



Peplink SDX

User Manual

Peplink Products:

Peplink Balance SDX / SDX Main Chassis (BPL-SDX) / SDX Main Chassis (BPL-SDX-LR1) / SDX Main Chassis (BPL-SDX-F1) / SDX Main Chassis (BPL-SDX-C1) / BPL-SDX / BPL-SDX-LR1 / BPL-SDX-F1 / BPL-SDX-C1 / EBX / PismoX03 / EXM-3LTEA-R / SDX Main Chassis (BPL-SDX-LK1) / BPL-SDX-LK1 / EXM-3LTEA-K

Peplink Balance Firmware 8.0.1
September 2019

Table of Contents

Introduction and Scope	6
Glossary	7
Product Features	9
Advanced Feature Summary	13
Drop-in Mode and LAN Bypass: Transparent Deployment	13
QoS: Clearer VoIP	13
Per-User Bandwidth Control	14
High Availability via VRRP	14
USB Modem and Android Tethering	15
Built-In Remote User VPN Support	15
LACP NIC Bonding	16
Peplink Balance Overview	17
Peplink Balance SDX	17
Installation	20
Preparation	20
Constructing the Network	20
Basic Configuration	21
Connecting to the Web Admin Interface	21
Configuration with the Setup Wizard	22
Network Tab	26
WAN	26
Health Check Settings	35
Bandwidth Allowance Monitor Settings	38
Additional Public IP Settings	39
Dynamic DNS Settings	39
LAN	42
Network Settings	42
Network Settings (Common Settings)	46
Port Settings	52
VPN	53
SpeedFusion	53

IPsec VPN	59
Outbound Policy	63
Inbound Access	73
Servers	74
Services	74
DNS Settings	77
NAT Mappings	95
MediaFast	97
Setting Up MediaFast Content Caching	97
Viewing MediaFast Statistics	99
Prefetch Schedule	100
ContentHub	102
Configure a website to be published from the ContentHub	103
Configure an application to be published from the contenthub	105
MDM Settings	107
Docker	108
Captive Portal	109
QoS	112
User Groups	112
Bandwidth Control	113
Application	114
Prioritization for Custom Application	114
DSL/Cable Optimization	116
Firewall	116
Access Rules	116
Intrusion Detection and DoS Prevention	120
Content Blocking	121
Application Blocking	122
Web Blocking	122
Customized Domains	123
Exempted User Groups	123
Exempted Subnets	123
URL Logging	123
OSPF & RIPv2	123
BGP	127
Remote User Access	129

L2TP with IPsec	129
OpenVPN	130
PPTP	130
Authentication Methods	131
Misc. Settings	132
High Availability	132
Certificate Manager	136
Service Forwarding	136
SMTP Forwarding	138
Web Proxy Forwarding	138
DNS Forwarding	139
Custom Service Forwarding	139
Service Passthrough	139
Grouped Networks	140
SIM Toolkit	141
AP Tab	143
AP	143
AP Controller	143
Wireless SSID	145
AP > Profiles	149
AP Controller Status	153
Info	153
Access Points (Usage)	155
Wireless SSID	158
Wireless Client	158
Nearby Device	159
Event Log	160
Toolbox	161
System Tab	162
System	162
Admin Security	162
Firmware	166
Web admin interface : install updates manually	167
The InControl method	168
Time	168
Schedule	169
Email Notification	170

Event Log	172
SNMP	172
InControl	175
Configuration	176
Feature Add-ons	177
Reboot	177
Tools	178
Ping	178
Traceroute	178
Wake-on-LAN	179
WAN Analysis	179
CLI (Command Line) Support	183
Status Tab	184
Status	184
Device	184
Active Sessions	186
Client List	188
WINS Clients	189
OSPF & RIPv2	189
MediaFast	189
SpeedFusion Status	190
Event Log	195
Device Event Log	196
IPsec Event Log	196
Bandwidth	197
Real-Time	197
Hourly	198
Daily	198
Monthly	201
Harrington Industrial Plastics	208
PLUSS	211

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.

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 Features

Peplink Balance Series products enable all LAN users to share broadband Internet connections and provide advanced features to enhance Internet access. The following is a list of supported features:

WAN

- Multiple public IP support (DHCP, PPPoE, static IP address)
- Static IP support for PPPoE
- 10/100/1000Mbps Ethernet connection in full/half duplex
- Built-in HSPA and EVDO cellular modems
- USB mobile connection (**only one USB modem can be connected at a time**)
- Drop-in mode on selectable WAN port with MAC address passthrough network address translation (NAT) / port address translation (PAT)
- Inbound and outbound NAT mapping
- Multiple static IP addresses per WAN connection
- MAC address clone
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS (supported service providers: changeip.com, dyndns.org, no-ip.org, tzo.com, and DNS-O-Matic)
- Ping, DNS lookup, and HTTP-based health check
- WAN throughput and consistency diagnosis
- WAN to WAN speed test

LAN

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

VPN

- Secure 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

3 Advanced Feature Summary

3.1 Drop-in Mode and LAN Bypass: Transparent Deployment



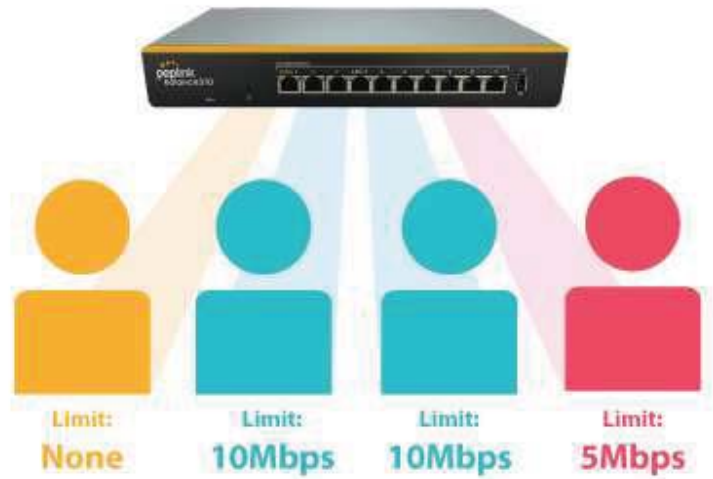
As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass**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

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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](#)

3.7 LACP NIC Bonding

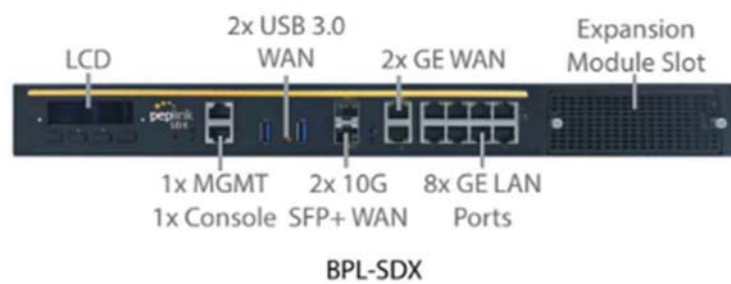


Use 802.3ad to combine multiple LAN connections into a virtual LAN connection. This virtual connection has higher throughput and redundancy in case any single link fails.

4 Peplink Balance Overview

4.1 Peplink Balance SDX

4.1.1 Panel Appearance



4.1.2 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

5 Installation

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

5.1 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.

5.2 Constructing the Network

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

1. With an Ethernet cable, connect a computer to one of the LAN ports on the Peplink Balance. For Peplink Balance models that support multiple connections, repeat with different cables for up to four computers to be connected.
2. With another Ethernet cable, connect the WAN/broadband modem to one of the WAN ports on the Peplink Balance. Repeat using different cables to connect from two to 13 WAN/broadband connections or connect a USB modem to the USB WAN port.
3. Connect the provided power adapter or cord to the power connector on the Peplink Balance, and then plug the power adapter into a power outlet.

6 Basic Configuration

6.1 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

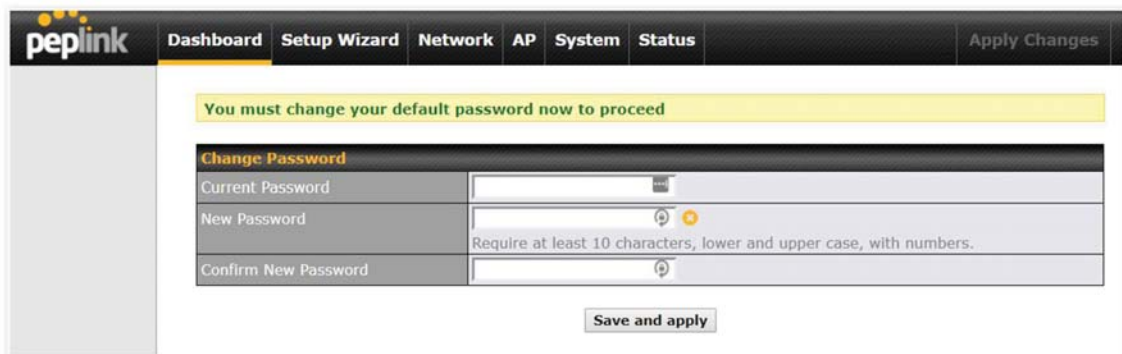


(This is the default admin user login of the Peplink Balance.)

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.

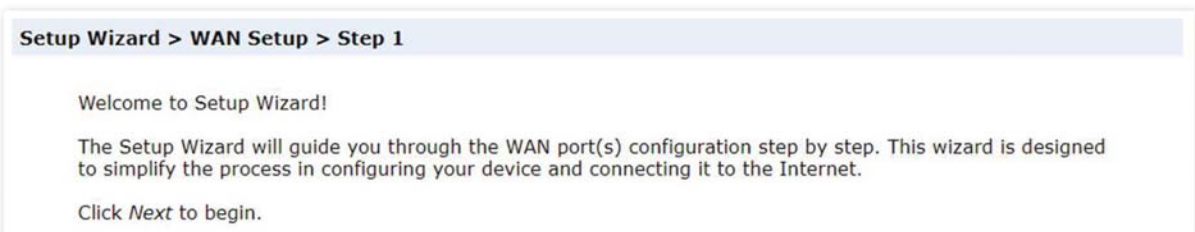
6.2 Configuration with the Setup Wizard

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

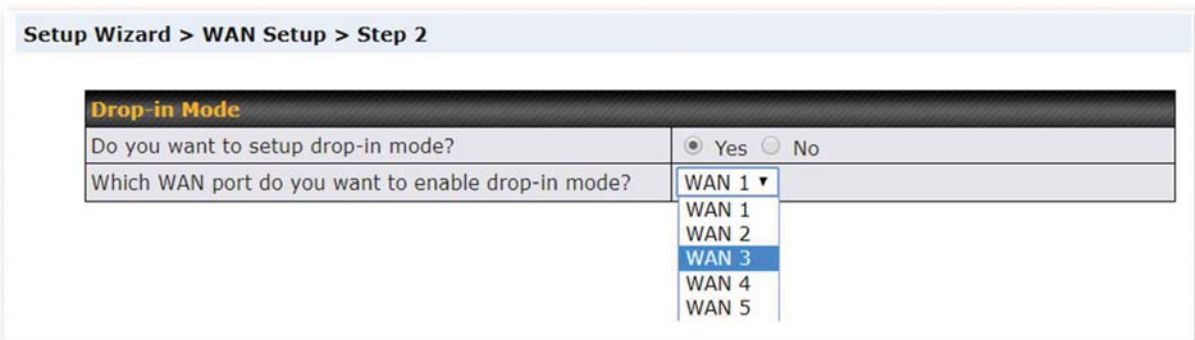
To begin, click **Setup Wizard** after connecting to the web admin interface.



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	1000 <input type="text"/> Mbps ▼
Download Bandwidth	1000 <input type="text"/> Mbps ▼

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

Setup Wizard > WAN Setup > Step 4

Choose a connection method for WAN 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, Lc ▼ (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.


7 Network Tab

7.1 WAN

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









Connection Name	Method	Routing Mode	Type
1. WAN_1	DHCP	NAT	Always-on
2. WAN_2	Not Configured	NAT	Always-on
3. WAN_3	Not Configured	NAT	Always-on

You can also enable IPv6 support in this section

IPv6
Disabled 

WAN Connection Settings (Ethernet)

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

Connection Settings	
WAN Connection Name	WAN 1 
Enable	<input checked="" type="checkbox"/> Office hours ▼
Connection Method	 DHCP ▼
Routing Mode	 <input checked="" type="radio"/> NAT
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="checkbox"/> Enable
Upload Bandwidth	 1 <input type="text"/> Gbps ▼
Download Bandwidth	 1 <input type="text"/> Gbps ▼


WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Enable	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.
Connection Method	<p>There are five possible connection methods for Ethernet WAN:</p> <ul style="list-style-type: none"> • DHCP • Static IP • PPPoE • L2TP • GRE <p>The connection method and details are determined by, and can be obtained from the ISP. See the following sections for details on each connection method. DNS server settings can be configured in the corresponding menu for each connection method.</p>
Routing Mode	This field shows that NAT (network address translation) will be applied to the traffic routed over this WAN connection. IP Forwarding is available when you click the link in the help text.
Connection Priority	<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>
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Reply to ICMP PING	<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 (enabled)</p>
Upload Bandwidth	<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</p>

	upstream bandwidth.
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

WAN Connection Settings (Cellular)

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


Connection Settings	
WAN Connection Name	Cellular
Enable	<input checked="" type="checkbox"/> Always on
Routing Mode	<input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
Network Mode	<input type="radio"/> Auto <input type="radio"/> Generic <input type="radio"/> AT&T / T-Mobile <input checked="" type="radio"/> Sprint <input type="radio"/> Verizon Wireless
Subnet Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Force /31 Subnet
Connection Priority	<input checked="" type="radio"/> Always-on (Priority 1) <input type="radio"/> Backup
Independent from Backup WANs	<input type="checkbox"/>
Idle Disconnect	<input checked="" type="checkbox"/> 1 minutes <small>Time value is global. A change will affect all WAN profiles.</small>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

Connection Settings	
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>
Subnet Selection	<p>Choose between:</p> <p>Auto: The subnet mask will be set automatically.</p> <p>Force /31 Subnet: The subnet mask will be set as 255.255.255.254(/31), and the gateway IP address will be recalculated.</p>
Connection Priority	<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>
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Idle Disconnect	If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default.
DNS Servers	<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</p>

assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.

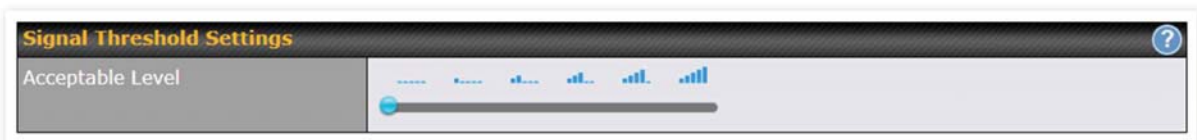
Cellular Settings		
SIM Card	<input checked="" type="radio"/> Both SIMs <input type="radio"/> SIM A Only <input type="radio"/> SIM B Only	
Preferred SIM Card	<input checked="" type="radio"/> No Preference <input type="radio"/> SIM A <input type="radio"/> SIM B	
	SIM Card A	SIM Card B
Network Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
LTE/3G	<input checked="" type="radio"/> LTE Only	<input checked="" type="radio"/> LTE Only
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"/> (Confirm)	<input type="text"/> (Confirm)
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Action	<input checked="" type="checkbox"/> Receive email notification <input type="checkbox"/> Reserve for management traffic when usage hits 100% <input type="checkbox"/> Disconnect when usage hits 100%	<input checked="" type="checkbox"/> Receive email notification <input type="checkbox"/> Reserve for management traffic when usage hits 100% <input type="checkbox"/> Disconnect when usage hits 100%
Start Day	On 26th of each month	On 21st of each month
Monthly Allowance	4 GB	22 GB

Cellular Settings	
SIM Card	Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards.
Preferred SIM	If both cards were enabled on the above field, then you can designate the priority of the SIM

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

Monthly Allowance This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Signal Threshold Settings



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.



WAN Connection Settings (Common)

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

Physical Interface Settings	
Speed	<input type="text" value="Auto"/>
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: <input type="text" value="1440"/> <input type="button" value="Default"/>
MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom Value: <input type="text"/>
MAC Address Clone	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="10:56:CA:0D:72:0D"/>
VLAN	<input type="checkbox"/> Enable

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 Check the box to assign a VLAN to the interface.

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

Health Check Settings

Health Check Method	<div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">Disabled</div> </div>
Health Check disabled. Network problem cannot be detected.	

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

Health Check Method: PING

Health Check Method	<div style="display: flex; align-items: center;"> ? <div style="border: 1px solid #ccc; padding: 2px;">PING</div> </div>
PING Hosts	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> ? Host 1: <input style="width: 100%; height: 15px; margin-top: 2px;" type="text"/> </div> <div style="margin-right: 5px;"> ? Host 2: <input style="width: 100%; height: 15px; margin-top: 2px;" type="text"/> </div> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </div>

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

PING Hosts

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

Health Check Method: DNS Lookup

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

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

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

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

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

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

Other Health Check Settings	
Timeout	<input type="text" value="5"/> second(s)
Health Check Interval	<input type="text" value="5"/> second(s)
Health Check Retries	<input type="text" value="3"/>
Recovery Retries	<input type="text" value="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.

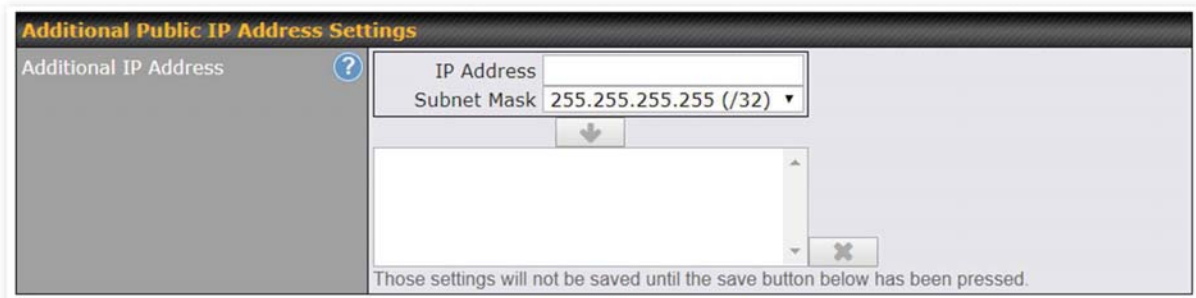
Bandwidth Allowance Monitor Settings

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

Additional Public IP Settings



Additional Public IP Settings

IP Address List

IP Address List represents the list of fixed Internet IP addresses assigned by the ISP in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address List**.

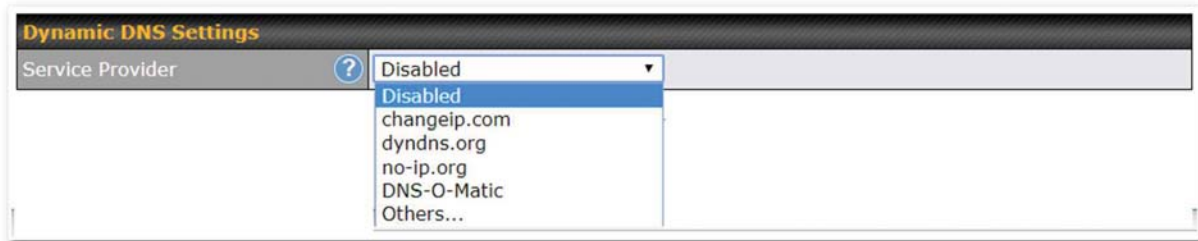
Dynamic DNS Settings

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	<input type="text" value="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 / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note

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

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

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

a WAN's IP address did not change.

7.2 LAN

7.2.1 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	X
VLAN2	2	3.3.3.3/24	X

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 ?	
Name	<input type="text"/>
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	? No profile is available
Remote Network Isolation	<input type="checkbox"/>
Spanning Tree Protocol	<input type="checkbox"/>
DHCP Option 82 Injection	<input checked="" type="checkbox"/>
Override IP Address when bridge connected	? <input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None

Layer 2 PepVPN Bridging	
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	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.

bridge connected	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 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	<p>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.</p> <p>When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP WINS 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.</p>
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	<p>In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.</p> <p>To define an extended DHCP option, click the Add button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.</p>
DHCP Reservation	<p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p>Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in 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.</p>

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.

7.2.2 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	<p>This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in w.x.y.z format.</p> <p>The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnet. Click to create a new route. Click to remove a route.</p> <p>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.</p>

Virtual Network Mapping			
One-to-One NAT	?	Local Network	Virtual Network
			+
Many-to-One NAT	?	Local Network	Virtual IP Address
			+

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

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

See: <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> </tr> </thead> <tbody> <tr> <td></td> <td></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> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Domain	Connection																
Domain	Connection																		
DNS Resolvers	<table border="1"> <thead> <tr> <th>WAN Connection</th> <th>DNS Servers</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> WAN 1</td> <td>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	<p>To enable the DNS proxy feature, check this box, and then set up the feature at Network>LAN>DNS Proxy Settings.</p> <p>A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the DNS servers/resolvers defined for each WAN connection.</p>
DNS Caching	<p>This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can improve DNS response time by storing all received DNS results for faster DNS lookup. However, it cannot return the most updated result for frequently updated DNS records. By default, DNS Caching is disabled.</p>
Include Google Public DNS Servers	<p>When this option is enabled, the DNS proxy server will forward DNS requests to Google's public DNS servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.</p>
Local DNS Records	<p>This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Peplink Balance, the corresponding IP address will be returned. To display the option to set</p>

	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	<p>Check the box to enable the WINS server. A list of WINS clients will be displayed at Network>LAN>DNS Proxy Settings>DNS Resolvers.</p> <p>This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es).</p> <p>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.</p>

^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.

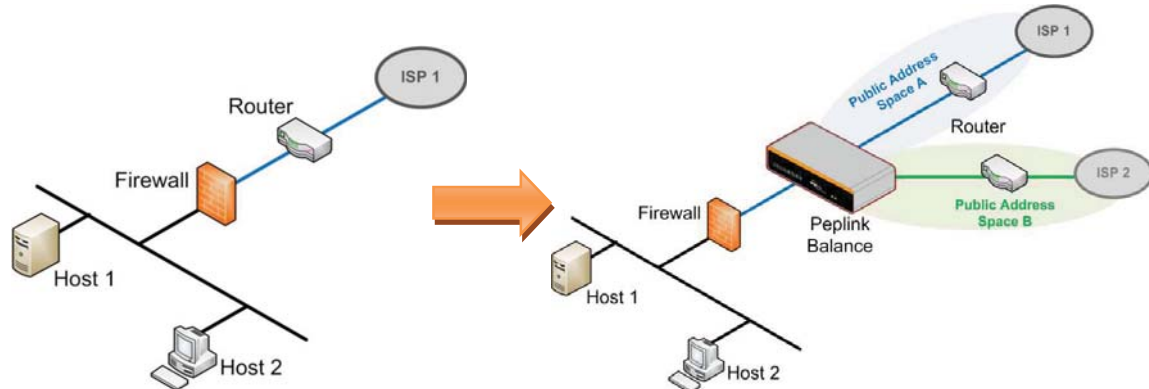


Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	<p>Choose Service and Client networks from the drop-down menus, and then click to add the networks. To delete an existing Bonjour listing, click .</p> <p>Bonjour Forwarding is supported on All Balance models,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

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</p>

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

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

7.2.3 Port Settings

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

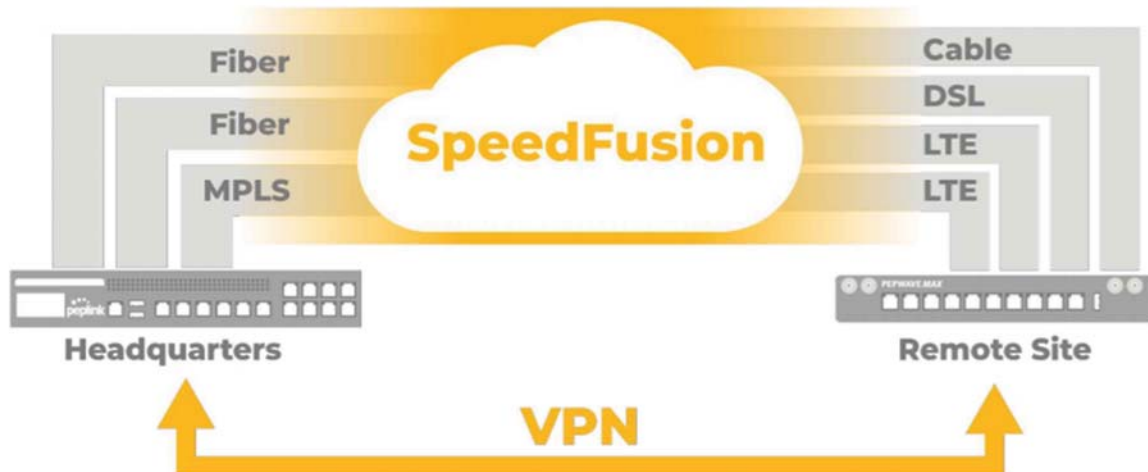
Port Settings						
	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port 1	<input checked="" type="checkbox"/>			Trunk ▾	Any ▾
2	LAN Port 2	<input type="checkbox"/>	Auto ▾	<input checked="" type="checkbox"/>	Trunk ▾	Any ▾
3	LAN Port 3	<input checked="" type="checkbox"/>			Trunk ▾	Any ▾

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)

7.3 VPN

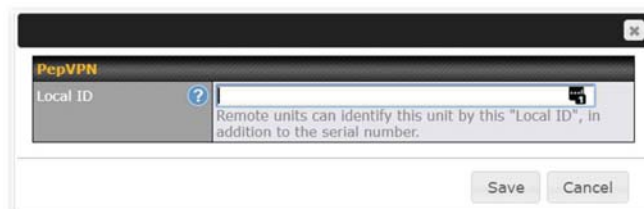
7.3.1 SpeedFusion



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 menu will

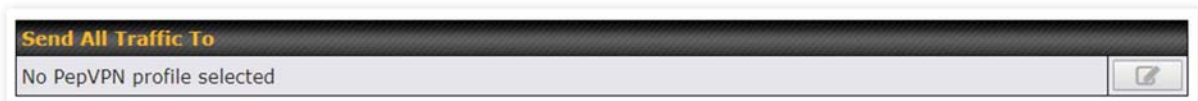
appear:



SpeedFusion Profiles

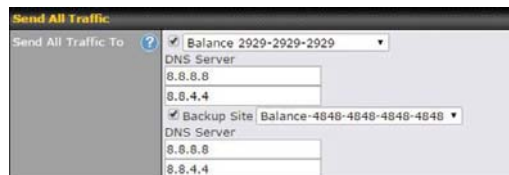
This table displays all defined profiles. Click the **New Profile** button to create a new profile for making a VPN connection to a remote unit via available WAN connections. Each pair of VPN connection requires its own profile.

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



Send All Traffic To

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



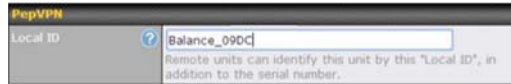
You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main PepVPN connection fail.



PepVPN Local ID

This feature allows you to change the local ID of a PepVPN connection. Click the button to select your

connection and the following menu will appear:



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



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	Remote ID
	Pre-shared Key
	<input type="text" value="Balance 9898-9898-9898"/> <input type="password" 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="1.0"/>
WAN Smoothing ?	Off ▼
Use IP ToS	<input type="checkbox"/>

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

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

Authentication	Select from By Remote ID Only , Preshared Key , or X.509 to specify the method the Peplink Balance will use to authenticate peers. When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field.
Remote ID / Pre-shared Key	<p>This optional field becomes available when Remote ID / Pre-shared Key is selected as the Peplink Balance's VPN Authentication method, as explained above. Pre-shared Key defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.</p> <p>Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the  icon next to the "Remote ID / Preshared Key" setting.</p>
Remote ID/Remote Certificate	These optional fields become available when X.509 is selected as the Peplink Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the Show Details link below the field.
Allow Shared Remote ID	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	<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 (TCP)</p>
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If Default is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If Custom is selected, enter an outgoing port number from 1 to 65535.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost.

Default: 10

WAN Smoothing^A

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

Off - Disable WAN Smoothing.

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

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

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

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

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

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

WAN Connection Priority

WAN Connection Priority

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

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

Peplink Balance IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between

these locations are kept safe and confidential across the public Internet.

IPsec VPN on the Peplink Balance is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for his multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g., unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

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>

7.3.2 IPsec VPN

All Peplink products can make multiple IPsec VPN connections with Peplink routers, as well as Cisco and Juniper routers.

Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN with a selection of encryption standards, such as 3DES, AES-128, and AES-256.

To configure, navigate to **Network>Interfaces>IPsec VPN**.




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 type="radio"/> 192.168.10.0/24</p> <p><input checked="" type="checkbox"/> 172.16.2.0/24 <input type="radio"/> 10.10.0.1/32</p> <p><input checked="" type="checkbox"/> 172.16.3.11/32 <input type="radio"/> 192.168.11.101/32</p> <p><input checked="" type="checkbox"/> 172.16.3.21/32 <input type="radio"/> 192.168.11.201/32</p> <p><input type="checkbox"/> Local Network <input type="radio"/> NAT Network</p>											
Remote Networks	<table border="1"> <thead> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="button" value="+"/></td> </tr> <tr> <td>192.167.11.193</td> <td>255.255.255.0 (/24)</td> <td></td> </tr> </tbody> </table>	Network	Subnet Mask		<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>	192.167.11.193	255.255.255.0 (/24)			
Network	Subnet Mask											
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>										
192.167.11.193	255.255.255.0 (/24)											
Authentication	<input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate											
Mode	<input checked="" type="radio"/> Main Mode (All WANs need to have Static IP) <input type="radio"/> Aggressive Mode											
Force UDP Encapsulation	<input type="checkbox"/>											
Preshared Key	<input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters											
Local ID	<input type="text"/>											
Remote ID	<input type="text"/>											
Phase 1 (IKE) Proposal	1 <input type="text" value="AES-256 & SHA1"/> 2 <input type="text" value="-----"/>											
Phase 1 DH Group	<input checked="" type="checkbox"/> Group 2: MODP 1024 <input type="checkbox"/> Group 5: MODP 1536											
Phase 1 SA Lifetime	<input type="text" value="3600"/>	seconds	<input type="button" value="Default"/>									
Phase 2 (ESP) Proposal	1 <input type="text" value="AES-256 & SHA1"/> 2 <input type="text" value="-----"/>											
Phase 2 PFS Group	<input checked="" type="radio"/> None <input type="radio"/> Group 2: MODP 1024 <input type="radio"/> Group 5: MODP 1536											
Phase 2 SA Lifetime	<input type="text" value="28800"/>	seconds	<input type="button" value="Default"/>									

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

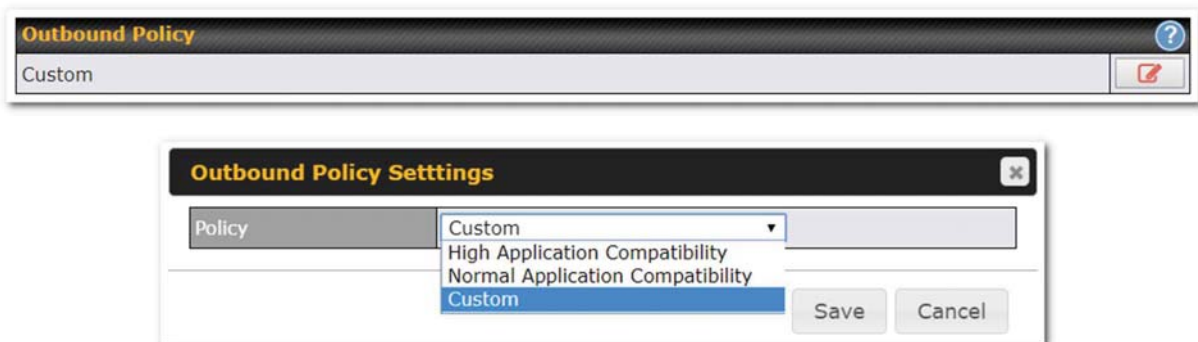
Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate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

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

7.4 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:

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

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

Add Rule

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

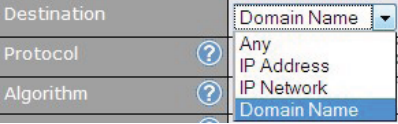
To create a custom rule, click **Add Rule** at the bottom of the table.

Add a New Custom Rule
✕

Service Name	<input style="width: 95%;" type="text"/>		
Enable	<input checked="" type="checkbox"/>	Always on ▾	
Source	Any ▾		
Destination	? IP Network ▾	<input style="width: 80%;" type="text"/>	Mask: 255.255.255.0 (/24) ▾
Protocol	? Any ▾	← :: Protocol Selection :: ▾	
Algorithm	? Weighted Balance ▾		
Load Distribution Weight	?	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="display: flex; align-items: center;"> WAN 1 10 <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; right: -10px; top: -5px; width: 10px; height: 10px; background-color: #00aaff; border-radius: 50%;"></div> </div> </div> <div style="display: flex; align-items: center;"> WAN 2 10 <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; right: -10px; top: -5px; width: 10px; height: 10px; background-color: #00aaff; border-radius: 50%;"></div> </div> </div> <div style="display: flex; align-items: center;"> WAN 3 10 <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; right: -10px; top: -5px; width: 10px; height: 10px; background-color: #00aaff; border-radius: 50%;"></div> </div> </div> <div style="display: flex; align-items: center;"> WAN 4 10 <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; right: -10px; top: -5px; width: 10px; height: 10px; background-color: #00aaff; border-radius: 50%;"></div> </div> </div> <div style="display: flex; align-items: center;"> WAN 5 10 <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; right: -10px; top: -5px; width: 10px; height: 10px; background-color: #00aaff; border-radius: 50%;"></div> </div> </div> <div style="display: flex; align-items: center;"> Mobile Internet 10 <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; right: -10px; top: -5px; width: 10px; height: 10px; background-color: #00aaff; border-radius: 50%;"></div> </div> </div> </div>	
When No Connections are Available	?	Drop the Traffic ▾	

Save
Cancel

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, or MAC address for traffic that matches the rule.
Destination	This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.

	 <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.</p>
<p>Algorithm</p>	<p>This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected (note that some Pepwave routers provide only some of these options):</p> <ul style="list-style-type: none"> • Weighted Balance • Persistence • Enforced • Priority • Overflow • Least Used • Lowest Latency • 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-algorithmns-work/8059</p>
<p>Load Distribution Weight</p>	<p>This is to define the outbound traffic weight ratio for each WAN connection.</p>
<p>Terminate Sessions on Link Recovery</p>	<p>This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the Weighted, Persistence, and Priority algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.</p>

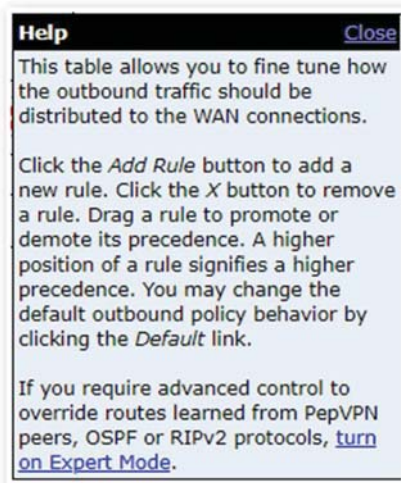
When No connections are available

This field allows you to configure the default action when all the selected Connections are not available.

Drop the Traffic - Traffic will be discarded.

Use Any Available Connections - Traffic will be routed to any available Connection, even it is not selected in the list.

Fall-through to Next Rule - Traffic will continue to match next Outbound Policy rule just like this rule is inactive.



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**.

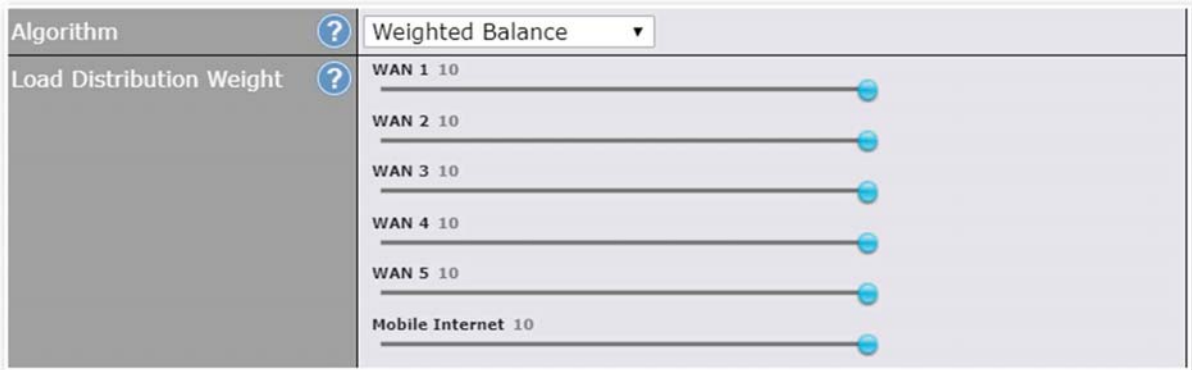
In Expert Mode, a new special rule, **SpeedFusion™ Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion™ routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets will be 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**.



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.

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**.

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

SpeedFusion™ connection.

Algorithm: Priority

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

Algorithm	?	Priority	
Priority Order	?	Highest Priority	Not In Use
		WAN: WAN 1	<input checked="" type="checkbox"/> VPN: Connection 1
		WAN: WAN 2	
		WAN: Wi-Fi WAN	
		WAN: Cellular 1	
		WAN: Cellular 2	
		WAN: USB	
		Lowest Priority	
Terminate Sessions on Link 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 type="text"/>
Enable	<input checked="" type="checkbox"/> Always on
Source	Any
Destination	IP Network <input 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	? IP Network ▾	<input type="text"/>	Mask: 255.255.255.0 (/24) ▾
Protocol	? Any ▾ ← :: Protocol Selection :: ▾		
Algorithm	? 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	?	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	? IP Network ▾	<input type="text"/>	Mask: 255.255.255.0 (/24) ▾
Protocol	? Any ▾	← :: 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	?	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.

7.5 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.

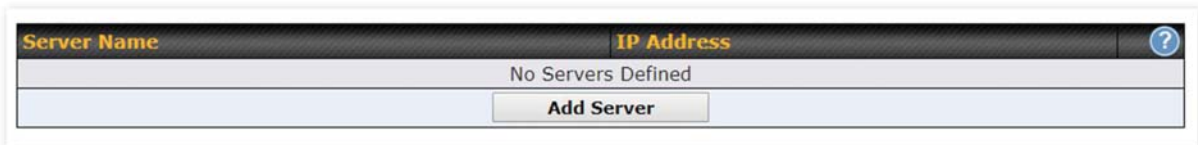
By the custom definition of servers and services for inbound access, Internet users can access the servers behind Peplink Balance. Advanced configurations allow inbound access to be distributed among multiple servers on the LAN.

Important Note

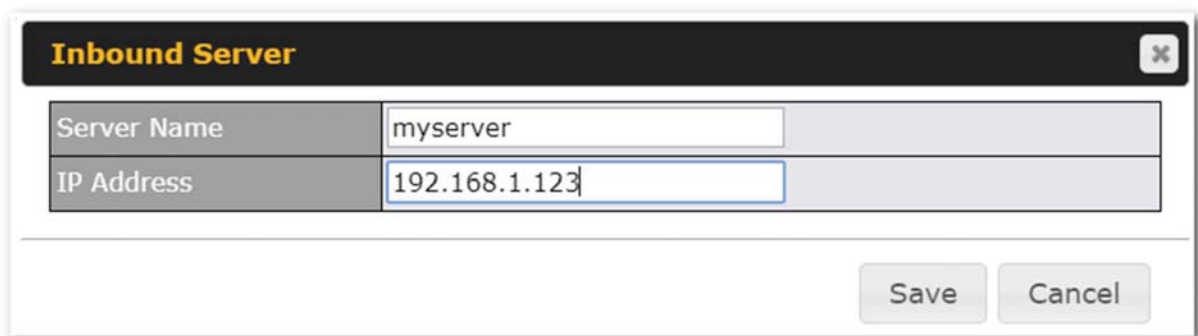
Inbound access applies only to WAN connections that operate in NAT mode. For WAN connections that operate in drop-in mode or IP forwarding, inbound traffic is forwarded to the LAN by default.

7.5.1 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.

7.5.2 Services

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



Tip

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

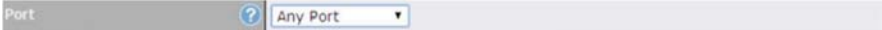
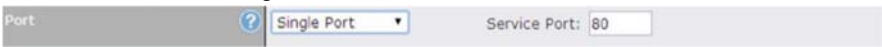
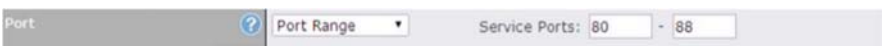


To define a new service, click the **Add Service** button, upon which the following menu appears:

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)	Connection / IP Address(es) All Clear
	<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)	Server
	<input type="checkbox"/> myserver (192.168.1.123)

Services Settings

Enable	<p>This setting specifies whether the inbound service rule takes effect.</p> <p>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.</p> <p>When No is selected, the inbound service rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.</p>
Service Name	<p>This setting identifies the service to the system administrator. Only alphanumeric and the underscore “_” characters are valid.</p>
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>
<p>Port</p>	<p>The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:</p>
	<p>Any Port, Single Port, Port Range, Port Map, and Range Mapping</p>
	
	<p>Any Port: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the Servers setting. For example, if IP Protocol is set to TCP and Port is set to Any Port, then all TCP traffic will be forwarded to the configured servers.</p>
	
<p>Single Port: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the Servers setting. For example, if IP Protocol is set to TCP, Port is set to Single Port, and Service Port is set to 80, then TCP traffic received on Port 80 will be forwarded to the configured servers via port 80.</p>	
	
<p>Port Range: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the Servers setting. For example, if IP Protocol is set to TCP, Port is set to Port Range, and Service Port set to 80-88, then TCP traffic received on ports 80 through 88 will be forwarded to the configured servers via the respective ports.</p>	
	
<p>Port Mapping: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the Servers setting. For example, if IP Protocol is set to TCP, Port is set to Port Mapping, Service Port is set to 80, and Map to Port is set to 88, then TCP traffic on port 80 is forwarded to the configured servers via port 88.</p>	
<p>(Please see below for details on the Servers setting.)</p>	
	
<p>Range Mapping: traffic that is received by Peplink Balance via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the Servers setting.</p>	
<p>Inbound IP Address(es)</p>	<p>This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.</p>
<p>Included Server(s)</p>	<p>This setting specifies the LAN servers that handle requests for the service, and the relative weight values. The amount of traffic that is distributed to a server is proportional to the weight value assigned to the server relative to the total weight. Example: With the following weight settings on a Peplink Balance:</p>

- demo_server_1: 10
- demo_server_2: 5

The total weight is 15 = (10 + 5)

Matching traffic distributed to demo_server_1: 67% = (10 / 15) x 100%

Matching traffic distributed to demo_server_2: 33% = (5 / 15) x 100%

UPnP / NAT-PMP Settings

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

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

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



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

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

7.5.3 DNS Settings



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

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

DNS Server	Disabled	
Zone Transfer	Disabled	
Default SOA / NS	Undefined	
Default Connection Priority		
Priority 1: WAN 1, WAN 2, WAN 3, WAN 4, WAN 5, Mobile Internet		
Domain Names		
Domain Name	<i>These is currently no DNS domains.</i>	
New Domain Name		
Reverse Lookup Zones		
Zone Name	<i>There is currently no Reverse Lookup Zones.</i>	
New Reverse Lookup Zone		

[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	When this function is enabled, the system will check to see if an incoming DNS client is within any WAN's ISP subnet. Only the matched WAN(s)'s IP addresses will be returned. Note that this feature is available only when a subnet database has been defined.
Default SOA / NS	Click the  button to define a default SOA / NS record for all domain names. When defining a default SOA record, Name Server IP Address is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain. For defining default NS records, the host <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.
Default Connection Priority	Default Connection Priority defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the Connection Priority set to Default . Please refer to Section 17.3.9 for details. The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable. To specify the primary and backup connections, click the  button that corresponds to Default Connection Priority . A selection screen will appear. Each WAN connection is associated with a priority number. Click Save to save the settings when configuration is complete.
Domain name	This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its "NS", "MX" and "TXT" records, and its sub-domains' "A" and "CNAME" records. Add a new record by clicking the New Domain Name button. Click on a domain name to edit. Press the red X to remove a domain name.

New Domain Name

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

SOA Record ?

Use Default SOA and NS Records ✎

NS Records ?

Host	Name Server	TTL (sec)	
<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

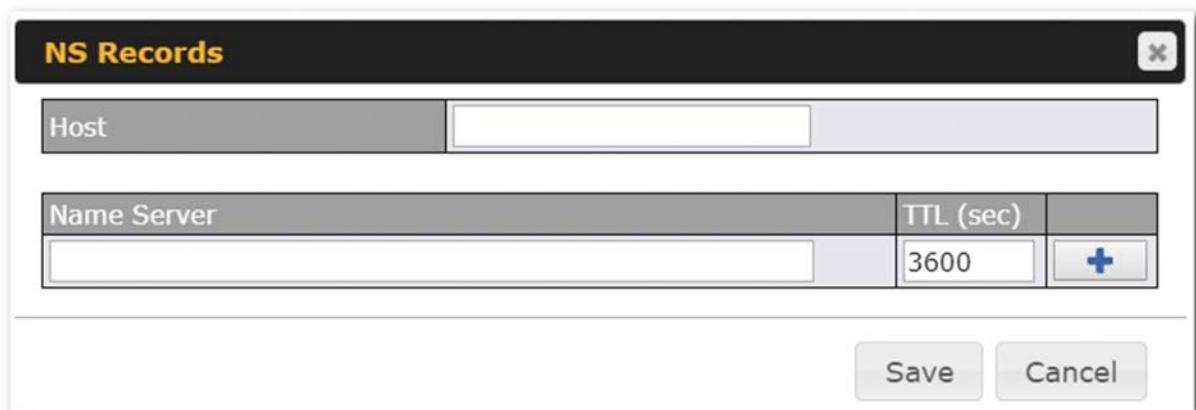
this field is optional. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically.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



NS Records		
Host <input type="text"/>		
Name Server	TTL (sec)	
<input type="text"/>	3600	<input data-bbox="1268 1332 1316 1377" type="button" value="+"/>
<input data-bbox="1050 1433 1177 1489" type="button" value="Save"/> <input data-bbox="1193 1433 1343 1489" type="button" value="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:

MX Records
✕

Host

This is equivalent to
demopeplink.com.

Priority	Mail Server	TTL (sec)	
1		3600	+

Save

Cancel

When creating an MX record for the domain itself (not a sub-domain), the **Host** field should be left blank. For each record, **Priority and Mail Server** name must be entered. **Priority** typically ranges from 10 to 100. Smaller numbers have a higher a priority. After finishing adding MX records, click the **Save** button.

CNAME Records

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

CNAME Record
✕

Host	
Points To	
TTL (sec)	3600

This is equivalent to
demopeplink.com.

Save

Cancel

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

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

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

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.
Priority	This option specifies the priority of different connections. Select the Default option to apply the Default Connection Priority (refer to the table shown on the main DNS settings page) to an A record. To customize priorities, choose the Custom option and a priority selection table will be shown at the bottom.

Included IP Address(es)

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**.

The IP addresses listed in each box as **default** are the Internet IP addresses associated with each of the WAN connections. Static IP addresses that are not associated with any WAN can be entered into the **Custom IP** list. A PTR record is also created for each custom IP.

For WAN connections that operate under drop-in mode, there may be other routable IP addresses in addition to the default IP address. Therefore, the Peplink Balance allows custom Internet IP addresses to be added manually via filling the text box on the right-hand side and clicking the  button.

Only the checked IP addresses in the lists are candidates to be returned when responding to a DNS query.

If a WAN connection is down, the corresponding set of IP addresses will not be returned. However, the IP addresses in the **Custom IP Address** field will always be returned.

If the **Connection Priority** field is set to **Custom**, you can also specify the usage priority of each WAN connection. Only selected IP address(es) of available connection(s) with the highest priority, and custom IP addresses will be returned. By default, **Connection Priority** is set to **Default**.

PTR Records

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

TXT Records

This table shows the TXT record of the domain name.

TXT Record ✕

Host	<input type="text"/>
TXT Value	<div style="border: 1px solid #ccc; padding: 5px; width: 80%;"> This is equivalent to demopeplink.com. </div>
TTL (sec)	<input type="text" value="3600"/>

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

When creating a TXT record for the domain itself (not a sub-domain), the **Host** field should be left blank. The maximum size of the TXT Value is 255 bytes.

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

SRV Records

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

SRV Records ✕

Service

Priority	Weight	Target	Port	TTL (sec)	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="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**.



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

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

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

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

- Create a reverse lookup zone that corresponds to the subnet network address of the host.
In the reverse lookup zone, add a pointer (PTR) resource record that maps the host IP address to the host name.
- Click the **New Reverse Lookup Zone** button and enter a reverse lookup zone name. If you are delegated the subnet *11.22.33.0/24*, the **Zone Name** should be *33.22.11.in-arpa.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: 50%;" type="text"/>
Email	?	<input style="width: 50%; value: webmaster;" type="text"/>
Refresh (sec)	?	<input style="width: 50%; value: 14400;" type="text"/>
Retry (sec)	?	<input style="width: 50%; value: 900;" type="text"/>
Expire (sec)	?	<input style="width: 50%; value: 1209600;" type="text"/>
Min Time (sec)	?	<input style="width: 50%; value: 3600;" type="text"/>
TTL (sec)	?	<input style="width: 50%; value: 3600;" type="text"/>

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

For example:

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

"ns2.mydomain.com."

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

NS Records

NS Records
✕

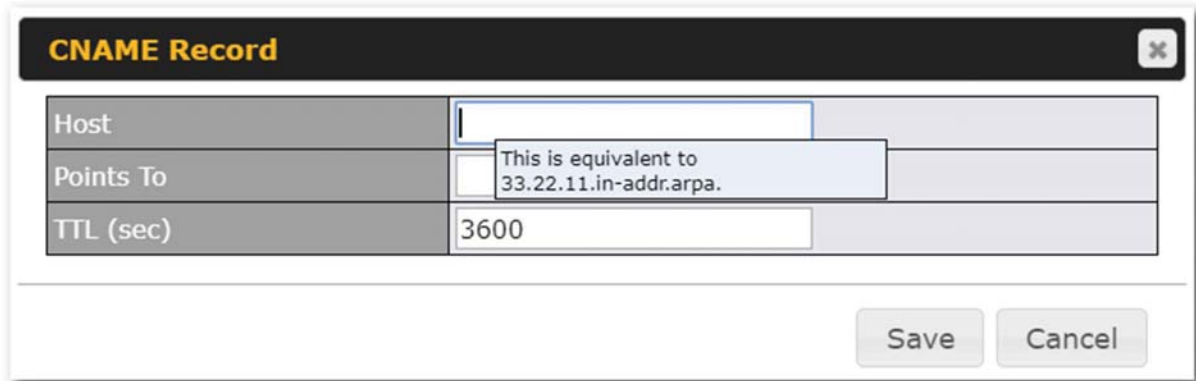
Host	<input style="width: 50%;" type="text"/>	
	This is equivalent to 33.22.11.in-addr.arpa.	
Name Server	TTL (sec)	+
<input style="width: 50%;" type="text"/>	<input style="width: 50%; value: 3600;" type="text"/>	<input type="button" value="+"/>

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



The screenshot shows a dialog box titled "CNAME Record" with a close button (X) in the top right corner. The dialog contains a table with three rows: "Host", "Points To", and "TTL (sec)". The "Host" field is empty. The "Points To" field has a tooltip that says "This is equivalent to 33.22.11.in-addr.arpa.". The "TTL (sec)" field contains the value "3600". At the bottom right of the dialog are "Save" and "Cancel" buttons.

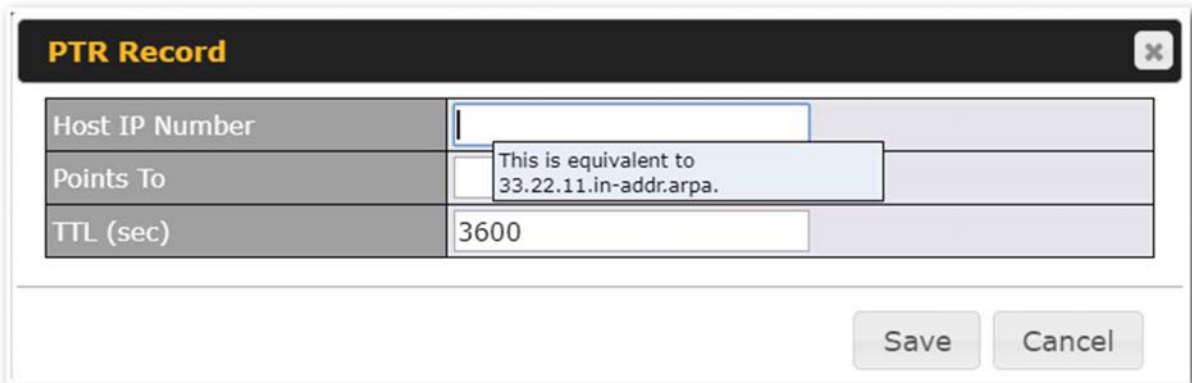
CNAME Record	
Host	
Points To	<input type="text" value="This is equivalent to 33.22.11.in-addr.arpa."/>
TTL (sec)	3600

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)	3600

Save Cancel

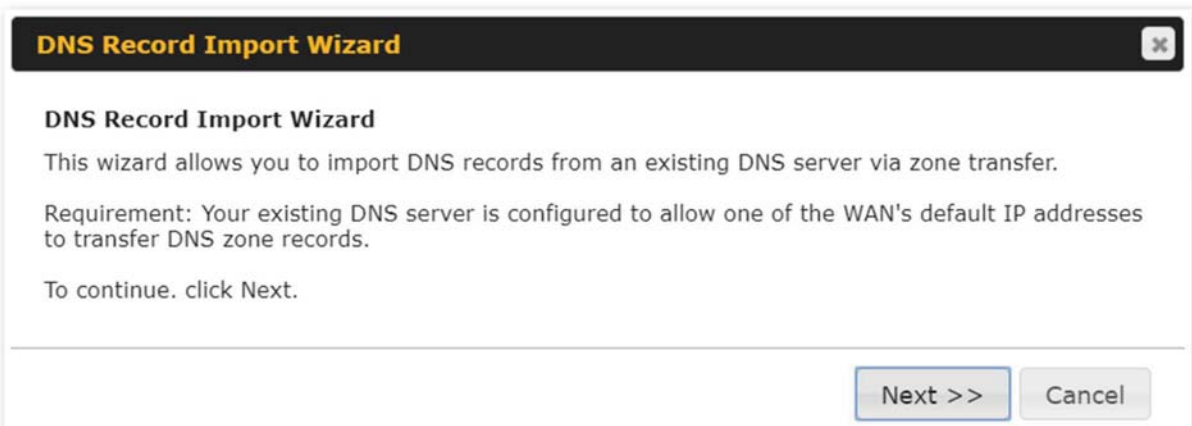
To create a new PTR record, click the **New PTR Record** button.

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

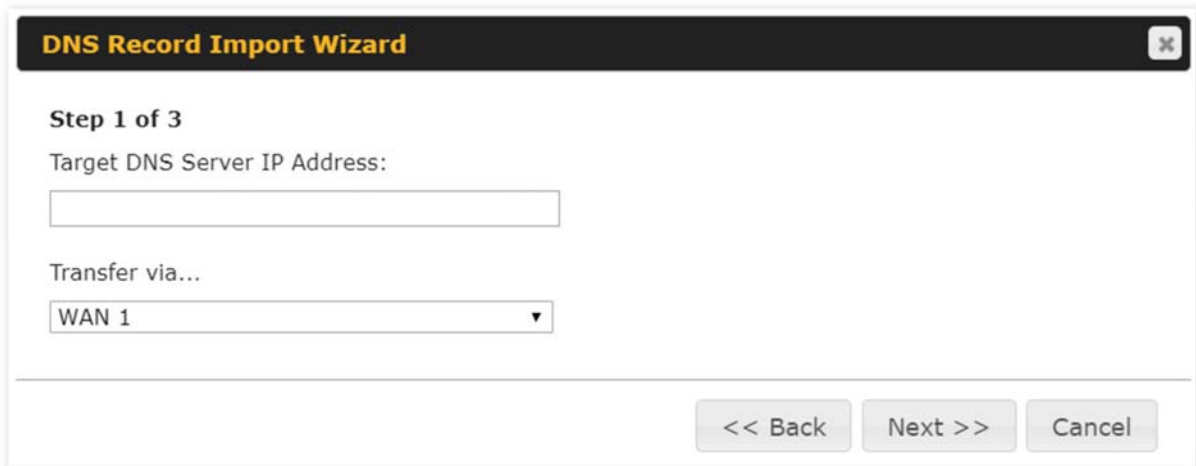
This wizard allows you to import DNS records from an existing DNS server via zone transfer.

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.

Next >> Cancel

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



DNS Record Import Wizard

Step 1 of 3

Target DNS Server IP Address:

Transfer via...

WAN 1

<< Back Next >> Cancel

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



DNS Record Import Wizard

Step 2 of 3

Domain Names (Zones):

(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

7.6 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 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.

7.7 MediaFast

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

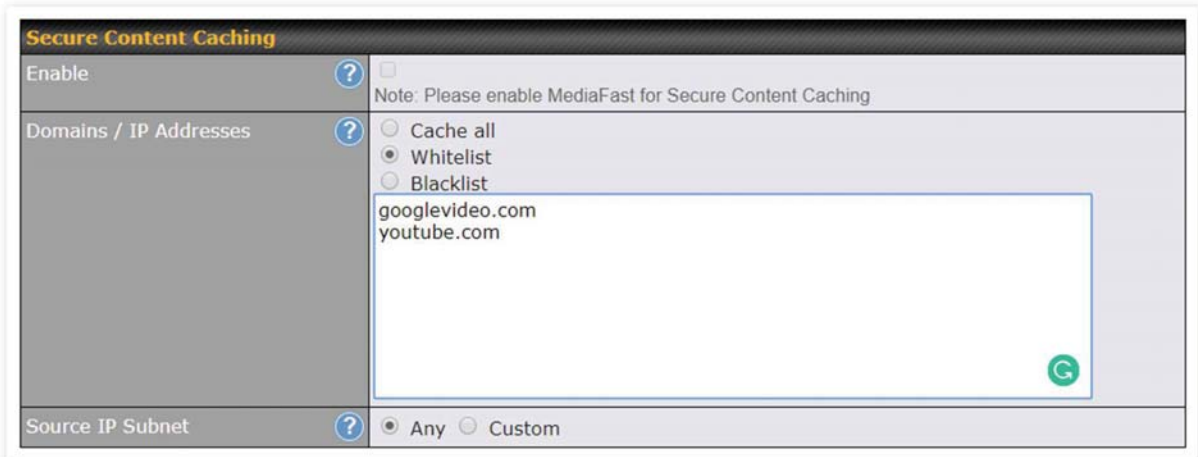
Setting Up MediaFast Content Caching

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



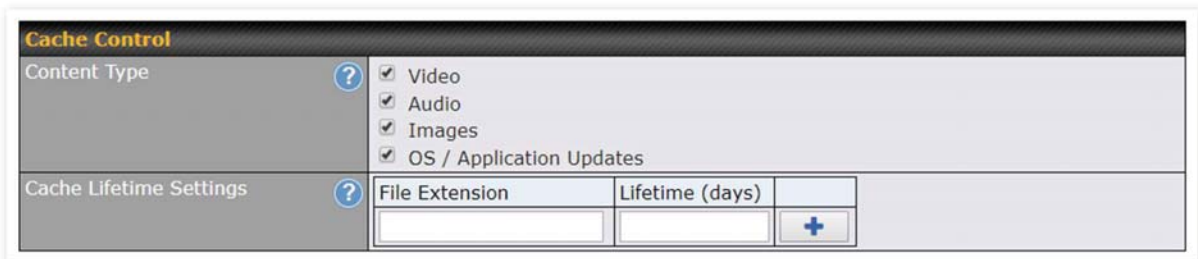
MediaFast

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*.

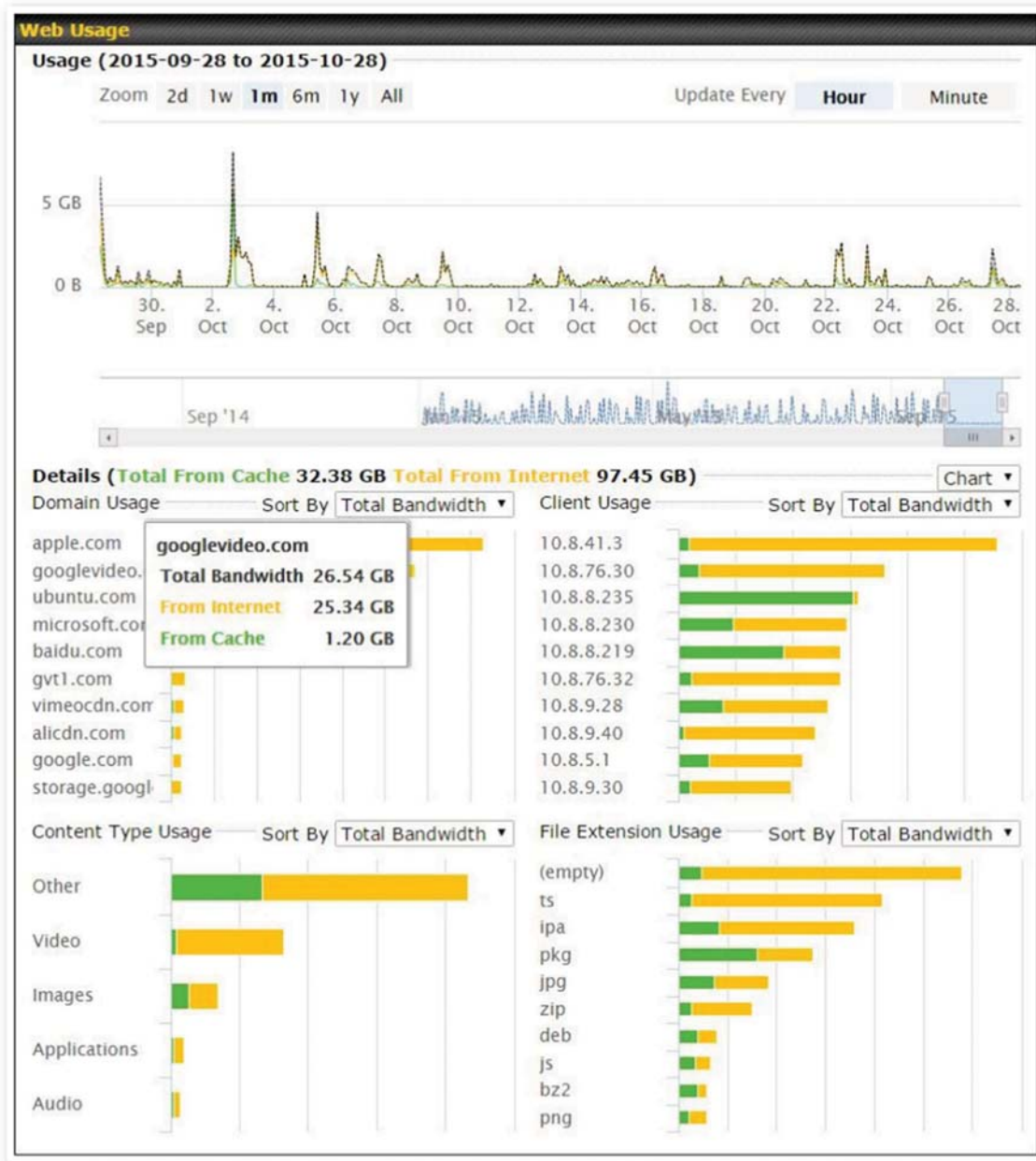
*See <https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/>



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	<p>To begin a scheduled download immediately, click .</p> <p>To cancel a scheduled download, click .</p> <p>To edit a scheduled download, click .</p>

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 type="text"/>	
Active	<input checked="" type="checkbox"/>	
URL	URL	<input type="text"/>
		<input style="border: none; background: none; border: 1px solid #ccc; padding: 2px 5px;" type="button" value="+"/>
Depth	2 <input type="button" value="v"/> levels	<input type="button" value="Default"/>
Time Period	From <input type="button" value="00"/> <input type="button" value=":"/> <input type="button" value="00"/> to <input type="button" value="01"/> <input type="button" value=":"/> <input type="button" value="00"/>	
Repeat	<input type="button" value="Everyday"/>	
Bandwidth Limit	<input type="text" value="0"/>	<input type="button" value="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.

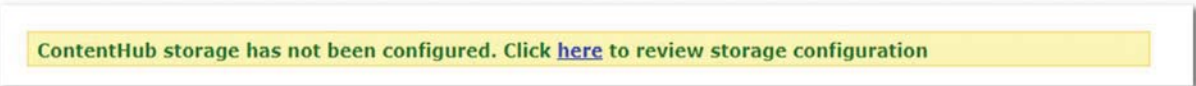
Clear Statistics Click to clear all prefetch and status page statistics.

7.8 ContentHub

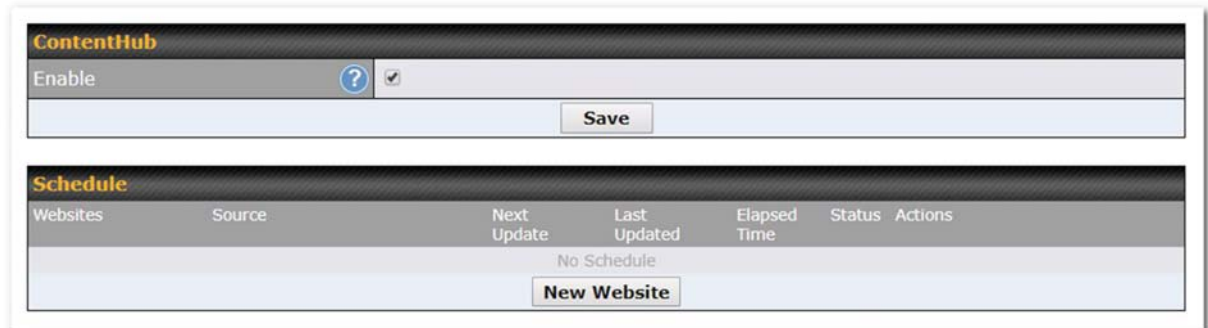
Integrated into MediaFast-enabled routers, ContentHub allows you to deliver webpages and applications using the local storage on your router.

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.



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



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


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

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

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

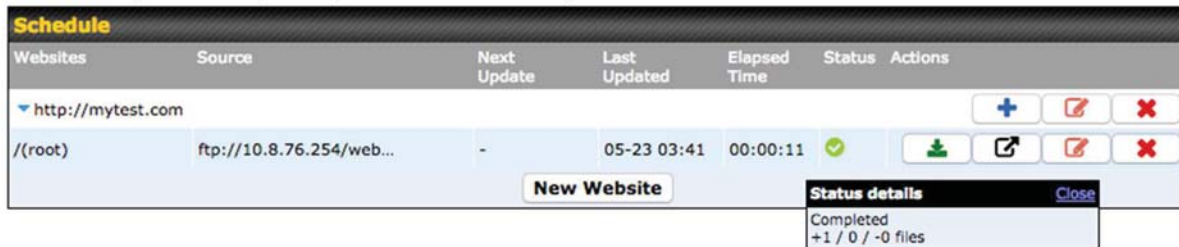


The content will be synced based on the **Period** that is configured before.

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:



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

Configure an application to be published from the contenthub

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

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

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

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

Package List		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	ftp :// <input type="text"/> Username: <input type="text"/> Password: <input type="text"/>
Period	Everyday From 00:00 to 01:00
Bandwidth Limit	0 Gbps (0: Unlimited)

The setting is 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

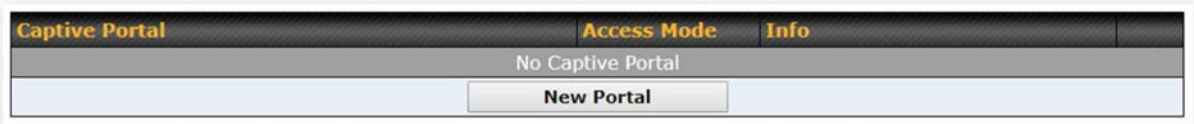
This will allow you to run for example a file sharing platform (Owncloud), a web server (Wordpress, Joomla) , a learning platform (Moodle) or a visualisation tool for viewing large scale data (Kibana).

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>

7.9 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

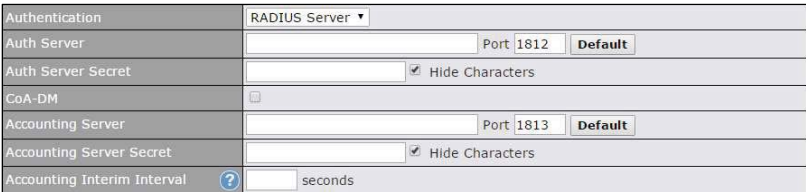
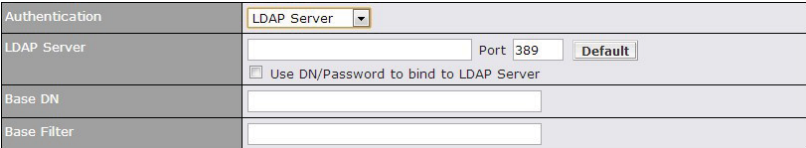
Name	<input type="text" value="demoportal"/>	
Enable	<input type="checkbox"/>	
Hostname	<input type="text" value="captive-portal.peplink.com"/> Default	
Access Mode	<input checked="" type="radio"/> Open Access <input type="radio"/> User Authentication <input type="radio"/> External Server	





Portal Access Settings

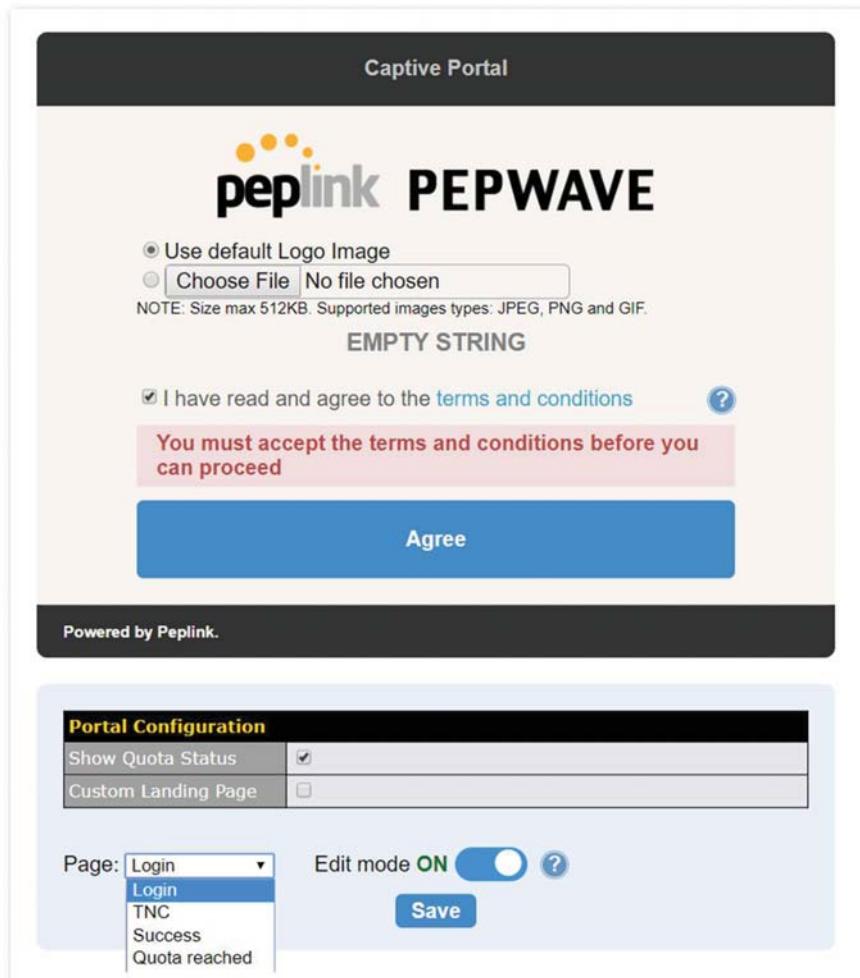
Access Quota	30	mins (0: Unlimited)	0	MB (0: Unlimited)
Quota Reset Time	<input checked="" type="radio"/> Daily at 00 :00 <input type="radio"/> 1440 minutes after quota reached			
Inactive Timeout	0 minutes (0: No Timeout)			
Allowed Networks	<input type="text" value="Domain Name / IP Address / Network"/>			+
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>  <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>
LDAP Server	<p>This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:</p>  <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to Daily will reset it at a specified time every day. Setting a number of minutes after quota reached establish a timer for each user that begins after the quota has been reached.

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



Captive Portal

peplink PEPWAVE

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 Login TNC Success Quota reached

Edit mode **ON** ?


Save

7.10 QoS

7.10.1 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.

7.10.2 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"/>		
	Manager	Staff	Guest
Bandwidth %	50%	30%	20%
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M

You can define a maximum download speed (over all WAN connections) and upload speed (for each

WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Managers. By default, download and upload bandwidth limits are set to unlimited (set as **0**).

Individual Bandwidth Limit			
Enable	<input checked="" type="checkbox"/>		
User Bandwidth Limit	Download	Upload	
	Manager: Unlimited	Unlimited	
	Staff: <input type="text" value="0"/> Mbps <input type="button" value="v"/> (0: unlimited)	<input type="text" value="0"/> Mbps <input type="button" value="v"/> (0: unlimited)	
	Guest: <input type="text" value="0"/> Mbps <input type="button" value="v"/>	<input type="text" value="0"/> Mbps <input type="button" value="v"/> (0: unlimited)	

7.10.3 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			<input type="button" value="x"/>
	Manager	Staff	Guest	
All Supported Streaming Applications	<input type="text" value="↑ High"/>	<input type="text" value="— Normal"/>	<input type="text" value="↑ High"/>	<input type="button" value="x"/>
All Email Protocols	<input type="text" value="↑ High"/>	<input type="text" value="↑ High"/>	<input type="text" value="↑ High"/>	<input type="button" value="x"/>
MySQL	<input type="text" value="↑ High"/>	<input type="text" value="— Normal"/>	<input type="text" value="↓ Low"/>	<input type="button" value="x"/>
SIP	<input type="text" value="↑ High"/>	<input type="text" value="↓ Low"/>	<input type="text" value="↓ Low"/>	<input type="button" value="x"/>
<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.

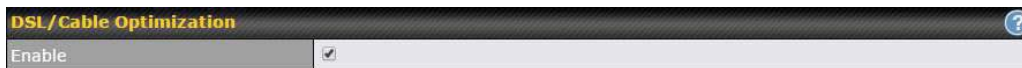
When **Supported Applications** is selected, the Peplink Balance will inspect network traffic and prioritize the selected applications. Alternatively, you can select **Custom Applications** and define the application by providing the protocol, scope, port number, and DSCP value.

Add / Edit Application	
Type	<input checked="" type="radio"/> Supported Applications <input type="radio"/> Custom Applications
Category	Miscellaneous
Application	All Supported Miscellaneous Protocols All Supported Miscellaneous Protocols HTTP NTP SNMP STUN USENET
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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.



7.11 Firewall

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

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

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

7.11.1 Access Rules

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

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

[Add Rule](#)

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on
Protocol	Any <small>← :: Protocol Selection Tool ::</small>
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 <small>Drag and drop rows to change rule order</small>						
Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy	
Default	Any	Any	Any	Any	Allow	
<input type="button" value="Add Rule"/>						


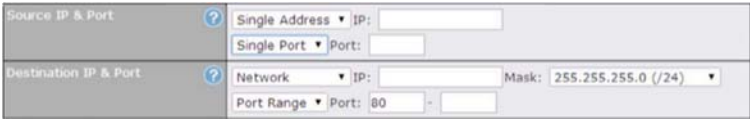
Click **Add Rule** to display the following window:

Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on
WAN Connection	Any
Protocol	Any <small>← :: Protocol Selection Tool ::</small>
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

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

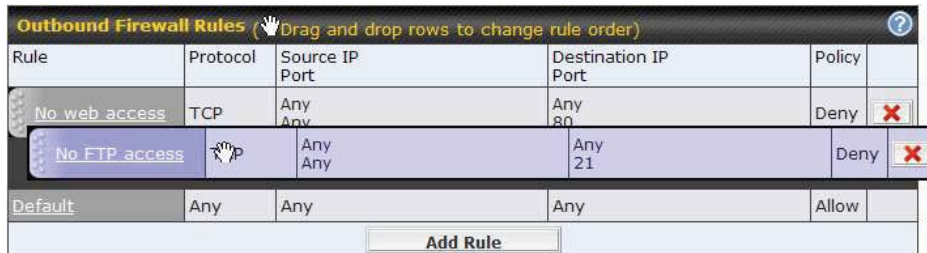
<p>Enable</p>	<p>This setting specifies whether the firewall rule should take effect.</p> <p>If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule.</p> <p>If the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

Action	<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>
Event Logging	<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:</p> <pre>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</pre> <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.



To remove a rule, click the button.

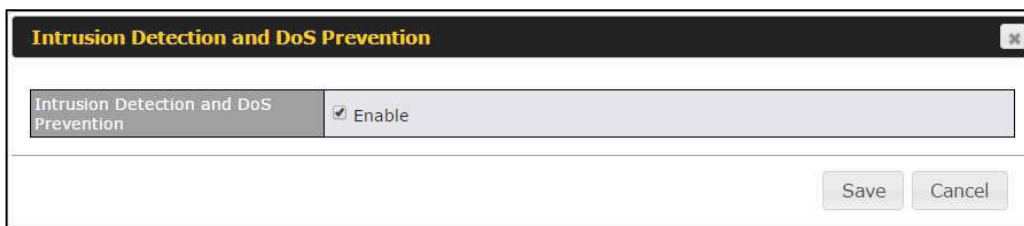
Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default** rule will be applied.

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

Tip

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

Intrusion Detection and DoS Prevention



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

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

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

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

7.11.2 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: 95%;" type="text"/>	255.255.255.0 (/24) ▼	+

URL Logging

Enable	<input type="checkbox"/>
Log Server Host	<input style="width: 60%;" 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 traffic. Secure web (HTTPS) traffic is not supported.

Customized Domains

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

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

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

Exempted User Groups

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

Exempted Subnets

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

URL Logging

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

7.12 OSPF & RIPv2

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

OSPF		
Router ID	LAN IP Address	
Area	Interfaces	
0.0.0.0	Untagged LAN (192.168.112.1/24), WAN 4 (192.168.254.10/24)	
Add		
RIPv2		
No RIPv2 Defined.		
OSPF & RIPv2 Route Advertisement		
PepVPN Route Isolation	<input type="checkbox"/> Enable	
Network Advertising	---	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)
Save		

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

OSPF settings ✕

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

To access RIPv2 settings, click .

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

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

7.13 BGP

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

BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	
Add			

Click "x" to delete a BGP profile

Click "Add" to add a new BGP profile

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

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

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

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

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

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

Filter Mode	This option selects the route import filter mode.
--------------------	---

	<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 specifies the network in the "route import" entry</p> <p>Exact Match: When this box is checked, only routes with the same Networks and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnet will be filtered.</p>

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

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


7.14 Remote User Access

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

7.14.1 L2TP with IPsec

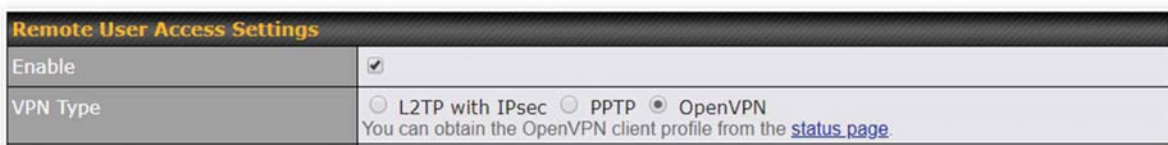
Remote User Access Settings	
Enable	<input checked="" type="checkbox"/>
VPN Type	<input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input type="radio"/> OpenVPN
Preshared Key	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

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.

7.14.2 OpenVPN



Remote User Access Settings

Enable

VPN Type L2TP with IPsec PPTP OpenVPN
You can obtain the OpenVPN client profile from the [status page](#).

Select OpenVPN and continue to configure the authentication method.

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



OpenVPN Client Profile  [Route all traffic](#) | [Split tunnel](#)

You have a choice between 2 different OpenVPN Client profiles.

8 "route all traffic" profile

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

9 "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.

9.1.1 PPTP



Remote User Access Settings

Enable

VPN Type L2TP with IPsec PPTP OpenVPN

No additional configuration required.

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