



Peplink Balance B30 LTE User Manual

Peplink Products:

Peplink Balance 30 LTE / Balance 30 LTE / BPL-031-LTE-E-T / Pismo 811AC /

Peplink Balance Firmware 7.1.1
April 2019

Table of Contents

Introduction and Scope	7
Glossary	8
Product Comparison Chart	10
Product Features	11
Supported Network Features	11
Other Supported Features	13
Advanced Feature Summary	14
Drop-in Mode and LAN Bypass: Transparent Deployment	14
QoS: Clearer VoIP	15
Per-User Bandwidth Control	15
High Availability via VRRP	16
USB Modem and Android Tethering	17
Built-In Remote User VPN Support	17
LACP NIC Bonding	18
Package Contents	19
Peplink Balance 30 LTE	19
Peplink Balance Overview	19
Peplink Balance 30 LTE	19
Installation	21
Preparation	21
Constructing the Network	21
Basic Configuration	21
Connecting to the Web Admin Interface	21
Configuration with the Setup Wizard	23
Network Tab	27
WAN	27
Health Check Settings	33
Bandwidth Allowance Monitor Settings	37
Additional Public IP Settings	37
Dynamic DNS Settings	38
LAN	40
Network Settings	40

Network Settings (Common Settings)	44
Port Settings	48
VPN	49
SpeedFusion	49
IPsec VPN	55
Outbound Policy	59
Inbound Access	62
Servers	62
Services	63
DNS Settings	66
SOA Records	69
NS Records	70
MX Records	71
CNAME Records	71
A Records	72
PTR Records	73
TXT Records	74
SRV Records	74
Reverse Lookup Zones	75
SOA Record	76
NS Records	77
CNAME Records	77
PTR Records	78
DNS Record Import Wizard	78
NAT Mappings	82
MediaFast	85
Setting Up MediaFast Content Caching	85
Viewing MediaFast Statistics	86
Prefetch Schedule	87
ContentHub	89
MDM Settings	91
Captive Portal	91
QoS	95
User Groups	95
Bandwidth Control	96
Application	96

Prioritization for Custom Application	97
DSL/Cable Optimization	98
Firewall	98
Access Rules	98
Intrusion Detection and DoS Prevention	102
Content Blocking	103
Application Blocking	105
Web Blocking	105
Customized Domains	105
Exempted User Groups	105
Exempted Subnets	105
URL Logging	106
OSPF & RIPv2	106
BGP	109
Remote User Access	111
Misc. Settings	113
High Availability	113
Certificate Manager	116
Service Forwarding	116
SMTP Forwarding	118
Web Proxy Forwarding	118
DNS Forwarding	119
Custom Service Forwarding	119
Service Passthrough	119
AP Tab	120
AP	120
AP Controller	120
Wireless SSID	121
Settings	127
AP Controller Status	131
Info	131
Access Points (Usage)	133
Wireless SSID	135
Wireless Client	136
Nearby Device	137
Event Log	138

Toolbox	139
System Tab	140
System	140
Admin Security	140
Firmware	142
Time	143
Schedule	144
Email Notification	146
Event Log	148
SNMP	149
InControl	151
Configuration	152
Feature Add-ons	153
Reboot	153
Tools	154
Ping	154
Traceroute	154
Wake-on-LAN	155
CLI (Command Line) Support	155
Status Tab	156
Status	156
Device	156
Active Sessions	158
Client List	160
WINS Clients	161
OSPF & RIPv2	161
MediaFast	161
SpeedFusion Status	162
Event Log	166
Device Event Log	167
IPsec Event Log	167
Bandwidth	167
Real-Time	168
Hourly	169
Daily	169
Monthly	172

Harrington Industrial Plastics	179
PLUSS	182

1 Introduction and Scope

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

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

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

This manual applies to the following Peplink Balance products:

- Peplink Balance 30 LTE
- Peplink Balance 30 Pro

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

2 Glossary

The following terms, acronyms, and abbreviations are frequently used in this manual:

Term	Definition
3G	3rd generation standards for wireless communications (e.g., HSDPA)
4G	4th generation standards for wireless communications (e.g., LTE)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVDO	Evolution-Data Optimized
FQDN	Fully Qualified Domain Name
HSDPA	High-Speed Downlink Packet Access
HTTP	Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC Address	Media Access Control Address
MTU	Maximum Transmission Unit
MSS	Maximum Segment Size
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
210+	Refers to Peplink Balance 210/310/380/580/710/1350/2500
380+	Refers to Peplink Balance 380/580/710/1350/2500

3 Product Comparison Chart

Click underlined features to reach the relevant portion of the manual.

Full product comparison available at:

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

4 Product Features

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

4.1 Supported Network Features

4.1.1 WAN

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

4.1.2 LAN

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

4.1.3 VPN

- Secure SpeedFusion™
- SpeedFusion performance analyzer
- X.509 certificate support (**feature activation required on some Balance models**)
- Bandwidth bonding and failover among selected WAN connections
- Ability to route traffic to a remote VPN peer
- Optional pre-shared key setting
- Layer 2 bridging
- Layer 2 Peer Isolation
- SpeedFusion™ throughput, ping, and traceroute tests

- Built-in L2TP / PPTP VPN server
- Authenticate L2TP / PPTP clients using RADIUS and LDAP servers
- Multi-Site PepVPN Profile
- IPsec VPN for network-to-network connections (works with Cisco and Juniper only)
- L2TP / PPTP and IPsec passthrough

4.1.4 Inbound Traffic Management

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

4.1.5 Outbound Policy

- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms
- Time-based scheduling

4.1.6 AP Controller

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

4.1.7 QoS

- Quality of service for different applications and custom protocols
- User group classification for different service levels
- Bandwidth usage control and monitoring on group- and user-level
- Application prioritization for custom protocols and DSL optimization

4.1.8 Firewall

- Outbound (LAN to WAN) firewall rules
- Inbound (WAN to LAN) firewall rules per WAN connection
- Intrusion detection and prevention
- Specification of NAT mappings
- Web blocking
- Application blocking
- Time-based scheduling
- Outbound firewall rules can be defined by destination domain name

4.1.9 Captive Portal

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

4.2 Other Supported Features

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

5 Advanced Feature Summary

5.1 Drop-in Mode and LAN Bypass: Transparent Deployment



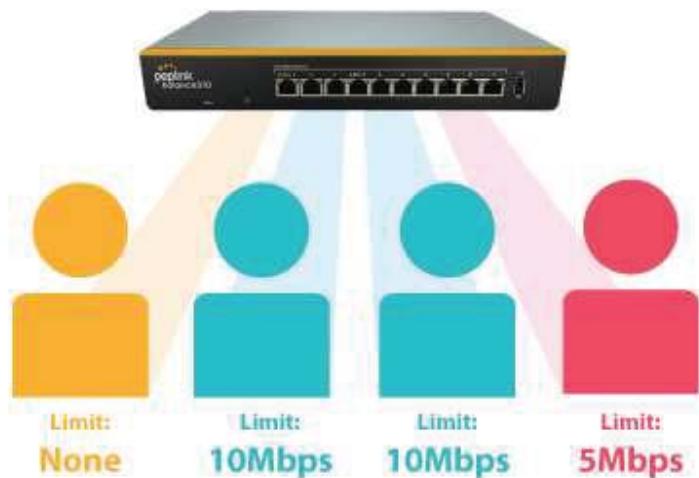
As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass**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

5.2 QoS: Clearer VoIP



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

5.3 Per-User Bandwidth Control



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

5.4 High Availability via VRRP



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

5.5 USB Modem and Android Tethering



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

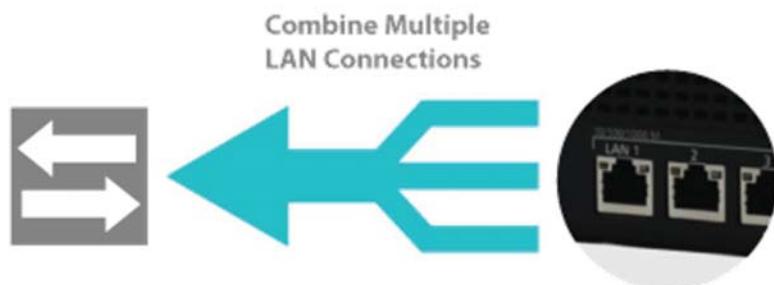
5.6 Built-In Remote User VPN Support



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

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

5.7 LACP NIC Bonding



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

6 Package Contents

The contents of Peplink Balance product packages are as follows:

6.1 Peplink Balance 30 LTE

- Peplink Balance 30 LTE
- 4G LTE Antennas
- Power adapter
- Information slip
- Rackmount kit

7 Peplink Balance Overview

7.1 Peplink Balance 30 LTE

7.1.1 Panel Appearance



7.1.2 LED Indicators

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

Power and Status Indicators

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

LAN and WAN Ports

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

USB Port

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

8 Installation

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

8.1 Preparation

Before installing your Peplink Balance, please prepare the following:

- At least one Internet/WAN access account
- For each network connection, one 10/100BaseT UTP cable with RJ45 connector, one 1000BaseT Cat5E UTP cable for the Gigabit port, or one USB modem for the USB WAN port
- A computer with the TCP/IP network protocol and a web browser installed—supported browsers include Microsoft Internet Explorer 8.0 and above, Mozilla Firefox 10.0 and above, Apple Safari 5.1 and above, and Google Chrome 18 and above

8.2 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.

9 Basic Configuration

9.1 Connecting to the Web Admin Interface

1. Start a web browser on a computer that is connected with the Peplink Balance through the LAN.
2. To connect to the web admin of the Peplink Balance, enter the following LAN IP address in the address field of the web browser:

`http://192.168.1.1`

(This is the default LAN IP address of the Peplink Balance.) Enter the following to access the web admin interface.

Username: admin

Password: admin

(This is the default admin user login of the Peplink Balance. The admin and read-only user password can be changed at **System>Admin Security**.)

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



The screenshot shows the Peplink Balance 710's web admin dashboard. It includes sections for network interfaces (3G, Wi-Fi, FBB, WAN1-WAN6, USB), a LAN interface (Router IP Address: 192.168.1.1), PepVPN with SpeedFusion™ (SDT: Established, IPTTest: N/A), AP Controller Information (Access Point: 0, Connected Clients: 0), and Device Information (Model: Peplink Balance 710, Firmware: 6.1.0 build 2863, Uptime: 38 days 22 hours 17 minutes, CPU Load: 5%, Throughput: 0.0 Mbps download / 0.0 Mbps upload).

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.

9.2 Configuration with the Setup Wizard

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

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



Click **Next >** to begin.

Setup Wizard > WAN Setup > Step 1

Welcome to Setup Wizard!

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

Click *Next* to begin.

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

Setup Wizard > WAN Setup > Step 2

Drop-in Mode	
Do you want to setup drop-in mode?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Which WAN port do you want to enable drop-in mode?	<select>WAN 1</select> WAN 1 WAN 2 WAN 3 WAN 4 WAN 5 WAN 6 WAN 7

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

Setup Wizard > WAN Setup > Step 3

Choose the WAN port(s) to be configured.

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

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

Setup Wizard > WAN Setup > Step 4

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

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

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

Setup Wizard > WAN Setup > Step 4

Choose a connection method for WAN 1.

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

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

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

Setup Wizard > WAN Setup > Step 3

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

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

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

Setup Wizard > WAN Setup > Step 4

Enter the parameters of Mobile Operator Settings for Mobile Internet.

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

Click on the appropriate check box(es) to select the preferred WAN connection(s). Connection(s) not selected in this step will be used as backup only. Click **Next >>** to continue.

Setup Wizard > WAN Setup > Step 5

Choose the preferred WAN Port(s) that is to be used as primary connection. The port(s) not selected in this step will only be used when none of the connection of the preferred port is up.

Preferred WAN Port Selection	
Port	Preferred
WAN 1	<input checked="" type="checkbox"/>
WAN 2	<input checked="" type="checkbox"/>
Mobile Internet	<input type="checkbox"/>

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

Setup Wizard > WAN Setup > Step 6

Choose time zone of your Country / Region.

Time Zone Settings	
Time Zone	(GMT+07:00) Krasnoyarsk
<input type="checkbox"/> Show all	

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

Setup Wizard > WAN Setup > Final Step

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

Summary of WAN Port(s) Configuration	
WAN 1	
Connection Method	Drop-in Static IP
IP Address	192.22.22.1
Subnet Mask	255.255.255.0
Default Gateway	192.22.22.1
DNS Server	192.22.22.1
Upload Bandwidth	1000 Mbps
Download Bandwidth	1000 Mbps
Preferred WAN Port(s)	
Ports	WAN 1 WAN 2
Time Zone Settings	

<< Back **Save Settings** **Cancel**

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

10 Network Tab

10.1 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. Mobile Internet	PPP	NAT	Backup Group 1

You can also enable IPv6 support in this section

IPv6
Disabled <input checked="" type="checkbox"/>

WAN Connection Settings (Ethernet)

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

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

WAN Connection Settings	
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 three possible connection methods for Ethernet WAN:</p> <ul style="list-style-type: none"> • DHCP • Static IP • PPPoE <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.
DNS Servers	Select a DNS server for this port to use. This port can either be automatically selected or manually designated.
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.
Standby State	This setting specifies the standby state of the WAN connection. The available options are Remain connected and Disconnect . The default state is Remain Connected .
Reply to ICMP PING	If No is selected, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: Yes
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 upstream bandwidth.</p>
Download Bandwidth	<p>This field refers to the maximum download speed.</p> <p>Default weight control for outbound traffic will be adjusted according to this value.</p>

WAN Connection Settings (Cellular)

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

Connection Settings	
WAN Connection Name	Cellular
Enable	<input type="checkbox"/>
Routing Mode	<input type="radio"/> NAT
Connection Type	<input type="radio"/> Always-on <input checked="" type="radio"/> Backup Priority Group 1 (Highest)
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Idle Disconnect	<input type="checkbox"/>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

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

gets disconnected.

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.

DNS Servers

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

Cellular Settings		
SIM Card	<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"/> [?]	
LTE/3G	Auto	Auto
Authentication	Auto	Auto
Data Roaming	<input type="checkbox"/>	
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom	
APN	<input type="text"/>	
Username	<input type="text"/>	
Password	<input type="text"/>	
Confirm Password	<input type="text"/>	
SIM PIN (Optional)	<input type="text"/> (Confirm) <input type="text"/> (Confirm)	
Bandwidth Allowance Monitor	<input type="checkbox"/> Enable <input type="checkbox"/> Enable	

Cellular Settings	
SIM Card	Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards.
Preferred SIM Card	If both cards were enabled on the above field, then you can designate the priority of the SIM card slots here.
3G/2G	This drop-down menu allows restricting cellular to particular band. Click the button to enable the selection of specific bands.
Authentication	Choose from PAP Only or CHAP Only to use those authentication methods exclusively.

	Select Auto to automatically choose an authentication method.
Data Roaming	This checkbox enables data roaming on this particular SIM card. Please check your service provider's data roaming policy before proceeding.
Operator Settings	This setting applies to 3G/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems. This allows you to configure the APN settings of your connection. If 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 connection, 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.

WAN Connection Settings (Common)

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

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

Physical Interface Settings

	<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>
Port Speed	<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.</p>
MSS	<p>This field is for specifying the Maximum Segment Size of the WAN connection.</p> <p>When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections.</p> <p>Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections.</p> <p>Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size.</p> <p>Default: Auto</p>
MAC Address Clone	<p>Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.</p>
VLAN	<p>Check the box to assign a VLAN to the interface.</p>

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

DHCP Settings	
Hostname	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

(Optional) provide you with a hostname, you can safely bypass this option.

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.

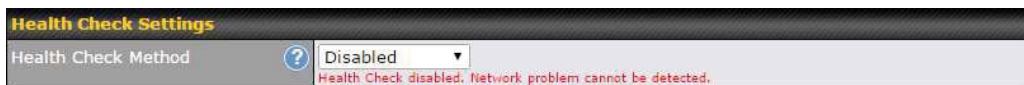
DNS Servers

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

Health Check Settings

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

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



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

Health Check Settings	
Method	This setting specifies the health check method for the WAN connection. This value can be configured as Disabled , PING , DNS Lookup , or HTTP . The default method is DNS Lookup . For mobile Internet connections, the value of Method can be configured as Disabled or SmartCheck .
Health Check Disabled	
<p>The screenshot shows a 'Health Check Settings' dialog box. At the top, it says 'Health Check Method'. Below it is a dropdown menu with 'Disabled' selected. A status message at the bottom states: 'Health Check disabled. Network problem cannot be detected.'</p>	
<p>When Disabled is chosen in the Method field, the WAN connection will always be considered as up. The connection will NOT be treated as down in the event of IP routing errors.</p>	

Health Check Method: PING

Health Check Method	PING
PING Hosts	Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts

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

PING Hosts

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

Health Check Method: DNS Lookup

Health Check Method	DNS Lookup
Health Check DNS Servers	Host 1: <input type="text"/> Host 2: <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 data-bbox="562 451 593 485" type="button" value="?"/> HTTP
URL 1	<input data-bbox="562 489 593 523" type="button" value="?"/> http:// <input data-bbox="636 489 1076 523" type="text"/> Matching String: <input data-bbox="716 525 740 559" type="checkbox"/>
URL 2	<input data-bbox="562 541 593 574" type="button" value="?"/> http:// <input data-bbox="636 541 1076 574" type="text"/> Matching String: <input data-bbox="716 577 740 610" type="checkbox"/>

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

URL1**WAN Settings>WAN Edit>Health Check Settings>URL1**

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

URL 2**WAN Settings>WAN Edit>Health Check Settings>URL2**

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

Other Health Check Settings

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

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

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

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

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

Note

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

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

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and checks fail, the Balance will automatically perform DNS lookups on some public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:

Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.

Bandwidth Allowance Monitor Settings

Bandwidth Allowance Monitor Settings	
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable
Action	<input type="checkbox"/> 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" value="100"/> GB

Bandwidth Allowance Monitor

If **Email Notification** is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance.

Action
If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.

Start Day This option allows you to define which day of the month each billing cycle begins.

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

Disclaimer

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

Additional Public IP Settings

Additional Public IP Settings	
IP Address List	<input type="text" value="210.10.10.0"/> <input type="text" value="255.255.255.255 (/32)"/> <input style="float: right; margin-right: 10px;" type="button" value="Delete"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> 210.10.10.1 210.10.10.2 210.10.10.3 210.10.10.4 210.10.10.5 </div> <div style="margin-top: 10px; font-size: small;"> Those settings will not be saved until the save button below has been pressed. </div>

Additional Public IP Settings

IP Address List

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

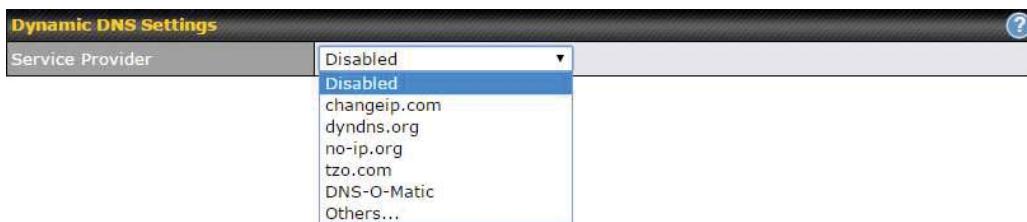
Dynamic DNS Settings

The Peplink Balance allows registering domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a hostname. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address externally even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

Either upon a change in IP addresses or every 23 days without link reconnection, the Peplink Balance will connect to the dynamic DNS service provider to update the provider's IP address records.

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



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

Dynamic DNS Settings	
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 type="checkbox"/>
Hosts / IDs	<input type="text"/>

Dynamic DNS Settings

This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:

- changeip.com
- dyndns.org
- no-ip.org
- tzo.com
- DNS-O-Matic
- Others...

support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.

Select **Disabled** to disable this feature.

User ID / User / Email

This setting specifies the registered user name for the dynamic DNS service.

Password / Pass / TZO Key

This setting specifies the password for the dynamic DNS service.

Update All Hosts

Check this box to automatically update all hosts.

Hosts / Domain

This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note

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

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

Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record

has not been 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.

10.2 LAN



10.2.1 Network Settings

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

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

IP Settings		
IP Address	192.168.1.1	255.255.255.0 (/24)

IP Settings

IP Address & Subnet Mask Enter the Peplink Balance's IP address and subnet mask values to be used on the LAN.

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

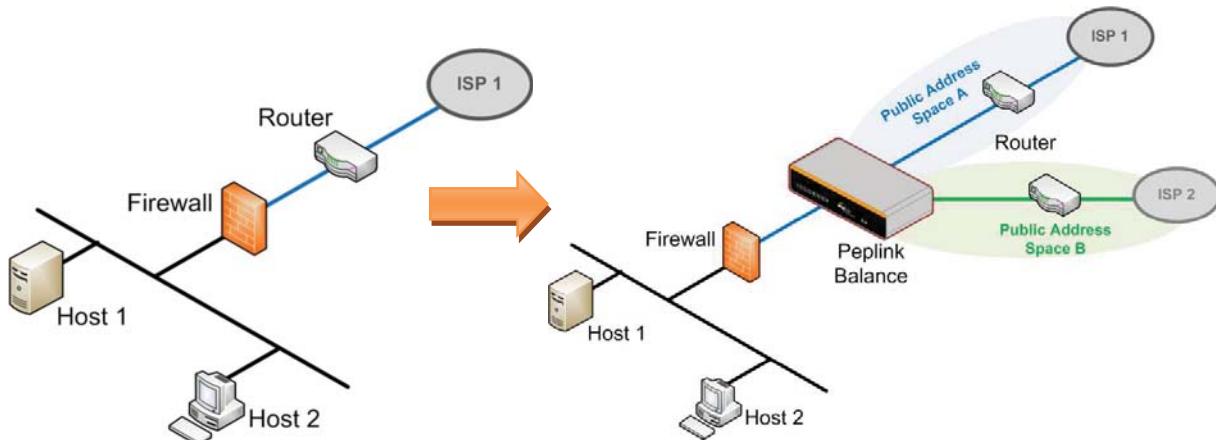
Network Settings

Name	Enter a name for the LAN.
VLAN ID	Enter a VLAN ID for your LAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.
Captive Portal	Check this box to turn on captive portals.

Drop-In Mode

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 with LAN bypass
WAN Default Gateway	<input type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) <input type="text"/> <input type="button"/>
WAN DNS Servers	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>

NOTE: The DHCP Server Settings will be overwritten.
 The following WAN 1 with LAN bypass settings will be overwritten: Enable, Connection Method, Routing Mode, Connection Type, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.
 The PPTP Server will be disabled.
 High Availability will be disabled.
 Tip: please review the DNS Forwarding setting under the Service Forwarding section.

Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of the Peplink Balance on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature. Please refer to Section 12, Drop-in Mode for details.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If WAN 1 with LAN Bypass is selected, the high availability feature will be disabled automatically.
Shared Drop-In IPA	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Balance will listen for this IP address when WAN hosts access services provided by the Balance (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The Balance will listen for this IP address when LAN hosts access services provided by the Balance (web admin access from the WAN, DNS proxy, etc.).
Shared IP	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

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

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

Layer 2 PepVPN Bridging			
PepVPN Profiles to Bridge		-----	
Remote Network Isolation		<input type="checkbox"/>	
Spanning Tree Protocol		<input type="checkbox"/>	
Override IP Address when bridge connected		<input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None	

Layer 2 PepVPN Bridging ^A	
PepVPN Profiles to Bridge^A	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN. They will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Remote Network Isolation^A	Enable this option if you want to block network traffic between remote networks. This will not affect the connectivity between them and this local LAN.
Spanning Tree Protocol^A	When Layer 2 bridging is enabled, this field specifies the port to be bridged to the remote site. If you choose WAN, the selected WAN will be dedicated to bridging with the remote site and will be disabled for WAN purposes. The LAN port will remain unchanged.
Override IP Address when bridge is connected^A	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up. If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.

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

10.2.2 Network Settings (Common Settings)

DHCP Server											
DHCP Server	<input type="checkbox"/> Enable										
DHCP Server Logging	<input type="checkbox"/>										
IP Range	192.168.1.10	-	192.168.1.250								
Lease Time	1 Days 0 Hours 0 Mins										
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically										
WINS Servers	<input checked="" type="checkbox"/> Assign WINS server <input type="radio"/> Built-in <input checked="" type="radio"/> External WINS Server 1: WINS Server 2:										
BOOTP	<input checked="" type="checkbox"/> Server IP Address: Boot File: Server Name: (Optional)										
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Extended DHCP Option</td> </tr> <tr> <td colspan="2"><input type="button" value="Add"/></td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		<input type="button" value="Add"/>			
Option	Value										
No Extended DHCP Option											
<input type="button" value="Add"/>											
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>00:00:00:00:00:00</td> <td></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>			Name	MAC Address	Static IP			00:00:00:00:00:00		<input type="button" value="+"/>
Name	MAC Address	Static IP									
	00:00:00:00:00:00		<input type="button" value="+"/>								

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

DHCP Server Settings	
DHCP Server	When this setting is enabled, the Peplink Balance's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Peplink Balance's DHCP server can prevent IP address collisions on the LAN.
DHCP Server Logging	<input type="checkbox"/> Check this box to log DHCP server activity.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Peplink Balance's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of Lease Time , the assigned IP address will no longer be valid and the IP address assignment must be renewed.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Peplink Balance's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Server	This option allows you to specify the Windows Internet Name Service (WINS) server. You

	<p>may choose to use the built-in WINS server or external WINS servers.</p> <p>When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP WINS Servers setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at Status>WINS Clients.</p>
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	<p>In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.</p> <p>To define an extended DHCP option, click the Add button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.</p>
DHCP Reservation	<p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses.</p> <p>The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p>Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in 00:AA:BB:CC:DD:EE format. Press to create a new record. Press to remove a record. Reserved clients information can be imported from the Client List, located at Status>Client List. For more details, please refer to Section 27.3.</p>

DHCP relay settings is an advanced feature. To enable it, click the button next to **DHCP Server**.

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

DHCP Relay Settings	
DHCP Relay	Enter the address of the DHCP server here. DHCP requests will be relayed to it.
DHCP Server IP Address	DHCP requests from the LAN are relayed to the entered DHCP server. For active-passive DHCP server configurations, enter active and passive DHCP server IPs into the DHCP Server 1 and DHCP Server 2 fields.

DHCP Option 82

This feature includes device information as relay agent for the attached client when forwarding DHCP requests from a DHCP client to a DHCP server. Device MAC address and network name are embedded to circuit ID and Remote ID in option 82.

DHCP Relay Logging

Check this box to log DHCP relay activity.

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

Static Route Settings

Static Route

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

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

WINS Server Settings

Enable	<input checked="" type="checkbox"/>
--------	-------------------------------------

WINS Server Settings

Enable

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

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

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

DNS Proxy Settings

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

DNS Resolvers^A

Check the box to enable the WINS server. A list of WINS clients will be displayed at **Network>LAN>DNS Proxy Settings>DNS Resolvers**.

This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es).

Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

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

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

Bonjour Forwarding Settings					
Enable	<input type="checkbox"/>				
Bonjour Service	<table border="1"> <tr> <td>Service Network</td> <td>Client Network</td> </tr> <tr> <td><input type="button" value="+"/></td> <td><input type="button" value="X"/></td> </tr> </table>	Service Network	Client Network	<input type="button" value="+"/>	<input type="button" value="X"/>
Service Network	Client Network				
<input type="button" value="+"/>	<input type="button" value="X"/>				
Save					

Bonjour Forwarding Settings

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

10.2.3 Port Settings

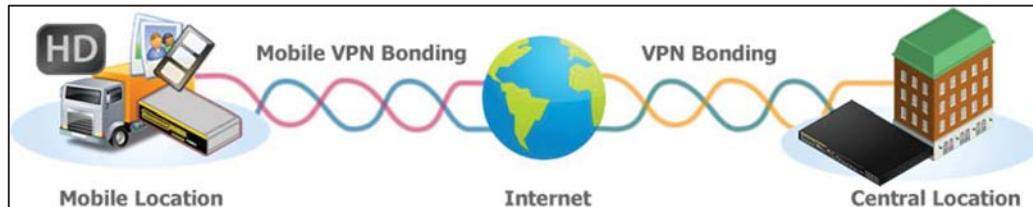
To configure port settings, navigate to **Network > Port Settings**

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

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

10.3 VPN

10.3.1 SpeedFusion



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

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

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

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

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

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

SpeedFusion Profiles

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

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



Send All Traffic To

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



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

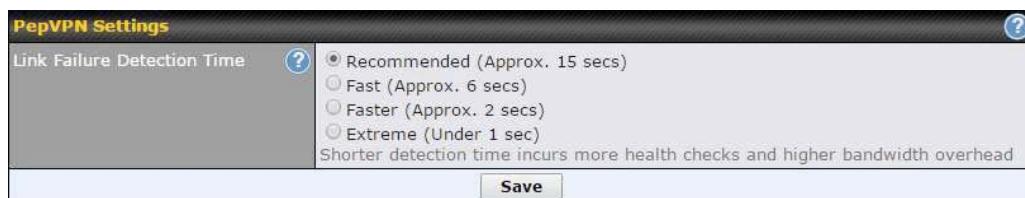


PepVPN Local ID

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



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



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

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

PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
	Click the icon next to the PepVPN Profile title bar to use the IP ToS field of your data packet on PepVPN WAN traffic.
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from By Remote ID Only , Preshared Key , or X.509 to specify the method the Peplink Balance will use to authenticate peers. When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field.

Remote ID / Pre-shared Key	This optional field becomes available when Remote ID / Pre-shared Key is selected as the Peplink Balance's VPN Authentication method, as explained above. Pre-shared Key defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.
Remote ID/Remote Certificate	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.
Allow Shared Remote ID	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.
NAT Mode	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
Remote IP Address / Host Names (Optional)	<p>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.</p> <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>
Data Port	<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>
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	<p>Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost.</p> <p>Default: 10</p>
WAN Smoothing^A	While using PepVPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the

WAN's available bandwidth.

Off - Disable WAN Smoothing.

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

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

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

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

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

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

WAN Connection Priority

WAN Connection Priority

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

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

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

IPsec VPN on the Peplink Balance is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for his multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen

problems (e.g.,unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

10.3.2 IPsec VPN

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

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

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

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

NAT-Traversal		Enabled (required by L2TP with IPsec)	<input type="checkbox"/>
IPsec VPN Profiles		Remote Networks	
Profile 1		192.168.11.193/24	<input type="button" value="X"/>
<input type="button" value="New Profile"/>			

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

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

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

Name	Profile 1												
Active	<input checked="" type="checkbox"/>												
Connect Upon Disconnection of	<input checked="" type="checkbox"/> WAN 2												
Remote Gateway IP Address / Host Name	12.12.12.12												
Local Networks	<p>Propose the following networks to remote gateway:</p> <p><input type="checkbox"/> 172.16.1.0/24 <input type="checkbox"/> 172.16.2.0/24 <input type="checkbox"/> 172.16.3.0/24 <input checked="" type="checkbox"/> 10.10.0.1/32 <input checked="" type="checkbox"/> 192.168.10.0/24 <input checked="" type="checkbox"/> 192.168.11.0/24 <input type="checkbox"/> []</p> <p>Apply the following NAT policies:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding-right: 20px;"><input checked="" type="checkbox"/> 172.16.1.0/24</td> <td style="width: 50%;"><input checked="" type="checkbox"/> 192.168.10.0/24</td> </tr> <tr> <td><input checked="" type="checkbox"/> 172.16.2.0/24</td> <td><input checked="" type="checkbox"/> 10.10.0.1/32</td> </tr> <tr> <td><input checked="" type="checkbox"/> 172.16.3.11/32</td> <td><input checked="" type="checkbox"/> 192.168.11.101/32</td> </tr> <tr> <td><input checked="" type="checkbox"/> 172.16.3.21/32</td> <td><input checked="" type="checkbox"/> 192.168.11.201/32</td> </tr> <tr> <td><input type="checkbox"/> Local Network</td> <td><input checked="" type="checkbox"/> NAT Network</td> </tr> </table>			<input checked="" type="checkbox"/> 172.16.1.0/24	<input checked="" type="checkbox"/> 192.168.10.0/24	<input checked="" type="checkbox"/> 172.16.2.0/24	<input checked="" type="checkbox"/> 10.10.0.1/32	<input checked="" type="checkbox"/> 172.16.3.11/32	<input checked="" type="checkbox"/> 192.168.11.101/32	<input checked="" type="checkbox"/> 172.16.3.21/32	<input checked="" type="checkbox"/> 192.168.11.201/32	<input type="checkbox"/> Local Network	<input checked="" type="checkbox"/> NAT Network
<input checked="" type="checkbox"/> 172.16.1.0/24	<input checked="" type="checkbox"/> 192.168.10.0/24												
<input checked="" type="checkbox"/> 172.16.2.0/24	<input checked="" type="checkbox"/> 10.10.0.1/32												
<input checked="" type="checkbox"/> 172.16.3.11/32	<input checked="" type="checkbox"/> 192.168.11.101/32												
<input checked="" type="checkbox"/> 172.16.3.21/32	<input checked="" type="checkbox"/> 192.168.11.201/32												
<input type="checkbox"/> Local Network	<input checked="" type="checkbox"/> NAT Network												
Remote Networks	Network	Subnet Mask											
	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 checked="" type="checkbox"/> Hide Characters												
Local ID	<input type="text"/>												
Remote ID	<input type="text"/>												
Phase 1 (IKE) Proposal	1	AES-256 & SHA1											
	2	-----											
Phase 1 DH Group	<input checked="" type="checkbox"/> Group 2: MODP 1024 <input type="checkbox"/> Group 5: MODP 1536												
Phase 1 SA Lifetime	3600	seconds	Default										
Phase 2 (ESP) Proposal	1	AES-256 & SHA1											
	2	-----											
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	28800	seconds	Default										

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

Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared 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**.

10.4 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 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.



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

To create a custom rule, click **Add Rule** at the bottom of the table. Note that some Pepwave routers display this button at **Advanced>PepVPN>PepVPN Outbound Custom Rules**.

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 <input type="button" value=":: Protocol Selection Tool ::"/>
Algorithm	? Weighted Balance
Load Distribution Weight	? <ul style="list-style-type: none"> WAN 1 10 WAN 2 10 Wi-Fi WAN 10 Cellular 1 10 Cellular 2 10 USB 10
Terminate Sessions on Link Recovery	? <input type="checkbox"/> Enable

Save **Cancel**

New Custom Rule Settings

Service Name	This setting specifies the name of the outbound traffic rule.						
Enable	This setting specifies whether the outbound traffic rule takes effect. When Enable is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When Enable is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule.						
	Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.						
Source	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.						
Destination	<p>This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.</p> <table border="1"> <tr> <td>Destination</td> <td><input type="button" value="Domain Name"/></td> </tr> <tr> <td>Protocol</td> <td> ? Any IP Address IP Network Domain Name </td> </tr> <tr> <td>Algorithm</td> <td> ? </td> </tr> </table> <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 (<i>*</i>) 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</p>	Destination	<input type="button" value="Domain Name"/>	Protocol	? Any IP Address IP Network Domain Name	Algorithm	?
Destination	<input type="button" value="Domain Name"/>						
Protocol	? Any IP Address IP Network Domain Name						
Algorithm	?						

	<p>not supported.</p> <p>NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.</p>
Protocol and Port	This setting specifies the IP protocol and port of traffic that matches this rule.
Algorithm	<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 <p>For a full explanation of each Algorithmn, please see the following article: https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithmns-work/8059</p>
Terminate Sessions on Link Recovery	<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>

10.5 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.

10.5.1 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:

Inbound Server

Server Name	myserver
IP Address	192.168.1.123

Save Cancel

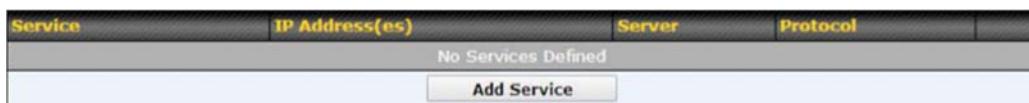
Enter a valid server name and its corresponding LAN IP address. Upon clicking **Save** after entering required information, the following screen appears.



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

10.5.2 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:

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No										
Service Name	Web										
IP Protocol	<input style="width: 40px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px; margin-right: 10px;" type="button" value="TCP"/> :: Protocol Selection Tool ::										
Port	<input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px; margin-right: 10px;" type="button" value="Single Port"/> Service Port: 80										
Inbound IP Address(es) (Require at least one IP address)	Connection / IP Address(es) <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">All</th> <th style="text-align: right; padding: 2px;">Clear</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"><input checked="" type="checkbox"/> WAN 1</td> <td style="text-align: right; padding: 2px;"><input checked="" type="checkbox"/> 10.88.3.184 (Interface IP)</td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/> WAN 2</td> <td style="text-align: right; padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/> WAN 3</td> <td style="text-align: right; padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/> Mobile Internet</td> <td style="text-align: right; padding: 2px;"></td> </tr> </tbody> </table>	All	Clear	<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.184 (Interface IP)	<input type="checkbox"/> WAN 2		<input type="checkbox"/> WAN 3		<input type="checkbox"/> Mobile Internet	
All	Clear										
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.184 (Interface IP)										
<input type="checkbox"/> WAN 2											
<input type="checkbox"/> WAN 3											
<input type="checkbox"/> Mobile Internet											
Included Server(s) (Require at least one IP address)	Server <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;"><input checked="" type="checkbox"/> myserver (192.168.1.123)</td> <td style="text-align: right; padding: 2px;">Weight 10</td> </tr> </table>	<input checked="" type="checkbox"/> myserver (192.168.1.123)	Weight 10								
<input checked="" type="checkbox"/> myserver (192.168.1.123)	Weight 10										

Services Settings						
Enable	This setting specifies whether the inbound service rule takes effect. When Yes is selected, the inbound service rule takes effect. If the inbound traffic matches the specified IP protocol and port, action will be taken by the Peplink Balance based on the other parameters of the rule. When No is selected, the inbound service rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.					
Service Name	This setting identifies the service to the system administrator. Only alphanumeric and the underscore “_” characters are valid.					
IP Protocol	The IP Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Inbound traffic that matches the specified IP Protocol and Port(s) will be forwarded to the LAN hosts specified by the Servers setting. Upon choosing a protocol, the Protocol Selection Tool drop-down menu can be used to automatically the port information of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and the port number will remain manually modifiable.					
Port	The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: Any Port, Single Port, Port Range, Port Map, and Range Mapping <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">Port</td> <td style="width: 10%; text-align: center; padding: 2px;"><input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px;" type="button" value="Any Port"/></td> </tr> </table> 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. <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">Port</td> <td style="width: 10%; text-align: center; padding: 2px;"><input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px;" type="button" value="Single Port"/></td> <td style="width: 10%; text-align: center; padding: 2px;">Service Port: 80</td> </tr> </table> 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.	Port	<input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px;" type="button" value="Any Port"/>	Port	<input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px;" type="button" value="Single Port"/>	Service Port: 80
Port	<input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px;" type="button" value="Any Port"/>					
Port	<input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px 5px;" type="button" value="Single Port"/>	Service Port: 80				

For example, if **IP Protocol** is set to **TCP**, **Port** is set to **Single Port**, and **Service Port** is set to 80, then TCP traffic received on Port 80 will be forwarded to the configured servers via port 80.

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

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

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

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

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

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

Inbound IP Address(es)

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

Included Server(s)

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

Example:

With the following weight settings on a Peplink Balance:

- demo_server_1: 10
- demo_server_2: 5

The total weight is $15 = (10 + 5)$

Matching traffic distributed to demo_server_1: $67\% = (10 / 15) \times 100\%$

Matching traffic distributed to demo_server_2: $33\% = (5 / 15) \times 100\%$

UPnP / NAT-PMP Settings

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

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

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

UPnP / NAT-PMP Settings	
UPnP	<input checked="" type="checkbox"/> Enable
NAT-PMP	<input checked="" type="checkbox"/> Enable
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**.

10.5.3 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, WAN 6, WAN 7, WAN 8, WAN 9, WAN 10, WAN 11, WAN 12, Mobile Internet		
Domain Names		
Domain Name	These is currently no DNS domains.	
New Domain Name		
Reverse Lookup Zones		
Zone Name	There is currently no Reverse Lookup Zones.	
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	<p>When this function is enabled, the system will check to see if an incoming DNS client is within any WAN's ISP subnet. Only the matched WAN(s)'s IP addresses will be returned. Note that this feature is available only when a subnet database has been defined.</p>
Default SOA / NS	<p>Click the button to define a default SOA / NS record for all domain names.</p> <p>When defining a default SOA record, Name Server IP Address is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain.</p> <p>For defining default NS records, the host <i>[domain]</i> indicates that this record is for the domain name itself without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the Host field left empty. When the entered name server is a fully qualified domain name (FQDN), the IP Address field will be disabled.</p>
Default Connection Priority	<p>Default Connection Priority defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the Connection Priority set to Default. Please refer to Section 17.3.9 for details.</p> <p>The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable.</p> <p>To specify the primary and backup connections, click the button that corresponds to Default Connection Priority. A selection screen will appear.</p> <p>Each WAN connection is associated with a priority number. Click Save to save the settings when configuration is complete.</p>
Domain name	<p>This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its "NS", "MX" and "TXT" records, and its sub-domains' "A" and "CNAME" records. Add a new record by clicking the New Domain Name button. Click on a domain name to edit. Press the red X to remove a domain name.</p>

New Domain Name

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

SOA Record			
Use Default SOA and NS Records			
<input type="checkbox"/>			
NS Records			
Host	Name Server	TTL (sec)	<input type="button" value="New NS Records"/>
<i>There is currently no NS records.</i>			
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)	<input type="button" value="New CNAME Record"/>
<i>There is currently no CNAME records.</i>			
A Records			
Host	Included IP Address(es)	TTL (sec)	<input type="button" value="New A Record"/>
<i>There is currently no A records.</i>			
TXT Records			
Host	TXT Value	TTL (sec)	<input type="button" value="New TXT Record"/>
<i>There is currently no default TXT records.</i>			
SRV Records			
Service	Priority	Weight	Target
<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.

10.5.3.1 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
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

SOA Record

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

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

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

Default values are set for SOA and NS records,

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

is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically. If it is left blank, the A record for the name server must be created manually.

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

10.5.3.2 NS Records

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

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

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

10.5.3.3 MX Records

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

MX Records			
Host	Mail Server	TTL (sec)	
<input type="text"/>	<input type="text"/>	3600	<input type="button" value="+"/>
<input type="button" value="Save"/> <input type="button" value="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 priority. After finishing adding MX records, click the **Save** button.

10.5.3.4 CNAME Records

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

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

10.5.3.5 A Records

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

A Record

Host	www
TTL (sec)	3600
Priority	<input checked="" type="radio"/> Default <input type="radio"/> Custom
Included IP Address(es)	
<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input type="checkbox"/> WAN 6 <input type="checkbox"/> WAN 7 <input type="checkbox"/> WAN 8 <input type="checkbox"/> WAN 9 <input type="checkbox"/> WAN 10 <input type="checkbox"/> WAN 11 <input type="checkbox"/> WAN 12 <input type="checkbox"/> Mobile Internet <input type="checkbox"/> Custom IP Address	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

10.5.3.6 PTR Records

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

10.5.3.7 TXT Records

This table shows the TXT record of the domain name.

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

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.

10.5.3.8 SRV Records

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

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

- **Service:** The symbolic name of the desired service.
- **Priority:** Indicates the priority of the target; the smaller the value, the higher the priority.

- **Weight:** A relative weight for records with the same priority.
- **Target:** The canonical hostname of the machine providing the service.
- **Port:** Enter the TCP or UDP port number on which the service is to be found.

Reverse Lookup Zones

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



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

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

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

- Create a reverse lookup zone that corresponds to the subnet network address of the host.
In the reverse lookup zone, add a pointer (PTR) resource record that maps the host IP address to the host name.
- Click the **New Reverse Lookup Zone** button and enter a reverse lookup zone name. If you are delegated the subnet 11.22.33.0/24, the **Zone Name** should be 33.22.11.in-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!		
New NS Records		
CNAME Records		
Host	Points To	TTL (sec)
There is currently no CNAME records.		
New CNAME Record		
PTR Records		
Host IP Number	Points To	TTL (sec)
There is currently no PTR records.		
New PTR Record		

[Close](#)

SOA Record

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

SOA Record

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

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

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

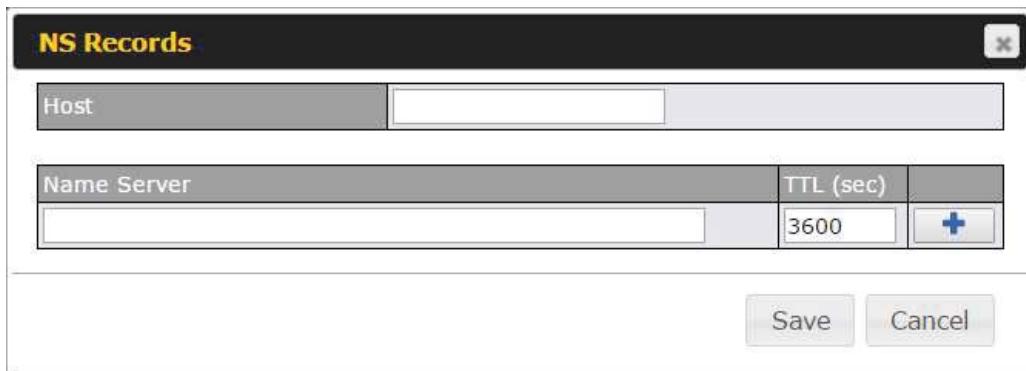
For example:

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

"ns2.mydomain.com."

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

NS Records

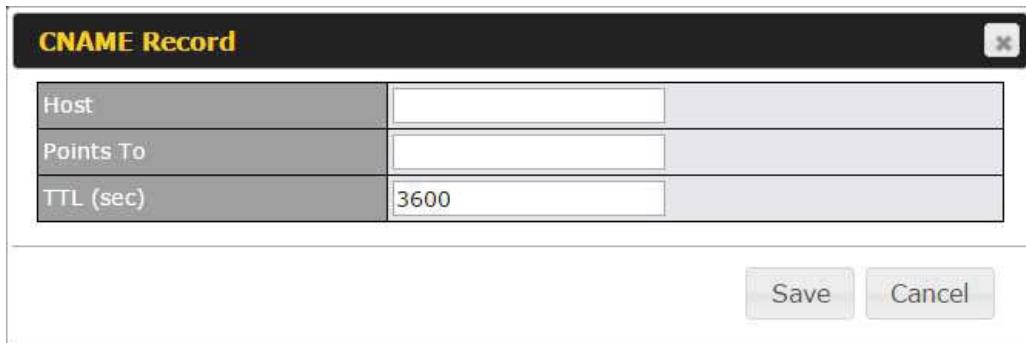


The screenshot shows a dialog box titled "NS Records". It contains two main sections: "Host" and "Name Server". The "Host" section has a single input field. The "Name Server" section has two input fields: "Name Server" and "TTL (sec)". A "Save" button and a "Cancel" button are located at the bottom right of the dialog.

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". It contains three input fields: "Host", "Points To", and "TTL (sec)". The "TTL (sec)" field is pre-filled with "3600". A "Save" button and a "Cancel" button are located at the bottom right of the dialog.

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"/>
TTL (sec)	<input type="text"/> 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-arp.a.addr, the **Host IP Number** should be 44.

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

DNS Record Import Wizard

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

DNS Record Import Wizard

DNS Record Import Wizard

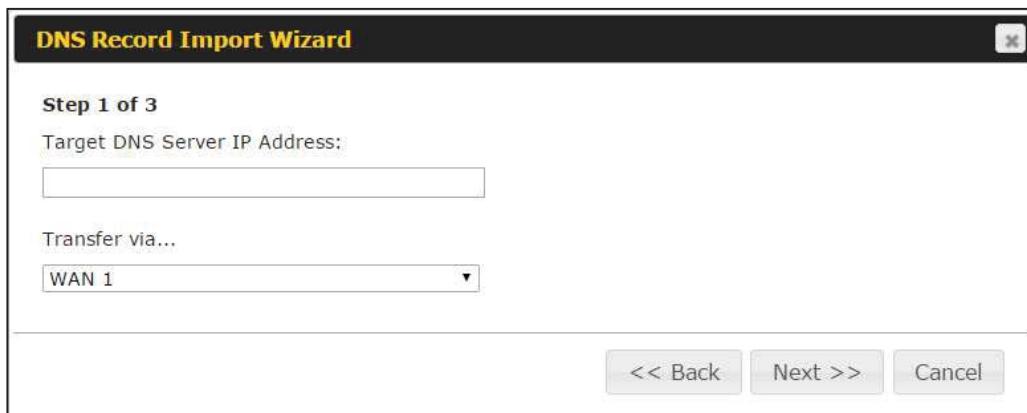
This wizard allows you to import DNS records from an existing DNS server via zone transfer.

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

To continue, click Next.

Next >> **Cancel**

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



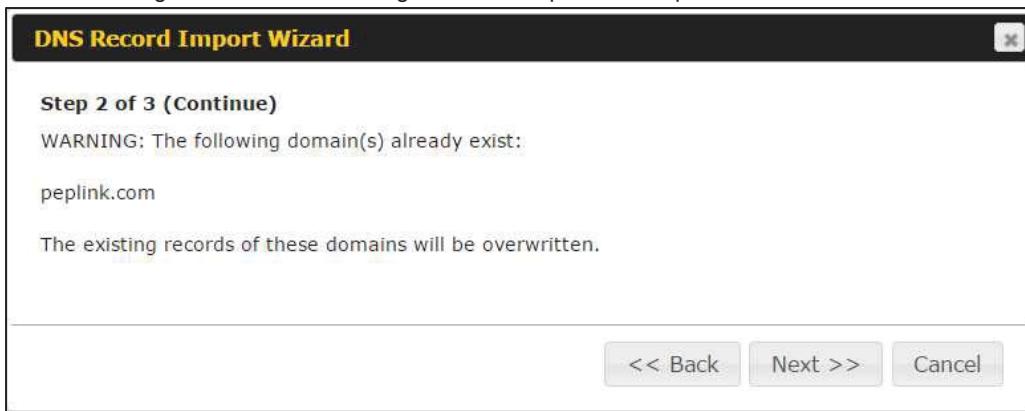
- In the **Target DNS Server IP Address** field, enter the IP address of the DNS server.
- In the **Transfer via...** field, choose the connection which you would like to transfer through.
- Select **Next >>** to continue.

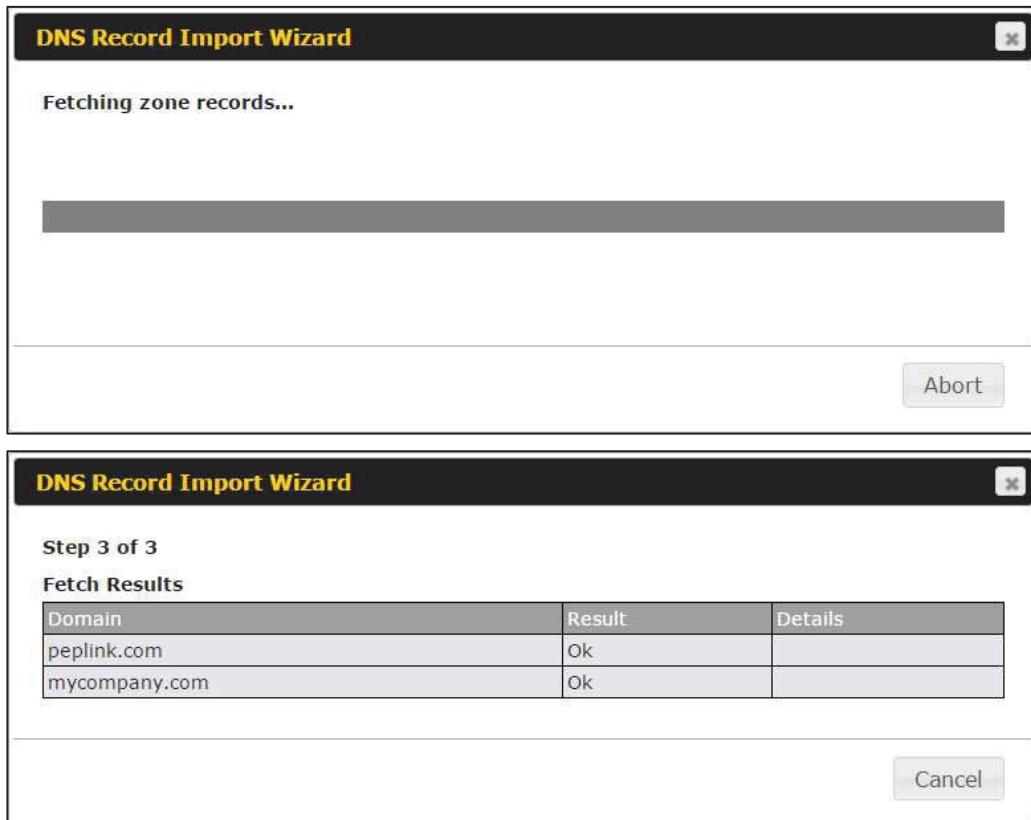


- In the blank space, enter the **Domain Names (Zones)** which you would like to assign the IP address entered in the previous step. Enter one domain name per line.
- Select **Next >>** to continue.

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.





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

10.6 NAT Mappings

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

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

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

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

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

NAT Mapping Settings

LAN Client(s)

NAT Mapping rules can be defined for a single LAN IP Address, an IP Range, or an IP Network.

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

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

Important Note

Inbound firewall rules override inbound mapping settings.

10.7 MediaFast

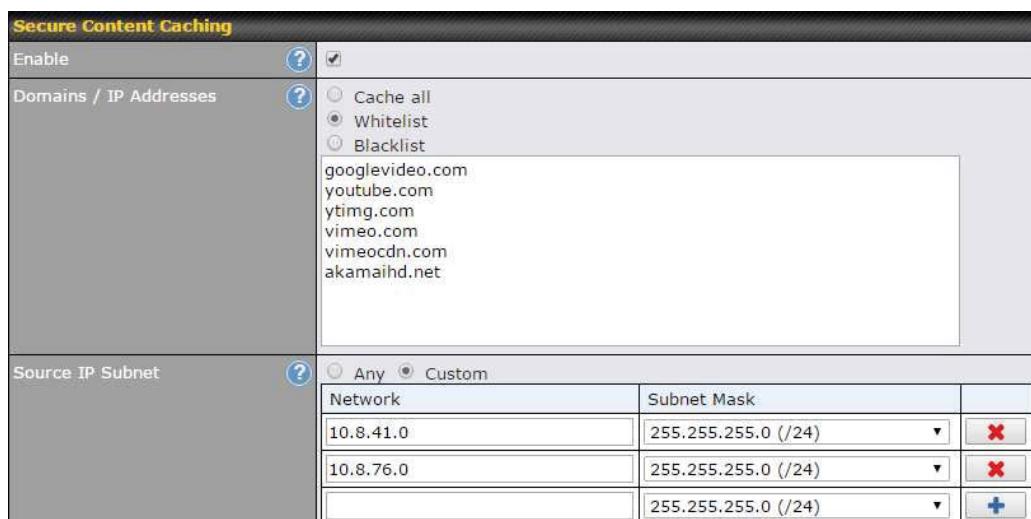
MediaFast settings can be configured by navigating to **Network > MediaFast**.

Setting Up MediaFast Content Caching

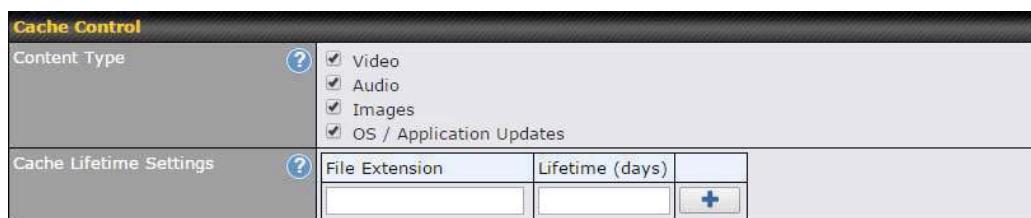
To access MediaFast content caching settings, select **Network > MediaFast**.



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).



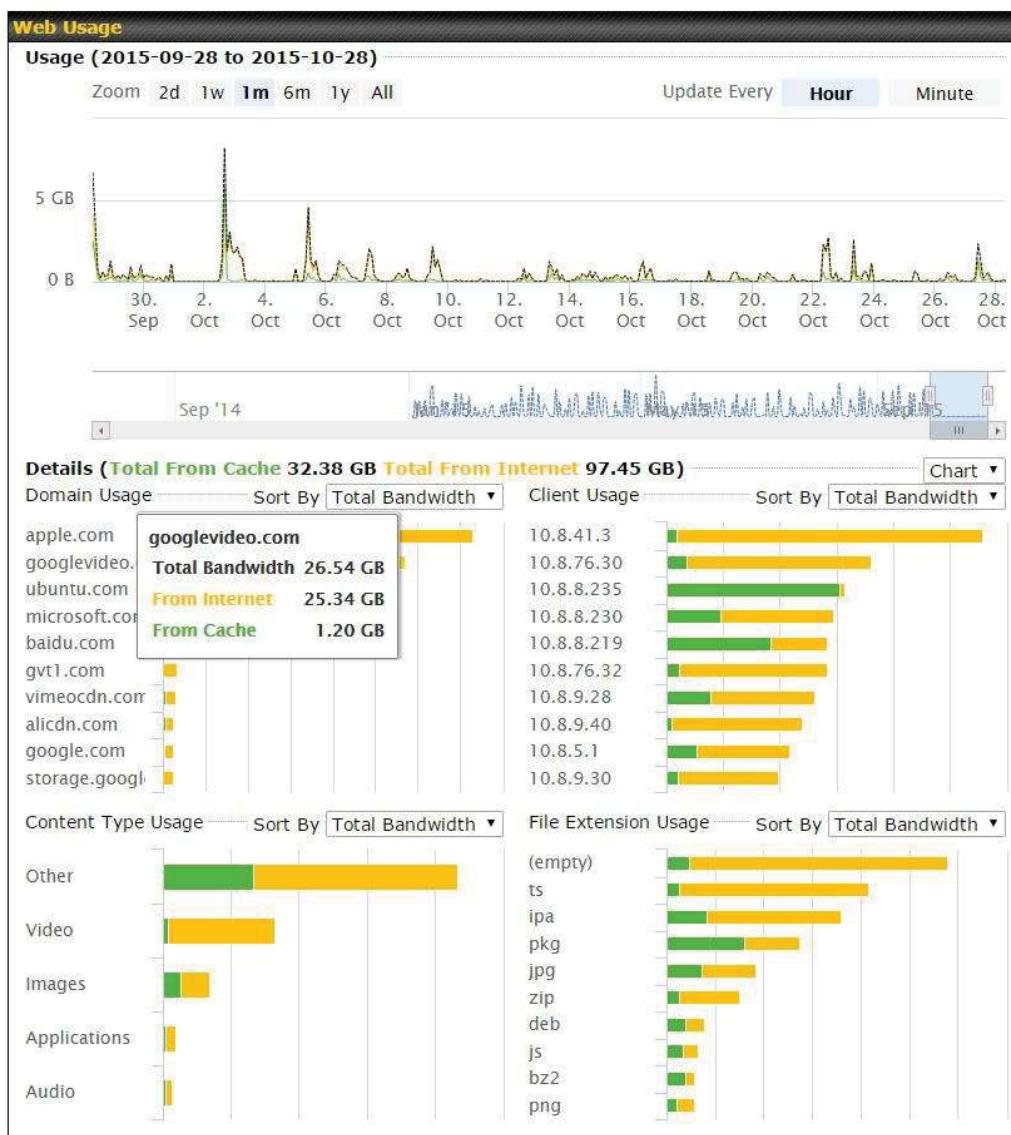
The **Secure Content Caching** menu operates identically to the **MediaFast** menu, except it is for secure contenting accessible through https://.



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**.



10.7.1 Prefetch Schedule

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

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

New Schedule

Tools

Clear Web Cache **Clear Statistics**

Prefetch Schedule Settings

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

MediaFast Schedule

Name (optional)	Cache Peplink Website
Active	<input checked="" type="checkbox"/>
URL	URL <input type="text" value="www.peplink.com"/> X <input type="text" value="www.peplink.com/knowledgebase"/> +
Depth	2 levels Default
Time Period	From 00:00 to 01:00
Repeat	Everyday

[Save & Apply Now](#) [Cancel](#)

Simply provide the requested information to create your schedule.

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

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

10.8 ContentHub

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

The screenshot shows a configuration window titled "ContentHub". It contains a single row with a "Enable" label and a checked checkbox. Below the row is a "Save" button.

Check the **Enable** box.

The screenshot shows a "Schedule" table with columns: Websites, Source, Next Update, Last Updated, Elapsed Time, Status, and Actions. A message "No Schedule" is displayed above the table. At the bottom center is a "New Website" button.

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

The screenshot shows a configuration window for a new website. It has two rows: "Active" with a checked checkbox, and "Type" with a radio button selected for "Website".

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

Selecting Website:

Domain/Path	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 Gbps (0: Unlimited)

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

Selecting Application:

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

Domain	Enter the domain your application is hosted at
Method	Enter the FTP server you will be downloading the content from. Enter your credentials under Username and Password .

Bandwidth Limit

This field determines the amount of bandwidth dedicated to this application.

10.9 MDM Settings

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

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

10.10 Captive Portal

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

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

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

	<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.
Allowed Networks	To whitelist a network, enter the domain name / IP address here and click  . To delete an existing network from the list of allowed networks, click the  button next to the listing.
Allowed Clients	To whitelist a client, enter the MAC address / IP address here and click  . To delete an existing client from the list of allowed clients, click the  button next to the listing.
Splash Page	Here, you can choose between using the Balance's built-in captive portal and redirecting clients to a URL you define.

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

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

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

Custom Landing Page

Fill in this field to redirect clients to an external URL.

10.11 QoS

10.11.1 User Groups

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

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

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

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

Subnet / IP Address		User Group
Add / Edit User Group		
Client	192.168.1.99	ager
Subnet / IP Address	IP Address ▾ 192.168.1.99	ager
Group	Manager ▾	ager
		Save Cancel

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.

10.11.2 Bandwidth Control

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

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

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

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

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

10.11.3 Application

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

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

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

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

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"/>		

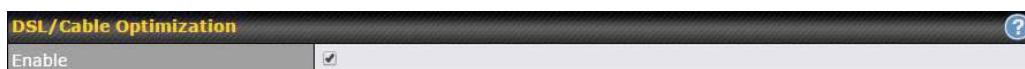
Category and **Application** availability will be different across different Peplink Balance models.

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.



10.12 Firewall

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

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

Outbound (LAN to WAN)

Inbound (WAN to LAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

10.12.1 Access Rules

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

Outbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
Default	Any	Any	Any	Allow	
Add Rule					

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

Add a New Outbound Firewall Rule

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

Save **Cancel**

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

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

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

Add a New Inbound Firewall Rule

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

Save **Cancel**

Inbound / Outbound Firewall Settings

Rule Name This setting specifies a name for the firewall rule.

	<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>Enable</p> <p>If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
	<p>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.) After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remains manually modifiable.</p>
Source IP & Port	<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>
Destination IP & Port	<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>