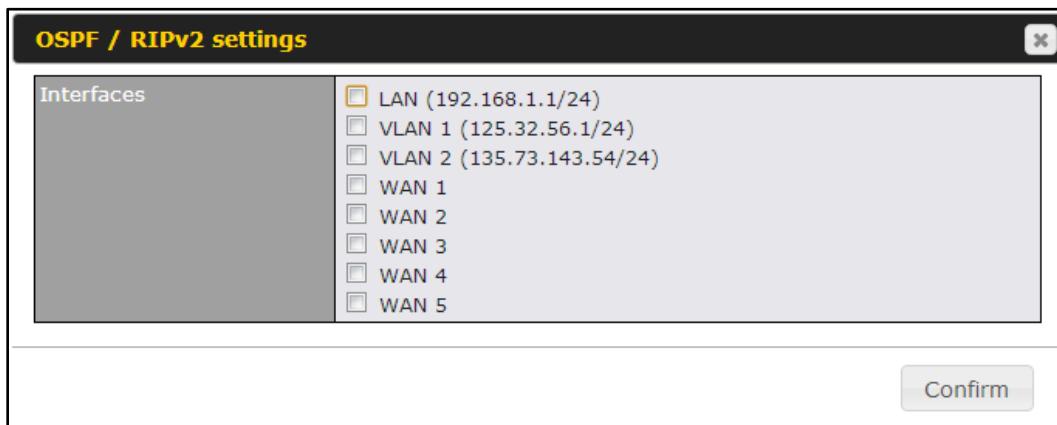


### OSPFv2 / RIPv2 Settings

<b>Area ID</b>	Determine the name of your Area ID to apply to this group. Machines linked to this group will send and receive related OSPFv2 packets, while unlinked machines will ignore it.
<b>Link Type</b>	Choose the network type that this area will use.
<b>Interfaces</b>	Determine which interfaces this area to use to listen to and deliver OSPFv2 packets



### RIPv2 Settings

<b>Interfaces</b>	Determine which interfaces this group to use to listen to and deliver RIPv2 packets.
-------------------	--

## 21 Miscellaneous Settings

The miscellaneous settings include configuration for High Availability, PPTP Server, Service Forwarding, and Service Passthrough.

### 21.1 High Availability

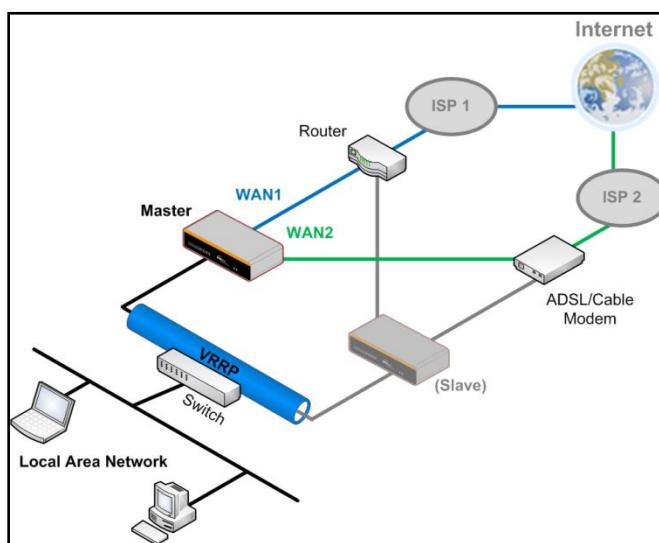
(Available on Peplink Balance 210+)

Peplink Balance supports High Availability (HA) configurations via an open standard Virtual Router Redundancy Protocol (VRRP, RFC 3768).

In an HA configuration, two same-model Peplink Balance units (e.g. a pair of Peplink Balance 210 units, or a pair of Peplink Balance 710 units) provide redundancy and failover in a master-slave arrangement. In the event that the Master Unit is down, the Slave Unit becomes active.

High Availability will be disabled automatically where there is a Drop-in connection configured on a LAN Bypass port.

The following diagram illustrates an HA configuration with two Peplink Balance 210 units, and two Internet connections:



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

An elaboration on the technical details of the implementation, by Peplink Balance, of Virtual Router Redundancy Protocol (VRRP, RFC 3768) is as follows:

- In an HA configuration, the two Peplink Balance units communicate with each other using VRRP over the LAN.
- The two Peplink Balance units broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the Master Peplink Balance unit is received in 3 seconds (or longer) since the last heartbeat signal, the Slave Peplink Balance unit becomes active.
- The Slave Peplink Balance unit initiates the WAN connections, and binds to a previously configured LAN IP address.
- At a subsequent point when the Master Peplink Balance unit recovers, it will once again become active.

You can configure High Availability at the following location: **Network>Misc. Settings > High Availability**.

Interface for Master Router

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

Interface for Slave Router

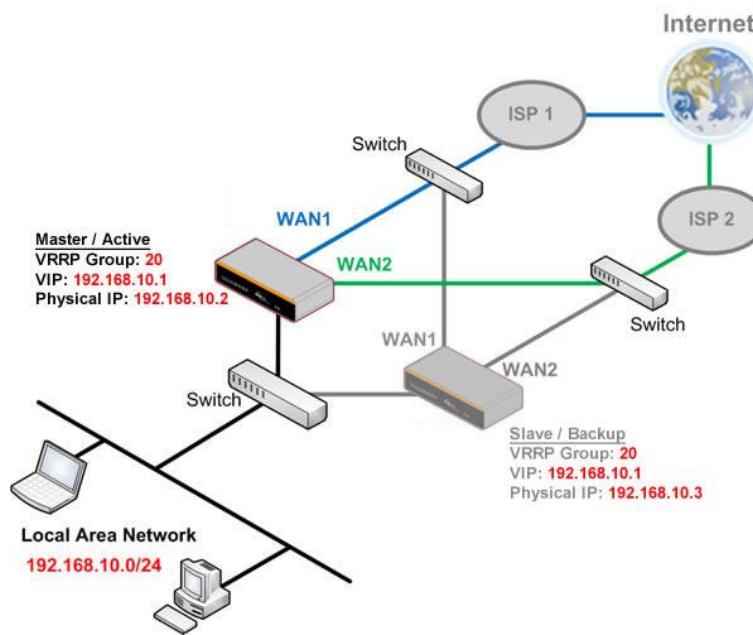
<b>High Availability</b>	
Enable	<input type="checkbox"/>
Group Number	5
Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/> Slave
Configuration Sync.	<input type="checkbox"/> Master Serial Number: 54BF-5WEY-E37Q
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

**High Availability**

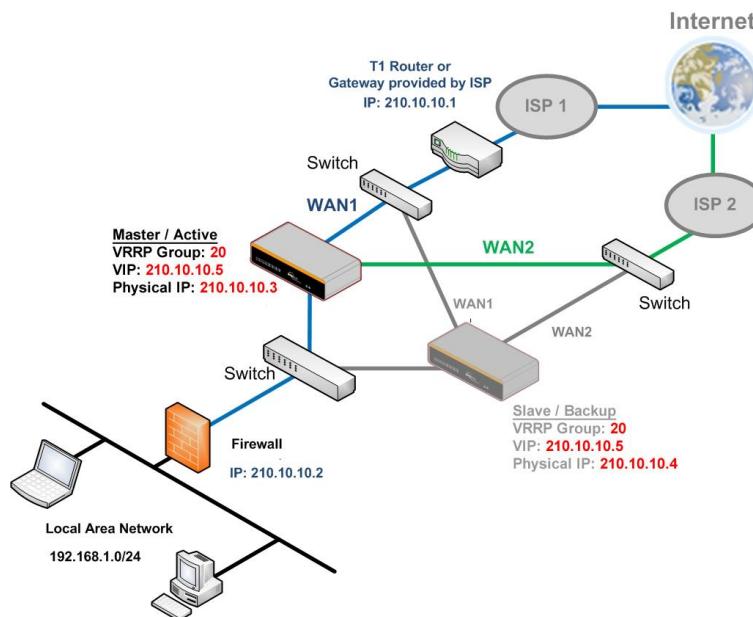
<b>High Availability</b>	
<b>Enable</b>	Checking this box specifies that the Peplink Balance unit is part of a High Availability configuration.
<b>Group Number</b>	This number identifies a pair of Peplink Balance units operating in a High Availability configuration. The two Peplink Balance units in the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

### Important Note

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

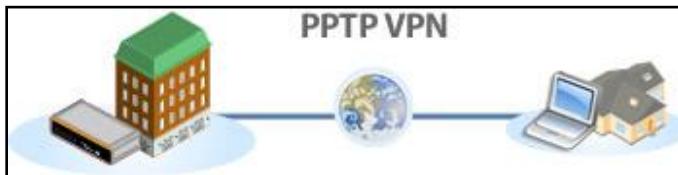


In Drop-in mode, no other configuration needs to be set.



Please note that the Drop-in WAN cannot be configured as a LAN Bypass port while it is configured for High Availability.

## 21.2 PPTP Server



Peplink Balance has a built-in PPTP Server, which enables remote computers to conveniently and securely access the local network.

PPTP server settings are located at: **Network > Misc. Settings > PPTP Server**

Simply check the box to enable the PPTP server function. All connected PPTP sessions are displayed on the Client List at **Status > Client List**. Please refer to section 25.3 for details.

<b>PPTP Server</b>	
Enable	<input checked="" type="checkbox"/>
Listen On	<input type="checkbox"/> <b>Connection / IP Address(es)</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> WAN1      <input type="checkbox"/> 123.123.123.1 (Interface IP)</li> <li><input type="checkbox"/> WAN2</li> <li><input type="checkbox"/> WAN3</li> <li><input type="checkbox"/> Mobile Internet</li> </ul>
Authentication	<input type="checkbox"/> Local User Accounts
User Accounts *	<input type="text"/> peplink <div style="float: right;"><input type="button" value="X"/> <input type="button" value="Add"/></div>

\* Required

<b>PPTP Server Setting</b>	
<b>Listen On</b>	<p>This setting is for specifying the WAN connection(s) and IP address(es) that the PPTP server should listen on.</p> <p><b>(This option is only applicable on Peplink Balance 305 and 380+.)</b></p> <p>This setting is for specifying the user database source for PPTP authentication. Three sources can be selected: <b>Local User Accounts</b>, <b>LDAP Server</b>, <b>RADIUS Server</b>.</p> <p><b>Local User Accounts</b> - User accounts are stored in the Peplink Balance locally. You can add/modify/delete accounts in the User Accounts table below.</p> <p><b>LDAP Server</b> - Authenticate with an external LDAP server. Tested with OpenLDAP server where passwords are NTLM hashed. Active Directory is not supported. (You can choose to use RADIUS to authenticate with a Windows Server.)</p> <p><b>RADIUS Server</b> - Authenticate with an external RADIUS server. Tested with Microsoft Windows Internet Authentication Service, and FreeRADIUS servers where passwords are NTLM hashed or in plain text.</p>
<b>Authentication</b>	
<b>User Accounts</b>	<p>This setting allows you to define the PPTP User Accounts <b>for authentication via Local User Accounts</b>. Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click the button  to delete the account in its corresponding row.</p>

### Important Note

PPTP server will be disabled automatically if the Balance is deployed in Drop-in mode.

## 21.3 Certificate Manager

Certificate Manager			
VPN Certificate	<a href="#">?</a>	No Certificate	<a href="#">Assign</a>
Web Admin SSL Certificate	<a href="#">?</a>	-----BEGIN CERTIFICATE----- MIIC2jCCAkOgAwIBAgIBADANBgkqhkiG9wOBAQUFADBkMQs...	<a href="#">Re-assign</a> <a href="#">more details</a>

This section allows you to assign certificates for Local VPN and Web Admin SSL. The local keys will not be transferred to another device by any means.

## 21.4 Service Forwarding

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

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

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

### 21.4.1 SMTP Forwarding

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

SMTP Forwarding Setup			
SMTP Forwarding	<input checked="" type="checkbox"/> Enable		
Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN1	<input type="checkbox"/>		
WAN2	<input checked="" type="checkbox"/>	22.2.2.2	25
WAN3	<input checked="" type="checkbox"/>	33.3.3.2	25
Mobile Internet	<input type="checkbox"/>		

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

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

### Note

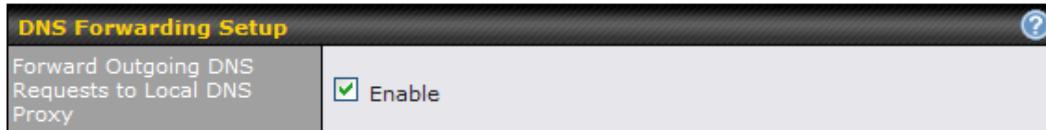
If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in Outbound Policy (see Section 14.1).

#### 21.4.2 Web Proxy Forwarding

Web Proxy Forwarding Setup			
Web Proxy Forwarding	<input checked="" type="checkbox"/> Enable		
Web Proxy Interception Settings			
Proxy Server	IP Address <input type="text" value="123.123.11.22"/> Port <input type="text" value="8080"/>	(Current settings in users' browser)	
Connection	Enable Forwarding?	Proxy Server IP Address : Port	
WAN1	<input type="checkbox"/>		:
WAN2	<input checked="" type="checkbox"/>	22.2.2.2	: 8765
WAN3	<input checked="" type="checkbox"/>	33.3.3.2	: 8080
Mobile Internet	<input type="checkbox"/>		:

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

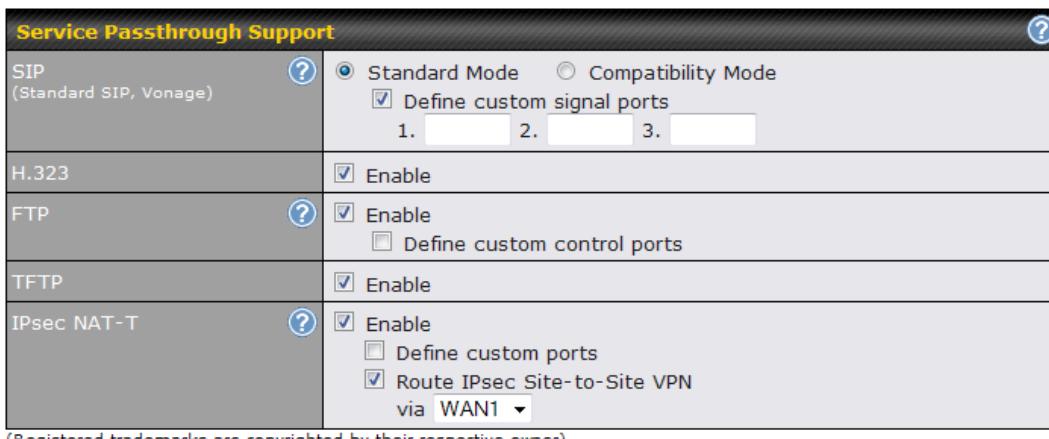
## 21.4.3 DNS Forwarding



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

## Service Passthrough

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



(Registered trademarks are copyrighted by their respective owner)

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

Service Passthrough Support	
<b>SIP</b>	Session Initiation Protocol, aka SIP, is a voice-over-IP protocol. The Peplink Balance can act as a SIP Application Layer Gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in NAT mode. Such passthrough support is always enabled and there are two modes for selection: <b>Standard Mode</b> and <b>Compatibility Mode</b>  If your SIP server's signal port number is non-standard, you can check the box <b>Define custom signal ports</b> and input the port numbers to the text boxes.
<b>H.323</b>	With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and passthrough the Balance.
<b>FTP</b>	FTP sessions consist of two TCP connections; one for control and one for data. In multi-WAN situation, they have to be routed to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Peplink Balance monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN.  If you have an FTP server listening on a port number other than 21, you can check the box <b>Define custom control ports</b> and enter the port numbers to the text boxes.

<b>TFTP</b>	The Peplink Balance monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select <b>Enable</b> if you want to enable the TFTP Passthrough support.
<b>IPsec NAT-T</b>	This field is for enabling the support of IPsec NAT-T Passthrough. UDP ports 500, 4500 and 10000 are monitored by default.  You may add more custom data ports that your IPsec system uses by checking the box <b>Define custom ports</b> . If the VPN contains IPsec Site-to-Site VPN traffic, you have to check the box <b>Route IPsec Site-to-Site VPN</b> and choose the WAN connection to route the traffic to.

## 22 AP

The AP Controller acts as a centralized controller of Pepwave AP devices. With this feature, users will be able to customize and manage multiple AP one a single Peplink Balance Interface.

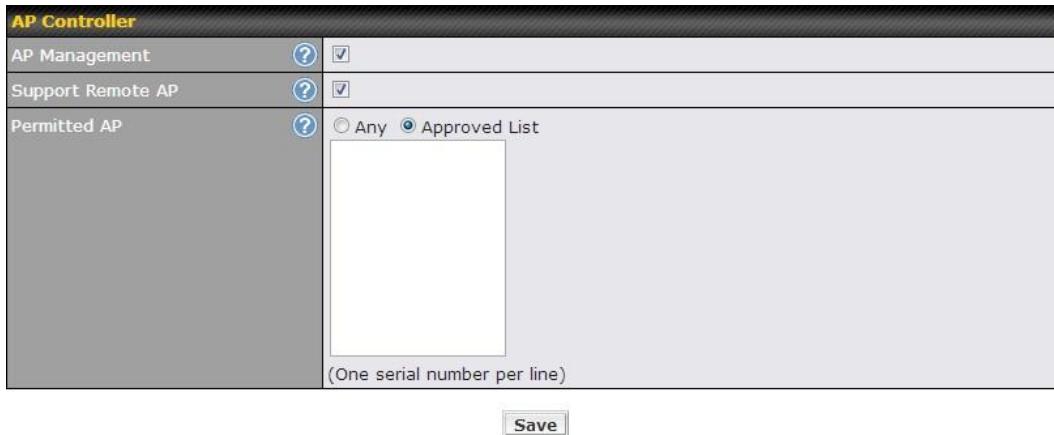
To configure, navigate to the **AP** tab and the following options will be shown.

### Special Note

Each Balance router can control a limited number of routers without cost. To manage more, a Full Edition license is required. Please contact our Authorized Reseller or Peplink Sales Team to obtain more information and price details.

### 22.1 AP Controller

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



AP Controller	
AP Management	<input type="checkbox"/>
Support Remote AP	<input type="checkbox"/>
Permitted AP	<input type="radio"/> Any <input checked="" type="radio"/> Approved List  (One serial number per line)

### Access Point Controller

#### AP Management

The AP Controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP Controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, **CAPWAP Access Controller addresses** (field 138), will be added to the DHCP server. A local DNS record, **AP Controller**, will add to the local DNS proxy.

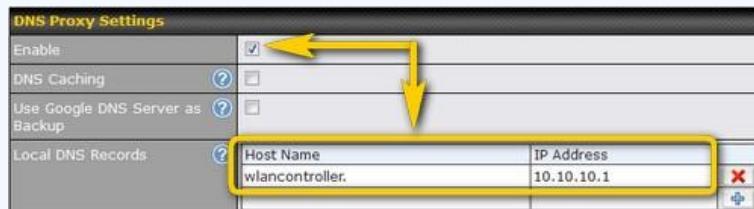
The AP Controller supports remote management of Pepwave APs. When this option is enabled, the AP Controller will wait for management connections originating from remote APs over the WAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443.

#### Support Remote AP

The DHCP server and/or local DNS server of the remote AP's network should be configured in the **DNS Proxy Settings menu** under **Network > LAN**. The procedure is as follows:

1. Define an extended DHCP option, **CAPWAP Access Controller addresses** (field 138), in the DHCP server, where the values are the AP Controller's public IP addresses; and/or

2. Create a local DNS record for **AP Controller** with a value corresponding to the AP Controller's public IP address.



#### Permitted AP

Access points to manage can be specified here. If **Any** is selected, the AP Controller will manage any AP that reports to it. If **Access points listed below:** is selected, only APs with a serial number listed in the provided text box will be managed.

## 22.2 Wireless SSID

Wireless network settings, including the name of the network (SSID) and security policy, can be defined and managed in this section. After defining a wireless network, users can choose the network in **AP Profiles**.

SSID	Security Policy	Used by	
Peplink WLAN FF03	Open (No Encryption)	Default	X
Manager	WPA/WPA2 - Personal	(None)	X
Staff	WPA/WPA2 - Personal	(None)	X
Customer	Open (No Encryption)	Coffee Shop	X
<b>New Network</b>			

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

SSID Settings	
SSID	<input type="text"/>
VLAN ID	0 (0: Untagged) <input type="checkbox"/> Use VLAN Pool
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Multicast Filter	<input type="checkbox"/>
Multicast Rate	<input type="button" value="MCS8/MCS0/6M"/>
IGMP Snooping	<input type="checkbox"/>
DHCP Option 82	<input type="checkbox"/>
Network Priority (QoS)	<input type="button" value="Gold"/>
Layer 2 Isolation	<input type="checkbox"/>
Band Steering	<input type="button" value="Disable"/>

SSID Settings	
<b>SSID</b>	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
<b>VLAN ID</b>	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is <b>0</b> , which means VLAN tagging is disabled (instead of tagged with zero).
<b>Broadcast SSID</b>	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. <b>Broadcast SSID</b> is <b>enabled</b> by default.
<b>Data Rate<sup>A</sup></b>	Select <b>Auto</b> to allow the Peplink Balance to set the data rate automatically or select <b>Fixed</b> and choose a rate from the displayed drop-down menu.
<b>Multicast Filter<sup>A</sup></b>	This setting enables the filtering of multicast network traffic to the wireless SSID.
<b>Multicast Rate<sup>A</sup></b>	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected <b>Protocol</b> and <b>Channel Bonding</b> settings will affect the rate options and values available here.
<b>IGMP Snooping<sup>A</sup></b>	To allow the Peplink Balance to listen to Internet Group Management Protocol (IGMP) network traffic, select this option.
<b>DHCP Option 82<sup>A</sup></b>	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
<b>Network Priority (QoS)<sup>A</sup></b>	Select from <b>Gold</b> , <b>Silver</b> , and <b>Bronze</b> to control the QoS priority of this wireless network's traffic.
<b>Layer 2 Isolation<sup>A</sup></b>	<b>Layer 2</b> refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is <b>disabled</b> .
<b>Band Steering<sup>A</sup></b>	Band steering allows the Peplink Balance to steer AP clients from the 2.4 GHz band to the 5GHz band for better usage of bandwidth. To make steering mandatory, select <b>Enforce</b> . To cause the Peplink Balance to preferentially choose steering, select <b>Prefer</b> . The default for this setting is <b>Disable</b> .

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

Security Settings	
Security Policy	Open (No Encryption)

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

Access Control	
Restricted Mode	<input type="text" value="None"/> <input type="button" value="▼"/>

### Access Control

The settings allow administrator to control access using Mac address filtering. Available options are **None**, **Deny all except listed**, **Accept all except listed**, and **RADIUS MAC Authentication**.

When **WPA/WPA2 - Enterprise** is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the **Shared Key** option should be disabled. When using this method, select the appropriate version using the **V1/V2** controls. The security level of this method is known to be very high.

#### Restricted Mode

When **WPA/WPA2- Personal** is configured, a **Shared Key** is used for data encryption and authentication. When using this configuration, the **Shared Key** option should be enabled. Key length must be between eight and 63 characters (inclusive). The security level of this method is known to be high.

The configuration of **static WEP** parameters enables pre-shared WEP key encryption. Authentication is not supported by this method. The security level of this method is known to be weak.

<b>MAC Address List</b>	Connection coming from the MAC Addresses in this list will be either denied or accepted based the option selected in the previous field.
-------------------------	--

RADIUS Server Settings	Primary Server	Secondary Server
Host	<input type="text"/>	<input type="text"/>
Secret	<input type="text"/>	<input type="text"/>
Authentication Port	1812 <input type="button" value="Default"/>	1812 <input type="button" value="Default"/>
Accounting Port	1813 <input type="button" value="Default"/>	1813 <input type="button" value="Default"/>

### RADIUS Server Settings

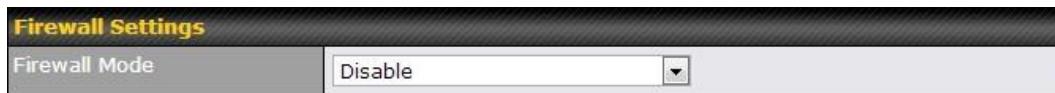
<b>Host</b>	Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.
<b>Secret</b>	Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
<b>Authentication Port</b>	In field, enter the UDP authentication port(s)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

Guest Protect			
Block All Private IP			<input type="checkbox"/>
Custom Subnet	Network	Subnet Mask	<input type="button" value="+"/>
	<input type="text"/>	255.255.255.0 (/24)	<input type="button" value="X"/>
Block Exception	Network	Subnet Mask	<input type="button" value="+"/>
	<input type="text"/>	255.255.255.0 (/24)	<input type="button" value="X"/>
Block PepVPN	<input type="checkbox"/>		

Guest Protect	
<b>Block All Private IP</b>	Check this box to deny all connection attempts by private IP addresses.
<b>Custom Subnet</b>	To create a custom subnet for guest access, enter the IP address and choose a subnet mask from the drop-down menu. To add the new subnet, click the  button. To delete a custom subnet, click the  button.
<b>Block Exception</b>	To block access from a particular subnet, enter the IP address and choose a subnet mask from the drop-down menu. To add the new subnet, click the  button. To delete a blocked subnet, click the  button.
<b>Block PepVPN</b>	To block PepVPN access, check this box.

Bandwidth Management	
Upstream Limit	<input type="text"/> 0 kbps (0: Unlimited)
Downstream Limit	<input type="text"/> 0 kbps (0: Unlimited)
Client Upstream Limit	<input type="text"/> 0 kbps (0: Unlimited)
Client Downstream Limit	<input type="text"/> 0 kbps (0: Unlimited)
Max number of Clients	<input type="text"/> 0 (0: Unlimited)

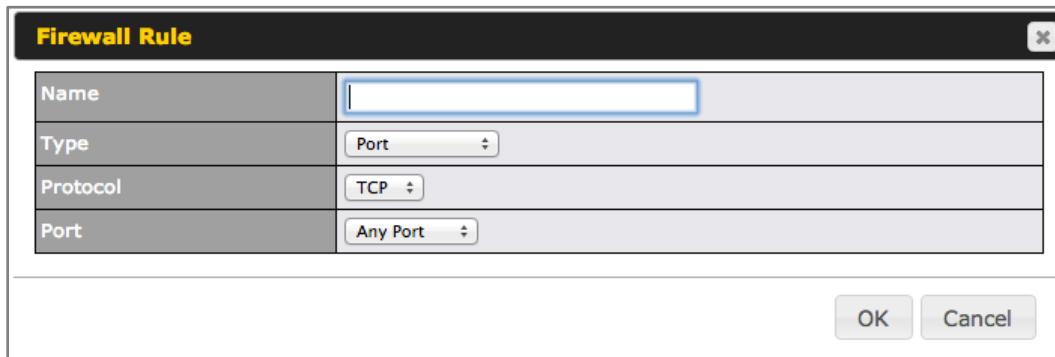
Bandwidth Management	
<b>Upstream Limit</b>	Enter a value in kbps to limit the wireless network's upstream bandwidth. Enter <b>0</b> to allow unlimited upstream bandwidth.
<b>Downstream Limit</b>	Enter a value in kbps to limit the wireless network's downstream bandwidth. Enter <b>0</b> to allow unlimited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



**Firewall Settings**

**Firewall Mode**

Choose Flexible – **Allow all except...** or **Lockdown – Block all except...** to turn on the firewall, then create rules for the firewall exceptions by click the **New Rule** button. See the discussion below for details on creating a firewall rule. To delete a rule, click the associated  button. To turn off the firewall, select **Disable**.



**Firewall Rule**

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

## 22.3 Profiles

AP profiles assigned to each Pepwave AP device can be configured at **AP > Profiles**

Name	Used by	Action
1. Default	(None)	<input type="button" value="Clone"/> <input type="button" value="Delete"/>
2. test	(None)	<input type="button" value="Clone"/> <input type="button" value="Delete"/>
<input type="button" value="New AP Profile"/>		

Each AP is associated with one AP Profile. By default, all devices are associated with the first (Default) profile. The Default profile cannot be removed.

You can define an AP profile by clicking the **New AP Profile** button. Click the **Clone** button of an existing profile to create a new profile based on it. To change the settings of an existing profile, click the profile name and the following screen will be shown.

**AP Settings**

AP Profile Name	<input type="text"/>	
SSID	<input type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz <input type="checkbox"/> <input type="checkbox"/> Peplink WLAN EFD1	
Operating Country	<input type="text" value="United States"/>	
Preferred Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz	
5 GHz Protocol	802.11na	
5 GHz Channel Bonding	<input type="text" value="20 MHz"/> <input type="button" value="Edit"/>	
5 GHz Channel	<input type="text" value="Auto"/> <input type="button" value="Edit"/> Channels: 36 40 44 48 ...	
2.4 GHz Protocol	802.11ng	
2.4 GHz Channel Bonding	<input type="text" value="20 MHz"/> <input type="button" value="Edit"/>	
2.4 GHz Channel	<input type="text" value="1 (2.412 GHz)"/> <input type="button" value="Edit"/>	
Management VLAN ID	<input type="text" value="0"/> <input type="button" value="Edit"/>	(0: Untagged)
Power Boost	<input type="checkbox"/>	
Output Power	<input type="text" value="Dynamic: Auto"/> <input type="button" value="Edit"/>	
Operating Schedule	<input checked="" type="radio"/> Always On <input type="radio"/> Custom Schedule	
Max number of Clients	<input type="text" value="0"/> <input type="button" value="Edit"/>	(0: Unlimited)
Client Signal Strength Threshold	<input type="text" value="0"/> <input type="button" value="Edit"/>	(0: Unlimited)
Beacon Rate	<input type="text" value="1Mbps"/> <input type="button" value="Edit"/>	
Beacon Interval	<input type="text" value="100ms"/> <input type="button" value="Edit"/>	
DTIM	<input type="text" value="1"/> <input type="button" value="Edit"/>	
RTS Threshold	<input type="text" value="0"/> <input type="button" value="Edit"/>	
Slot Time	<input type="text" value="9"/> <input type="button" value="Edit"/>	μs
ACK Timeout	<input type="text" value="48"/> <input type="button" value="Edit"/>	μs
Frame Aggregation	<input checked="" type="checkbox"/>	
Frame Length	<input type="text" value="50000"/> <input type="button" value="Edit"/>	

### AP Settings

**AP Profile Name** This field specifies the name of this AP Profile.

<b>SSID</b>	These buttons specify which wireless networks will use this AP Profile. You can also select the frequencies at which each network will transmit. Please note that the Peplink Balance does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.
<b>Operating Country</b>	<p>This drop-down menu specifies the national / regional regulations which the AP should follow.</p> <ul style="list-style-type: none"> <li>• If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).</li> <li>• If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).</li> </ul> <p>NOTE: Users are required to choose an option suitable to local laws and regulations. Per FCC regulation, the country selection is not available on all models marketed in US. All US models are fixed to US channel only.</p>
<b>Preferred Frequency</b>	<p>These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for AP that can transmit at both 5.4GHz and 5GHz frequencies,</p>
<b>Protocol (5GHz, 2.4 GHz)</b>	This section displays the wireless protocols which your AP are using.
<b>Channel Bonding (5GHz, 2.4 GHz)</b>	<p>This drop-down menu is only available for 802.11bgn or 802.11n protocols only. There are three options: 20 MHz, 20/40 MHz and 40 MHz. With this feature enabled, it allows the Wi-Fi system to use two channels at once. Using two channels improves the performance of the Wi-Fi connection</p>
<b>Channel (5GHz, 2.4 GHz)</b>	<p>This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11, and from 1 to 13 for the country setting of North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.)</p> <p>If Auto is set, the system would perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.</p>
<b>Management VLAN ID</b>	<p>This field specifies the VLAN ID to tag to management traffic, such as AP to AP-controller communication traffic. The value is zero by default, meaning that no VLAN tagging will be applied. NOTE: Change this value with caution as alterations may result in loss of connection to the AP controller.</p>
<b>Power Boost<sup>A</sup></b>	<p>With this option enabled, the AP under this profile will transmit using additional power. Please note that using this option with several AP in close proximity will lead to increased interference.</p>
<b>Output Power<sup>A</sup></b>	<p>This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level regardless of context. When Dynamic settings are selected, the AP will adjust its power level based on its surrounding AP in order to maximize performance.</p> <p>The <b>Dynamic: Auto</b> setting will set the AP to do this automatically. Otherwise, the <b>Dynamic: Manual</b> setting will set the AP to dynamically adjust only if instructed to do so. If you have set Dynamic:Manual, you can go to <b>AP &gt; Toolbox &gt; Auto Power Adj.</b> to give your AP further instructions.</p>

### Operating Schedule<sup>A</sup>

These buttons determine the time period at which the AP under this profile will be activated. Clicking the Custom Schedule option will open the following diagram:



Click the desired time periods to toggle the activation state of AP under this profile.

<b>Max number of Clients<sup>A</sup></b>	This field determines the maximum clients that can be connected to AP under this profile.
<b>Client Signal Strength Threshold<sup>A</sup></b>	This field determines that maximum signal strength each individual client will receive. The measuring unit is Megawatts.
<b>Beacon Rate<sup>A</sup></b>	This drop-down menu provides the option to send beacon in different transmit bit rate and the bit rates are: 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps.
<b>Beacon Interval<sup>A</sup></b>	This drop-down menu provides the option to set the time between each beacon send. Available options are: 100ms, 250ms and 500ms.
<b>DTIM<sup>A</sup></b>	This field provides the option to set the frequency for beacon to include Delivery Traffic Indication Message, DTIM. The interval unit is measured in milliseconds.
<b>RTS Threshold<sup>A</sup></b>	This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting zero would disable this feature.
<b>Slot Time<sup>A</sup></b>	This field provides the option to modify the unit wait time before it transmits. The default value is 9μs.
<b>ACK Timeout<sup>A</sup></b>	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is 48μs.
<b>Frame Aggregation<sup>A</sup></b>	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.
<b>Frame Length</b>	This field is only available when Frame Aggregation is enabled. It specifies the frame length for frame aggregation. By default, it is set as 50000.

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

Web Administration Settings	
Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	443
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username	admin
Admin Password	a33d3f7b2aab <input type="button" value="Generate"/>

### Web Administration Settings

<b>Enable</b>	Check the box to allow Peplink Balance to manage the web admin access information of the AP.
<b>Web Access Protocol</b>	These buttons specify the web access protocol used for accessing the web admin of AP. The two available options are HTTP and HTTPS.
<b>Management Port</b>	This field specifies the management port used for accessing the device.
<b>HTTP to HTTPS Redirection</b>	This option will be available if you have chosen HTTPS as the Web Access Protocol. With this enabled, any HTTP access to the web admin will be redirect to HTTPS automatically.
<b>Admin User Name</b>	This field specifies the administrator username of the web admin. It is set as admin by default.
<b>Admin Password</b>	This field allows you to specify a new administrator password. You may also click the Generate button and let the system generate a random password automatically.

AP Time Settings	
Time Zone	<input checked="" type="radio"/> Follow controller time zone selection <input type="radio"/> (GMT) Casablanca
Time Server	<input checked="" type="radio"/> Follow controller NTP server selection <input type="radio"/> [ ]

### AP Time Settings

<b>Time Zone</b>	Check the box to allow Peplink Balance to manage the web admin access information of the AP.
<b>Time Server</b>	These buttons specify the web access protocol used for accessing the web admin of AP. The two available options are HTTP and HTTPS.

## 22.4 Info

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



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

Events		<a href="#">View Alerts</a>
Jan 2 11:01:11	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	

[More...](#)

## Events

This event log displays all activity on your AP network, down to the client level. Click **View Alerts** to see only alerts, and click the **More...** link for additional records.

## 22.5 Usage

A detailed breakdown of data usage for each AP is available on **AP > Status**. The information is organized by device groups as defined in section **22.3**

Managed Wireless Devices						
Group Name	Device Name / Serial Number	Online Channel	Clients (2.4 / 5 GHz)	Upload (kbps)	Download (kbps)	
Default		4	11 0	170.89	11.70	 
	Desk	1	1 -	15.44	0.16	  
	2830-CAB6-3EF7	-	- -	-	-	 
	Fiber AP	6	10 -	155.45	11.54	  
	2830-CA54-D0DB	-	- -	-	-	 
Main_Office		0	0 0	0.00	0.00	 
Main_Office_11a		4	0 21	4947.18	206.41	 
Marketing		0	0 0	0.00	0.00	 
Marketing_11a		0	0 0	0.00	0.00	 
PLHQ_Conference_Room		0	0 0	0.00	0.00	 
Dual Radio PLHQ		2	6 0	69.06	5.31	 

### Usage

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

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

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

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



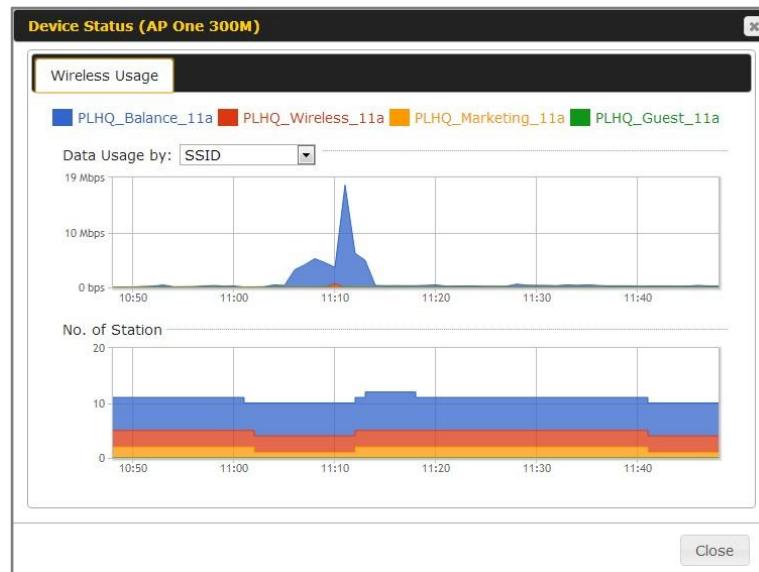
Clicking the icon, and a usage table of each client will appear:

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

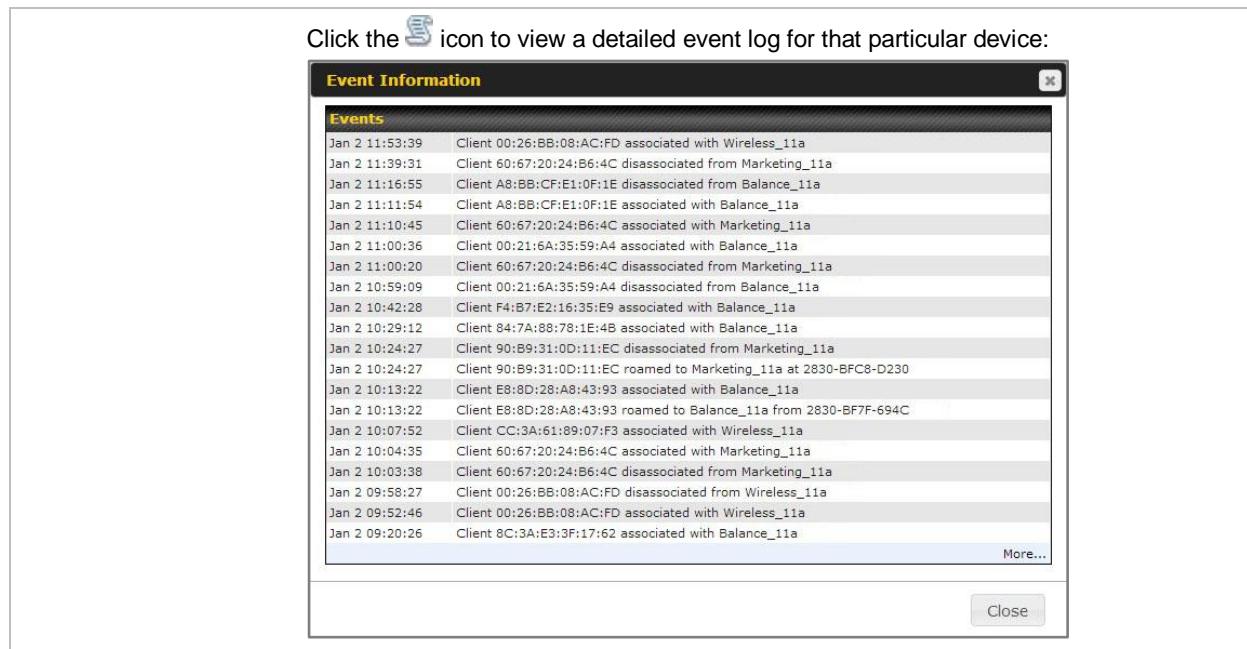
**Close**

### Managed Wireless Devices

Click the icon, and a graph displaying usage will appear:



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



## 22.6 AP Status

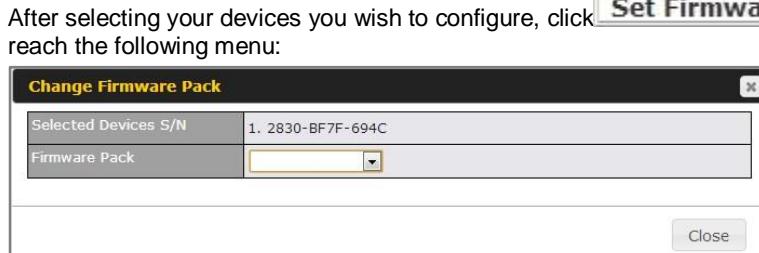
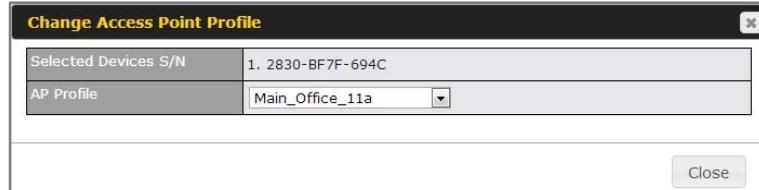
A detailed breakdown of the status of each device is available on **AP >Status**. The information is organized by device groups as defined in section 22.3

**Search Filter**

Device Name / Serial Number	<input type="text"/>
Online Status	<input type="checkbox"/> Include Offline Devices
Search Result	

**Managed Wireless Devices**

Group Name (Online Devices Count)							Expand	Collapse
Device Name / SN	MAC Address	Location	IP Address	Firmware	Pack ID	Configurations		
▶ Default (4 online)								
▶ Main_Office (0 online)								
▶ Main_Office_11a (4 online)								
■ AP One 300M /...	00:1A:DD:C0:B2:E0	Long's Desk	10.9.2.42	3.4.0	None ✓	5 GHz: Ch 60	<a href="#">Details</a>	<a href="#">Edit</a>
■ Conference Ro...	00:1A:DD:C0:B3:20	A8 confer...	10.9.2.3	3.4.0	None ✓		<a href="#">Details</a>	<a href="#">Edit</a>
■ AP One 300M /...	00:1A:DD:C0:BC:00	Keith's Desk	10.9.2.71	3.4.0	Default - None ✓		<a href="#">Details</a>	<a href="#">Edit</a>
■ AP One 300M /...	00:1A:DD:C2:03:20	Lewis's Desk	10.9.2.65	3.4.0	Default - None ✓		<a href="#">Details</a>	<a href="#">Edit</a>
▶ Marketing (0 online)								
▶ Marketing_11a (0 online)								
▶ PLHQ_Conference_Room (0 online)								
▶ Dual Radio PLHQ (2 online)								
<a href="#">Remove Offline Units</a>							<a href="#">Set Firmware Pack</a>	<a href="#">Change AP Profile</a>

AP Status	
<b>Device Name/Serial Number</b>	This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.
<b>Online Status</b>	This button toggles weather your search will include offline devices.
	This table displays the MAC address, IP Address, firmware version, and specific configurations of each device. Clicking the <b>Details</b> button of each device will result in the following menu:
	
<p>Here, you can edit the name and location of your AP. You can also choose the channel to will transmit from.</p>	
<p>You can also batch configure devices on this table by selecting the items you wish to configure, then clicking <b>Set Firmware Pack</b> <b>Change AP Profile</b></p>	
<b>Managed Wireless Devices</b>	<p>After selecting your devices you wish to configure, click <b>Set Firmware Pack</b> to reach the following menu:</p>  <p>Select the pull-down menu to choose a firmware pack for the devices that you have selected.</p>
<p>After selecting your devices you wish to configure, click <b>Change AP Profile</b> to reach the following menu:</p>  <p>Select the pull-down menu to choose an AP profile for the devices that you have selected.</p>	

## 22.7 Rogue AP

A listing of suspected Rogue devices can be accessed by navigating to **AP >Rogue AP**.

Suspected Rogue Devices						
BSSID	SSID	Channel	Encryption	Last Seen	Mark as	
00:1A:DD:B8:78:C1	Balance	5	WPA2	1 minute ago		
00:1A:DD:B8:78:C2	Wireless	5	WPA2	1 minute ago		
00:1A:DD:B8:78:C3	Marketing	5	WPA2	1 minute ago		
00:1A:DD:B8:78:C4	Guest	5	WPA2	1 minute ago		
00:03:7F:00:00:00	T4B1	5	WPA2	1 minute ago		
00:03:7F:00:00:02		5	WPA2	1 minute ago		
00:18:39:CC:8B:FE	PDF	11	WPA	3 hours ago		
00:1A:1E:F3:0E:40	Aruba3200	6	WPA2	1 minute ago		
00:1A:1E:F3:0E:41		6	OPEN	1 minute ago		
00:1A:1E:F3:0E:48	Aruba3200	40	WPA2	2 minutes ago		
00:1A:1E:F3:0E:49		40	OPEN	2 minutes ago		
00:1A:DD:00:28:11	PEPWAVE_2800	149	OPEN	7 hours ago		
00:1A:DD:9F:AA:45	OTGH	11	WPA2	1 minute ago		
00:1A:DD:AD:C7:A1	test	1	OPEN	14 minutes ago		
00:1A:DD:AD:C7:B1	test	161	OPEN	2 minutes ago		
00:1A:DD:B8:87:05	BM_LB	36	WPA2	2 minutes ago		
00:1A:DD:B9:1A:65	test	1	OPEN	3 hours ago		
00:1A:DD:B9:1C:05	pep test	9	WPA2	46 minutes ago		
00:1A:DD:B9:5D:88	PEPWAVE_F8F5	1	WPA2	1 minute ago		
00:1A:DD:B9:60:88	KNMAX700	3	WPA2	1 minute ago		

[Prev](#) [1-20](#) [\(204\)](#) [Next](#)

Identified Known/Rogue Devices						
	BSSID	SSID	Channel	Encryption	Last Seen	Unmark
	00:03:7F:00:00:01	!T4B1	5	WPA2	1 minute ago	
	00:1A:DD:B6:A3:21	S_Room	1	WPA2	1 minute ago	

[Prev](#) [1-2](#) [\(2\)](#) [Next](#)

## Suspected Rogue Devices

Hoving over the device MAC address will result in a popup with information on how this device was detected. Click the icons and the device will be moved to the bottom table of identified devices.

## 22.8 Toolbox

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

Firmware Packs	Auto Power Adj.	Dynamic Channel Assignment								
<table border="1"> <thead> <tr> <th>Pack ID</th> <th>Release Date</th> <th>Details</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>1. 1126</td> <td>2013-08-26</td> <td></td> <td></td> </tr> </tbody> </table> <a href="#">Check for Updates</a> <a href="#">Manual Upload</a> <a href="#">Default...</a>	Pack ID	Release Date	Details	Action	1. 1126	2013-08-26				
Pack ID	Release Date	Details	Action							
1. 1126	2013-08-26									

## Firmware Packs

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

## 23 System Settings

### 23.1 Admin Security

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



Admin Account UI



User Account UI

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

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

**Default:** 4 hours 0 minutes.

For security reason, after logging in to the Web Admin Interface for the first time, it is recommended to change the administrator password.

Configuring the administration interface to be accessible only from the LAN can further improve system security.

Administrative Settings configuration is located at:**System>Admin Security**

Admin Settings	
Router Name	Balance_EFD1 hostname: balance-efd1
Admin User Name	admin
Admin Password	*****
Confirm Admin Password	*****
Read-only User Name	user
User Password	*****
Confirm User Password	*****
Web Session Timeout	4 Hours 0 Minutes
Authentication by RADIUS	<input checked="" type="checkbox"/> Enable
Auth Protocol	MS-CHAP v2
Auth Server	Port Default
Auth Server Secret	<input type="text"/> Hide Characters
Auth Timeout	3 seconds
Accounting Server	Port Default
Accounting Server Secret	<input type="text"/> Hide Characters
Network Connection	LAN
CLI SSH & Console	<input checked="" type="checkbox"/> Enable
CLI SSH Port	22
CLI SSH Access	LAN/WAN
Security	HTTP
Web Admin Port	80 Default
Web Admin Access	LAN/WAN

Admin Settings	
<b>Router Name</b>	This field allows you to define a name for this Peplink Balance unit.
<b>Admin User Name</b>	It is set as <b>admin</b> by default and is not customizable.
<b>Admin Password</b>	This field allows you to specify a new administrator password.
<b>Confirm Admin Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Read-only User Name</b>	It is set as <b>user</b> by default and is not customizable.
<b>User Password</b>	This field allows you to specify a new user password. Once the user password is set, the feature of read-only user will be enabled.
<b>Confirm User Password</b>	This field allows you to verify and confirm the new user password.

<b>Web Session Timeout</b>	This field specifies the number of hours and minutes that a web session can remain idle before the Balance terminates its access to the Web Admin Interface.  By default, it is set to <b>4 hours</b> .
<b>Authentication by RADIUS</b>	With this box is checked, the Web Admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local "admin" and "user" accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access.  Additional authentication options will be available once this box is checked.
<b>Auth Protocol</b>	This specifies the authentication protocol used. Available options are <b>MS-CHAP v2</b> and <b>PAP</b> .
<b>Auth Server</b>	This specifies the access address of the external RADIUS server.
<b>Auth Server Secret</b>	This field is meant for the secret key for accessing the RADIUS server.
<b>Auth Timeout</b>	This option specifies the time value for authentication timeout.
<b>Accounting Server</b>	This specifies the access address of the external Accounting server.
<b>Accounting Server Secret</b>	This field is meant for the secret key for accessing the Accounting server.
<b>Network Connection</b>	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN and VPN connections.
<b>CLI SSH &amp; Console</b>	The CLI (Command Line Interface) can be accessed via SSH. It can also be accessed from the serial console port for Peplink Balance 305, 380, 580, 710, 1350 and 2500. This field enables CLI support.  For additional information regarding CLI, please refer to section <a href="#">22.5</a> of this manual
<b>CLI SSH Port</b>	This field determines the port on which clients can access CLI SSH
<b>CLI SSH Access</b>	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
<b>Security</b>	This option is for specifying the protocol(s) through which the Web Admin Interface can be accessible: <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> </ul> HTTP/HTTPS
<b>Web Admin Port</b>	These fields are for specifying the port number at which the Web Admin Interface can be accessible.
<b>Web Admin Access</b>	This option is for specifying the network interfaces through which the Web Admin Interface can be accessible: <ul style="list-style-type: none"> <li>• LAN only</li> <li>• LAN/WAN</li> </ul>

If LAN/WAN is chosen, the WAN Connection Access Settings form will be displayed.

**WAN Connection Access Settings**

Allowed Source IP Subnets	<input type="radio"/> Any <input checked="" type="radio"/> Allow access from the following IP subnets only						
Allowed WAN IP Address(es)	<b>Connection / IP Address(es)</b> <table border="1"> <tr> <td><input checked="" type="checkbox"/> WAN1</td> <td><input checked="" type="checkbox"/> 10.8.8.240 (Interface IP)</td> </tr> <tr> <td><input checked="" type="checkbox"/> WAN2</td> <td><input checked="" type="checkbox"/> Interface IP</td> </tr> <tr> <td><input checked="" type="checkbox"/> Mobile Internet</td> <td><input checked="" type="checkbox"/> Interface IP</td> </tr> </table>	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> 10.8.8.240 (Interface IP)	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> Interface IP	<input checked="" type="checkbox"/> Mobile Internet	<input checked="" type="checkbox"/> Interface IP
<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> 10.8.8.240 (Interface IP)						
<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> Interface IP						
<input checked="" type="checkbox"/> Mobile Internet	<input checked="" type="checkbox"/> Interface IP						

### WAN Connection Access Settings

This field allows you to restrict the ability to access web admin to only defined IP subnets.

- **Any** - Allow web admin accesses from anywhere, without IP address restrictions.
- **Allow access from the following IP subnets only** - Restricts the ability to access web admin to only defined IP subnets. When this is chosen, a text input area will appear beneath:

**WAN Connection Access Settings**

Allowed Source IP Subnets	<input type="radio"/> Any <input checked="" type="radio"/> Allow access from the following IP subnets only <input type="text" value="192.168.0.0/24"/>
---------------------------	---

Enter your allowed IP subnet addresses into this text area. Each IP subnet must be in the form of  $w.x.y.z/m$ .  $w.x.y.z$  represents an IP address (e.g. 192.168.0.0), and  $m$  represents the subnet mask in CIDR format, which is between 0 and 32 inclusively. For example:  
192.168.0.0/24

To define multiple subnets, separate each IP subnet one in a line. For example:

192.168.0.0/24  
10.8.0.0/16

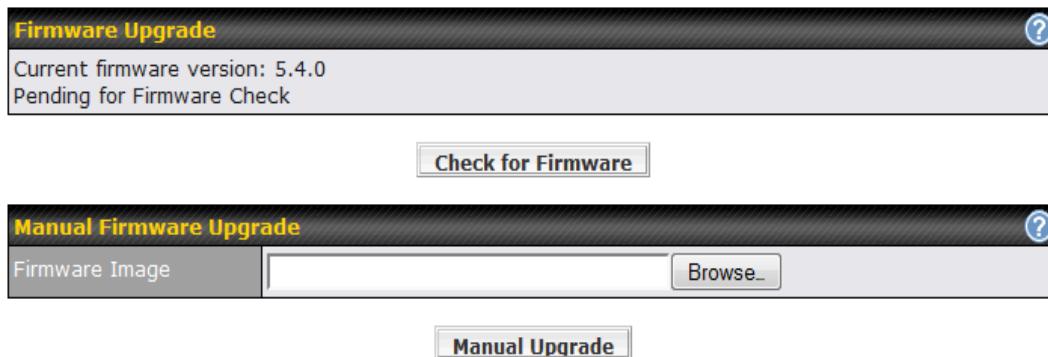
This is to choose which WAN IP address(es) the web server should listen on.

**Allowed WAN IP Address(es)**

Allowed WAN IP Address(es)	<b>Connection / IP Address(es)</b> <table border="1"> <tr> <td><input checked="" type="checkbox"/> WAN1</td> <td><input checked="" type="checkbox"/> 210.10.10.1 (Interface IP)</td> </tr> <tr> <td><input type="checkbox"/> WAN2</td> <td><input type="checkbox"/> 210.10.10.2</td> </tr> <tr> <td><input type="checkbox"/> WAN3</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Mobile Internet</td> <td></td> </tr> </table>	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> 210.10.10.1 (Interface IP)	<input type="checkbox"/> WAN2	<input type="checkbox"/> 210.10.10.2	<input type="checkbox"/> WAN3		<input type="checkbox"/> Mobile Internet	
<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> 210.10.10.1 (Interface IP)								
<input type="checkbox"/> WAN2	<input type="checkbox"/> 210.10.10.2								
<input type="checkbox"/> WAN3									
<input type="checkbox"/> Mobile Internet									

## Firmware

The firmware of Peplink Balance is upgradeable through the Web Admin Interface. Firmware upgrade functionality is located at: **System>Firmware**



The screenshot shows two main sections of the 'Firmware' page:

- Firmware Upgrade:** Shows the current firmware version as 5.4.0 and a 'Pending for Firmware Check' message. A 'Check for Firmware' button is available.
- Manual Firmware Upgrade:** Features a 'Firmware Image' input field, a 'Browse...' button to select a local file, and a 'Manual Upgrade' button.

There are two ways to upgrade the unit. The first method is through an online download, the system can **Download and Upgrade** over the Internet. The second method is to upload a firmware file manually.

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

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

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

### Firmware Upgrade Status for Peplink Balance 20, 30, 30 LTE, 210 and 310

Status LED Information during firmware upgrade:

- OFF – Firmware upgrade in progress (DO NOT disconnect power.)
- Red – Unit is rebooting
- Green – Firmware upgrade successfully completed

### Important Note

The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the Release Notes for the particular firmware version before installing.

Do not disconnect the power during firmware upgrade process.

Do not attempt to upload a non-firmware file, or a firmware file that is not supported, by Peplink.

Upgrading Peplink Balance with an invalid firmware file will damage the unit, and may void the warranty.

### 23.3 Time

The Time Server functionality enables the system clock of Peplink Balance to be synchronized with a specified Time Server.

The settings for Time Server configuration are located at: **System > Time**

Time Settings	
Time Zone	(GMT-08:00) Pacific Time (US & Canada) <input type="checkbox"/> Show all
Time Server	time.nist.gov <input type="button" value="Default"/>
<input type="button" value="Save"/>	

#### Time Server Settings

This specifies the time zone (along with the corresponding Daylight Savings Time scheme) in which Peplink Balance operates.

**Time Zone** The Time Zone value affects the time stamps in the Event Log of Peplink Balance and E-mail notifications.  
Checked the box **Show all** to show all time zone options.

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

## 23.4 Email Notification

The Email Notification functionality of Peplink Balance provides a System Administrator with up to date information on network status.

The settings for configuring Email Notification are found at: **System > Email Notification**

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	<input type="text" value="smtp.mycompany.com"/> <input checked="" type="checkbox"/> Require authentication
SSL Encryption	<input type="checkbox"/> (Note: any server certificate will be accepted)
SMTP Port	25 <input type="button" value="Default"/>
SMTP User Name	<input type="text" value="smptuser"/>
SMTP Password	<input type="password" value="*****"/>
Confirm SMTP Password	<input type="password" value="*****"/>
Sender's Email Address	<input type="text" value="admin@mycompany.com"/>
Recipient's Email Address	<input type="text" value="system@mycompany.com&lt;br/&gt;staff@mycompany.com"/>

### Email Notification Settings

<b>Email Notification</b>	This setting specifies whether or not to enable Email Notification. If the box <b>Enable</b> is checked, then the Peplink Balance will send email messages to the System Administrators when the WAN status changes, or when new firmware is available. If the box <b>Enable</b> is not checked, Email Notification is disabled and the Peplink Balance will not send email messages.
<b>SMTP Server</b>	This setting specifies the SMTP server to be used for sending email. If the Server requires authentication, check the box <b>Require authentication</b> .
<b>SSL Encryption</b>	Check the box to enable SMTPS. When the box is checked, the next field <b>SMTP Port</b> will be changed to <b>465</b> automatically.
<b>SMTP Port</b>	This field is for specifying the SMTP Port number. By default, this is set to <b>25</b> ; when the <b>SSL Encryption</b> box is checked, the default port number will be set to <b>465</b> . You may customize the port number by editing this field. Click the button <b>Default</b> to restore the number to its default setting.
<b>SMTP User Name / Password</b>	This setting specifies the SMTP username and password while sending email. These options are shown only if the <b>Require authentication</b> check box is checked in the <b>SMTP Server</b> setting.

<b>Confirm SMTP Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Sender's Email Address</b>	This setting specifies the email address which the Peplink Balance will use to send its reports.
<b>Recipient's Email Address</b>	This setting specifies the email address(es) to which the Peplink Balance will send email notifications. For multiple recipients, separate each email using the enter key.

After you have completed the settings, you can click the **Test Email Notification** button to test the settings before saving it. After it is clicked, you will see this screen to confirm the settings:

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	25
SMTP User Name	smptuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

**Send Test Notification** **Cancel**

Click **Yes** to confirm. In a few seconds, you will see a message with detailed test results.

**Test email sent. Email notification settings are not saved, it will be saved after clicked the 'Save' button.**

### Test Result

```
[INFO] Try email through connection #3
[<-] 220 ESMT
[->] EHLO balance
[<-] 250-smtp Hello balance [210.210.210.210]
250-SIZE 100000000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250-ENHANCEDSTATUSCODES
```

## 23.5 Event Log

The Event Log functionality enables event logging at a specified remote Syslog server. The settings for configuring Remote System Log are found at: **System>Event Log**

<b>Send Events to Remote Syslog Server</b>	
Remote Syslog	<input type="checkbox"/>
Remote Syslog Host	<input type="text"/>
<b>Push Events to Mobile Devices</b>	
Push Events	<input type="checkbox"/>
<input type="button" value="Save"/>	

### Remote Syslog Settings

<b>Remote Syslog</b>	This setting specifies whether or not to log events at the specified remote Syslog server.
<b>Remote Syslog Host</b>	This setting specifies the IP address or hostname of the remote Syslog server.
The Peplink Balance can also send push notifications to mobile devices that have our Mobile Router Utility installed. Click the square to activate this feature.	
<b>Push Events</b>	 For more information regarding the Router Utility, please go to: <a href="http://www.peplink.com/products/router-utility">www.peplink.com/products/router-utility</a>

## 23.6 SNMP

SNMP or Simple Network Management Protocol is an open standard that can be used to collect information about the Peplink Balance unit.

SNMP configuration is located at: **System > SNMP**

<b>SNMP Settings</b>															
SNMP Device Name	Balance_XXXX														
SNMP Port	161	Default	<input type="button" value="Edit"/>												
SNMPv1	<input checked="" type="checkbox"/> Enable														
SNMPv2c	<input type="checkbox"/> Enable														
SNMPv3	<input type="checkbox"/> Enable														
<input type="button" value="Save"/>															
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Community Name</th> <th>Allowed Source Network</th> <th>Access Mode</th> <th></th> </tr> </thead> <tbody> <tr> <td>MyCompany</td> <td>192.168.1.20/24</td> <td>Read Only</td> <td><input type="button" value="Delete"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Add SNMP Community"/></td> </tr> </tbody> </table>				Community Name	Allowed Source Network	Access Mode		MyCompany	192.168.1.20/24	Read Only	<input type="button" value="Delete"/>	<input type="button" value="Add SNMP Community"/>			
Community Name	Allowed Source Network	Access Mode													
MyCompany	192.168.1.20/24	Read Only	<input type="button" value="Delete"/>												
<input type="button" value="Add SNMP Community"/>															
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>SNMPv3 User Name</th> <th>Authentication / Privacy</th> <th>Access Mode</th> <th></th> </tr> </thead> <tbody> <tr> <td>snmpuser</td> <td>MD5 / DES</td> <td>Read Only</td> <td><input type="button" value="Delete"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Add SNMP User"/></td> </tr> </tbody> </table>				SNMPv3 User Name	Authentication / Privacy	Access Mode		snmpuser	MD5 / DES	Read Only	<input type="button" value="Delete"/>	<input type="button" value="Add SNMP User"/>			
SNMPv3 User Name	Authentication / Privacy	Access Mode													
snmpuser	MD5 / DES	Read Only	<input type="button" value="Delete"/>												
<input type="button" value="Add SNMP User"/>															

<b>SNMP Settings</b>				
<b>SNMP Device Name</b>	This field shows the router name defined in <b>System &gt; Admin Security</b> .			
<b>SNMP Port</b>	This option specifies the port which SNMP used. The default port is set as <b>161</b> .			
<b>SNMPv1</b>	This option allows you to enable SNMP version 1.			
<b>SNMPv2</b>	This option allows you to enable SNMP version 2.			
<b>SNMPv3</b>	This option allows you to enable SNMP version 3.			

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

<b>SNMP Community</b>	
Community Name	<input type="text" value="MyCompany"/>
Allowed Network	<input type="text" value="192.168.1.20"/> / <input type="text" value="255.255.255.0 (/24)"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

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

<b>SNMPv3 User</b>	
User Name	<input type="text" value="SNMPUser"/>
Authentication	<input type="text" value="SHA"/> <input type="text" value="password"/>
Privacy	<input type="text" value="DES"/> <input type="text" value="privacypassword"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

## 23.7 InControl



InControl is a cloud based service which allows you to manage all of your Peplink and Pepwave devices with one unified system. With it, you can generate reports, gather statistics, and configure your devices automatically. All of this is now possible with InControl.

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

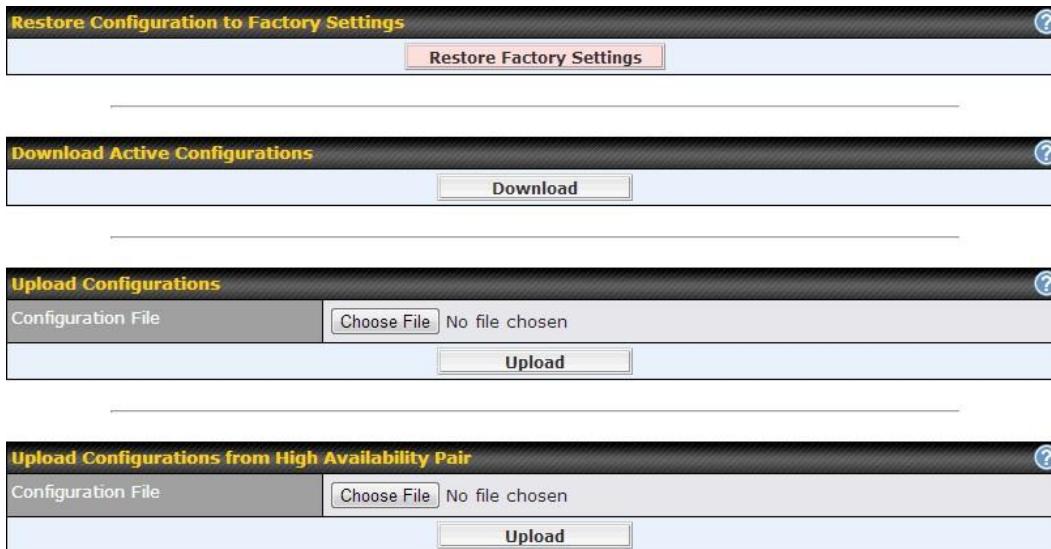
You can sign up for an InControl account at <https://incontrol2.peplink.com/>. You can register your devices under the account, monitor their status, see their usage reports and receive offline notifications.

## 23.8 Configuration

Backing up the Peplink Balance settings immediately after the successful completion of the initial setup is strongly recommended.

The functionality to download and upload Peplink Balance settings is found at:

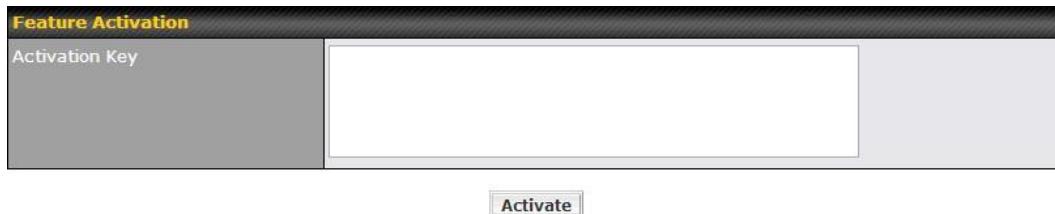
**System> Configuration**



Configuration	
<b>Restore Configuration to Factory Settings</b>	The <b>Restore Factory Settings</b> button is to reset the configuration to the factory default settings. After clicking the button, you will need to click the <b>Apply Changes</b> button on the top right corner to make the settings effective.
<b>Downloading Active Configurations</b>	The purpose of the <b>Download</b> button is to backup the current active settings. Click <b>Download</b> and save the configuration file.
<b>Uploading Configurations</b>	To restore or change settings based on a configuration file, click <b>Choose File</b> to locate the configuration file on the local computer, and then click <b>Upload</b> . The new settings can then be applied by clicking the <b>Apply Changes</b> button on the page header, or you can cancel the procedure by pressing <b>discard</b> on the Main page of Web Admin Interface.
<b>Uploading Configuration from High Availability Pair</b>	<b>(Available on Peplink Balance 210+)</b> In a High Availability (HA) configuration, the Balance unit can quickly load the configuration of its HA counterpart. To do so, click the <b>Upload</b> button. After loading the settings, configure the LAN IP address of the Peplink Balance unit to be different from the HA counterpart.

## 23.9 Feature Add-ons

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



The screenshot shows a user interface titled "Feature Activation". It has a single input field labeled "Activation Key" which is currently empty. Below the input field is a button labeled "Activate".

## 23.10 Reboot

This page provides a Reboot button for restarting the system.

For maximum reliability, the Peplink Balance series can equip with two copies of firmware; each copy a different version. You can select the firmware version you would like to reboot the device with.

The firmware marked with **(Running)** is the current system boot up firmware.

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



The screenshot shows a user interface titled "Reboot System". It displays two firmware options:

- Firmware 1: 6.1.0 build 2816 **(Running)**
- Firmware 2: 6.1.0b18 build 2780

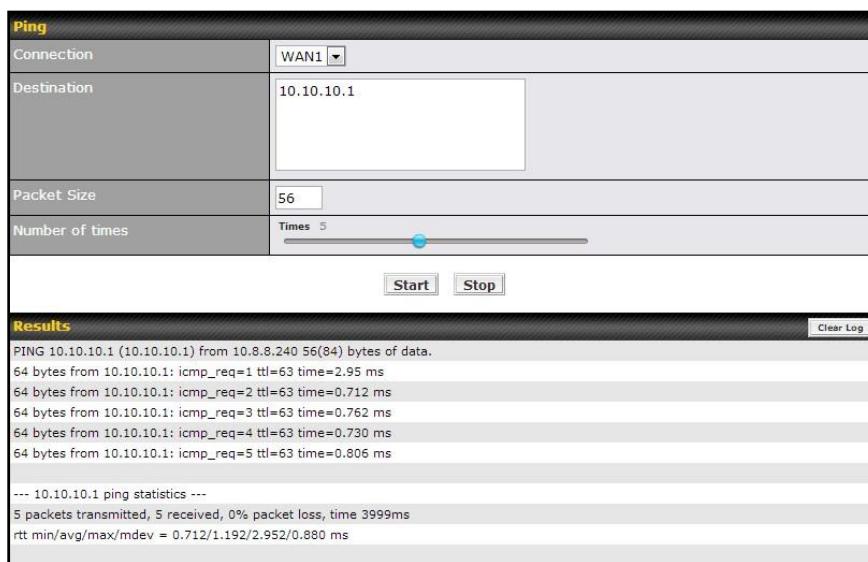
Below the options is a large red "Reboot" button.

## 24 Tools

### 24.1 Ping

The Ping Test tool in the Peplink Balance performs Pings through a specified Ethernet interface or a SpeedFusion™ VPN connection. You can specify the number of pings in the field **Number of times** to a maximum number of **10** times, and Packet Size can be specified in the field **Packet Size** to a maximum of **1472** bytes.

The Ping utility is located at **System > Tools > Ping**, illustrated as follows:

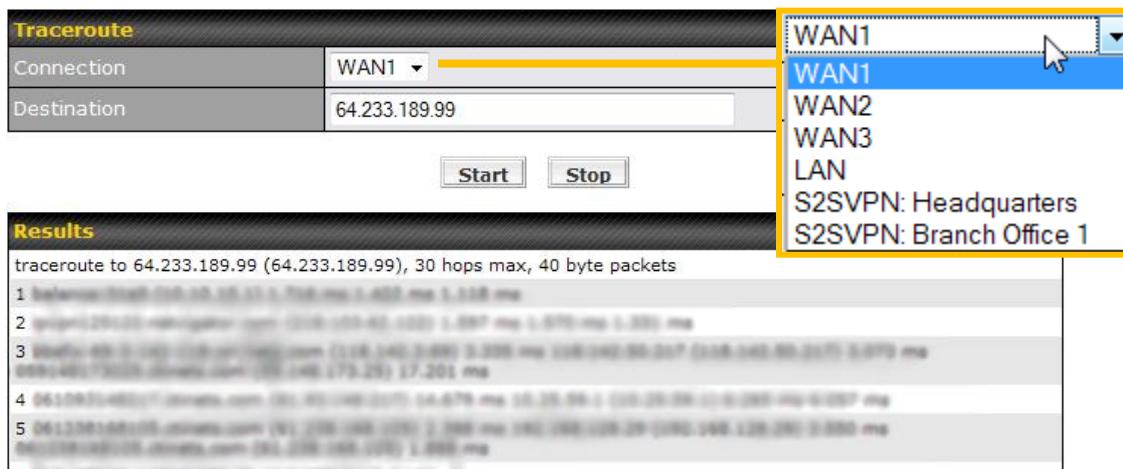


#### Tip

A System Administrator can use the Ping utility to manually check the connectivity of a particular LAN/WAN connection.

## 24.2 Traceroute Test

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



### Tip

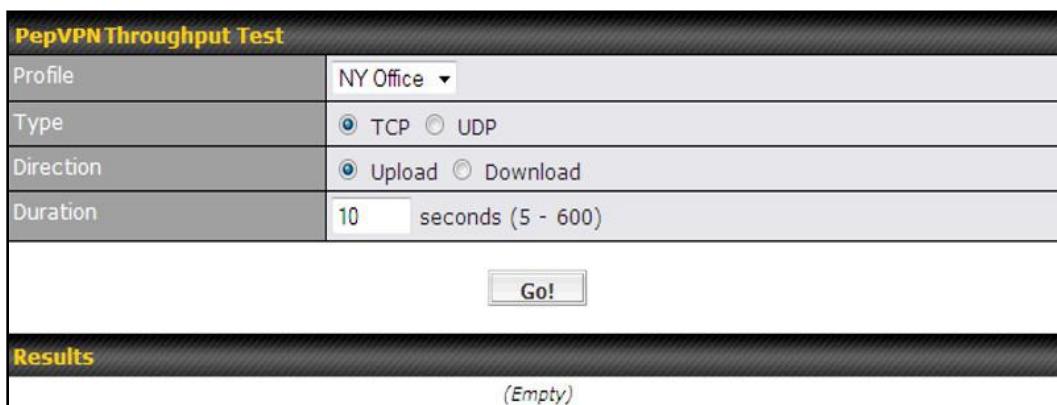
A System Administrator can use the Traceroute utility to analyze the connection path of a LAN/WAN connection.

## 24.3 PepVPN Test

(Available on Peplink Balance 210+)

The PepVPN Test tool can help to test the throughput between different VPN peers.

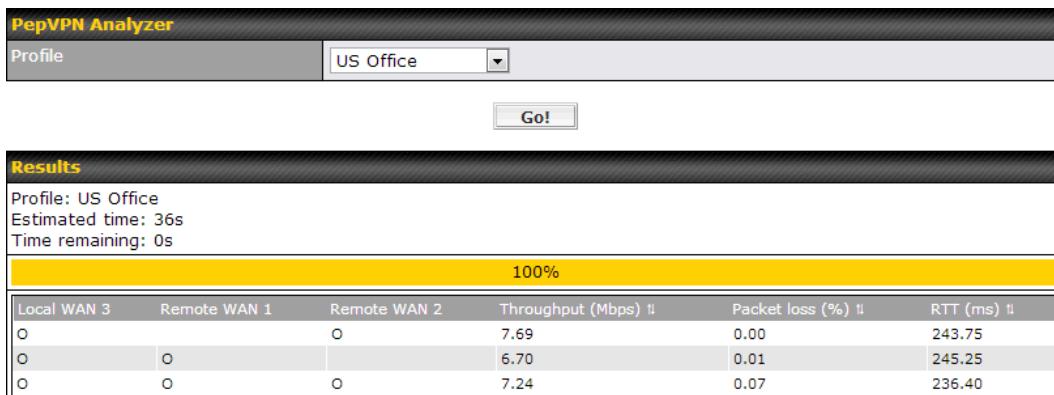
You can define the **Test Type**, **Direction**, and **Duration** of the test, and press **Go!** to perform the throughput test. The VPN Test utility is located at **System > Tools > PepVPN Test** illustrated as follows:



## 24.4 PepVPN Analyzer

The bandwidthbonding feature of PepVPN occurs when multiple WAN lines from one end merge with multiple WAN lines from the other end. For this to happen, each WAN line needs to form a connection with all the WAN lines on the opposite end. The function of the PepVPN Analyzer is to report the throughput, packet loss, and latency of all possible combinations of connections.

This feature is located in **System > PepVPN Analyzer**. To utilize this feature, simply choose your profile from the drop-down menu and click **Go!**



The screenshot shows the PepVPN Analyzer interface. At the top, there is a header bar with the title "PepVPN Analyzer". Below it, a dropdown menu is set to "US Office". A "Go!" button is located to the right of the dropdown. The main area is titled "Results" and displays the following information:

Profile: US Office  
Estimated time: 36s  
Time remaining: 0s

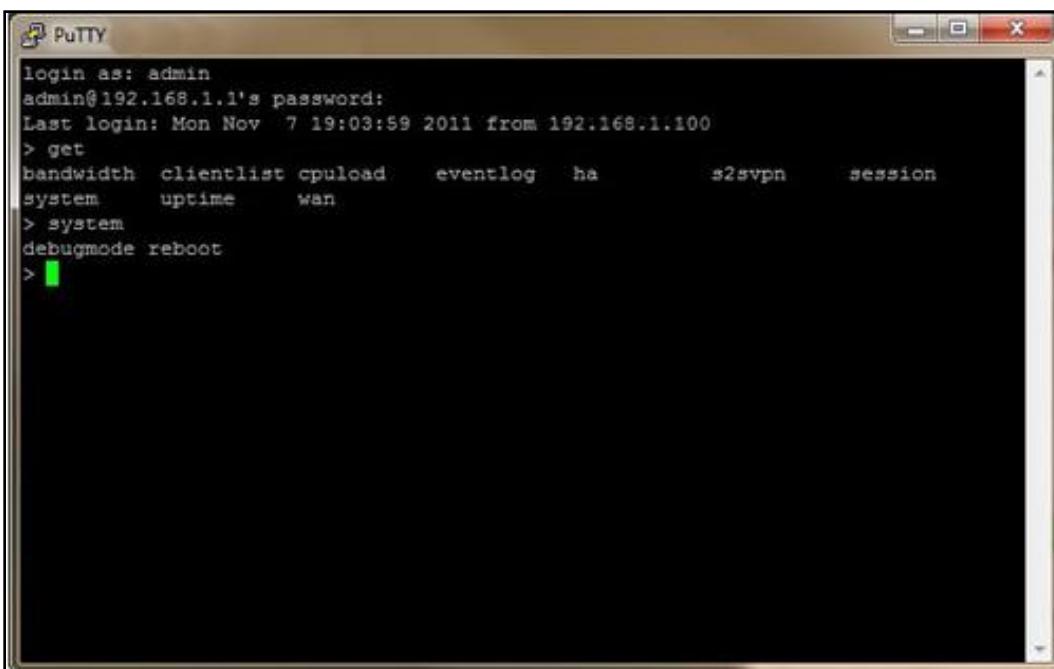
A progress bar at the top of the results section is at 100%. Below it is a table with the following data:

Local WAN 3	Remote WAN 1	Remote WAN 2	Throughput (Mbps) ↴	Packet loss (%) ↴	RTT (ms) ↴
○	○	○	7.69	0.00	243.75
○	○	○	6.70	0.01	245.25
○	○	○	7.24	0.07	236.40

## 24.5 CLI (Command Line Interface Support)

The serial console connector with the Peplink Balance 305, 380 HW rev 5, Peplink Balance 580, Peplink Balance 710 HW rev 2, Peplink Balance 1350 and Peplink Balance 2500 is RJ-45. To access the serial console port, prepare a RJ-45 to DB-9 console cable. Connect the RJ-45 end to the unit's console port and the DB-9 end to a terminal's serial port. The port setting will be 115200,8N1.

The serial console connector with the Peplink Balance 305, 380 HW rev 1 to 4, Peplink Balance 710 HW rev 1 is DB-9 male connector. To access the serial console port, connect a null modem cable with a DB-9 connector on both ends to a terminal with the port setting of 115200,8N1.



## 25 Status

### 25.1 Device

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

<b>System Information</b>	
Router Name	<b>Balance_EFD1</b>
Model	<b>Peplink Balance 710</b>
Hardware Revision	<b>2</b>
Serial Number	<b>1824-A193-EFD1</b>
Firmware	<b>6.1.0 build 2816</b>
PepVPN Version	<b>3.0.0</b>
Modem Support Version	<b>1014 (<a href="#">Modem Support List</a>)</b>
Host Name	<b>balance-efd1</b>
Uptime	<b>7 hours 46 minutes</b>
System Time	<b>Mon Dec 30 08:16:42 WET 2013</b>
Diagnostic Report	<b><a href="#">Download</a></b>

<b>Interface</b>	<b>MAC Address</b>
LAN	10:56:CA:06:E2:E4
WAN 1	10:56:CA:06:E2:E5
WAN 2	10:56:CA:06:E2:E6
WAN 3	10:56:CA:06:E2:E7
WAN 4	10:56:CA:06:E2:E8
WAN 5	10:56:CA:06:E2:E9
WAN 6	10:56:CA:06:E2:EA
WAN 7	10:56:CA:06:E2:EB

System Information	
<b>Router Name</b>	This is the name specified in the field Router Name located in <b>System &gt; Admin Security</b> .
<b>Model</b>	This shows the model name and number of this device.
<b>Hardware Revision</b>	This shows the hardware version of this device.
<b>Serial Number</b>	This shows the serial number of this device.
<b>Firmware</b>	This shows the firmware version this device is currently running.
<b>Uptime</b>	This shows the length of time since the device has been rebooted.
<b>System Time</b>	This shows the current system time.
<b>Diagnostic Report</b>	The Download button is for exporting a diagnostic report file required for system investigation.

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

Important Note
If you encounter issues and would like to contact Peplink Support Team ( <a href="http://www.peplink.com/contact">http://www.peplink.com/contact</a> ), please download the diagnostic report file and attach it along with a description of your encountered issue.
In firmware 5.1 or before, Diagnostic Report file can be obtain at <b>System &gt; Reboot</b>

## 25.2 Active Sessions

Information on Active Sessions is at: **Status > Active Sessions > Overview**

The screenshot shows the 'Active Sessions' overview page with three main sections:

- Services:** A table showing inbound and outbound sessions for various services. All values are 0 except for Outbound Sessions for AIM/ICQ (1), BitTorrent (32), DNS (51), Jabber (5), MSN (11), NTP (4), QQ (1), Remote Desktop (3), SSH (12), SSL (64), XMPP (4), and Yahoo (1).
- Interfaces:** A table showing inbound and outbound sessions for different WAN ports. Values are 0 for all entries.
- Top Clients:** A table showing the total number of sessions initiated by client IP addresses. The top client is 10.9.66.66 with 1069 sessions.

Service	Inbound Sessions	Outbound Sessions
AIM/ICQ	0	1
BitTorrent	0	32
DNS	0	51
Flash	0	1
HTTPS	0	76
Jabber	0	5
MSN	0	11
NTP	0	4
QQ	0	1
Remote Desktop	0	3
SSH	0	12
SSL	0	64
XMPP	0	4
Yahoo	0	1

Interface	Inbound Sessions	Outbound Sessions
WAN1	0	219
WAN2	0	0
WAN3	0	0
Mobile Internet	0	0

Top Clients	
Client IP Address	Total Sessions
10.9.66.66	1069
10.9.98.144	147
10.9.2.18	63
10.9.66.14	56
10.9.2.26	33

This screen displays the number of sessions initiated by each application. Click on each Service to obtain additional information. This screen also indicates the number of sessions initiated by each WAN port. Finally, you can see which clients are initiating the most sessions.

In addition, you can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to: **Status > Active Sessions > Search**

IP / Subnet	Source or Destination	/ 255.255.255.255 (/32)
Port	Source or Destination	
Protocol / Service	SSL	
Interface	<input type="checkbox"/> 1 WAN1 <input type="checkbox"/> 2 WAN2 <input type="checkbox"/> 3 WAN3 <input type="checkbox"/> Mobile Internet <input type="checkbox"/> VPN	
<a href="#">Search</a>		

<b>Outbound</b>					
Protocol	Source IP	Destination IP	Service	Interface	Idle Time
TCP	10.9.2.18:63700	74.125.71.17:443	HTTPS/SSL	Core	00:00:01
TCP	10.9.60.11:52204	74.125.71.138:443	HTTPS/SSL	Core	00:00:01
TCP	10.9.166.11:55879	74.125.71.102:443	HTTPS/SSL	Core	00:00:01
TCP	10.9.222.223:53474	74.125.71.102:443	HTTPS/SSL	Core	00:00:03
TCP	10.9.66.67:51211	63.150.131.43:443	HTTPS/SSL	Core	00:00:04
TCP	10.9.99.99:47115	74.125.71.18:443	HTTPS/SSL	Core	00:00:04
TCP	10.9.2.26:53786	74.125.71.17:443	HTTPS/SSL	Core	00:00:05
TCP	10.9.98.144:56428	74.125.71.106:443	HTTPS/SSL	Core	00:00:05
TCP	10.9.98.144:56435	74.125.71.84:443	HTTPS/SSL	Core	00:00:05
TCP	10.9.2.26:53780	74.125.71.139:443	HTTPS/SSL	Core	00:00:06
TCP	10.9.19.9:50903	74.125.71.113:443	HTTPS/SSL	Core	00:00:06
TCP	10.9.66.67:51118	74.125.71.19:443	HTTPS/SSL	Core	00:00:06
TCP	10.9.19.9:54822	74.125.71.19:443	HTTPS/SSL	Core	00:00:07
TCP	10.9.60.11:37178	184.31.32.225:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.60.11:37179	184.31.32.225:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.60.11:37181	184.31.32.225:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.66.67:51114	74.125.71.101:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.66.67:51207	74.125.71.101:443	HTTPS/SSL	Core	00:00:08
TCP	10.9.2.18:63779	74.125.71.101:443	HTTPS/SSL	Core	00:00:10
TCP	10.9.99.99:47114	74.125.71.113:443	HTTPS/SSL	Core	00:00:11
TCP	10.9.60.11:40078	74.125.71.18:443	HTTPS/SSL	Core	00:00:12
TCP	10.9.66.66:52642	74.125.71.19:443	HTTPS/SSL	Core	00:00:12
TCP	10.9.166.11:50436	74.125.71.125:443	HTTPS/SSL	Core	00:00:13
TCP	10.9.2.26:53800	74.125.71.139:443	HTTPS/SSL	Core	00:00:14
TCP	10.9.98.144:56172	74.125.71.101:443	HTTPS/SSL	Core	00:00:14

Total searched results: 64      [Show All](#) | [Next >](#)

<b>Inbound</b>					
Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

This Active Sessions section displays the active inbound / outbound sessions of each WAN connection on Peplink Balance.

A filter is available to help sort out the active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering.

## 25.3 Client List

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

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

Filter		<input type="checkbox"/> Online Clients Only	<input type="checkbox"/> DHCP Clients Only
<b>Client List</b>			
IP Address	Name	Download (kbps)	Upload (kbps)
192.168.0.10		17	0 00:00:22:11:CC:0D
192.168.0.150	Desktop	22	18 00:22:44:DD:11:33
192.168.0.200		0	0 00:1A:AA:AA:33:A0
192.168.1.99		0	0
192.168.1.138	Smart Phone	0	0
192.168.50.150	Site-to-Site VPN	0	0
Scale: <input checked="" type="radio"/> kbps <input type="radio"/> Mbps			

If PPTP Server in section **21.2**, SpeedFusion™ in section **12.1**, or AP Controller in section **17** is enabled, you may see the corresponding connection name listed in the **Name** field.

## 25.4 WINS Client

The WINS client list table is located at **Status > WINS Client**.

WINS Client List	
Name	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4
<b>Flush All</b>	

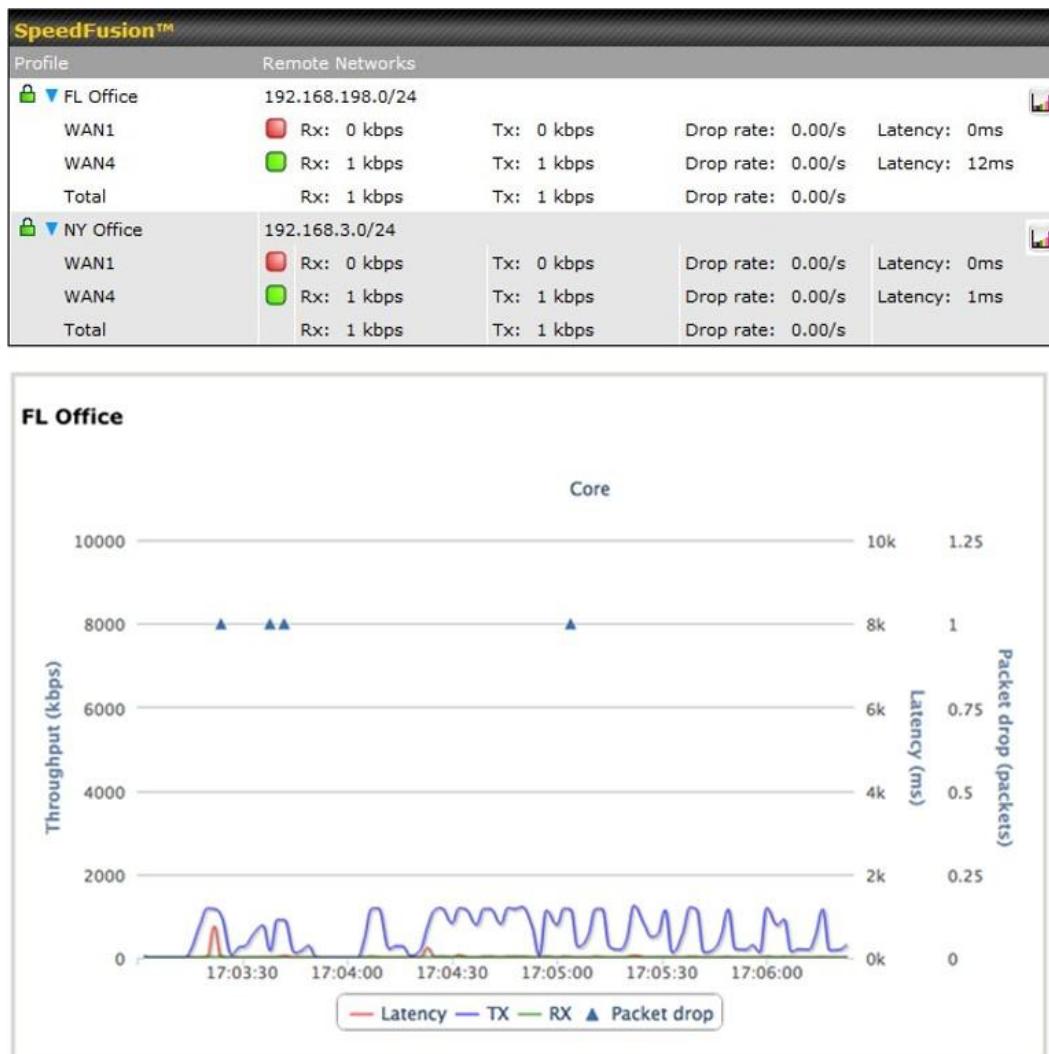
It lists the IP addresses and Names of WINS clients. This option will only be available when you have enabled the WINS Server in section **0**. Name of clients retrieved will be automatically matched into Client List in the previous section. Click the button **Flush All** to flush all WINS client records.

## 25.5 SpeedFusion™ Status

This is a page showing the current status of SpeedFusion™, located at: **Status > SpeedFusion™**  
Details about SpeedFusion™ connection peers would be shown as below.

PepVPN with SpeedFusion™		
Profile	Remote Networks	
NY Office	192.168.3.0/24	
FL Office	192.168.50.0/24	

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



## 25.6 Event Log

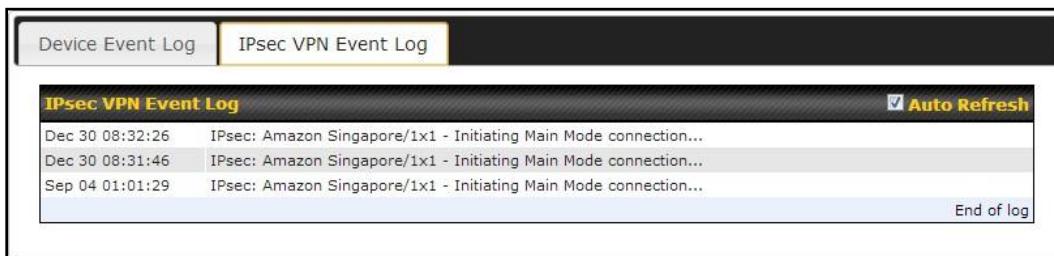
Event Log information is located at: **Status>Event Log**

### 25.6.1 Device Event Log



The log section displays a list of events that have taken place on the Peplink Balance unit. Click the **Refresh** button to retrieve log entries again. Click the **Clear Log** button to clear the log. Select **50**, **100**, or **all** to show the corresponding number of events in the log.

## 25.6.2 IPsec Event Log



Date	Event
Dec 30 08:32:26	IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
Dec 30 08:31:46	IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
Sep 04 01:01:29	IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...

End of log

This section displays a list of events that has taken place within an IPsec VPN connection. Check the box next to **Auto Refresh** and the log will be refreshed automatically.

For an AP event Log, navigate to: **AP > Info**

## 25.7 Bandwidth

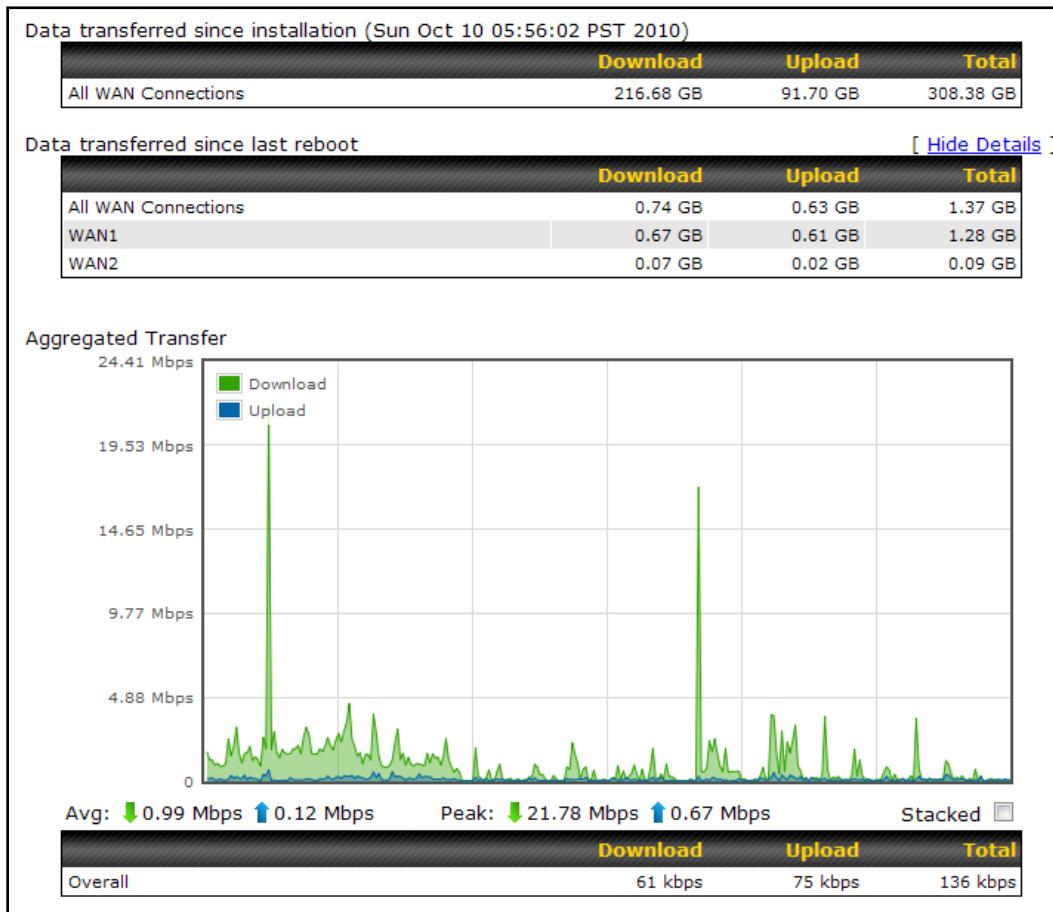
This section shows the bandwidth usage statistics, located at: **Status >Bandwidth**.

Bandwidth usage at the LAN while the device is switched off (e.g. LAN Bypass) are neither recorded nor shown.

### 25.7.1 Real-Time

The **Data transferred since installation** table indicates how much network traffic has been processed by the device since first bootup. The **Data transferred since last reboot** table indicates how much network traffic has been processed by the device since the last bootup.

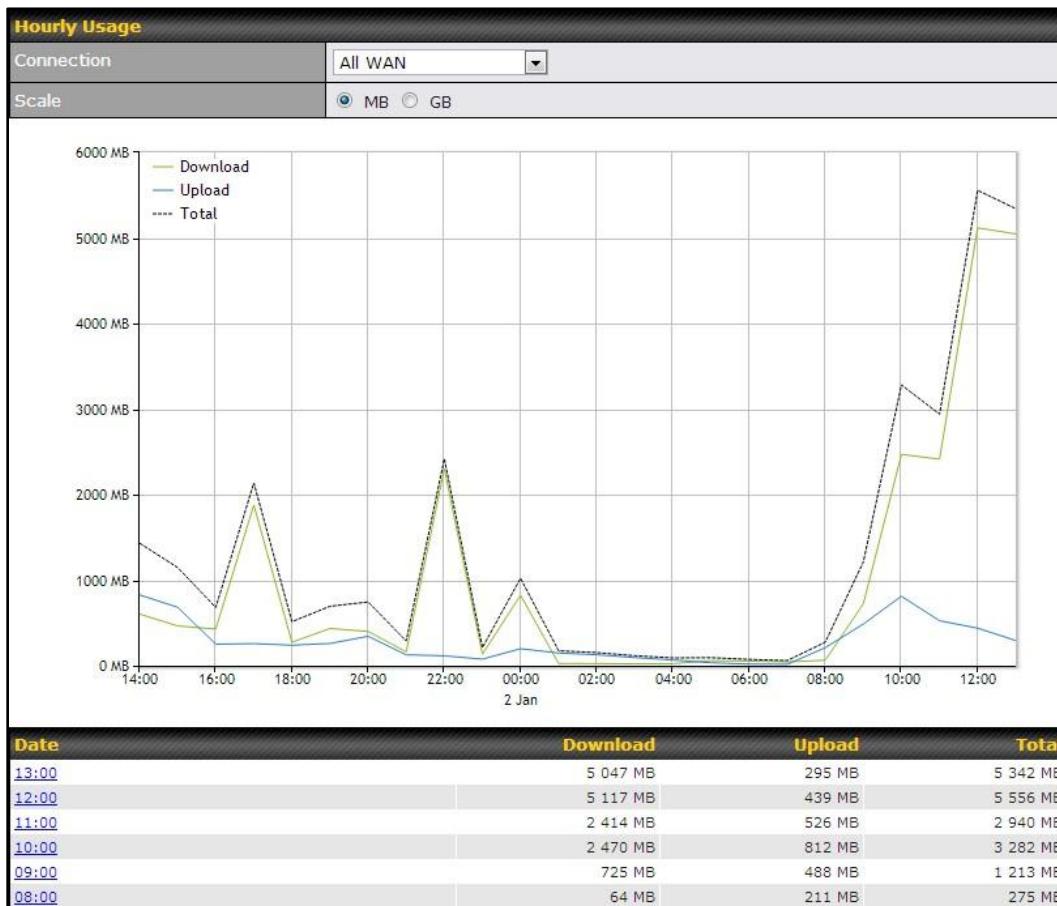
Click the **Show Details** link on the top right hand corner of each table, and a breakdown of the data transferred will be shown. The check box **Stacked** below the data transferred graph can be checked to show the aggregated transferred rate of both traffic directions.



## 25.7.2 Hourly

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

Select the desired connection to check from the drop down menu.



### 25.7.3 Daily

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

Select the connection to check from the drop down menu. If you have enabled the **Bandwidth Monitoring** feature as shown in section 11.4, the **Current Billing Cycle** table for that WAN connection will be displayed.

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection.

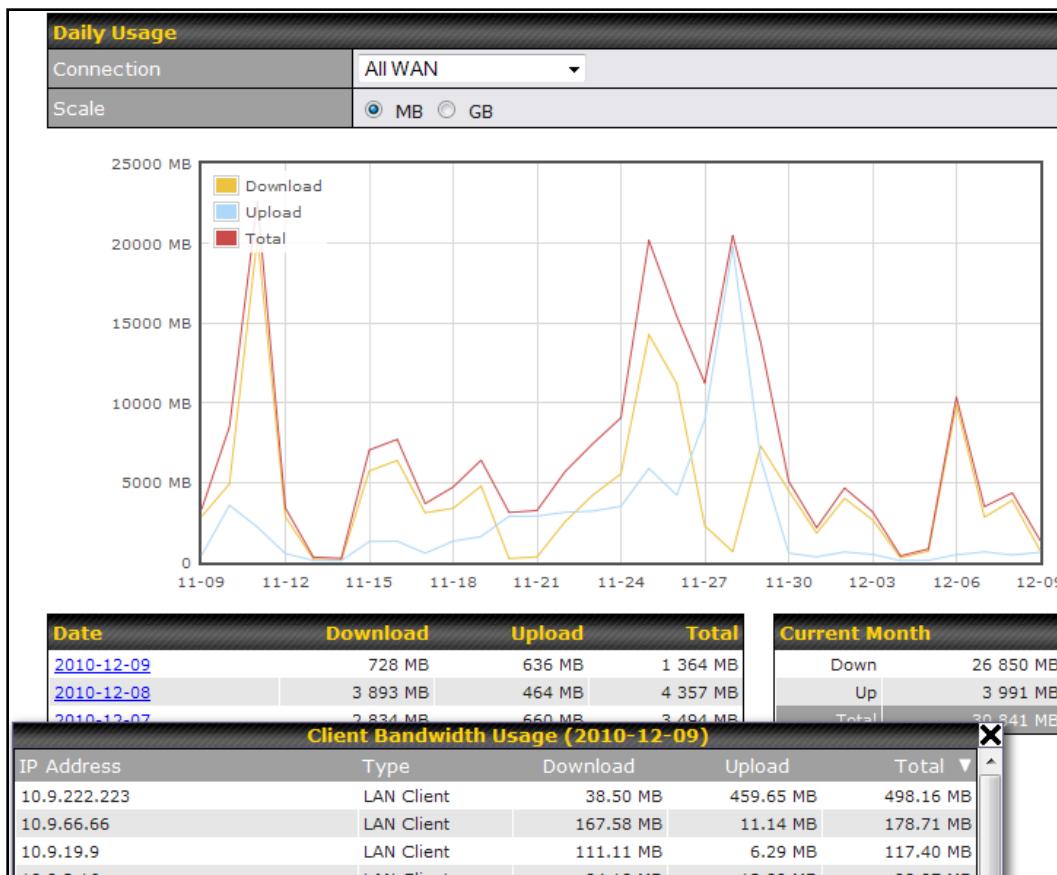
The Scale of the graph can be set to show in **Megabyte (MB)** or **Gigabyte (GB)**.



Status

# USER MANUAL

## Peplink Balance Series



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

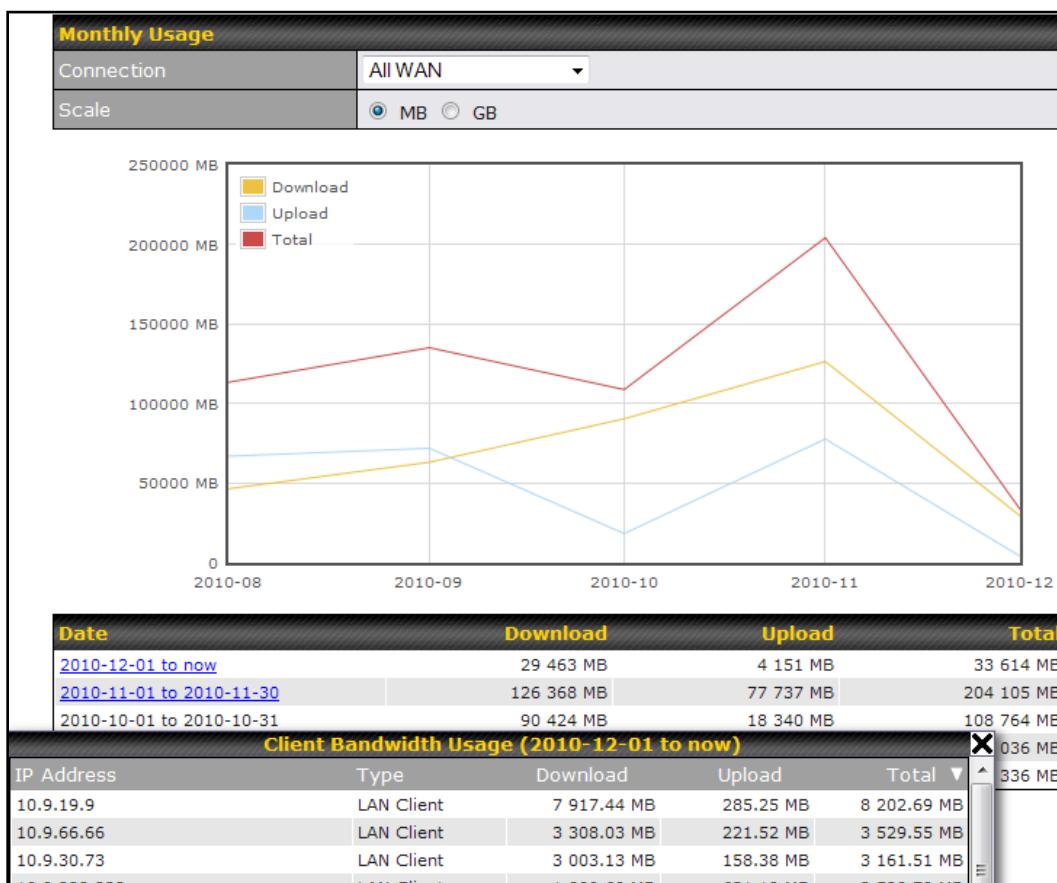
## 25.7.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection.

If you have enabled **Bandwidth Monitoring** feature as shown in section 11.4, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

Click the first two rows to view the client bandwidth usage on the last two months. This feature is not available if you have chosen to view the bandwidth of an individual WAN connection.

The Scale of the graph can be set to show in **Megabyte (MB)** or **Gigabyte(GB)**.



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

## Appendix A. Restoration of Factory Defaults

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

**For Balance 20/30/30 LTE/210/310:**

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

**For Balance 305/380/580/710/1350/2500:**

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

Afterwards, the factory default settings will be restored.

### Important Note

All user settings will be lost after restoring the factory default settings.

Regular backup of configuration parameters is strongly recommended.

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

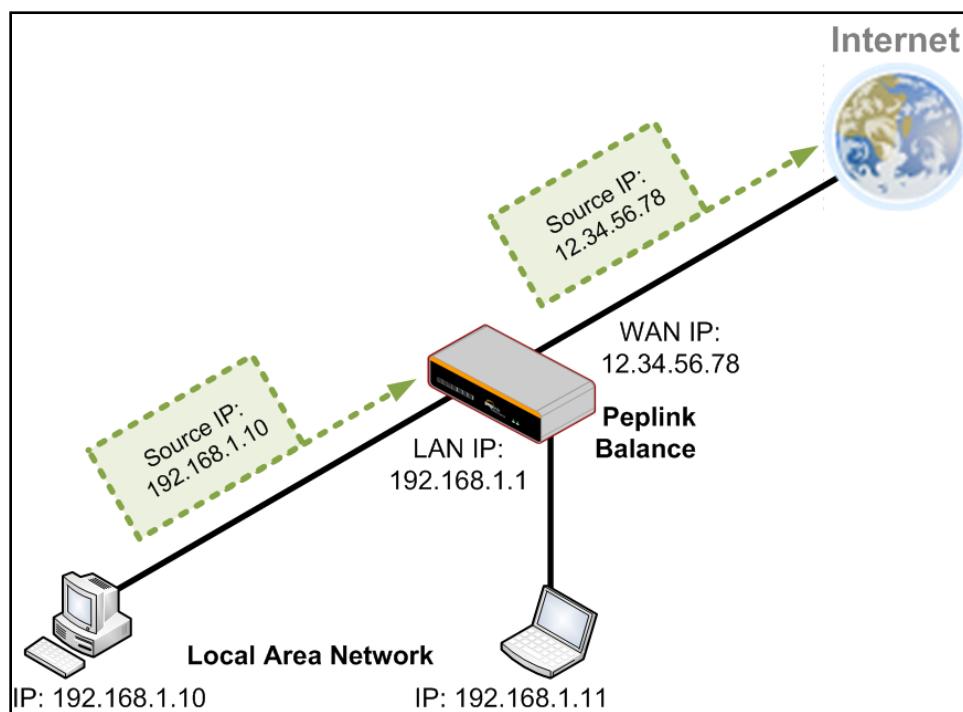
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, and PPPoE.

### B.1 Routing via Network Address Translation (NAT)

When the Peplink Balance is operating under NAT mode, the source IP addresses of outgoing IP packets are translated to the WAN IP address of Peplink Balance. With NAT, all LAN devices share the same WAN IP address to access the Internet (i.e. the WAN IP address of Peplink Balance).

Operating the Peplink Balance in NAT mode requires only one WAN (Internet) IP address. In addition, operating in NAT mode also has security advantages because LAN devices are hidden behind the Peplink Balance. They are not directly accessible from the Internet, and, hence, less vulnerable to attacks.

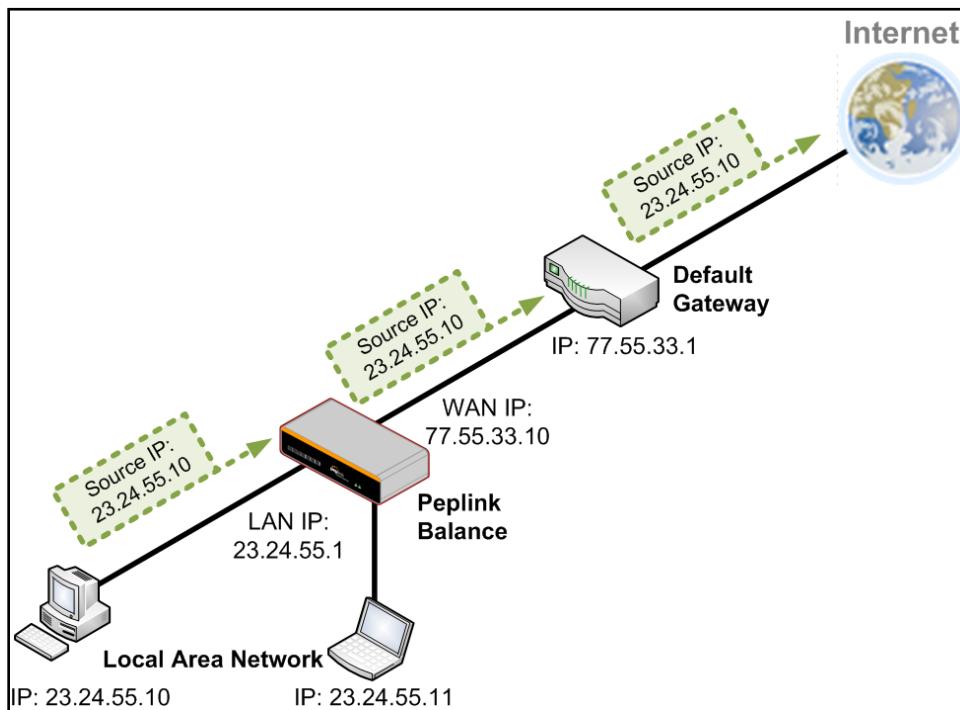
The following figure shows the packet flow in NAT mode:



## B.2 Routing via IP Forwarding

When Peplink Balance is operating under IP Forwarding mode, the IP addresses of IP packets are unchanged; Peplink Balance forwards both inbound and outbound IP packets without changing their IP addresses.

The following figure shows the packet flow in IP Forwarding mode:



## Appendix C. Case Studies

### C.1 Performance Optimization

#### C.1.1 Scenario

In this scenario, email and web browsing are the two main Internet services used by the LAN users. The mail server is external to the network. The connections are ADSL (WAN1, with slow uplink and fast downlink) and Metro Ethernet (WAN2, symmetric).

#### C.1.2 Solution

For optimal performance with this configuration, individually set the WAN load balance according to the characteristics of each service.

- Web browsing mainly downloads data; sending e-mails mainly consumes upload bandwidth.
- Both connection offer good download speeds; WAN2 offers good upload speeds.
- Define WAN1 and WAN2's inbound and outbound bandwidths to be 3M/512k and 4M/4M respectively. This will ensure that outbound traffic is more likely to be routed through WAN2.
- For HTTP, set the weight to 3:4.
- For SMTP, set the weight to 1:8, such that users will have a greater chance to be routed via WAN2 when sending e-mail.

#### C.1.3 Settings

1. Add a new outbound traffic rule for HTTP.
2. Add a new outbound traffic rule for SMTP.

In general, to add a new outbound traffic rule, navigate to **Network > Outbound Policy**.

Click here and Select **Managed by Custom Rules**

Outbound Policy

Managed by Custom Rules

Custom Rules (Drag and drop rows to change rule order)

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

Add Rule

Click **Add Rule** to add a new load distribution rule.

Settings for HTTP:

**Add a New Custom Rule**

New Custom Rule	
Service Name *	SMTP
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Source	Any
Destination	Any
Protocol	TCP ← <b>HTTP</b>
Port *	Single Port <input type="button" value="Port: 80"/>
Algorithm	Weighted Balance
Load Distribution Weight	<div style="display: flex; align-items: center;"> <span>WAN1</span> <input type="button" value="3"/> <span>WAN2</span> <input type="button" value="4"/> <span>WAN3</span> <input type="button" value="0"/> <span>Mobile Internet</span> <input type="button" value="0"/> </div>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Set the weight of WAN1 and WAN2 for HTTP to 3 and 4, respectively

Settings for SMTP:

**Add a New Custom Rule**

New Custom Rule	
Service Name *	SMTP
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Source	Any
Destination	Any
Protocol	TCP ← <b>SMTP</b>
Port *	Single Port <input type="button" value="Port: 25"/>
Algorithm	Weighted Balance
Load Distribution Weight	<div style="display: flex; align-items: center;"> <span>WAN1</span> <input type="button" value="1"/> <span>WAN2</span> <input type="button" value="8"/> <span>WAN3</span> <input type="button" value="0"/> <span>Mobile Internet</span> <input type="button" value="0"/> </div>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Set the weight of WAN1 and WAN2 for SMTP to 1 and 8, respectively

## C.2 Maintaining the Same IP Address throughout a Session

### C.2.1 Scenario

Some IP address sensitive web sites (for example, Internet banking) use both client IP address and cookie matching for session identification. Since load balancing uses different IP addresses, the session is dropped when a mismatching IP is detected resulting in frequent interruptions while visiting such sites.

### C.2.2 Solution

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

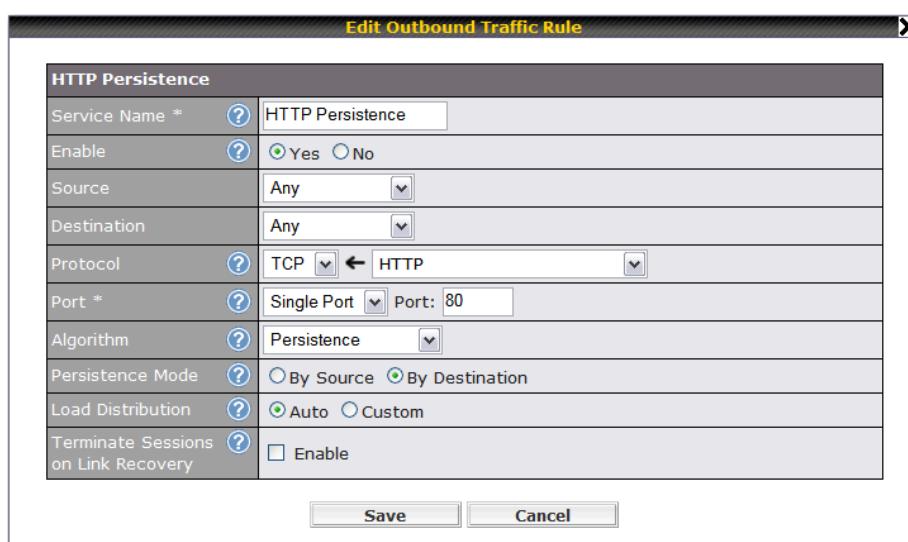
With Persistence is configured and the option **By Source** is selected, Peplink Balance uses a consistent WAN connection for same source IP addresses. This option offers higher application compatibility, but may inhibit the load balancing function unless there are many clients using the internet.

### C.2.3 Settings

Set persistence in:

**Network > Outbound Policy**

Click **Add Rule**, select **HTTP**(TCP port 80) for web service, and select **Persistence**. Click **Save** and then Click **Apply Changes** on the top right corner to complete the process.



#### Tip

A network administrator can use the Traceroute utility to manually analyze the connection path of a particular WAN connection.

## C.3 Bypassing the Firewall to Access Hosts on LAN

### C.3.1 Scenario

There are times when remote access to computers on the LAN is desirable; for example, when hosting web sites, online businesses and FTP download and upload areas, etc.

In such cases, it may be appropriate to create an inbound NAT mapping for the network to allow some hosts on the LAN to be accessible from outside of the firewall.

### C.3.2 Solution

The Web Admin Interface can be used to add an inbound NAT mapping to a host and to bind the host to the WAN connection(s) of your choice. To begin, navigate to **Network>NAT Mappings> AddNAT Rule**

In this example, the host with an IP address of 192.168.1.102 is bound to 211.123.123.100 of WAN1:

LAN Client(s)	?	IP Address								
Address	?	192.168.1.102								
Inbound Mappings	?	<b>Connection / Inbound IP Address(es)</b> <input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> 211.123.123.100 (Interface IP) <input type="checkbox"/> 211.123.123.101  <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> Mobile Internet								
Outbound Mappings	?	<b>Connection / Outbound IP Address</b> <table border="1"><tr><td>WAN1</td><td>211.123.123.100 (Interface IP)</td></tr><tr><td>WAN2</td><td>Interface IP</td></tr><tr><td>WAN3</td><td>Interface IP</td></tr><tr><td>Mobile Internet</td><td>Interface IP</td></tr></table>	WAN1	211.123.123.100 (Interface IP)	WAN2	Interface IP	WAN3	Interface IP	Mobile Internet	Interface IP
WAN1	211.123.123.100 (Interface IP)									
WAN2	Interface IP									
WAN3	Interface IP									
Mobile Internet	Interface IP									

Click **Apply Changes** on the top right corner to complete the process.

## C.4 Inbound Access Restriction

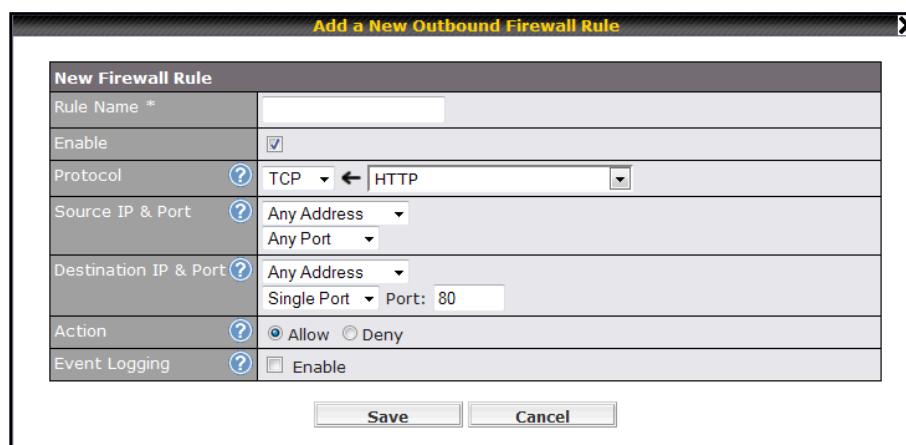
### C.4.1 Scenario

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

### C.4.2 Solution

Firewall functionality is built into the Peplink Balance. By default, inbound access is unrestricted. Enabling a basic level of protection involves setting up firewall rules.

For example, in order to protect your private network from external access, you can set up a firewall rule between the Internet and your private network. To do so, navigate to **Network > Access Rules**. Then click the **Add Rule** button in the **Inbound Firewall Rule** table and change the settings according to the following screenshot:



After the fields have been entered as in the screenshot, click **Save** to add the rule.

Afterwards, change the default inbound rule to **Deny** by clicking the **defaultrule** in the **Inbound Firewall Rule** table. Click **Apply Changes** on the top right corner to complete the process.

## C.5 Outbound Access Restriction

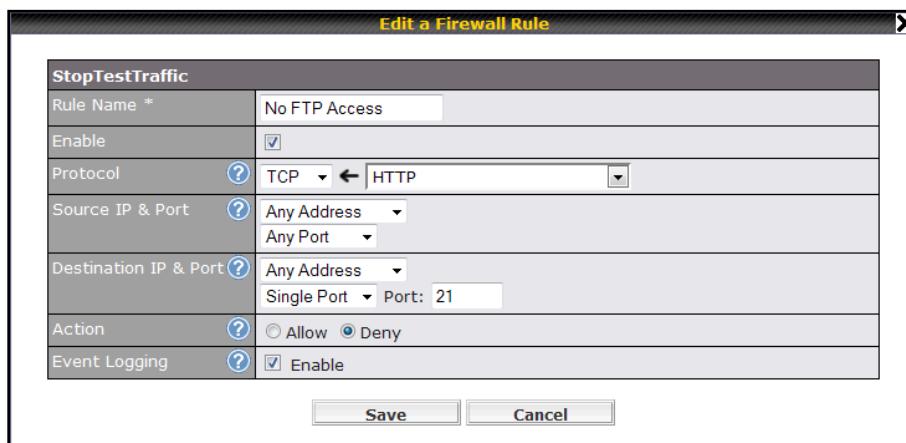
### C.5.1 Scenario

For security reasons, it may be appropriate to restrict outbound access. For example, you may want to prevent LAN users from using ftp to transfer files to and from the Internet.

This can easily be achieved by setting up an outbound firewall rule with Peplink Balance.

### C.5.2 Solution

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



After the fields have been entered as in the screenshot, click **Save** to add the rule. Click **Apply Changes** on the top right corner to complete the process.

## Appendix D. Troubleshooting

### Problem 1

Outbound load is only distributed over one WAN connection.

#### Solution

Outbound load balancing can only be distributed evenly between available WAN connections if many outbound connections are made. If there is only one user on the LAN and only one download session is made from his/her browser, the WAN connections cannot be fully utilized.

For a single user, download management applications are recommended. The applications can split a file into pieces and download the pieces simultaneously. Examples include: DownThemAll (Firefox Extension), iGetter (Mac), etc.

If the outbound traffic is going across the SpeedFusion™ tunnel, (i.e. transferring a file to a VPN peer) the bandwidth of all WAN connections will be bonded. In this case, all bandwidth will be utilized and a file will be transferred across all available WAN connections.

For additional details, please refer to this FAQ:

<http://www.peplink.com/knowledgebase/maximizing-your-wan-connections-without-speedfusion/>

### Problem 2

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

#### Solution

First, check whether all WAN connections are up.

Second, ensure your download manager application has split the file into 3 parts or more.

It is also possible that all of 2 or even 3 download sessions were being distributed to the same link by chance.

### Problem 3

I am using some websites to lookup my public IP address, e.g. [www.whatismyip.com](http://www.whatismyip.com). When I keep pressing the browser's Refresh button, the server almost always returns the same address. The IP address supposed to be changing for every refresh.

#### Solution

The web server has enabled the **Keep Alive** function, which ensures that you use the same TCP session to query the server.

Try to test with a web site that does not enable **Keep Alive**.

For example, try <http://private.dnsstuff.com/tools/aboutyou.ch> (This third-party web site is provided only for reference. Peplink has no association with the site and does not guarantee the site's validity or availability.)

### Problem 4

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

#### Solution

You can test the LAN connection using **Ping**.

For example, if you are using DOS/Windows, at the Command Prompt, type:  
`ping 192.168.1.1`

This pings the Peplink Balance device (provided that Peplink Balance device's IP is 192.168.1.1) to test whether the connection to Peplink Balance is OK.

**Problem 5**

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

**Solution**

You can test the WAN connection by **Ping**, which is similar to problem 4.

As we want to isolate the problems from the LAN, **Ping** will be performed from Peplink Balance. By using the **Ping/Traceroute** under the tab **Status** of the Peplink Balance, you may able to find out the source of problem.

**Problem 6**

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

**Solution**

The Maximum Transmission Unit (MTU) or MSS setting may need to be adjusted.

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

## Appendix E. Product Specifications

### E.1 Peplink Balance 20, 30 and 30 LTE

#### Routing

- Flexible Custom Outbound Routing Policy

#### WAN Support

- DHCP, PPPoE and Static IP
- Outbound Link Load Balance

#### Device Management

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Configurations Upload and Download

#### Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

#### Security

- IPsec (Network-to-Network)
- Compatible with IPsec and PPTP VPNNPassthrough
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Intrusion Detection System

#### Physical Interface

- Two (Balance 20) / Three (Balance 30, 30 LTE) RJ-45 for an IEEE 802.3u 10/100/1000M WAN
- Four RJ-45 for an IEEE 802.3ab 10/100/1000M LAN

#### Power Specification

- DC Input 9-16V

#### Operating Environment

- Kensington Lock Interface
- Temperature: 0°C - 55°C
- Humidity: 10% - 90% (non-condensing)

## E.2 Peplink Balance 210 and 310

### Routing

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### WAN Support

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### Device Management

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### Security

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Bandwidth Bonding SpeedFusion™
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### Physical Interface (Balance 210 Hardware Revision 2)

- Two RJ-45 for an IEEE 802.3u 10/100/1000M WAN
- Four RJ-45 for an IEEE 802.3ab 10/100/1000M LAN

### Physical Interface (Balance 310 Hardware Revision 2)

- Three RJ-45 for an IEEE 802.3u 10/100/1000M WAN
- Four RJ-45 for an IEEE 802.3ab 10/100/1000M LAN

### Power Specification

- DC Input 9-16V

### Operating Environment

- Temperature: 0°C - 65°C
- Humidity: 10% - 90% (non-condensing)

## E.3 Peplink Balance 380

### **Routing**

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### **WAN Support**

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### **Device Management**

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### **Internet Access Sharing**

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### **Security**

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Bandwidth Bonding SpeedFusion™
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### **Physical Interface (Balance 380 Hardware Revision 5)**

- Three RJ-45 for an IEEE 802.3ab 10/100M/1000M WAN
- One RJ-45 for an IEEE 802.3ab 10/100M/1000M LAN
- One RJ-45 Console / Serial Port

### **Power Specification**

- AC input 100-240V

### **Operating Environment**

- Temperature: 0°C - 40°C
- Humidity: 10% - 90% (non-condensing)

## E.4 Peplink Balance 305

### Routing

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### WAN Support

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### Device Management

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### Security

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### Physical Interface

- Three RJ-45 for an IEEE 802.3ab 10/100M/1000M WAN
- One RJ-45 for an IEEE 802.3ab 10/100M/1000M LAN
- One RJ-45 Console / Serial Port

### Power Specification

- AC input 100-240V

### Operating Environment

- Temperature: 0°C - 40°C
- Humidity: 10% - 90% (non-condensing)

## E.5 Peplink Balance 380

### Routing

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### WAN Support

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### Device Management

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### Security

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Bandwidth Bonding SpeedFusion™
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### Physical Interface (Balance 380 Hardware Revision 5)

- Three RJ-45 for an IEEE 802.3ab 10/100M/1000M WAN
- One RJ-45 for an IEEE 802.3ab 10/100M/1000M LAN
- One RJ-45 Console / Serial Port

### Power Specification

- AC input 100-240V

### Operating Environment

- Temperature: 0°C - 40°C
- Humidity: 10% - 90% (non-condensing)

## E.6 Peplink Balance 580

### Routing

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### WAN Support

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### Device Management

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### Security

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Bandwidth Bonding SpeedFusion™
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### Physical Interface

- Five RJ-45 for an IEEE 802.3ab 10/100M/1000M WAN
- One RJ-45 for an IEEE 802.3ab 10/100M/1000M LAN
- One RJ-45 Console / Serial (modem / TA) Port
- LAN Bypass from WAN5 to LAN

### Power Specification

- AC input 100-240V

### Operating Environment

- Temperature: 0°C - 40°C
- Humidity: 10% - 90% (non-condensing)

## E.7 Peplink Balance 710

### Routing

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### WAN Support

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### Device Management

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### Security

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Bandwidth Bonding SpeedFusion™
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### Physical Interface

- Seven RJ-45 for an IEEE 802.3ab 10/100/1000M WAN
- One RJ-45 for an IEEE 802.3ab 10/100/1000M LAN
- One RJ-45 Console / Serial Port

### Power Specification

- AC input 100-240V

### Operating Environment

- Temperature: 0°C - 40°C
- Humidity: 10% - 90% (non-condensing)

## E.8 Peplink Balance 1350

### **Routing**

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### **WAN Support**

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### **Device Management**

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### **Internet Access Sharing**

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### **Security**

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Bandwidth Bonding SpeedFusion™
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### **Physical Interface**

- Thirteen RJ-45 for an IEEE 802.3ab 10/100/1000M WAN
- One RJ-45 for an IEEE 802.3ab 10/100/1000M LAN
- One RJ-45 Console / Serial (modem / TA) Port
- LAN Bypass from WAN1 to LAN

### **Power Specification**

- AC input 100-240V

### **Operating Environment**

- Temperature: 0°C - 40°C
- Humidity: 10% - 90% (non-condensing)

## E.9 Peplink Balance 2500

### Routing

- Drop-in Mode and NAT
- Flexible Custom Outbound Routing Policy

### WAN Support

- DHCP, PPPoE and Static IP
- Inbound and Outbound Link Load Balance

### Device Management

- Wizard & Menu Driven Web Management Interface over HTTP / HTTPS
- Remote Reporting and Management
- Bandwidth Usage Monitor
- Configurations Upload and Download

### Internet Access Sharing

- SUA (Single User Account) / Multi-to-Multi NAT
- NAT supports PAT (Port Address Translation)

### Security

- PPTP VPN Server
- IPsec (Network-to-Network)
- Rules-based Stateful Firewall, with IP, Protocol, and Port filtering
- Bandwidth Bonding SpeedFusion™
- VPN Encryption: 256-bit AES
- Intrusion Detection System

### Physical Interface

- Twelve RJ-45 for an IEEE 802.3ab 10/100/1000M WAN
- Eight RJ-45 for an IEEE 802.3ab 10/100/1000M LAN /Two SFP+ for an IEEE 802.3ae 10G LAN
- One RJ-45 Console / Serial Port

### Power Specification

- AC input 100-240V

### Operating Environment

- Temperature: 0°C - 40°C
- Humidity: 10% - 90% (non-condensing)

## Appendix F. Declaration

### 1. CAUTION:

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

### 2. Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

### 3. Radiation Exposure Statement (for Balance One):

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 22cm between the radiator & your body.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.



What are we doing at the moment?  
Follow us on [Twitter!](#)  
<http://twitter.com/Peplink>



Want to know more about us?  
Add us on [Facebook!](#)  
<http://www.facebook.com/peplink>



Difficulties when configuring the device?  
Visit our [YouTube Channel!](#)  
<http://www.youtube.com/PeplinkChannel>



Anything want to share with everyone?  
Discuss on [Peplink Forum!](#)  
<http://forum.peplink.com>

#### Contact Us:

**Sales**  
<http://www.peplink.com/contact/sales/>

**Support**  
<http://www.peplink.com/contact/>

**Certified Peplink Partner**  
<http://www.peplink.com/partners/channel-partner-program/>

#### Contact Address:

**United States Office**  
800 West El Camino Real,  
Mountain View  
CA 94040  
United States  
Tel: +1 (650) 450 9668  
Fax: +1 (866) 625 4664

**Italy Office**  
Via Sismondi 50/3  
20133 Milan  
Italy  
Tel: +39 02 8986 6852

**South Africa Office**  
Unit 24, Cambridge Office  
Park, 5 Bauhinia Street,  
Highveld, Centurion,  
South Africa  
Tel: +27 12 665 5829

**Hong Kong Office**  
A5, 5/F, HK Spinners  
Industrial Building, Phase 6,  
481 Castle Peak Road,  
Cheung Sha Wan, Hong  
Kong  
Tel: +852 2990 7600  
Fax: +852 3007 0588

**Saudi Arabia Office**  
3/F, Saudi Business Center,  
Jeddah,  
Saudi Arabia  
Tel: +39 02 8986 6852