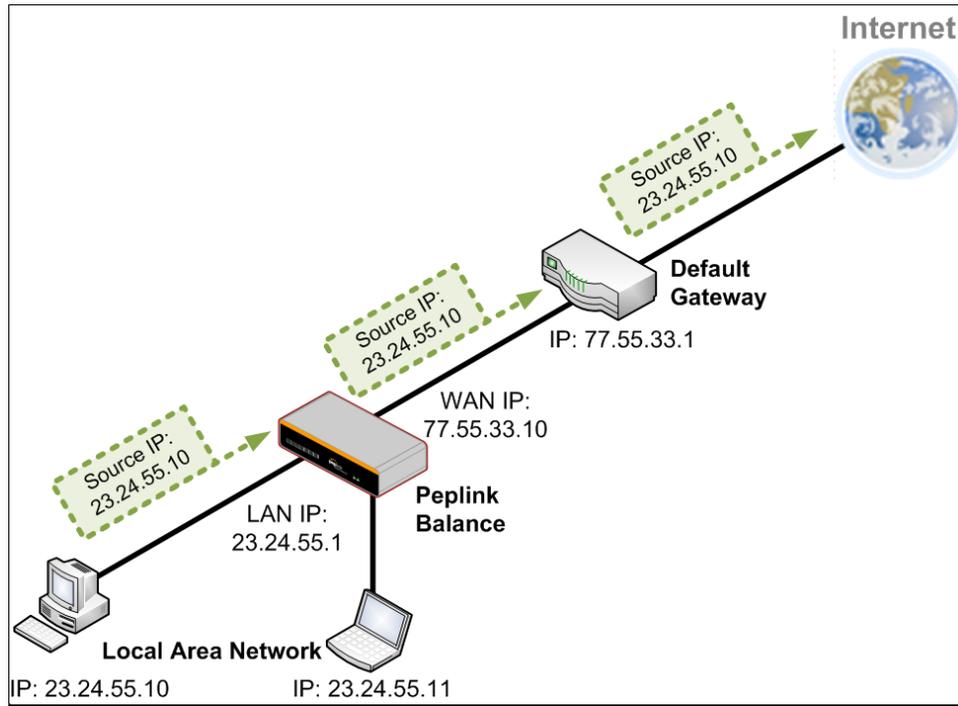
Peplink Balance. They are not directly accessible from the Internet and hence less vulnerable to attacks. The following figure shows the packet flow in NAT mode:



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. FusionSIM Manual

Peplink has developed a unique technology called FusionSIM, which allows SIM cards to remotely link to a cellular router. This can be done via cloud or within the same physical network. There are a few key scenarios to fit certain applications.

The purpose of this manual is to provide an introduction on where to start and how to set up for the most common scenarios and uses.

Requirements

1. A Cellular router that supports FusionSIM technology
2. SIM Injector
3. SIM card

Notes:

- Always check for the latest [Firmware version](#) for both the cellular router and the SIM Injector. You can also check for the latest Firmware version on the device's WEB configuration page.
- A list of products that support FusionSIM can be found on the SIM Injector [WEB page](#). Please check under the section **Supported models**.

SIM Injector reset and login details

How to reset a SIM Injector:

- Hold the reset button for 5-10 seconds. Once the LED status light turns RED, the reset button can be released. SIM Injector will reboot and start with the factory default settings.

The default WEB login settings:

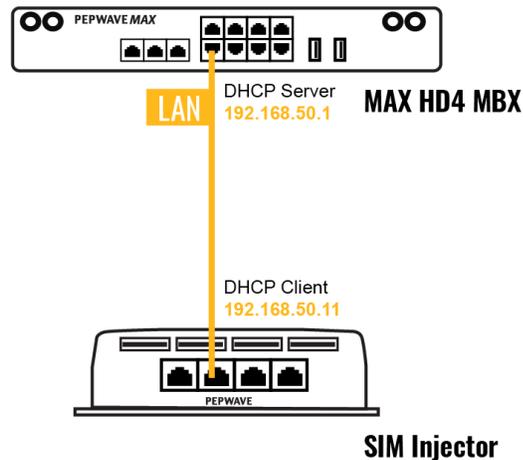
- **User:** admin
- **Password:** admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

Notes:

- The SIM Injector can be monitored via InControl 2. Configuration is not supported.

Scenario 1: SIM Injector in LAN of Cellular Router

Setup topology



This is the most basic scenario in which the SIM Injector is connected directly to the cellular router's LAN port via an ethernet cable. This allows for the cellular router to be positioned for the best possible signal. Meanwhile, the SIM cards can be conveniently located in other locations such as the office, passenger area, or the bridge of a ship. The SIM Injector allows for easily swapping SIM cards without needing to access a cellular router.

IMPORTANT: Cellular WAN will not fallback to the local SIM if it is configured to use the SIM Injector.

Configuring the SIM Injector

1. Connect the SIM Injector to the LAN port of the cellular router.
2. Insert SIM cards into the SIM Injector. The SIM cards will be automatically detected.

IMPORTANT: SIM cards inserted into SIM Injector must not have a PIN code.

Note 1: The SIM Injector gets its IP address via DHCP and doesn't have a static IP address. To find it's address, please check the DHCP lease on the cellular router.

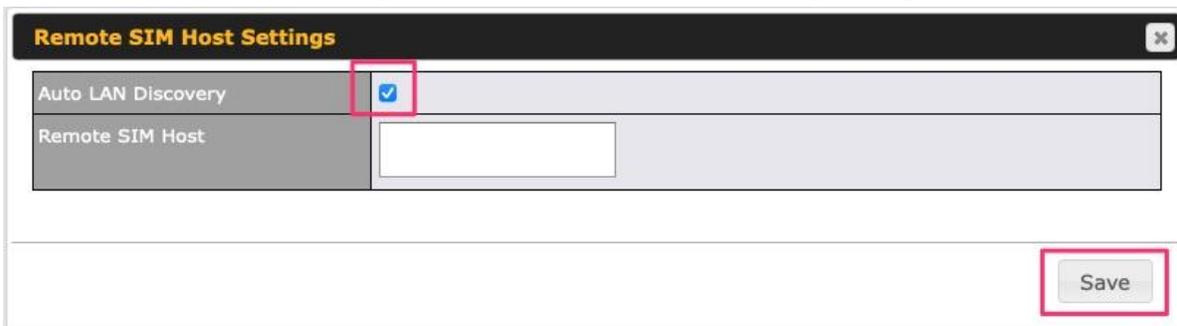
Configuring the Cellular Router

Step 1. Enable the SIM Injector communication protocol.

- 1a. If you are using a Balance cellular router, go to the **Network** tab (top navigation bar).
- 1b. If you are using a MAX cellular router, go to the **Advanced** tab (top navigation bar).
2. Under **Misc. settings** (left navigation bar) find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.



4. Check the **Auto LAN discovery** checkbox and click **Save** and **Apply Changes**.



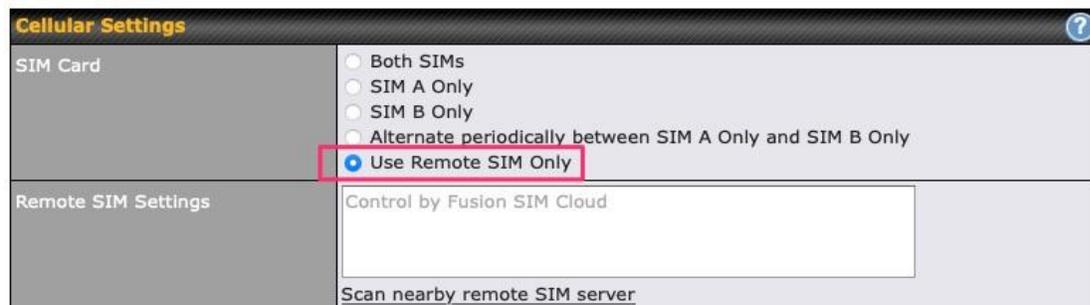
5. Click **Save** and then **Apply Changes**.

Step 2. Enable RemoteSIM for the selected Cellular interface.

1. Go to **Network** (top navigation bar), then **WAN** (left navigation bar) and click **Details** for a selected cellular WAN. This will open the WAN Connection Settings page.



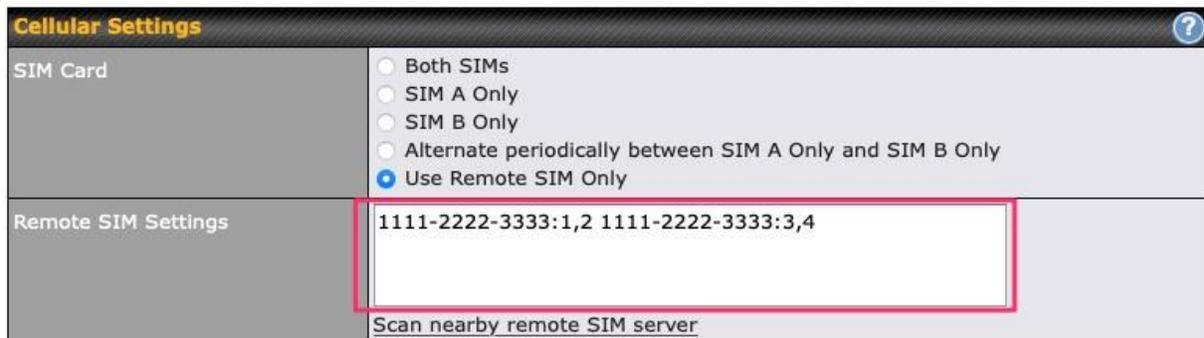
2. Scroll down to **Cellular settings**.
3. In the **SIM Card** section, select **Use Remote SIM Only**.



4. Enter configuration settings in **Remote SIM Settings** section. Click on **Scan nearby remote SIM server** to show the serial number(s) of the connected SIM Injector(s). Available configuration options for cellular interface are shown below:

- A. Defining SIM Injector(s)
 - Format: <S/N>
 - Example 1: 1111-2222-3333
 - Example 2: 1111-2222-3333 4444-5555-6666

- B. Defining SIM Injector(s) SIM slot(s):
 - Format: <S/N:slot number>
 - Example 1: 1111-2222-3333:7,5 (the Cellular Interface will use SIM in slot 7, then 5)
 - Example 2: 1111-2222-3333:1,2 1111-2222-3333:3,4 (the cellular Interface will use SIM in slot 1, then in 2 from the first SIM Injector, and then it will use 3 and 4 from the second SIM Injector).



Note: It is recommended to use different SIM slots for each cellular interface.

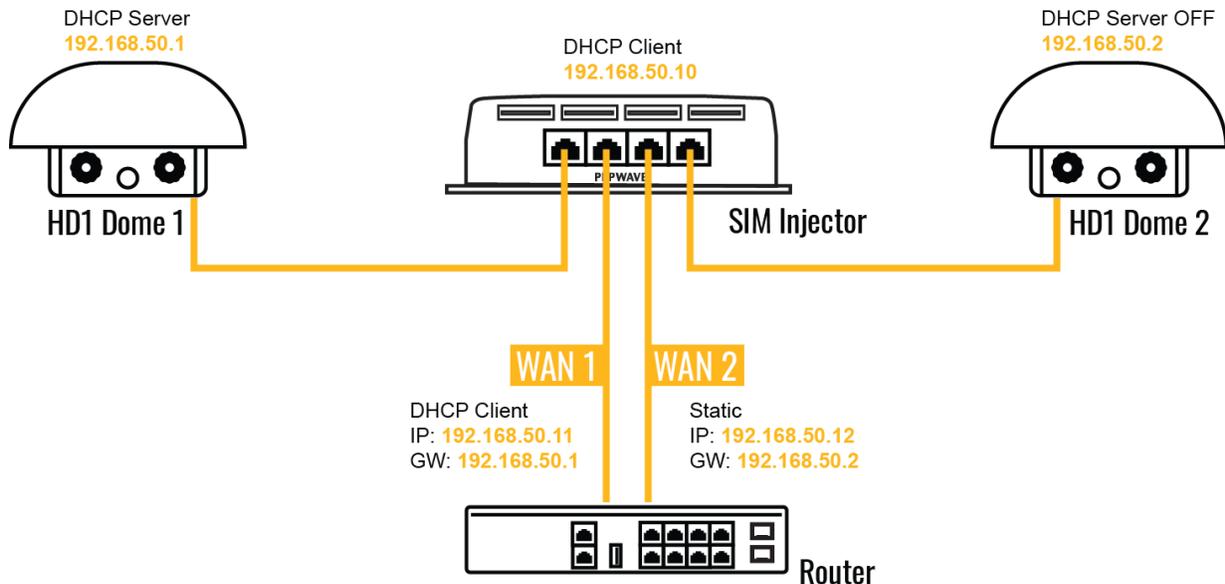
5. Click **Save** and **Apply Changes**.

Step 3. (Optional) Custom SIM cards settings.

- 1a. For a Balance router, go to the **Network** (Top tab).
- 1b. For a MAX router, go to the **Advanced** (Top tab).
2. Under **Misc. settings** (Left-side tab) find **Remote SIM Management**.
3. Click on the **Add Remote SIM** button, fill in all the required info and click **Save**. This section allows defining custom requirements for a SIM card located in a certain SIM slot:
 - Enable/Disable roaming (by default roaming is disabled).
 - Add Custom mobile operator settings (APN, user name, password).
4. Repeat configuration for all SIM cards which need custom settings.
5. Click **Apply Changes** to take effect.

Scenario 2: SIM Injector in WAN of main Router and multiple Cellular Routers

Setup topology



In this scenario, each HD Dome creates a WAN connection to the main router. A single SIM Injector is used to provide SIM cards for each HD Dome. The HD Dome can be replaced with any Peplink cellular router supporting RemoteSIM technology.

This scenario requires the completion of the configuration steps shown in Scenario 1 in addition to the configuration steps explained below.

Additional configurations for Cellular Routers

Step 1. Disable the DHCP server.

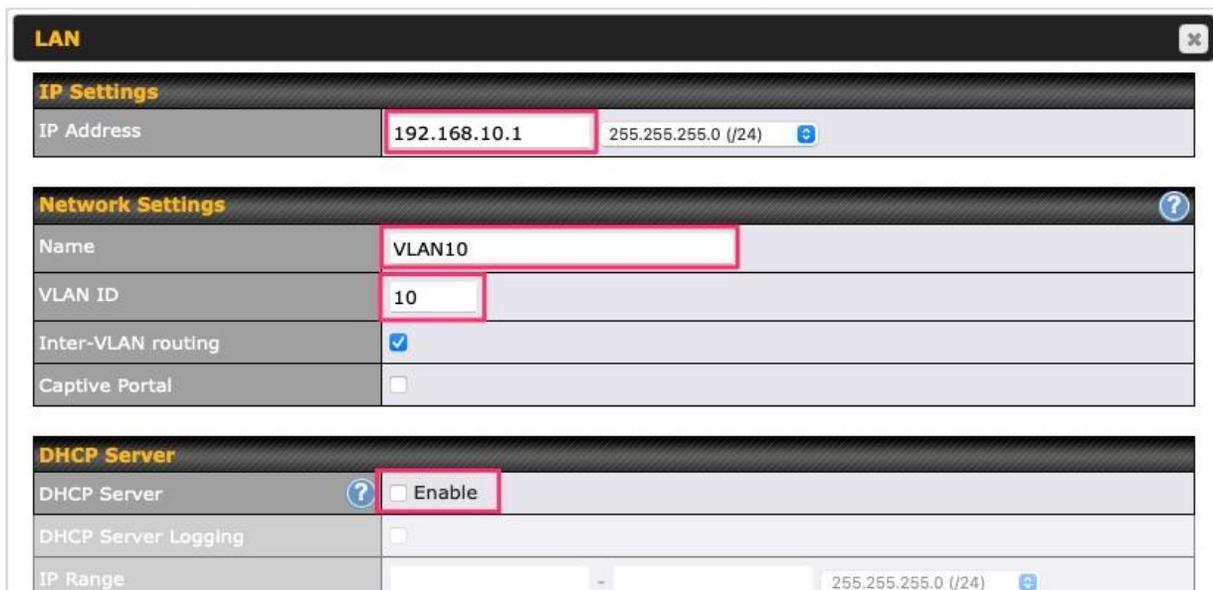
- HD Dome 1 should act as a DHCP server.
- HD Dome 2 should be configured to have a static IP address with DHCP disabled.
- Both routers should be in the same subnet (e.g. 192.168.50.1 and 192.168.50.2).

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **Untagged LAN**. This will open up the LAN settings page.
2. Change the IP address to 192.168.50.2.
3. In the **DHCP Server** section, uncheck the checkbox to disable DHCP Server.
4. Click **Save** and **Apply Changes**.

Step 2. Ethernet port configuration

The Ethernet port must be set to **ACCESS** mode for each HD Dome. To do this, dummy VLANs need to be created first.

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **New LAN**. This will open the settings page to create a dummy VLAN.
2. The image below shows the values that need to be changed to create a new VLAN:



The screenshot shows the LAN configuration interface with three sections: IP Settings, Network Settings, and DHCP Server. The IP address field in IP Settings is highlighted with a red box and contains '192.168.10.1'. In the Network Settings section, the Name field is highlighted with a red box and contains 'VLAN10', and the VLAN ID field is highlighted with a red box and contains '10'. In the DHCP Server section, the 'Enable' checkbox is highlighted with a red box and is unchecked.

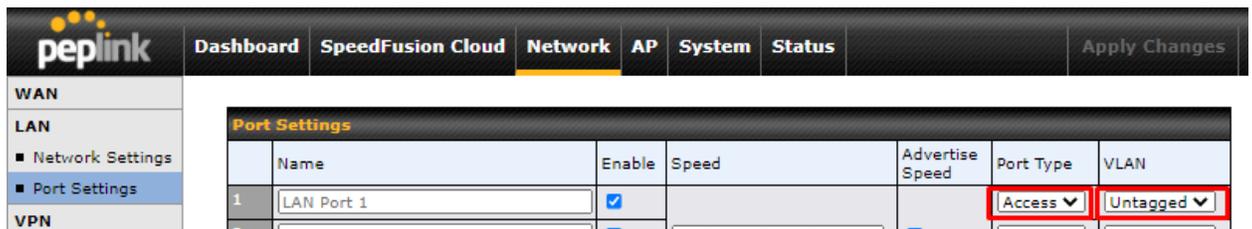
IP Settings	
IP Address	192.168.10.1 255.255.255.0 (/24)

Network Settings	
Name	VLAN10
VLAN ID	10
Inter-VLAN routing	<input checked="" type="checkbox"/>
Captive Portal	<input type="checkbox"/>

DHCP Server	
DHCP Server	<input type="checkbox"/> Enable
DHCP Server Logging	<input type="checkbox"/>
IP Range	- 255.255.255.0 (/24)

Note: set different IP addresses for each HD dome (e.g. 192.168.10.1 and 192.168.10.2).

3. Click **Save** and **Apply Changes**.
4. Go to **Network** (Top tab), then **Port Settings** (Left-side tab).
5. Set the Port Type to **Access** and set VLAN to **Untagged LAN** (see picture below).



6. Click **Save** and **Apply Changes**.

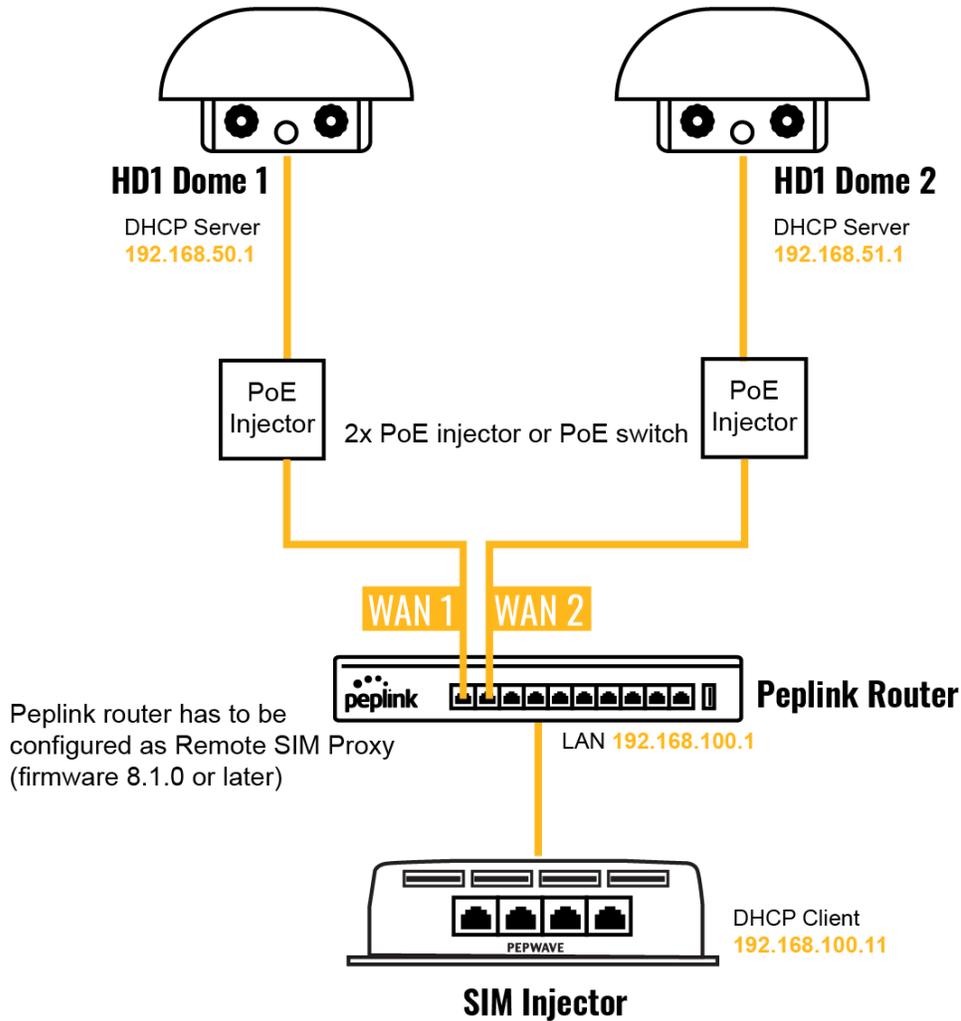
Configuration requirements for the main Router

Requirements for the main router are:

- Configure **WAN 1** as a DHCP client.
- **WAN 1** will automatically get the Gateway IP address from HD Dome 1.
- Configure **WAN 2** as a Static IP and set it to 192.168.50.12.
- Configure **WAN 2** Gateway to 192.168.50.2. Same as the HD Dome 2's IP address.

Scenario 3: SIM Injector in LAN of main Router and multiple Cellular Routers

Setup topology



In this scenario, SIMs are provided to the HD Domes via the main router. In this example, the **Remote SIM Proxy** functionality needs to be enabled on the main router.

Notes:

- HD Dome can be replaced with any other cellular router that supports RemoteSIM.
- It is recommended to use Peplink [Balance series](#) or [X series](#) routers as the main router.

This scenario requires the completion of the configuration steps for the cellular router and the SIM Injector as in Scenario 1. The configuration for the main router is explained below.

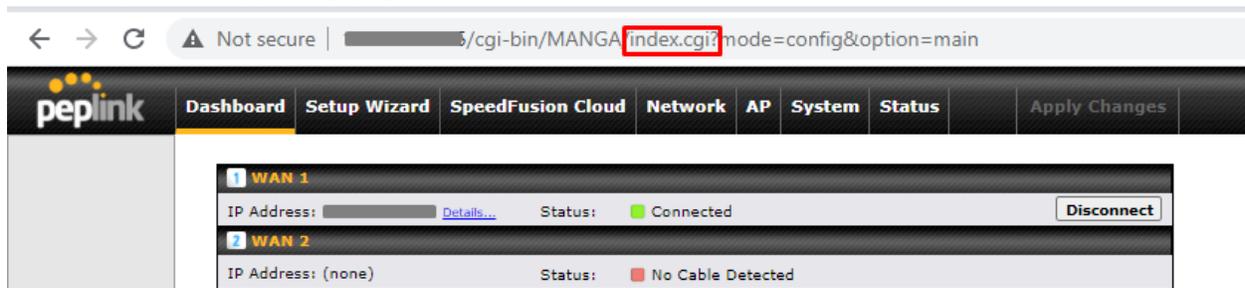
Main Router configuration

IMPORTANT: Main router LAN side and Cellular Routers must be configured using different subnets, e.g. 192.168.**50**.1/24 and 192.168.**100**.1/24.

Note: please make sure the Peplink router is running Firmware 8.1.0 or above.

1. Open the main router WEB interface and change:
From <IP address>/cgi-bin/MANGA/**index.cgi** to <IP address>/cgi-bin/MANGA/**support.cgi**.

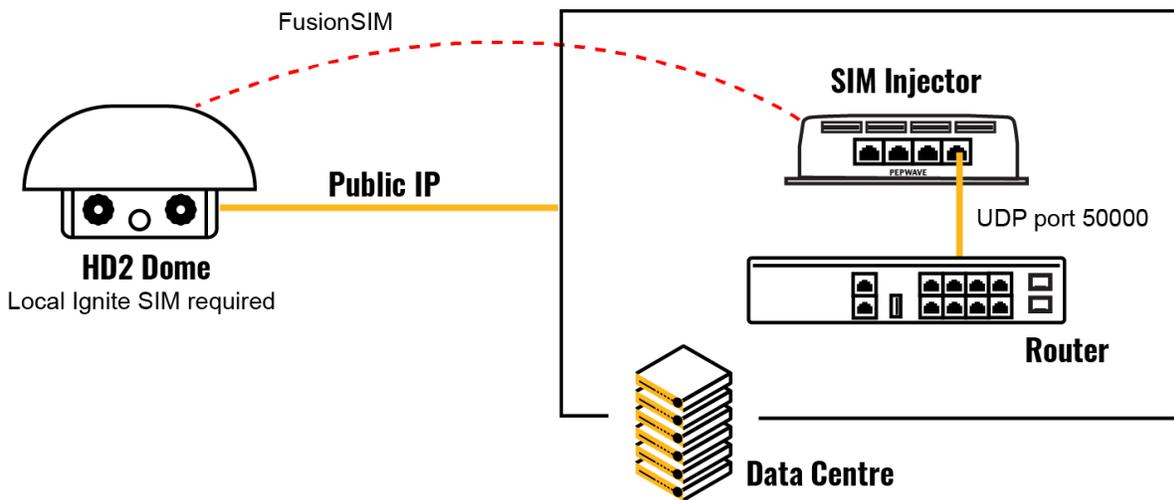
This will open the support.cgi page.



2. Scroll down to find **Remote SIM Proxy** and click on **[click to configure]** that is located next to it.
3. Check the **Enable** checkbox.
4. Click on **Save**.
5. Go back to the index.cgi page and click on **Apply Changes**.

Scenario 4: SIM Injector in a remote location

Setup topology



Requirements for installing a SIM Injector in a remote location:

- Cellular router communicates with the SIM Injector via UDP port 50000. Therefore this port must be reachable via public IP over the Internet.
- The one way latency between the cellular router and the SIM Injector should be **up to 250 ms**. A higher latency may lead to stability issues.
- The cellular router must have Internet connection to connect to the SIM Injector. It can be another Internet connection via Ethernet or Fiber if possible, or a secondary cellular interface with a local SIM (Ignite SIM).
- Due to its high latency, it is not recommended to use satellite WAN for connecting to a SIM Injector in remote locations.

SIM Injector configuration is the same as in Scenario 1.

Cellular Router configuration

Step 1. Enable the SIM Injector communication protocol.

- 1a. For a Balance cellular router, go to the **Network** (Top tab).
- 1b. For a MAX cellular router, go to the **Advanced** (Top tab).
2. Under **Misc. settings** (Left-side tab), find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.
4. Enter the public IP of the SIM Injector and click **Save** and **Apply Changes**.

Remote SIM Host Settings	
Auto LAN Discovery	<input type="checkbox"/>
Remote SIM Host	84.199.92.62

Notes:

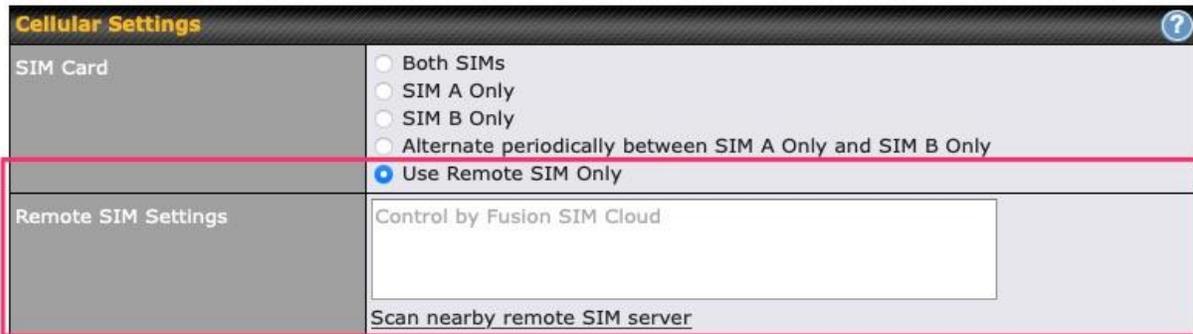
- Do NOT check **Auto LAN Discovery**.
- Adding a SIM Injector serial number to the **Remote SIM Host** field is a mistake!

Step 2. RemoteSIM and custom SIM card settings configurations are the same as in Scenario 1.

How to check if a Pepwave Cellular Router supports Remote SIM

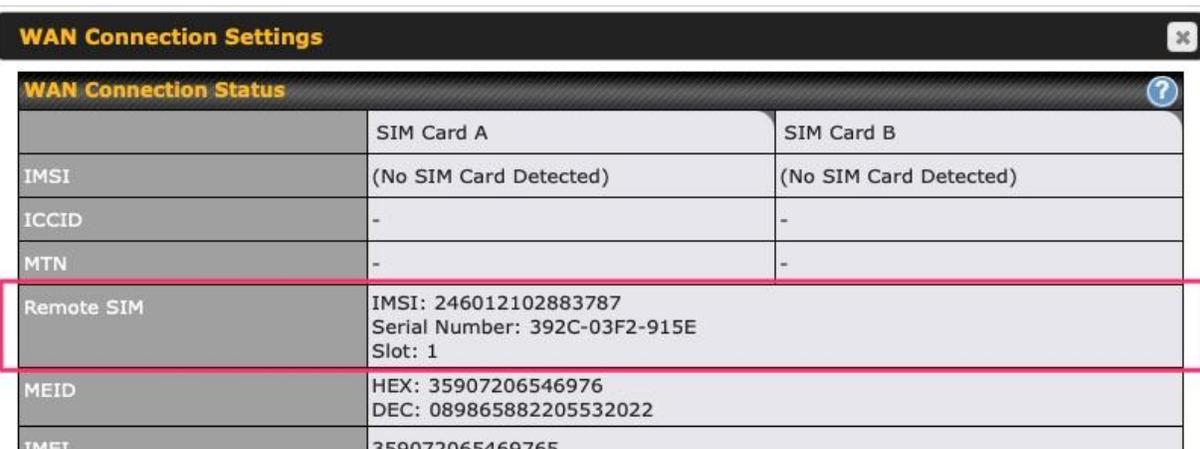
1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on any cellular WAN. This will open the WAN Connection Settings page.
2. Scroll down to **Cellular settings**.

If you can see the **Remote SIM Settings** section, then the cellular router supports RemoteSIM.



Monitor the status of the Remote SIM

1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on the cellular WAN which was configured to use RemoteSIM.
2. Check the **WAN Connection Status** section. Within the cell WAN details, there is a section for **Remote SIM** (SIM card IMSI, SIM Injector serial number and SIM slot).



Appendix D. 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.

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

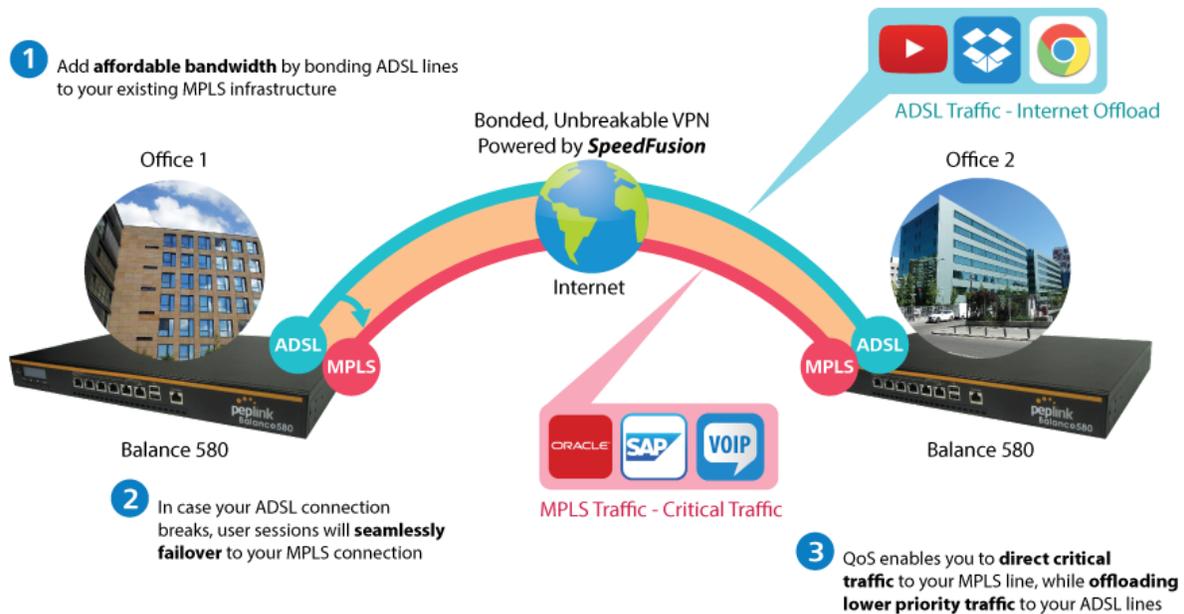
Special features of Balance 580: have high availability capability

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

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

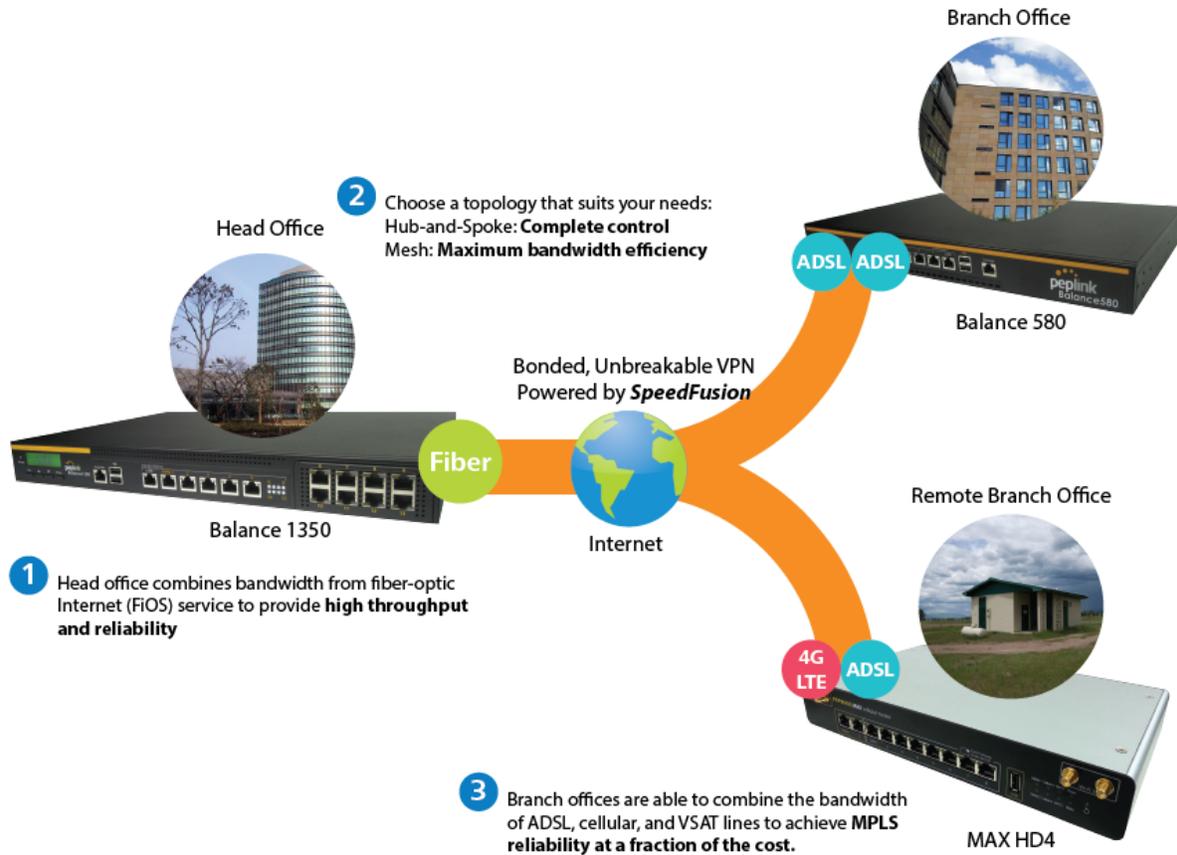
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement



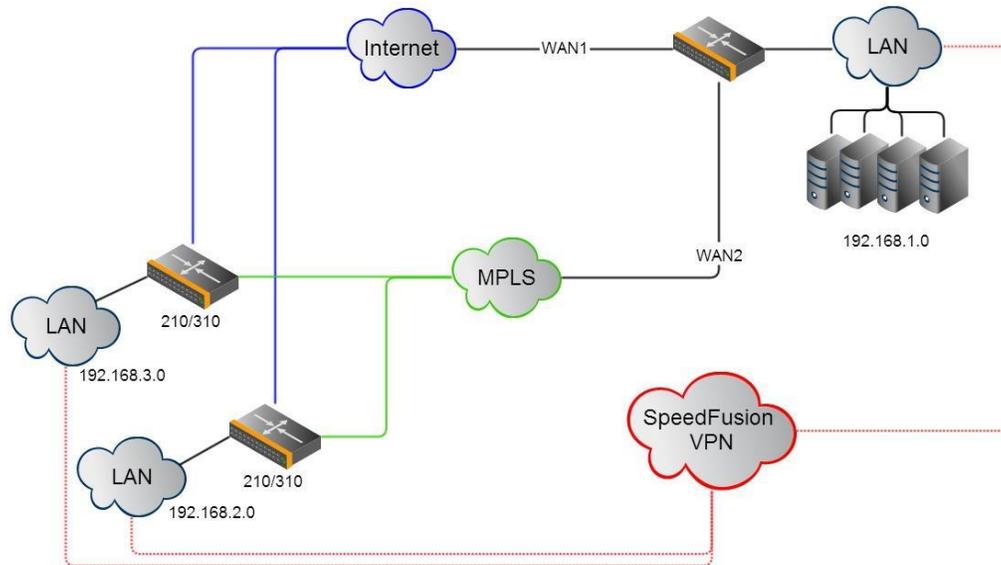
Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your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

Option 2: MPLS Alternative



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

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



Environment:

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

Requirement:

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

Recommended Solution:

- Form a SpeedFusion tunnel between the branch offices and head office to bond the MPLS and additional DSL lines.

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

Devices Deployed: Balance 210, Balance 310, Balance 580

Harrington Industrial Plastics



Overview

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

Requirements

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

Solution

- Peplink Balance 1350
- Peplink Balance 380
- Unbreakable VPN

Benefits

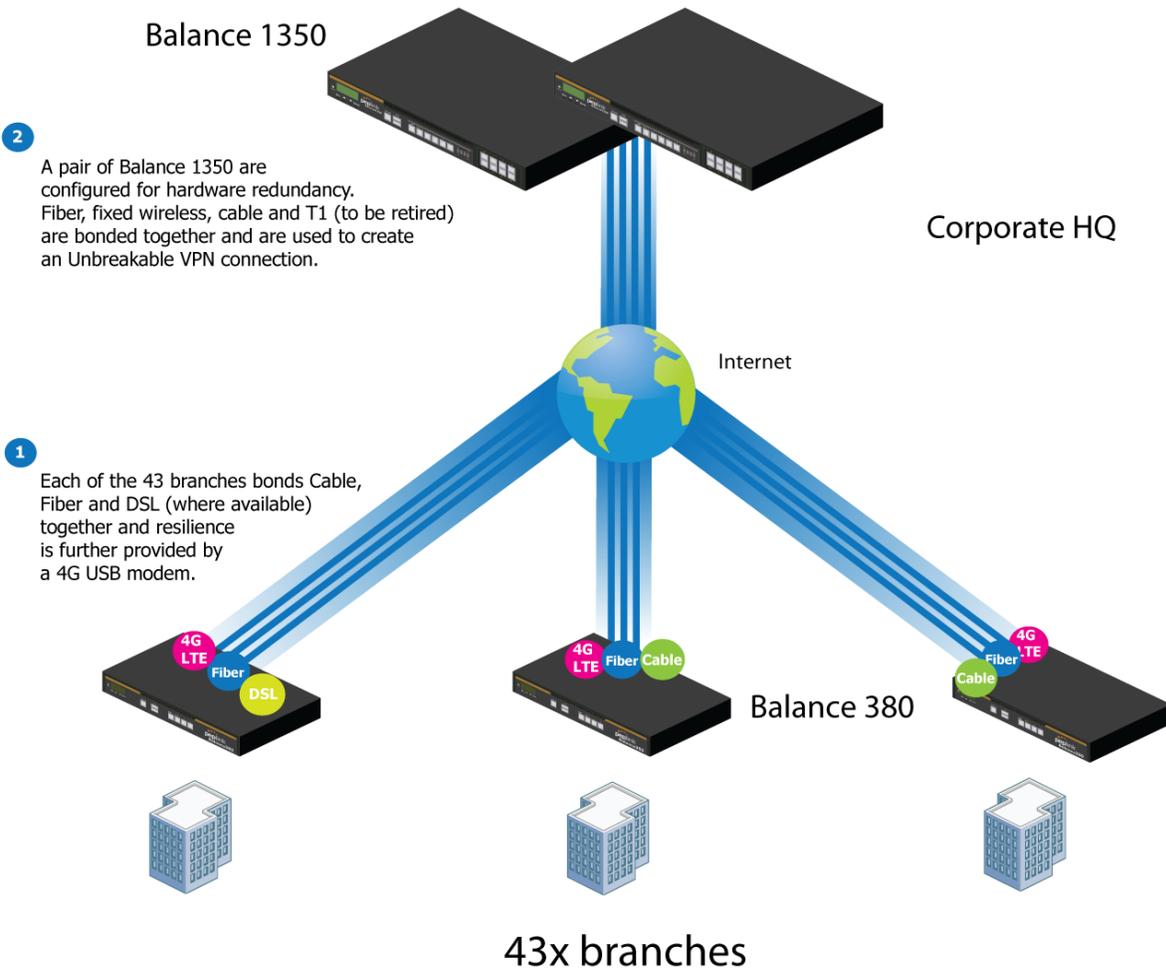
- Extreme savings of \$100,000 per year
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

Time For An Upgrade

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

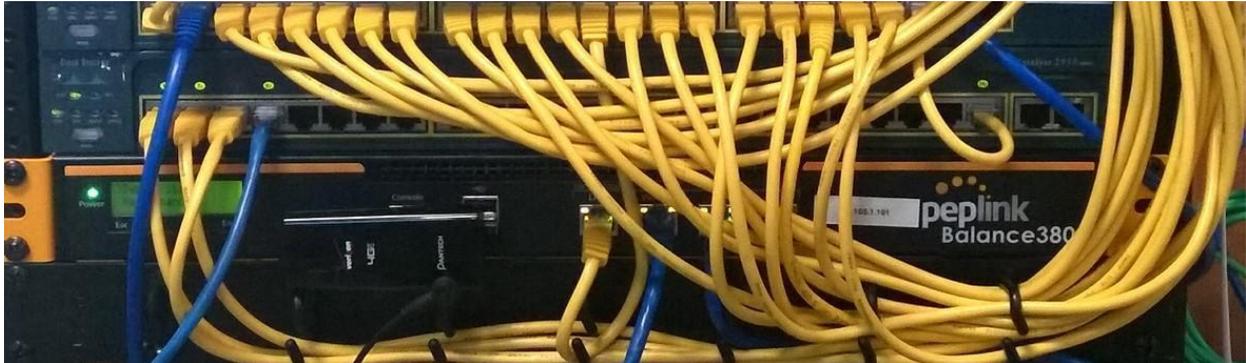
Quick Deployment and Unbreakable Connectivity

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



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

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



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

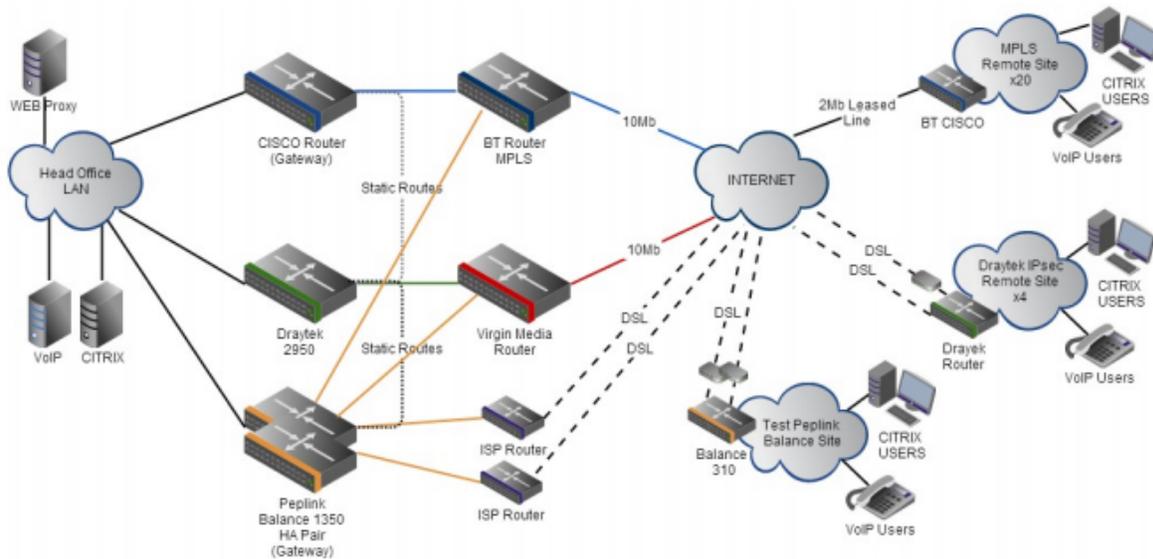
PLUS

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

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

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

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



Colégio Next - Enabling eLearning



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

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

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

Requirements

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

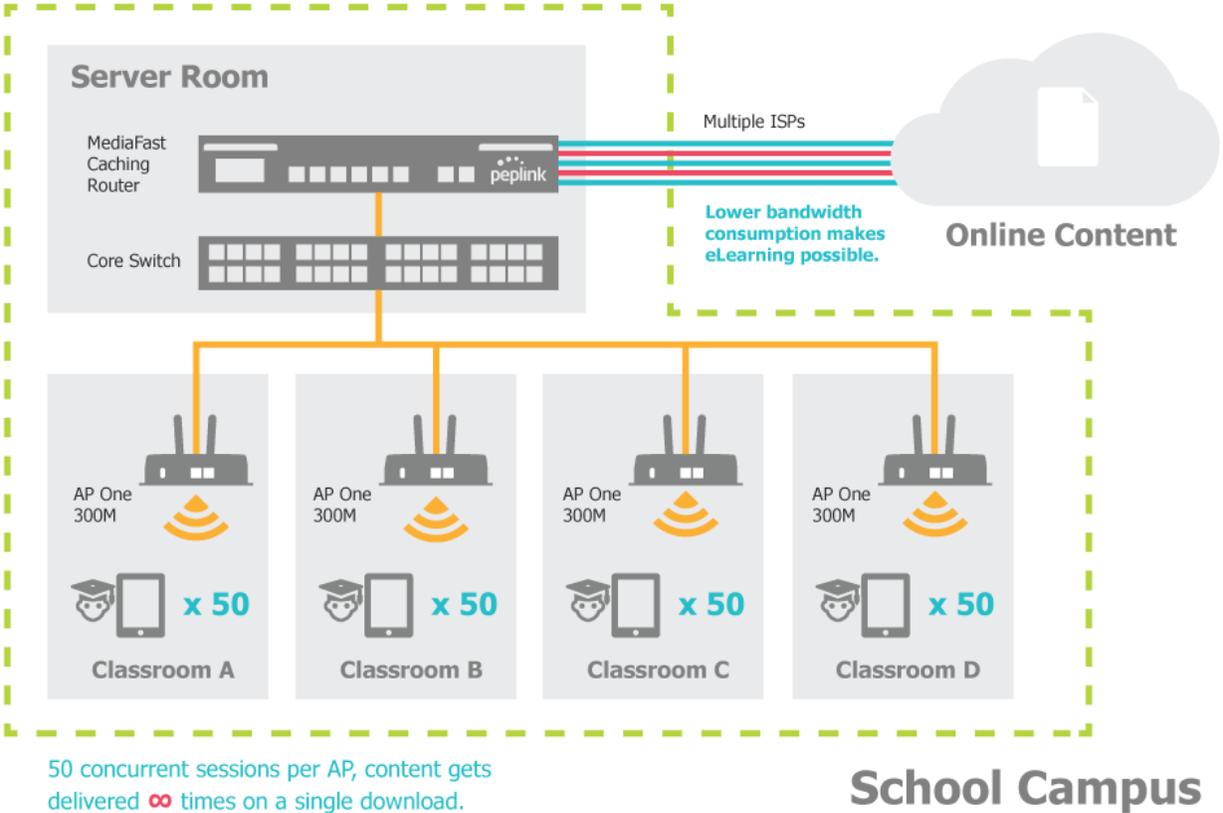
Solution

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

Benefits

- Instant, simultaneous access to media-rich educational content for 500+ iPads
- Wi-Fi connection stability for 50+ users per classroom, not achievable by other tested equipment
- Teachers, students and guests can be assigned access priority to available bandwidth, further preventing congestion
- iOS updates (often 2GB size) no longer congest the network as they are downloaded only once, cached on the MediaFast and then distributed to all iOS devices

- AP Controller makes MAC Address Filtering easy. Students are assigned to designated APs by their devices' MAC Address in order to prevent saturating any single AP.
- Flawless iPad AirPlay mirroring at all times
- iPads are used all day, reaching their full potential with a fast and stable network all the time
- Students are far more engaged and teachers rely on their iPads all day



Performance Optimization

Scenario

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

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

Solution

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

- Web browsing mainly downloads data; sending emails 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 email.

Maintaining the Same IP Address Throughout a Session

Scenario

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

Solution

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

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

Settings

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

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

Add a New Custom Rule ✖

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

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)
	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> 10.90.0.75 (Interface IP)
	<input type="checkbox"/> WAN 2
	<input type="checkbox"/> WAN 3
	<input type="checkbox"/> WAN 4
	<input type="checkbox"/> WAN 5
	<input type="checkbox"/> WAN 6
	<input type="checkbox"/> WAN 7
<input type="checkbox"/> Mobile Internet	
Outbound Mappings ?	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 Exce
Enable	<input checked="" type="checkbox"/>
WAN Connection	Any ▾
Protocol	TCP ▾ ← HTTP ▾
Source	Any Address ▾ Any Port ▾
Destination	Any Address ▾ Single Port ▾ Port: 80
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

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

Outbound Access Restriction

Scenario

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

Solution

To setup a firewall between 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	<input checked="" type="checkbox"/>
Protocol	TCP ▾ ← FTP ▾
Source	Any Address ▾ Any Port ▾
Destination	Any Address ▾ Single Port ▾ Port: 21
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

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

Appendix E. Troubleshooting

Problem 1

Outbound load is only distributed over one WAN connection.

Solution

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

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

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

For additional details, please refer to this FAQ:

<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 be able to find the source of the 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 the problem still persists, change the size to progressively 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 F.

FCC Requirements for Operation in the United States

Federal Communications Commission (FCC) Compliance Notice:

For Balance 30 Pro

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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.

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

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 49 cm 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

CE Statement for Pepwave Routers (Balance 30 Pro)

DECLARATION OF CONFORMITY

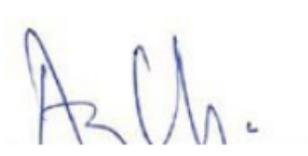
We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building Phase 6, 481 Castle Peak Road Cheung Sha Wan Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Peplink Balance 30 Pro BPL-031-LTEA-W-T Balance 30 Pro Pismo 811AC B30 Pro
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 301908-1 V11.1.1
- EN 301 489-1 V2.2.1
- Draft EN 301 489-17 V3.2.0
- Draft EN 301 489-52 V1.1.0
- EN 55032: 2015 + AC:2016
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013
- EN 55024: 2010 + A1 :2015
- EN 62311 : 2008
- EN 62368-1:2014/AC:2015

Yours sincerely,




Antony Chong
 Director of Hardware Engineering
 Peplink International Limited



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(NI)

2.4GHz (2412 – 2472 MHz) : 19.93 dBm

5GHz (5150 - 5250 MHz) : 22.88 dBm

This equipment complies with CE 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 & your body.

Contact as: <https://www.peplink.com/>

**FCC Requirements for Operation in the United States
Federal Communications Commission (FCC) Compliance Notice:**

For Balance 380X, Balance 580X

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Industry Canada Statement (Balance 380X, Balance 580X)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Ce produit répond aux spécifications techniques applicables à l'innovation, Science et Développement économique Canada.

CE Statement for Pepwave Routers (Balance 380X / Balance 580X)

DECLARATION OF CONFORMITY

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
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Balance 380X Balance 580X Peplink Balance 380X Peplink Balance 580X BPL-380X BPL-580X EXM-MINI-15GD FlexModule Mini 1x 5G Module
Trade name of the appliance	PEPWAVE / PEPLINK

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

EN 301 908-1 V13.1.1
 EN 62311: 2008
 EN 301 489-1 V2.2.3
 Draft EN 301 489-52 V1.1.2
 EN 55032: 2015 + A11:2020
 EN 55035: 2017 + A11:2020
 EN 61000-3-2: 2014
 EN 61000-3-3: 2013
 EN 62368-1:2014 + A11:2017

Yours sincerely,



Antony Chong
 Director of Hardware Engineering
 Peplink International Limited



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(NI)

This equipment complies with CE 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 & your body.

Contact as: <https://www.peplink.com/>