

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

Algorithm	?	Priority	▼
Priority Order	?	Highest Priority	Not In Use
		WAN: WAN 1	VPN: FL_Office
		WAN: WAN 2	VPN: NY_Office
		WAN: WAN 3	
		WAN: Mobile Internet	
		Lowest Priority	

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

Tip

Configure multiple distribution rules to accommodate different kinds of services.

17.2.5 Algorithm: Overflow

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

Algorithm	?	Overflow	▼
Overflow Order	?	Highest Priority	
		WAN: WAN 1	
		WAN: WAN 2	
		WAN: WAN 3	
		WAN: Mobile Internet	
		Lowest Priority	

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

17.2.6 Algorithm: Least Used

Algorithm	(?)	Least Used ▾
Connection		<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> Mobile Internet

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

17.2.7 Algorithm: Lowest Latency

Algorithm	(?)	Lowest Latency ▾
Connection		<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> Mobile Internet

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

Tip

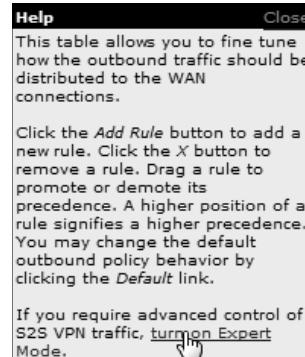
The round trip time of a 6M down /640k uplink can be higher than that of a 2M down /2M up link because the overall round trip time is lengthened by its slower upload bandwidth, despite its higher downlink speed. Therefore, this algorithm is good for two scenarios:

- All WAN connections are symmetric; or
- A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN's available bandwidth.

17.2.8 Expert Mode

Expert Mode is available for advanced users. To enable the feature, click on the help icon beside the **Rules** menu and click **turn on Expert Mode**.

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



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

Custom Rules (Drag and drop rows to change rule order) ?					
Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persis...	Persistence (Src) (Auto)	Any	IP Network 192.168.50.0/24	TCP 443	X
Site-to-Site VPN Routes					
Default	Lowest Latency				
Add Rule					

18 Inbound Access

Inbound access is also known as inbound port address translation. On a NAT WAN connection, all inbound traffic to the server behind the Peplink unit requires inbound access rules.

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

Important Note

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

18.1 Definition of Servers on LAN

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

Inbound connections from the Internet will be forwarded to the specified Inbound IP address(es) based on the protocol and port number. When more than one server is defined, requests will be distributed to the servers in the weight ratio specified for each server.



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

Server Name	myserver
IP Address	192.168.1.123

Save Cancel

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



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

18.2 Definition of Port Forwarding

Inbound port forwarding rules are defined at **Network>Inbound Access>Services**.

Service	IP Address(es)	Server	Protocol	Action
Web	WAN1: Interface IP	192.168.10.1	TCP:80	Delete
Add Service				

To define a new service, click the **Add Service** button after adding a server under **Network>Inbound Access>Service**. The following screen is displayed:

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Service Name *	Web
IP Protocol	<input type="button" value="TCP"/> <input type="button" value="HTTP"/>
Port	<input type="button" value="Single Port"/> <input type="button" value="Range Port"/> Service Port: 80
Inbound IP Address(es) * <small>(Require at least one IP address)</small>	<input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> 218.100.66.100 (Interface IP) <input type="checkbox"/> 218.100.66.66 <input type="checkbox"/> 218.100.66.103 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> Mobile Internet
Server IP Address	192.168.1.10
<small>* Required Fields</small> <div style="text-align: center;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </div>	

Port Forwarding Settings

Enable	This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Peplink Balance based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Peplink Balance disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.
IP Protocol	<p>The IP Protocol setting, along with the Port setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Peplink Balance via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the Servers setting. Please see below for details on the Port and Servers settings.</p> <p>Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.) After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remain manually modifiable.</p>

The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:

Any Port, Single Port, Port Range, Port Map, and Range Mapping

Port

?

Any Port

Any Port: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.

Port

?

Single Port

Service Port: 80

Single Port: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port 80**, TCP traffic received on port 80 is forwarded to the configured servers via port 80.

Port

?

Port Range

Service Ports: 80 - 88

Port

Port Range: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports 80-88**, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.

Port

?

Port Mapping

Service Port: 80

Map to Port: 88

Port Mapping: traffic that is received by Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. For example, with IP Protocol set to **TCP**, and Port set to **Port Mapping**, **Service Port 80**, and **Map to Port 88**, TCP traffic on Port 80 is forwarded to the configured servers via Port 88.

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

Port

?

Range Mapping

Service Ports: 80 - 88

Map to Ports: 88 - 96

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

Inbound IP Address(es)

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

Server IP Address

This setting specifies the LAN IP address of the server that handles the requests for the service.

18.3 Inbound Access Services

18.3.1 Definition of Services

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

Service	IP Address(es)	Server	Protocol
No Services Defined			
Add Service			

Tip

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

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

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No																
Service Name	Web																
IP Protocol	<input style="width: 40px; height: 20px; border: none; background-color: transparent; font-size: small; padding: 0; margin: 0;" type="button" value="TCP"/> <input style="width: 150px; height: 20px; border: none; background-color: transparent; font-size: small; padding: 0; margin: 0;" type="button" value=":: Protocol Selection Tool ::"/>																
Port	<input style="width: 100px; height: 20px; border: none; background-color: transparent; font-size: small; padding: 0; margin: 0;" type="button" value="Single Port"/> Service Port: 80																
Inbound IP Address(es) (Require at least one IP address)	<div style="border: 1px solid #ccc; padding: 5px; width: 300px;"> <p>Connection / IP Address(es)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10px; vertical-align: middle;"><input checked="" type="checkbox"/></td> <td style="vertical-align: middle;">WAN 1</td> <td style="width: 10px; vertical-align: middle;"><input checked="" type="checkbox"/></td> <td style="vertical-align: middle;">10.88.3.184 (Interface IP)</td> </tr> <tr> <td><input type="checkbox"/></td> <td>WAN 2</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>WAN 3</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>Mobile Internet</td> <td><input type="checkbox"/></td> <td></td> </tr> </table> </div>	<input checked="" type="checkbox"/>	WAN 1	<input checked="" type="checkbox"/>	10.88.3.184 (Interface IP)	<input type="checkbox"/>	WAN 2	<input type="checkbox"/>		<input type="checkbox"/>	WAN 3	<input type="checkbox"/>		<input type="checkbox"/>	Mobile Internet	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	WAN 1	<input checked="" type="checkbox"/>	10.88.3.184 (Interface IP)														
<input type="checkbox"/>	WAN 2	<input type="checkbox"/>															
<input type="checkbox"/>	WAN 3	<input type="checkbox"/>															
<input type="checkbox"/>	Mobile Internet	<input type="checkbox"/>															
Included Server(s) (Require at least one IP address)	<div style="border: 1px solid #ccc; padding: 5px; width: 300px;"> <p>Server</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10px; vertical-align: middle;"><input checked="" type="checkbox"/></td> <td style="vertical-align: middle;">myserver (192.168.1.123)</td> <td style="width: 10px; vertical-align: middle; text-align: right;">Weight 10</td> <td style="vertical-align: middle; text-align: right;"><input style="width: 20px; height: 20px; border: none; background-color: transparent; font-size: small; padding: 0; margin: 0;" type="button" value="..."/></td> </tr> </table> </div>	<input checked="" type="checkbox"/>	myserver (192.168.1.123)	Weight 10	<input style="width: 20px; height: 20px; border: none; background-color: transparent; font-size: small; padding: 0; margin: 0;" type="button" value="..."/>												
<input checked="" type="checkbox"/>	myserver (192.168.1.123)	Weight 10	<input style="width: 20px; height: 20px; border: none; background-color: transparent; font-size: small; padding: 0; margin: 0;" type="button" value="..."/>														

Services Settings

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

The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:

Any Port, Single Port, Port Range, Port Map, and Range Mapping

Port	?	Any Port
------	---	----------

Any Port: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the **Servers** setting.

For example, if **IP Protocol** is set to **TCP** and **Port** is set to **Any Port**, then all TCP traffic will be forwarded to the configured servers.

Port	?	Single Port	Service Port: 80
------	---	-------------	------------------

Single Port: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting.

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

Port	?	Port Range	Service Ports: 80 - 88
------	---	------------	------------------------

Port

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

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

Port	?	Port Mapping	Service Port: 80
			Map to Port: 88

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

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

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

Port	?	Range Mapping	Service Ports: 80 - 88
			Map to Ports: 88 - 96

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

Inbound IP Address(es)

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

Included Server(s)

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

Example:

With the following weight settings on a Peplink Balance:

- demo_server_1: 10
- demo_server_2: 5

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

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

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

18.3.2 UPnP / NAT-PMP SETTINGS

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

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

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



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

Save

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

18.3.3 Definition of DNS Records

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

For example:

(This example is for illustration only; the actual resolution that takes place in implementation will likely be different.)

The DNS resolution of the domain name www.mycompany.com is delegated to the WAN2 Internet IP addresses of the Peplink Balance.

Upon receiving the DNS query, the Peplink Balance returns (as an "A" record) the IP address for www.mycompany.com on WAN1 because WAN1 is the most appropriate healthy link.

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

DNS Server		Disabled	
Zone Transfer		Disabled	
Default SOA / NS		Undefined	
Default Connection Priority			
Priority 1: WAN 1, WAN 2, WAN 3, WAN 4, WAN 5, WAN 6, WAN 7, WAN 8, WAN 9, WAN 10, WAN 11, WAN 12, Mobile Internet			
Domain Names			
Domain Name			
These is currently no DNS domains.			
New Domain Name			
Reverse Lookup Zones			
Zone Name			
There is currently no Reverse Lookup Zones.			
New Reverse Lookup Zone			

[Import records via zone transfer...](#)

DNS Settings

This setting specifies the WAN IP addresses on which the DNS server of the Peplink Balance should listen.

If no addresses are selected, the inbound link load balancing feature will be disabled and the Peplink Balance will not respond to DNS requests.

To specify and/or modify the IP addresses on which the DNS server should listen, click the button that corresponds to **DNS Server**, and the following screen is displayed:

DNS Servers	
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> Interface IP
<input type="checkbox"/> WAN 2	
<input type="checkbox"/> WAN 3	
<input type="checkbox"/> WAN 4	
<input type="checkbox"/> WAN 5	
<input type="checkbox"/> WAN 6	
<input type="checkbox"/> WAN 7	
<input type="checkbox"/> WAN 8	
<input type="checkbox"/> WAN 9	
<input type="checkbox"/> WAN 10	
<input type="checkbox"/> WAN 11	
<input type="checkbox"/> WAN 12	
<input type="checkbox"/> Mobile Internet	

Save **Cancel**

DNS Servers

To specify the Internet IP addresses on which the DNS server should listen, select the desired WAN connection then select the desired associated IP addresses. (Multiple items in the list can be selected by holding CTRL and clicking on the items.)

Click **Save** to save the settings when configuration is complete.

Zone Transfer

This setting specifies the IP address(es) of the secondary DNS server(s) authorized to retrieve zone records from the DNS server of the Peplink Balance.

The zone transfer server of the Peplink Balance listens on TCP port 53.

Zone Transfer Settings	
Enable	<input checked="" type="checkbox"/>
Allowed Clients	
11.12.13.123	<input type="button" value="x"/>
	<input type="button" value="+"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

The Peplink Balance serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing its LAN interface.

Routing Control by Subnet Database

When this function is enabled, the system will check to see if an incoming DNS client is within any WAN's ISP subnet. Only the matched WAN(s)'s IP addresses will be returned. Note that this feature is available only when a subnet database has been defined.

Default SOA / NS

Click the  button to define a default SOA / NS record for all domain names. For configuration details please refer to **Section 18.3.5**.

Default SOA Record	
Name Server	<input type="text" value="ns1"/>
Name Server IP Address	<input type="text"/>
Email	<input type="text" value="webmaster"/>
Refresh (sec)	<input type="text" value="16384"/>
Retry (sec)	<input type="text" value="2048"/>
Expire (sec)	<input type="text" value="1048576"/>
Min Time (sec)	<input type="text" value="2560"/>
TTL (sec)	<input type="text" value="3600"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

When defining a default SOA record, **Name Server IP Address** is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain.

For defining default NS records, the host *[domain]* indicates that this record is for the domain name itself without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the **Host** field left empty. When the entered name server is a fully qualified domain name (FQDN), the **IP Address** field will be disabled.

Default Connection Priority

Default Connection Priority defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the **Connection Priority** set to **Default**. Please refer to **Section 18.3.9** for details.

The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable.

To specify the primary and backup connections, click the  button that corresponds to **Default Connection Priority**. The following screen will appear:

Default Connection Priority

Connection	Priority
WAN 1	1 (Highest) ▾
WAN 2	1 (Highest) ▾
WAN 3	1 (Highest) ▾
WAN 4	1 (Highest) ▾
WAN 5	1 (Highest) ▾
WAN 6	1 (Highest) ▾
WAN 7	1 (Highest) ▾
WAN 8	1 (Highest) ▾
WAN 9	1 (Highest) ▾
WAN 10	1 (Highest) ▾
WAN 11	1 (Highest) ▾
WAN 12	1 (Highest) ▾
Mobile Internet	1 (Highest) ▾

Save **Cancel**

Each WAN connection is associated with a priority number. Click **Save** to save the settings when configuration is complete.

Domain name

This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its “NS”, “MX” and “TXT” records, and its sub-domains’ “A” and “CNAME” records. Add a new record by clicking the **New Domain Name** button. Click on a domain name to edit. Press  to remove a domain name.

18.3.4 Creating DNS Records

To create new DNS records for a domain, perform the following steps:

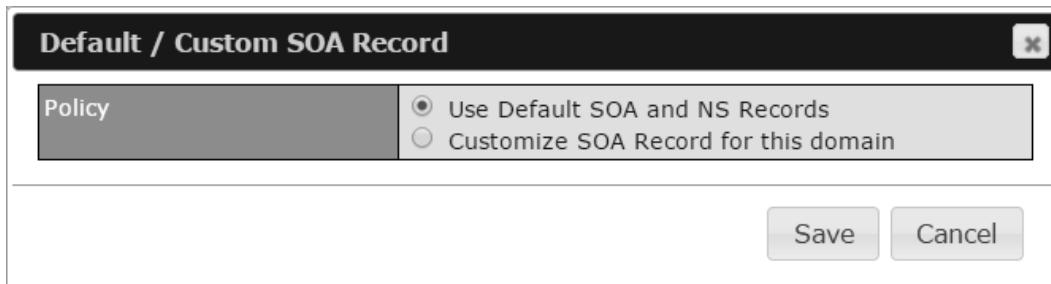
From **Network>Inbound Access>DNS Settings**, click **New Domain Name** in the **Domain Name** field. Then click on the newly created domain name and the following screen will be displayed:

The screenshot shows the DNS Settings interface for a domain named "peplink.com". It consists of seven tabs, each with a "New [Record Type] Records" button:

- SOA Record**: Use Default SOA and NS Records
- NS Records**: Host | Name Server | TTL (sec)
There is currently no NS records.
- MX Records**: Host | Priority | Mail Server | TTL (sec)
There is currently no MX records.
- CNAME Records**: Host | Points To | TTL (sec)
There is currently no CNAME records.
- A Records**: Host | Included IP Address(es) | TTL (sec)
There is currently no A records.
- TXT Records**: Host | TXT Value | TTL (sec)
There is currently no default TXT records.
- SRV Records**: Service | Priority | Weight | Target | Port | TTL (sec)
There is currently no SRV records

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

18.3.5 SOA Records



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

Name Server	(?)	ns1
Name Server IP Address	(?)	
Email	(?)	webmaster
Refresh (sec)	(?)	14400
Retry (sec)	(?)	900
Expire (sec)	(?)	1209600
Min Time (sec)	(?)	3600
TTL (sec)	(?)	3600

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

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

Default values are set for SOA and NS records,

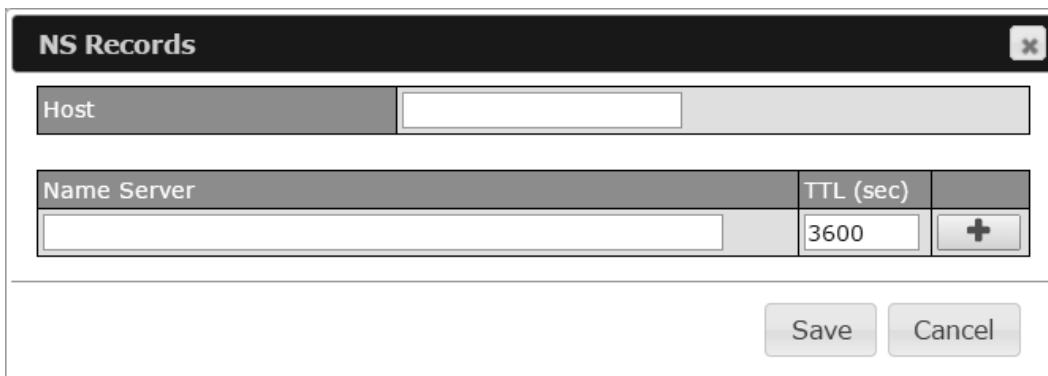
- **Name Server IP Address:** This is the IP address of the authoritative name server. An entry in this field is optional. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically. If it is left blank, the A record for the name server must be created manually.

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

18.3.6 NS Records

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

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



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

Save Cancel

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

Enter a name server host name and its IP address into the corresponding boxes. The host name can be a non-FQDN (fully qualified domain name). Please be sure that a corresponding A record is created. Click the button on the right to finish and to add other name servers. Click the **Save** button to save your changes.

18.3.7 MX Records

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

The dialog box is titled "MX Records". It contains a table with three columns: "Priority", "Mail Server", and "TTL (sec)". A "Host" input field is positioned above the table. At the bottom right are "Save" and "Cancel" buttons.

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

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

For each record, **Priority** and **Mail Server** name must be entered. **Priority** typically ranges from 10 to 100. Smaller numbers have a higher priority. After finishing adding MX records, click the **Save** button.

18.3.8 CNAME Record

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

The dialog box is titled "CNAME Record". It contains a table with three columns: "Host", "Points To", and "TTL (sec)". A "Host" input field is positioned above the table. At the bottom right are "Save" and "Cancel" buttons.

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

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

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

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

18.3.9 A Record

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

A Record

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

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

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

	<p>recovery, this value should be set to a smaller value, e.g., 5 secs, 60 secs, etc.</p>
Priority	<p>This option specifies the priority of different connections. Select the Default option to apply the Default Connection Priority (refer to the table shown on the main DNS settings page) to an A record. To customize priorities, choose the Custom option and a priority selection table will be shown at the bottom.</p>
Included IP Address(es)	<p>This setting specifies lists of WAN-specific Internet IP addresses that are candidates to be returned when the Peplink Balance responds to DNS queries for the domain name specified by Host Name. The IP addresses listed in each box as default are the Internet IP addresses associated with each of the WAN connections. Static IP addresses that are not associated with any WAN can be entered into the Custom IP list. A PTR record is also created for each custom IP.</p> <p>For WAN connections that operate under drop-in mode, there may be other routable IP addresses in addition to the default IP address. Therefore, the Peplink Balance allows custom Internet IP addresses to be added manually via filling the text box on the right-hand side and clicking the  button.</p> <p>Only the checked IP addresses in the lists are candidates to be returned when responding to a DNS query.</p> <p>If a WAN connection is down, the corresponding set of IP addresses will not be returned. However, the IP addresses in the Custom IP Address field will always be returned.</p> <p>If the Connection Priority field is set to Custom, you can also specify the usage priority of each WAN connection. Only selected IP address(es) of available connection(s) with the highest priority, and custom IP addresses will be returned. By default, Connection Priority is set to Default.</p>

18.3.10 PTR Records

PTR records are created along with A records pointing to custom IPs. Please refer to **Section 18.3.9** for details. For example, if you created an A record `www.mydomain.com` pointing to `11.22.33.44`, then a PTR record `44.33.22.11.in-addr.arpa` pointing to `www.mydomain.com` will also be created. When there are multiple host names pointing to the same IP address, only one PTR record for the IP address will be created. In order for PTR records to function, you also need to create NS records. For example, if the IP address range `11.22.33.0` to `11.22.33.255` is delegated to the DNS server on the Peplink Balance, you will also have to create a domain `33.22.11.in-addr.arpa` and have its NS records pointing to your DNS server's (the Peplink Balance's) public IP addresses. With the above records created, the PTR record creation is complete.

18.3.11 TXT Records

This table shows the TXT record of the domain name.

The dialog box is titled "TXT Record". It contains three input fields: "Host" (blank), "TXT Value" (empty text area), and "TTL (sec)" with the value "3600". At the bottom are "Save" and "Cancel" buttons.

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

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

The maximum size of the TXT Value is 255 bytes.

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

18.3.12 SRV Records

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

The dialog box is titled "SRV Records". It has a "Service" field (empty) and a table for adding records. The table columns are: Priority, Weight, Target, Port, TTL (sec). A "+" button is at the bottom right of the table. At the bottom are "Save" and "Cancel" buttons.

- **Service:** The symbolic name of the desired service.
- **Priority:** Indicates the priority of the target; the smaller the value, the higher the priority.
- **Weight:** A relative weight for records with the same priority.
- **Target:** The canonical hostname of the machine providing the service.
- **Port:** Enter the TCP or UDP port number on which the service is to be found.

Domain Delegation

These are the steps to follow when you host your domain at an ISP or domain registrar and want to delegate a sub-domain to be resolved and managed by the Peplink Balance.

- Click the **New Domain Name** button to add a domain name (e.g., *www.mycompany.com*). Click the corresponding domain name to view and edit record details.



The screenshot shows a table titled "Domain Names". It has one row with a "Domain Name" field containing "peplink.com". There is a delete icon next to the entry and a "New Domain Name" button at the bottom.

- Create SOA/NS records named *ns1*, *ns2*, etc. The IP addresses are the Balance's DNS server addresses.



The screenshot shows two tables. The top table is titled "SOA Record" and has a "Name Server" column with "ns1" and a "Details" column with various DNS parameters. The bottom table is titled "NS Records" and has a "Host" column with "peplink.com." and a "Name Server" column with "ns1". Both tables have "TTL (sec)" and "(SOA)" columns.

- Then create an A record with an empty host name.

A Record

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

A Records			
Host	Included IP Address(es)	TTL (sec)	
ns1	220.246.168.80	3600	(SOA)
<input type="button" value="New A Record"/>			

If ISC BIND 8 or 9 is being utilized in the zone file mycompany.com, add the following lines:

```
www           IN      NS      balancewan1
www           IN      NS      balancewan2
balancewan1   IN      A       202.153.122.108
balancewan2   IN      A       67.38.212.18
```

202.153.122.108 and 67.38.212.18 represent the WAN1 and WAN2 Internet IP addresses of the Peplink Balance, respectively. The values of the IP addresses are fictitious and for illustration only.

Hosting the complete domain at Peplink Balance

To host your own DNS server, contact the DNS registrar to have the NS records of the domain (e.g., *mycompany.com*) point to your Balance's WAN IP addresses. Then follow these instructions:

1. Under **Network>Inbound Access>DNS Settings**, create a new domain (e.g., *mycompany.com*).
2. Create NS records named *ns1*, *ns2*, etc. The IP addresses are the Balance's DNS server addresses (same

as above).

3. Create the corresponding A, CNAME, MX, and TXT records as you wish. The A record resembles the one below:

A Records			
Host	Included IP Address(es)	TTL (sec)	
www	WAN1:default WAN2:default	3600	
New A Record			

Testing the DNS Configuration

The following steps can be used to test the DNS configuration:

From a host on the Internet, use an IP address of the Peplink Balance and nslookup to lookup the corresponding host name. Check the information that is returned for the expected results.

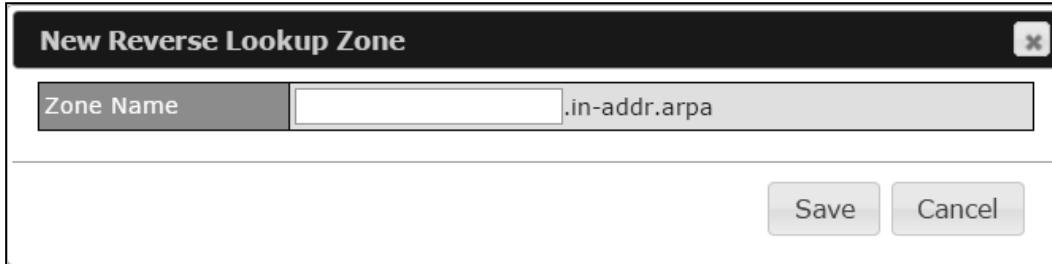
An nslookup in Windows will appear as follows:

```
C:\Documents and Settings\User Name>nslookup
Default Server: ns1.myisp.com
Address: 147.22.11.2
>server 202.153.122.108 (This is Peplink Balance's WAN IP address.)
Default Server: balance.mycompany.com
Address: 202.153.122.108
>www.mycompany.com (This is the hostname to be looked up.)
Default Server: balance.mycompany.com
Address: 202.153.122.108
Name: www.mycompany.com
Address: 202.153.122.109, 67.38.212.19
```

Please note that the values of the IP addresses are fictitious and for illustration only.

18.4 Reverse Lookup Zones

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



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

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

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

- Create a reverse lookup zone that corresponds to the subnet network address of the host.
In the reverse lookup zone, add a pointer (PTR) resource record that maps the host IP address to the host name.
- Click the **New Reverse Lookup Zone** button and enter a reverse lookup zone name. If you are delegated the subnet 11.22.33.0/24, the **Zone Name** should be 33.22.11.in-arpa.addr. PTR records for 11.22.33.1, 11.22.33.2, ... 11.22.33.254 should be defined in this zone where the host IP numbers are 1, 2, ... 254, respectively.



18.4.1 SOA Record

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

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

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

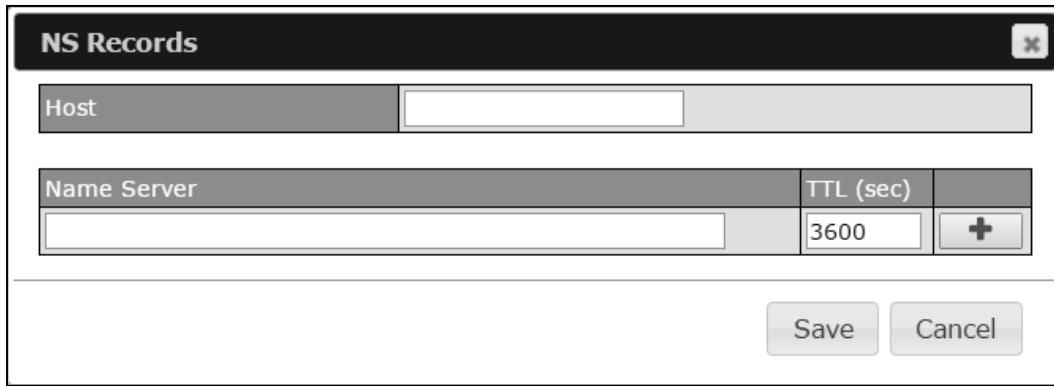
For example:

"ns1.mydomain.com" (equivalent to "www.1stdomain.com.")
 "ns2.mydomain.com."

Email, Refresh, Retry, Expire, Min Time, and TTL are entered in the same way as in

the forward zone. Please refer to **Section 18.3.5** for details.

18.4.2 NS Records

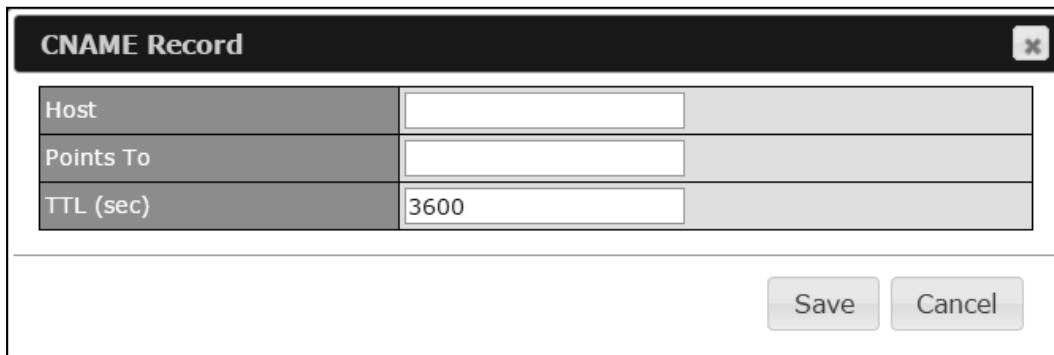


The screenshot shows a software interface titled "NS Records". It contains two main sections: "Host" and "Name Server". The "Host" section has a single input field. The "Name Server" section has two input fields: "Name Server" and "TTL (sec)". A "Save" and "Cancel" button are located at the bottom right.

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

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

18.4.3 CNAME Records



The screenshot shows a software interface titled "CNAME Record". It contains three main sections: "Host", "Points To", and "TTL (sec)". The "Host" and "Points To" sections each have a single input field. The "TTL (sec)" section has a single input field containing the value "3600". A "Save" and "Cancel" button are located at the bottom right.

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

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

18.4.4 PTR Records

The screenshot shows a window titled "PTR Record". It contains three input fields: "Host IP Number" (empty), "Points To" (empty), and "TTL (sec)" with the value "3600". At the bottom right are "Save" and "Cancel" buttons.

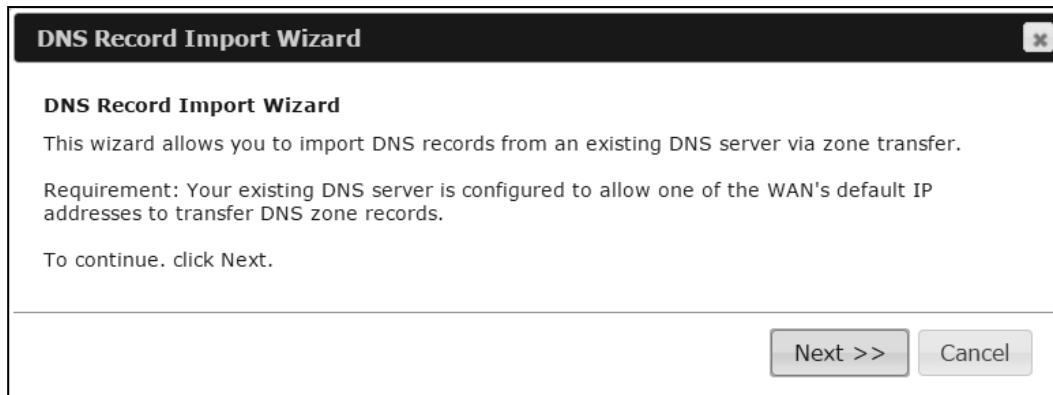
To create a new PTR record, click the **New PTR Record** button.

For **Host IP Number** field, enter the last integer in the IP address of a PTR record. For example, for the IP address 11.22.33.44, where the reverse lookup zone is 33.22.11.in-arpa.addr, the **Host IP Number** should be 44.

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

18.5 DNS Record Import Wizard

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



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



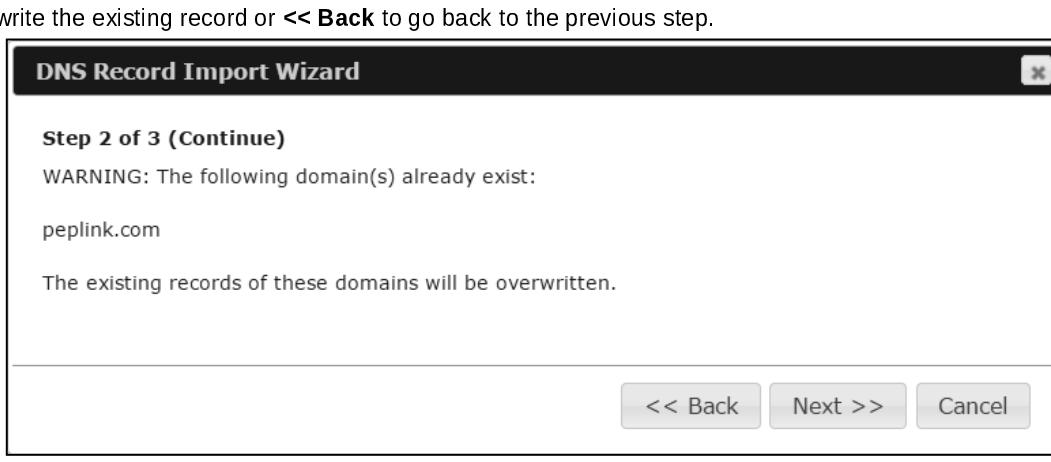
- In the **Target DNS Server IP Address** field, enter the IP address of the DNS server.
- In the **Transfer via...** field, choose the connection which you would like to transfer through.
- Select **Next >>** to continue.

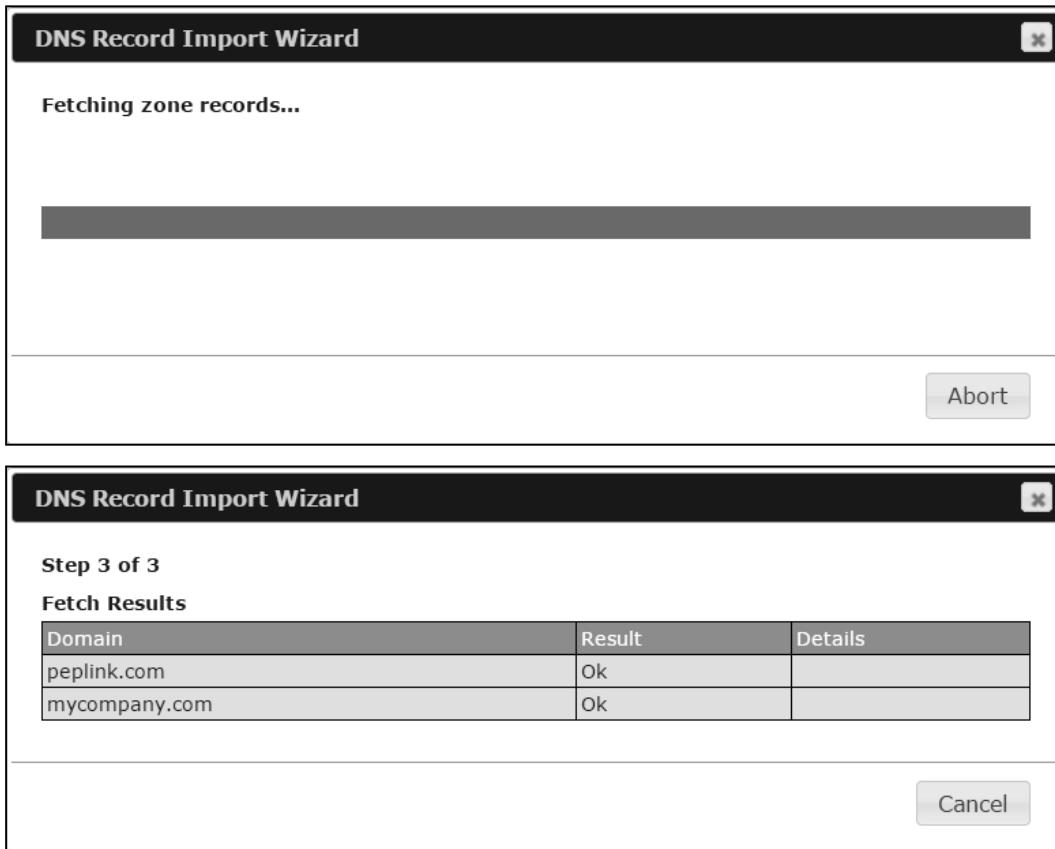


- In the blank space, enter the **Domain Names (Zones)** which you would like to assign the IP address entered in the previous step. Enter one domain name per line.
- Select **Next >>** to continue.

Important Note

If you have entered domain(s) which already exist in your settings, a warning message will appear. Select **Next >>** to overwrite the existing record or **<< Back** to go back to the previous step.





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

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

19 NAT Mappings

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

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

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

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

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

NAT Mapping Settings

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

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

Important Note

Inbound firewall rules override inbound mapping settings.

20 Captive Portal

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

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

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

This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:

LDAP Server

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

Fill in the necessary information to complete your connection to the server and enable authentication.

Access Quota

Set a time and data cap to each user's Internet usage.

Quota Reset Time

This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.

Allowed Networks

To whitelist a network, enter the domain name / IP address here and click  . To delete an existing network from the list of allowed networks, click the  button next to the listing.

Allowed Clients

To whitelist a client, enter the MAC address / IP address here and click  . To delete an existing client from the list of allowed clients, click the  button next to the listing.

Splash Page

Here, you can choose between using the Balance's built-in captive portal and redirecting clients to a URL you define.

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

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

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

21 QoS

21.1 User Groups

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

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

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

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

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

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

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

21.2 Bandwidth Control

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

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

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

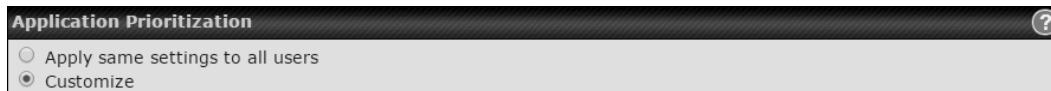
You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Managers. By default, download and upload bandwidth limits are set to unlimited (set as **0**).

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

21.3 Application

21.3.1 Application Prioritization

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



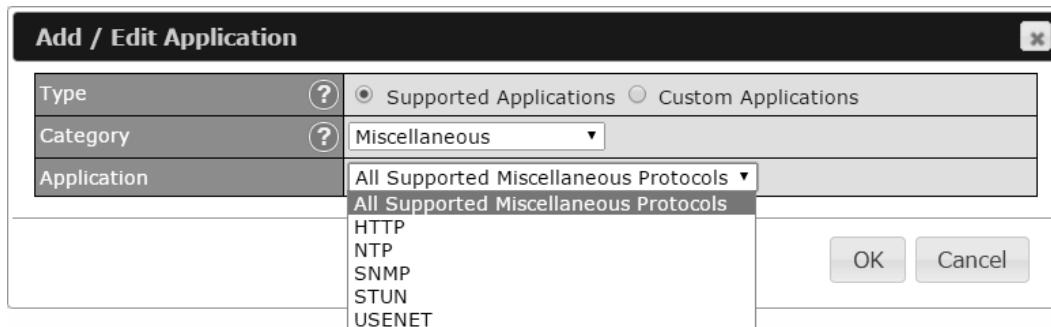
Three priority levels can be set for application prioritization: **↑ High**, **— Normal**, and **↓ Low**. The Peplink Balance can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually.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

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

21.3.2 Prioritization for Custom Application

Click the **Add** button to define a custom application. Click the button  in the **Action** column to delete the custom application in the corresponding row.

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



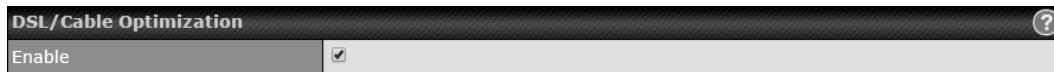
Type	<input type="radio"/> Supported Applications <input checked="" type="radio"/> Custom Applications
Category	Miscellaneous
Application	All Supported Miscellaneous Protocols HTTP NTP SNMP STUN USENET
OK Cancel	

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

21.3.3 DSL/Cable Optimization

DSL/cable-based WAN connections have lower upload bandwidth and higher download bandwidth.

When a DSL/cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data at full speed until the uplink becomes less congested. **DSL/Cable Optimization** can relieve such an issue. When it is enabled, the download speed will become less affected by the upload traffic. By default, this feature is enabled.



22 Firewall

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

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

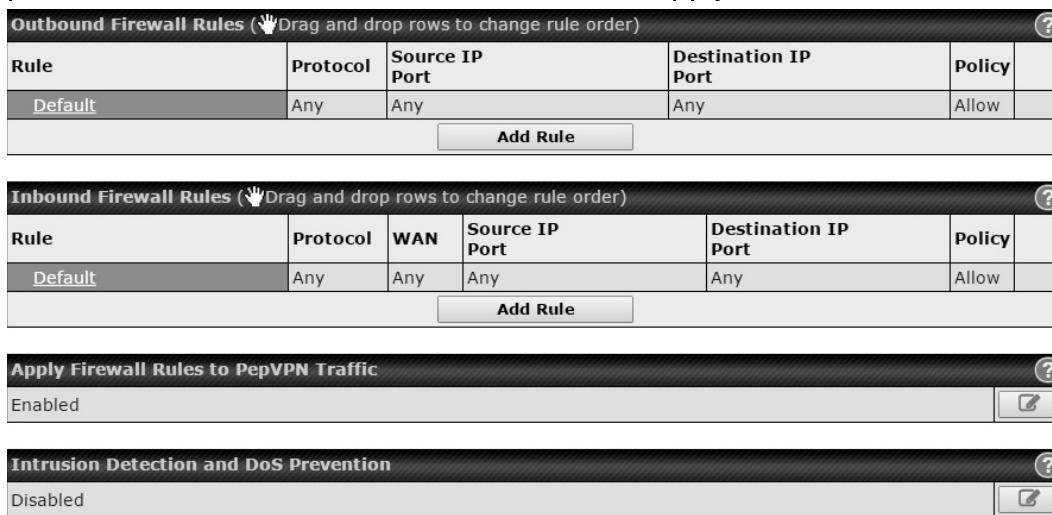
Outbound (LAN to WAN)

Inbound (WAN to LAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion™ enabled, the firewall rules also apply to VPN tunneled traffic.



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

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

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

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

Apply Firewall Rules to PepVPN Traffic

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

Intrusion Detection and DoS Prevention

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

22.1 Outbound and Inbound Firewall Rules

22.1.1 Access Rules

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



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

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

Add Rule

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

Add a New Outbound Firewall Rule

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

Save **Cancel**

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

Inbound Firewall Rules (Drag and drop rows to change rule order) [\(?\)](#)

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

Add Rule

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

Add a New Inbound Firewall Rule

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

Save **Cancel**

Inbound / Outbound Firewall Settings

Rule Name	This setting specifies a name for the firewall rule.
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule.
WAN Connection (Inbound)	If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.
	Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.

This setting specifies the protocol to be matched.

Via a drop-down menu, the following protocols can be specified:

- TCP
- UDP
- ICMP
- IP

Protocol

Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)

After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.

This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Source IP & Port** setting, as indicated with the following screenshots:

Source IP & Port

The screenshot shows a configuration panel for 'Source IP & Port'. It has two main sections: 'Source IP & Port' and 'Destination IP & Port'. Under 'Source IP & Port', there are dropdown menus for 'Single Address' (selected), 'IP:' (with a text input field), 'Single Port' (selected), and 'Port:' (with a text input field). Under 'Destination IP & Port', there are dropdown menus for 'Network' (selected), 'IP:' (with a text input field), 'Mask:' (set to '255.255.255.0 (/24)'), and 'Port Range' (selected), with a 'Port:' input field containing '80'.

In addition, a single port, or a range of ports, can be specified for the **Source IP & Port** settings.

This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Destination IP & Port** setting, as indicated with the following screenshots:

Destination IP & Port

The screenshot shows a configuration panel for 'Destination IP & Port', which has the same structure as the 'Source IP & Port' panel above it. It includes fields for 'Source IP & Port' and 'Destination IP & Port' with dropdown menus for 'Single Address', 'Single Port', 'Network', and 'Port Range'.

In addition, a single port, or a range of ports, can be specified for the **Destination IP & Port** settings.

This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:

Action

- Source IP & port
- Destination IP & port

With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded).

This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows:

Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1

DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80

Event Logging

- **CONN:** The connection where the log entry refers to
- **SRC:** Source IP address
- **DST:** Destination IP address
- **LEN:** Packet length

- **PROTO:** Protocol
- **SPT:** Source port
- **DPT:** Destination port

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

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

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

Outbound Firewall Rules ( Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	
No FTP access	FTP	Any Any	Any 21	Deny	
Default	Any	Any	Any	Allow	

To remove a rule, click the  button.

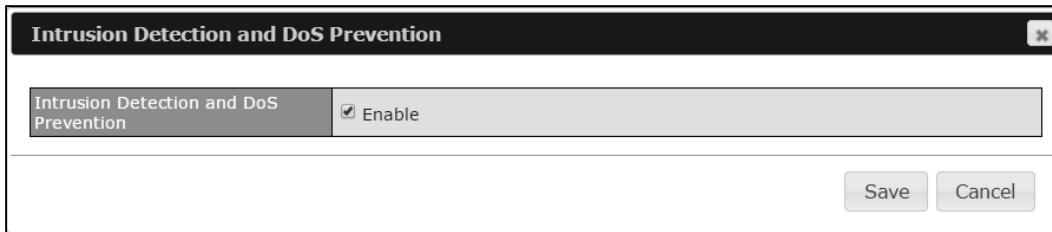
Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default** rule will be applied.

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

Tip

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

22.1.2 Intrusion Detection and DoS Prevention



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

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

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

22.1.3 Content Blocking

Application Blocking

Please Select Application...

Web Blocking

Preset Category

<input type="radio"/> High	<input type="checkbox"/> Abortion	<input type="checkbox"/> Adware	<input type="checkbox"/> Aggressive
<input type="radio"/> Moderate	<input type="checkbox"/> Alcohol	<input type="checkbox"/> Anti-Spyware	<input type="checkbox"/> Chatroom
<input type="radio"/> Low	<input type="checkbox"/> Dating	<input type="checkbox"/> Drugs	<input type="checkbox"/> Ecommerce/Shopping
<input checked="" type="radio"/> Custom	<input type="checkbox"/> Entertainment	<input type="checkbox"/> File Hosting	<input type="checkbox"/> P2P/File sharing
	<input type="checkbox"/> Gambling	<input type="checkbox"/> Games	<input type="checkbox"/> Hacking
	<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Job Search/Employment	<input type="checkbox"/> Kids Time Wasting
	<input type="checkbox"/> Lingerie	<input type="checkbox"/> Malware	<input type="checkbox"/> Manga/Anime/Webcomic
	<input type="checkbox"/> Nudity	<input type="checkbox"/> News/Media	<input type="checkbox"/> Auctions
	<input type="checkbox"/> Phishing	<input type="checkbox"/> Pornography	<input type="checkbox"/> Proxy/Anonymizer
	<input type="checkbox"/> Radio	<input type="checkbox"/> Remote Access	<input type="checkbox"/> Ringtones
	<input type="checkbox"/> Search Engines	<input type="checkbox"/> Sexuality Education	<input type="checkbox"/> Social Networking
	<input type="checkbox"/> Sports	<input type="checkbox"/> Spyware	<input type="checkbox"/> Tobacco
	<input type="checkbox"/> Update Sites	<input type="checkbox"/> Vacation	<input type="checkbox"/> Violence
	<input type="checkbox"/> Viruses	<input type="checkbox"/> Weapons	<input type="checkbox"/> Weather
	<input type="checkbox"/> Webmail	<input type="checkbox"/> WebTV	

Customized Domains

cbs.com	<input type="button" value="X"/>
<input type="text"/>	<input type="button" value="+"/>

Exempted Domains from Web Blocking

<input type="text"/>	<input type="button" value="+"/>
----------------------	----------------------------------

Exempted User Groups

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

Exempted Subnets

Network	Subnet Mask
<input type="text"/>	255.255.255.0 (/24) <input type="button" value="?"/> <input type="button" value="+"/>

URL Logging

Enable	<input type="checkbox"/>
Log Server Host	<input type="text"/> Port: <input type="text"/>

22.1.3.1 Application Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted User Groups or Exempted Subnets defined below.

22.1.3.2 Web Blocking

Defines web site domain names to be blocked from LAN/PPTP/PepVPN peer clients'

access except for those on the Exempted User Groups or Exempted Subnets defined below.

If "foobar.com" is entered, any web site with a host name ending in foobar.com will be blocked, e.g. www.foobar.com, foobar.com, etc. However, "myfoobar.com" will not be blocked.

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

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

22.1.3.3 Customized Domains

Enter an appropriate website address, and the Peplink Balance will block and disallow LAN/PPTP/SpeedFusion™ peer clients to access these websites. Exceptions can be added using the instructions in **Sections 22.1.3.4** and **22.1.3.5**.

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

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

22.1.3.4 Exempted User Groups

Check and select pre-defined user group(s) who can be exempted from the access blocking rules. User groups can be defined at **QoS>User Groups** section. Please refer to **Section 21.1** for details.

22.1.3.5 Exempted Subnets

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

22.1.3.6 URL Logging

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

23 OSPF & RIPv2

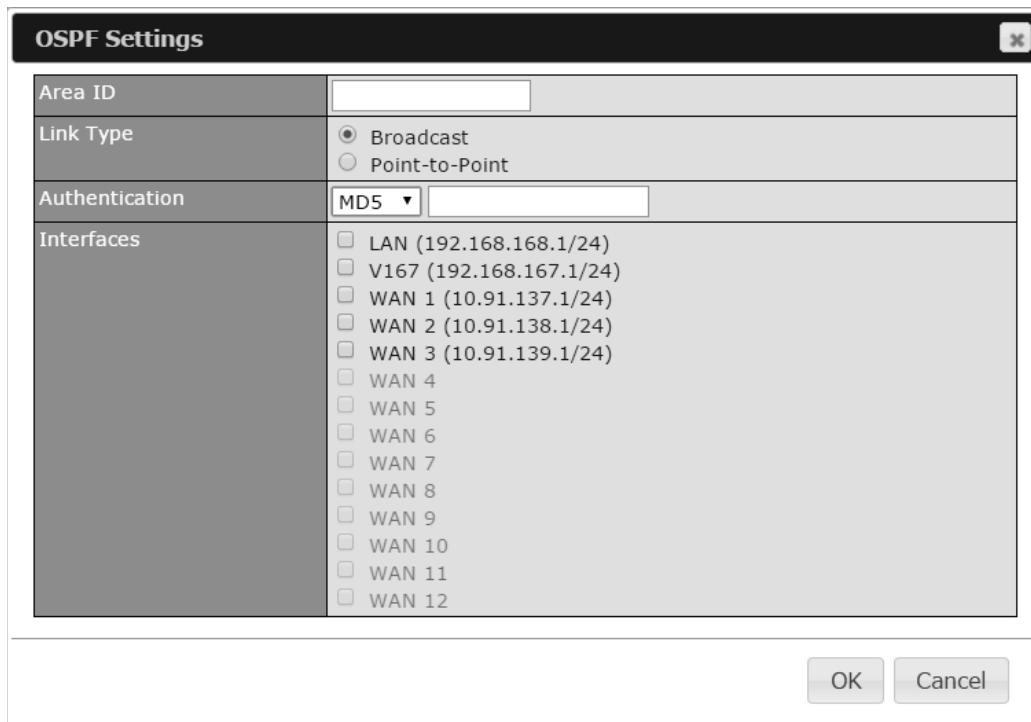
The Peplink Balance supports OSPF and RIPv2 dynamic routing protocols. Click the **Network** tab from the top bar, and then click the **OSPF & RIPv2** item on the sidebar to reach the following menu:

OSPF	
Router ID	Interfaces
<input checked="" type="radio"/> LAN IP Address <input type="radio"/> Custom: <input type="text"/>	
Area	Interfaces
0	PepVPN
<input type="button" value="Add"/>	

RIPv2	
No RIPv2 Defined.	<input type="button" value=""/>

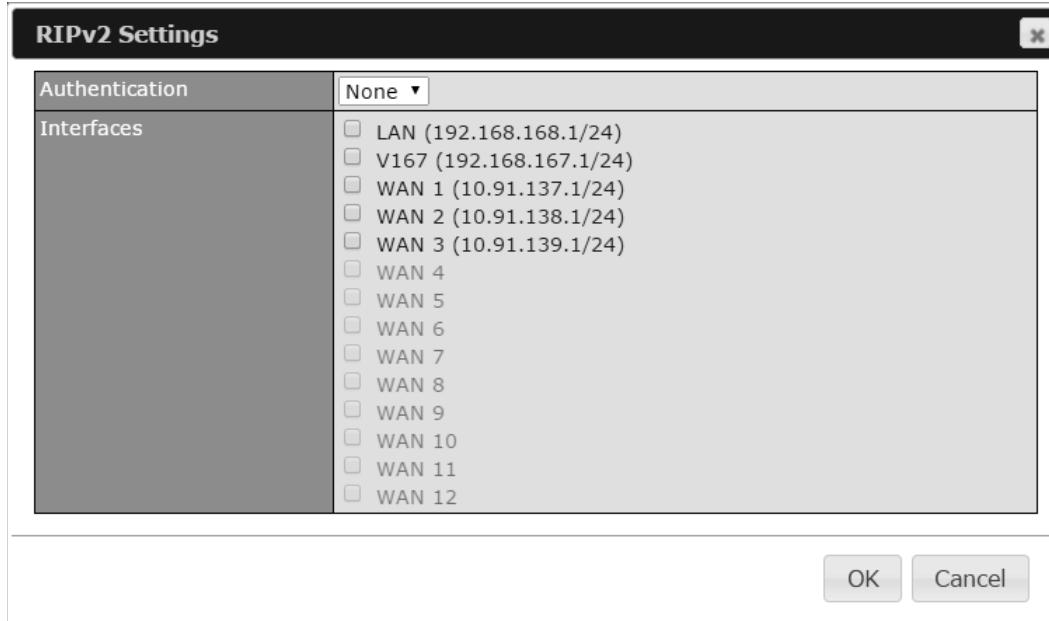
OSPF

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



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

To access RIPv2 settings, click .



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

24 Remote User Access

Networks routed by a Peplink Balance can be remotely accessed via L2TP with IPsec or PPTP. To configure this feature, navigate to **Network > Remote User Access**

Remote User Access Settings											
Enable	<input checked="" type="checkbox"/>										
VPN Type	<input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP IPsec NAT-Traversal will be enabled to ensure compatibility for most of the devices										
Preshared Key	***** <input checked="" type="checkbox"/> Hide Characters										
Listen On	Connection / IP Address(es) <table border="1"> <tr> <td><input checked="" type="checkbox"/> WAN1</td> <td><input checked="" type="checkbox"/> 10.10.12.47 (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"/> WAN3</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"/> 10.10.12.47 (Interface IP)	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> Interface IP	<input checked="" type="checkbox"/> WAN3	<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"/> 10.10.12.47 (Interface IP)										
<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> Interface IP										
<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> Interface IP										
<input checked="" type="checkbox"/> Mobile Internet	<input checked="" type="checkbox"/> Interface IP										
User Accounts	<table border="1"> <thead> <tr> <th>Username</th> <th>Password</th> <th></th> </tr> </thead> <tbody> <tr> <td>admin</td> <td>*****</td> <td><input type="button" value="X"/></td> </tr> <tr> <td></td> <td></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>		Username	Password		admin	*****	<input type="button" value="X"/>			<input type="button" value="+"/>
Username	Password										
admin	*****	<input type="button" value="X"/>									
		<input type="button" value="+"/>									

Remote User Access Settings		
Enable	Click the checkbox to enable Remote User Access.	
VPN Type	Determine whether remote devices can connect to the Balance using L2TP with IPsec or PPTP. For greater security, we recommend you connect using L2TP with IPsec.	
Preshared Key	Enter your preshared key in the text field. Please note that remote devices will need this preshared key to access the Balance.	
Listen On	This setting is for specifying the WAN IP addresses where the PPTP server of the router should listen on.	
User Accounts	This setting allows you to define the PPTP User Accounts. Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click the button X to delete the account in its	

corresponding row.

Click the  button to switch to enters user accounts by pasting the information in.CSV format.

Miscellaneous Settings

The miscellaneous settings include configuration for high availability, PPTP server, service forwarding, and service passthrough.

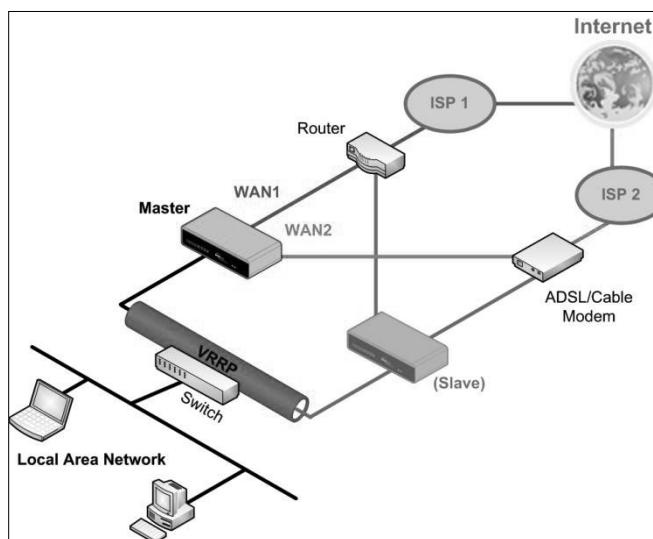
24.1 High Availability

The Peplink Balance supports high availability (HA) configurations via an open standard virtual router redundancy protocol (VRRP, RFC 3768).

In an HA configuration, two same-model Peplink Balance units provide redundancy and failover in a master-slave arrangement. In the event that the master unit is down, the slave unit becomes active.

High availability will be disabled automatically where there is a drop-in connection configured on a LAN bypass port.

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



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

An elaboration on the technical details of the implementation of virtual router redundancy protocol (VRRP, RFC 3768) by the Balance follows:

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

once again become active.

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

Interface for Master Router

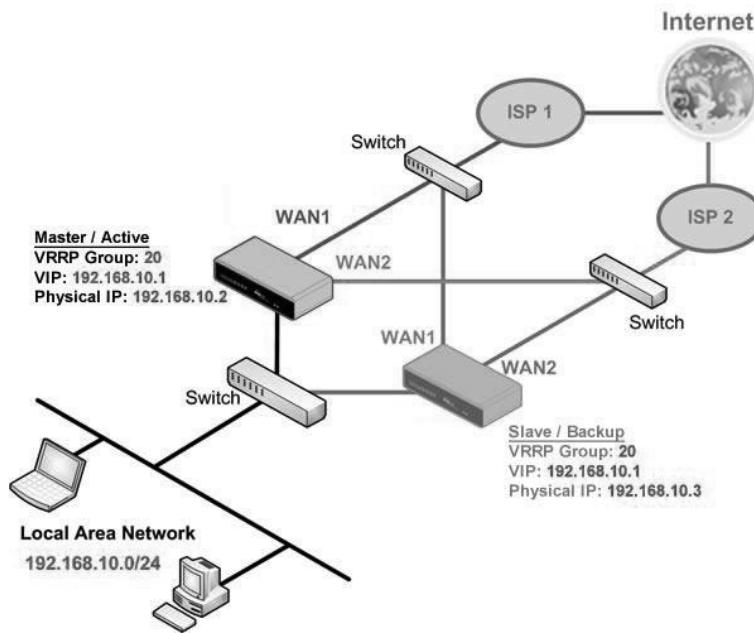
High Availability		High Availability	
Enable	<input type="checkbox"/>	Enable	<input checked="" type="checkbox"/>
Group Number	5	Group Number	5
Preferred Role	<input checked="" type="radio"/> Master <input type="radio"/> Slave	Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/>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

Interface for Slave Router

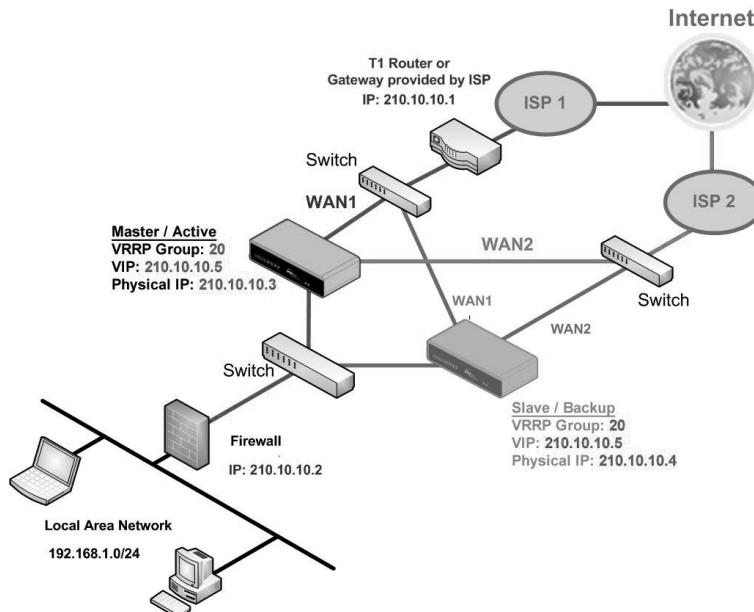
High Availability	
Enable	Checking this box specifies that the Peplink Balance unit is part of a high availability configuration.
Group Number	This number identifies a pair of Peplink Balance units operating in a high availability configuration. The two Peplink Balance units in the pair must have the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

Important Note

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



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



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

24.2 Certificate Manager

Certificate Manager			
VPN Certificate	(?)	No Certificate	Assign
Web Admin SSL Certificate	(?)	No Certificate	Assign
Captive Portal SSL Certificate		No Certificate	Assign

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.

24.3 Service Forwarding

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

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

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

24.3.1 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
WAN 1	<input type="checkbox"/>		
WAN 2	<input checked="" type="checkbox"/>	22.2.2.2	25
WAN 3	<input checked="" type="checkbox"/>	33.3.3.2	25
WAN 4	<input type="checkbox"/>		

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

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

Note

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see **Section 17.1**).

24.3.2 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	
WAN 1	<input type="checkbox"/>		:
WAN 2	<input checked="" type="checkbox"/>	22.2.2.2	: 8765
WAN 3	<input checked="" type="checkbox"/>	33.3.3.2	: 8080
WAN 4	<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.

24.3.3 DNS Forwarding

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

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

24.3.4 Custom Service Forwarding

Custom Service Forwarding Setup									
Custom Service Forwarding	<input checked="" type="checkbox"/> Enable								
Settings	<table border="1"> <tr> <td>TCP Port</td> <td>Server IP Address</td> <td>Server Port</td> <td>+</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td>+</td> </tr> </table>	TCP Port	Server IP Address	Server Port	+	<input type="text"/>	<input type="text"/>	<input type="text"/>	+
TCP Port	Server IP Address	Server Port	+						
<input type="text"/>	<input type="text"/>	<input type="text"/>	+						

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

24.4 Service Passthrough

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

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

(Registered trademarks are copyrighted by their respective owner)

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

Service Passthrough Support	
SIP	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Peplink Balance can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets

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

25 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 APs from a single Peplink Balance interface.

Special Note

With the installation of Firmware 6.2.1 and upwards, full AP support is included free.

25.1 AP Controller

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



AP Controller	
AP Management	The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, CAPWAP Access Controller addresses (field 138), will be added to the DHCP server. A local DNS record, AP Controller , will be added to the local DNS proxy.
Support Remote AP	<p>The AP controller supports remote management of Pepwave APs. When this option is enabled, the AP controller will wait for management connections originating from remote APs over the WAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443.</p> <p>The DHCP server and/or local DNS server of the remote AP's network should be configured in the DNS Proxy Settings menu under Network>LAN. The procedure is as follows:</p> <ol style="list-style-type: none">1. Define an extended DHCP option, CAPWAP Access Controller addresses (field 138), in the DHCP server, where the values are the AP controller's public IP addresses; and/or2. Create a local DNS record for the AP controller with a value corresponding to the AP controller's public IP address.

DNS Proxy Settings										
Enable	<input checked="" type="checkbox"/>									
DNS Caching	<input type="checkbox"/>	?								
Include Google Public DNS Servers	<input type="checkbox"/>	?								
Local DNS Records	<table border="1"> <tr> <td>?</td> <td>Host Name</td> <td>IP Address</td> <td>+</td> </tr> <tr> <td></td> <td>wlancontroller</td> <td>10.10.10.1</td> <td></td> </tr> </table>		?	Host Name	IP Address	+		wlancontroller	10.10.10.1	
?	Host Name	IP Address	+							
	wlancontroller	10.10.10.1								

Permitted AP

Access points to manage can be specified here. If **Any** is selected, the AP controller will manage any AP that reports to it. If **Approved List** is selected, only APs with serial numbers listed in the provided text box will be managed.

25.2 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
PEPLINK_E73D	WPA/WPA2 - Personal

New SSID

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

SSID

SSID Settings	
SSID	<input type="text"/>
VLAN ID	<input type="button" value="LAN (No VLAN)"/>
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"/>
Layer 2 Isolation	<input type="checkbox"/>
Band Steering	<input type="button" value="Disable"/>

SSID Settings

SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
VLAN ID	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is 0 , which means VLAN tagging is disabled (instead of tagged with zero).

Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate ^A	Select Auto to allow the Peplink Balance to set the data rate automatically, or select Fixed and choose a rate from the displayed drop-down menu.
Multicast Filter^A	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate^A	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected Protocol and Channel Bonding settings will affect the rate options and values available here.
IGMP Snooping ^A	To allow the Peplink Balance to listen to internet group management protocol (IGMP) network traffic, select this option.
DHCP Option 82 ^A	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
Network Priority (QoS) ^A	Select from Gold , Silver , and Bronze to control the QoS priority of this wireless network's traffic.
Layer 2 Isolation ^A	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
Band Steering ^A	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 Enforce . To cause the Peplink Balance to preferentially choose steering, select Prefer . The default for this setting is Disable .

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

Security Settings	
Security Policy	<input type="button" value="WPA2 - Personal"/>
Encryption	AES:CCMP
Shared Key	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

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

Access Control	
Restricted Mode	<input type="button" value="None"/> <input type="button" value="Deny all except listed"/> <input type="button" value="Accept all except listed"/> <input type="button" value="RADIUS MAC Authentication"/>

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 .	
Restricted Mode	When WPA/WPA2 - Enterprise is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the Shared Key option should be disabled. When using this method, select the appropriate version using the V1/V2 controls. The security level of this method is known to be very high.
	When WPA/WPA2- Personal is configured, a shared key is used for data encryption and authentication. When using this configuration, the Shared Key option should be enabled. Key length must be between eight and 63 characters (inclusive). The security level of this method is known to be high.
	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.
MAC Address List	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			
Secret			
Authentication Port	<input type="text" value="1812"/> <input type="button" value="Default"/>	<input type="text" value="1812"/> <input type="button" value="Default"/>	
Accounting Port	<input type="text" value="1813"/> <input type="button" value="Default"/>	<input type="text" value="1813"/> <input type="button" value="Default"/>	

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

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

Guest Protect	
Block All Private IP	Check this box to deny all connection attempts by private IP addresses.
Custom Subnet	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 <input type="button" value="+"/> . To delete a custom subnet, click <input type="button" value="X"/> .
Block Exception	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 <input type="button" value="+"/> . To delete a blocked subnet, click <input type="button" value="X"/> .
Block PepVPN	To block PepVPN access, check this box.

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

Bandwidth Management	
Upstream Limit	Enter a value in kpbs to limit the wireless network's upstream bandwidth. Enter 0 to allow unlimited upstream bandwidth.
Downstream Limit	Enter a value in kpbs to limit the wireless network's downstream bandwidth. Enter 0 to allow unlimited downstream bandwidth.
Client Upstream Limit	Enter a value in kpbs to limit connected clients' upstream bandwidth. Enter 0 to allow unlimited upstream bandwidth.
Client	Enter a value in kpbs to limit connected clients' downstream bandwidth. Enter 0 to allow

Downstream Limit	unlimited downstream bandwidth.
Max Number of Clients	Enter the maximum number of clients that can simultaneously connect to the wireless network or enter 0 to allow an unlimited number of connections.

Firewall Settings		
Firewall Mode	Lockdown - Block all except... ▾	
Firewall Exceptions	Name	Type
		Item
		New Rule

Firewall Settings

Firewall Mode Choose Flexible – **Allow all except...** or **Lockdown – Block all except...** to turn on the firewall. Once you save changes, the **New Rule** button will appear for you to create rules for the firewall exceptions. 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	
Name	<input type="text"/>
Type	Port ▾
Protocol	TCP ▾
Port	Any Port ▾
OK Cancel	

Firewall Rule

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

25.3 Profiles

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

Name	Used by	Action
1. Default	(None)	
New AP Profile		

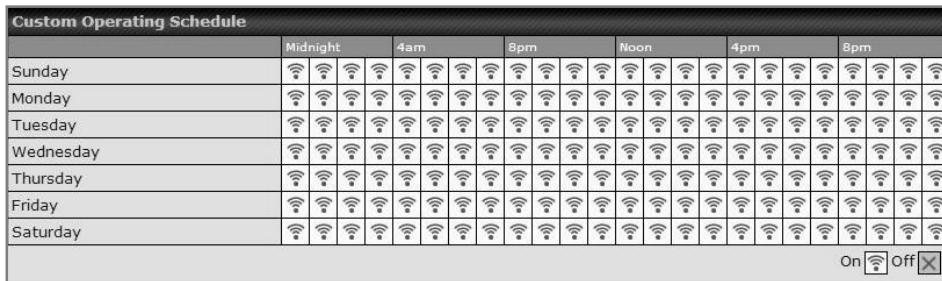
Each AP is associated with one AP profile. By default, all devices are associated with the first (default) profile. The default profile cannot be removed.

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 Profile

AP Settings	
AP Profile Name	
SSID	2.4 GHz 5 GHz <input type="checkbox"/> <input type="checkbox"/> PEPLINK_01AA
Operating Country	United States
Preferred Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz
5 GHz Protocol	802.11n/ac
5 GHz Channel Width	20 MHz
5 GHz Channel	Auto Channels: 36 40 44 48 ...
2.4 GHz Protocol	802.11ng
2.4 GHz Channel Width	20 MHz
2.4 GHz Channel	1 (2.412 GHz)
Management VLAN ID	0 (0: Untagged)
Power Boost	<input type="checkbox"/>
Output Power	Dynamic: Auto
Operating Schedule	<input checked="" type="radio"/> Always On <input type="radio"/> Custom Schedule
Max number of Clients	0 (0: Unlimited)
Client Signal Strength Threshold	0 (0: Unlimited)
Beacon Rate	1Mbps
Beacon Interval	100ms
DTIM	1
RTS Threshold	0
Slot Time	9 μs
ACK Timeout	48 μs
Frame Aggregation	<input checked="" type="checkbox"/>
Frame Length	50000

AP Settings	
AP Profile Name	This field specifies the name of this AP profile.
SSID	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.
Operating Country	<p>This drop-down menu specifies the national / regional regulations which the AP should follow.</p> <ul style="list-style-type: none"> • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). <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 channels only.</p>
Preferred Frequency	These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies.
5 GHz Protocol	This section displays the 5 GHz protocols your APs are using.
5GHz Channel Bonding	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
5 GHz Channel	This drop-down menu selects the 5 GHz 802.11 channel to be utilized. If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
2.4 GHz Protocol	This section displays the 2.4 GHz protocols your APs are using.
2.4 GHz Channel Bonding	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
2.4 GHz Channel	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 North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is 0 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.
Power Boost^A	With this option enabled, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to

	increased interference.
Output Power^A	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 APs in order to maximize performance. The Dynamic: Auto setting will set the AP to do this automatically. Otherwise, the Dynamic: Manual setting will set the AP to dynamically adjust only if instructed to do so. If you have set Dynamic:Manual , you can go to AP>Toolbox>Auto Power Adj. to give your AP further instructions.
Operating Schedule^A	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 APs under this profile.
Max number of Clients^A	This field determines the maximum clients that can be connected to APs under this profile.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Beacon Rate^A	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are 1Mbps , 2Mbps , 5.5Mbps , 6Mbps , and 11Mbps .
Beacon Interval^A	This drop-down menu provides the option to set the time between each beacon send. Available options are 100ms , 250ms , and 500ms .
DTIM^A	This field provides the option to set the frequency for beacon to include delivery traffic indication messages (DTIM). The interval unit is measured in milliseconds.
RTS Threshold^A	This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.
Slot Time^A	This field provides the option to modify the unit wait time before it transmits. The default value is 9μs .
ACK Timeout^A	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is 48μs .
Frame	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.

Aggregation^A

Frame Length	This field is only available when Frame Aggregation is enabled. It specifies the frame length for frame aggregation. By default, it is set to 50000 .
---------------------	---

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

Web Administration Settings (on External AP)	
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	ebb7a61c9901 <input type="button" value="Generate"/>

Web Administration Settings

Enable	Check the box to allow Peplink Balance to manage the web admin access information of the AP.
Web Access Protocol	These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are HTTP and HTTPS .
Management Port	This field specifies the management port used for accessing the device.
HTTP to HTTPS Redirection	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 redirect to HTTPS automatically.
Admin User Name	This field specifies the administrator username of the web admin. It is set as <i>admin</i> by default.
Admin Password	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 type="radio"/> Follow controller time zone selection <input checked="" type="radio"/> (GMT-08:00) Pacific Time (US & Canada) <input type="button" value="▼"/>
Time Server	<input type="radio"/> Follow controller NTP server selection <input type="radio"/>

AP Time Settings

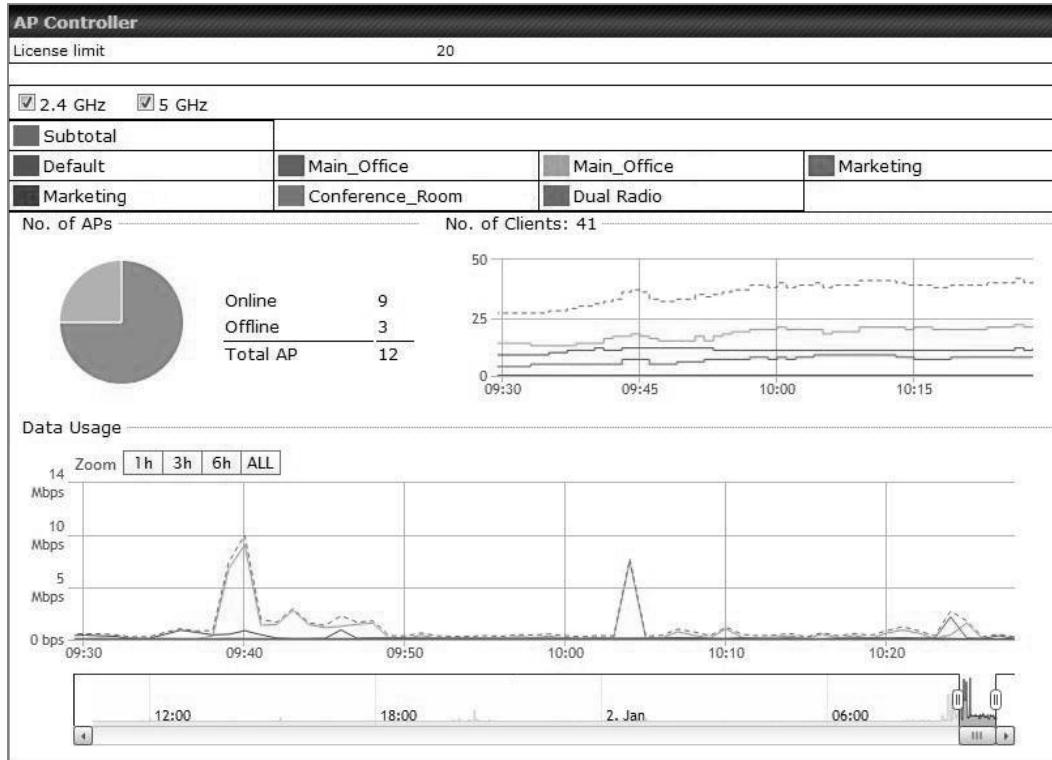
Time Zone	Check the box to allow the Peplink Balance to manage the web admin access information of the AP.
Time Server	These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are HTTP and HTTPS .

AP Controller Settings	
Client Load Balancing	<input checked="" type="checkbox"/>
Coverage Redundancy	High ▾

AP Controller Settings	
Client Load Balancing	Check the box to turn on client load balancing.
Coverage Redundancy	Select the degree of coverage redundancy to use. Available values are Low , Medium , and High .

25.4 Info

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



AP Controller	
License Limit	This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage.
Frequency	Underneath, there are two check boxes labeled 2.4 Ghz and 5 Ghz . Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.

SSID	The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs.
No. of APs	This pie chart and table indicates how many APs are online and how many are offline.
No. of Clients	This graph displays the number of clients connected to each network at any given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time.
Data Usage	This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to Zoom to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

Events		View Alerts
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.	

25.5 Usage

A detailed breakdown of data usage for each AP is available at **AP> Access Point**. The information is organized by device groups as defined in **Section 22.3**.

Search Filter															
AP Name / Serial Number / SSID	All <input type="checkbox"/> Include Offline APs														
Search Result															
Managed APs															
<table border="1"> <thead> <tr> <th>Name</th> <th>IP Address</th> <th>MAC</th> <th>Location</th> <th>Firmware Pack ID</th> <th>Configuration</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Default (8/9 online)</td> <td>10.8.82.11</td> <td>00:1A:DD:BD:73:E0</td> <td>-</td> <td>3.5.2</td> <td>None ✓ -</td> <td></td> </tr> </tbody> </table>		Name	IP Address	MAC	Location	Firmware Pack ID	Configuration	Actions	Default (8/9 online)	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None ✓ -	
Name	IP Address	MAC	Location	Firmware Pack ID	Configuration	Actions									
Default (8/9 online)	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None ✓ -										

Usage

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

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

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

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

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

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

Close

Managed Wireless Devices

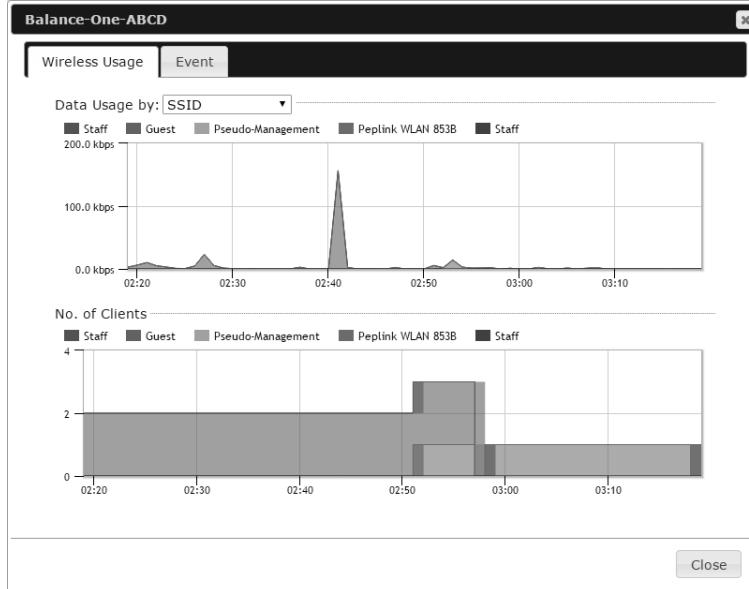
Click the  icon to configure each client

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

Close

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

Click the  icon to see a graph displaying usage:



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

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

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

More...

Close

25.6 SSID

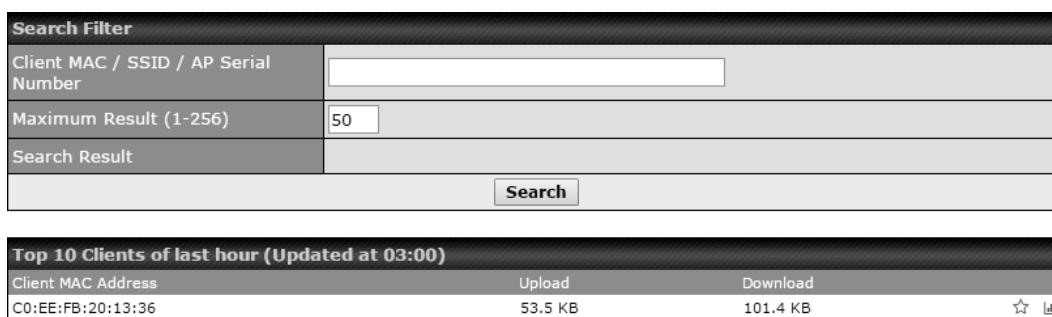
In-depth SSID reports are available under AP > SSID.



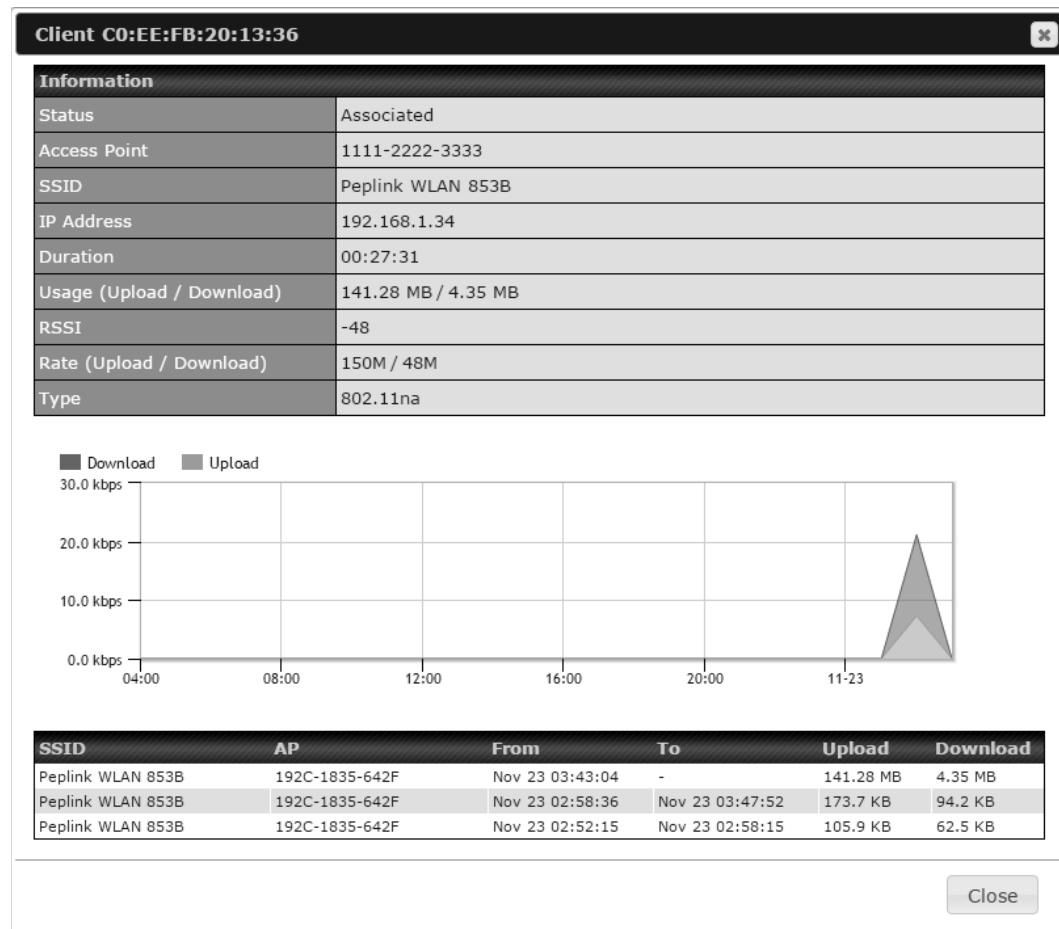
Click the blue arrow on any SSID to obtain more detailed usage information on each SSID.

25.7 Wireless Client

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



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



25.8 Rogue AP

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

Suspected Rogue APs						
BSSID	SSID	Channel	Encryption	Last Seen	Mark as	
00:1A:DD:EC:25:22	Wireless	11	WPA2	10 hours ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:EC:25:23	Accounting	11	WPA2	10 hours ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:EC:25:24	Marketing	11	WPA2	11 hours ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:03:7F:00:00:00	MYB1PUSH	1	WPA & WPA2	11 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:03:7F:00:00:01	MYB1	1	WPA2	15 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:B9:60:88	PEPWAVE_CB7E	1	WPA & WPA2	5 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:BB:09:C1	Micro_S1_1	6	WPA & WPA2	1 hour ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:BB:52:A8	MAX HD2 Gobi	11	WPA & WPA2	2 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:BF:75:81	PEPLINK_05B5	4	WPA & WPA2	1 minute ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:BF:75:82	LK_05B5	4	WPA2	1 minute ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:BF:75:83	LK_05B5_VLAN22	4	WPA2	1 minute ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C1:ED:E4	dev_captive_portal_test	1	WPA & WPA2	3 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C2:E4:C5	PEPWAVE_7052	11	WPA & WPA2	2 hours ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C3:F1:64	dev_captive_portal_test	6	WPA & WPA2	6 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C4:DC:24	ssid_test	8	WPA & WPA2	2 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C4:DC:25	SSID New	8	WPA & WPA2	2 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C5:46:04	Guest SSID	9	WPA2	2 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C5:47:04	PEPWAVE_67B8	1	WPA & WPA2	5 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C5:4E:24	G BR1 Portal	2	WPA2	2 minutes ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
00:1A:DD:C6:9A:48	ssid_test	8	WPA & WPA2	2 hours ago	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	

Suspected Rogue Devices

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

25.9 Toolbox

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

Firmware Packs	Auto Power Adj.	Dynamic Channel Assignment	
Pack ID	Release Date	Details	Action
1126	2013-08-26		
Check for Updates Manual Upload Default...		No default defined.	

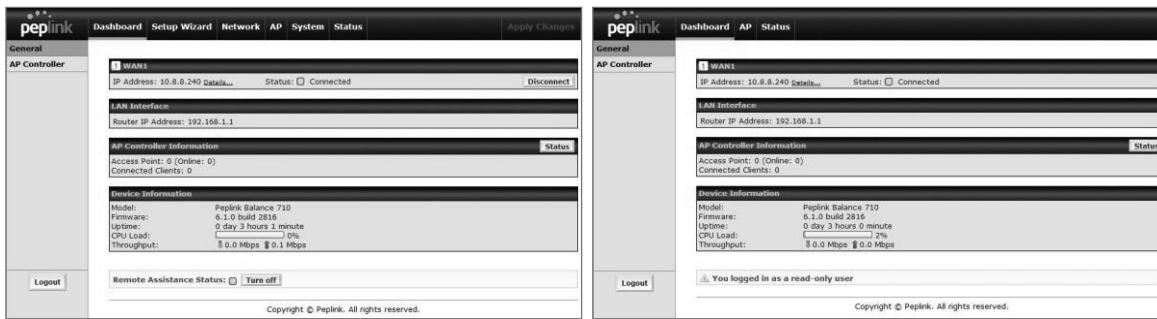
Firmware Packs

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

26 System Settings

26.1 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, while the user level is read-only. The user level can access only the device's status information; users cannot make any changes on the device.



The image shows two side-by-side screenshots of the Peplink Balance Series web admin interface. Both screenshots have a header with the peplink logo, navigation tabs (Dashboard, Setup Wizard, Network, AP, System, Status), and an 'Apply Changes' button. A sidebar on the left includes 'General' and 'AP Controller' sections, with a 'Logout' button at the bottom.

- Admin account UI:** Shows the full dashboard with WAN, LAN Interface, AP Controller Information, Device Information, and Remote Assistance Status. It also includes a 'Status' button next to the AP Controller Information section.
- User account UI:** Shows the same dashboard structure but with limited functionality. The 'AP Controller Information' and 'Device Information' sections are displayed in a read-only format, indicated by a 'Status' button at the top right of each section. A message 'You logged in as a read-only user' is displayed below the Device Information section.

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

Admin Settings	
Router Name	182C-124B-09DC hostname: 182c-124b-09dc
Admin User Name	admin
Admin Password	*****
Confirm Admin Password	*****
Read-only User Name	user
User Password	
Confirm User Password	
Front Panel Passcode	<input type="checkbox"/>
Web Session Timeout	(?) <input type="text" value="4"/> Hours <input type="text" value="0"/> Minutes
Authentication by RADIUS	(?) <input checked="" type="checkbox"/> Enable
Auth Protocol	MS-CHAP v2 ▾
Auth Server	<input type="text"/> Port <input type="button" value="Default"/>
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Auth Timeout	3 seconds
Accounting Server	<input type="text"/> Port <input type="button" value="Default"/>
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Restricted Admin Access	<input type="checkbox"/> by Management Port Only
CLI SSH	(?) <input checked="" type="checkbox"/> Enable
CLI SSH Port	8822 <input type="button" value="Default"/>
CLI SSH Access	LAN/WAN ▾
Security	HTTP ▾
Web Admin Port	80 <input type="button" value="Default"/>
Web Admin Access	LAN/WAN ▾

Admin Settings

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

Password	
Front Panel Passcode	To require a 4-digit passcode to access front panel controls, check this box and then select the code from the drop-down menus.
Web Session Timeout	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 4 hours .
Authentication by RADIUS	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.
Auth Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.
Network Connection	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
Restricted Admin Access	Check this box to restrict management to administrators connected to the management port.
CLI SSH & Console	The CLI (command line interface) can be accessed via SSH. It can also be accessed from the serial console port on some Peplink Balance models. This field enables CLI support. For additional information regarding CLI, please refer to Section 22.5 .
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: <ul style="list-style-type: none"> • HTTP • HTTPS

- HTTP/HTTPS

Web Admin Port

This field is for specifying the port number on which the web admin interface can be accessed.

Web Admin Access

This option is for specifying the network interfaces through which the web admin interface can be accessed:

- LAN only
- LAN/WAN

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

Connection / IP Address(es)	
<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> 10.91.195.1 (Interface IP)	
<input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> 10.91.196.1 (Interface IP)	
<input checked="" type="checkbox"/> WAN 3 <input checked="" type="checkbox"/> 10.91.197.1 (Interface IP)	

WAN Connection Access Settings

This field allows you to restrict access to the 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 option is chosen, a text input area will appear:

Allowed Source IP Subnets

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

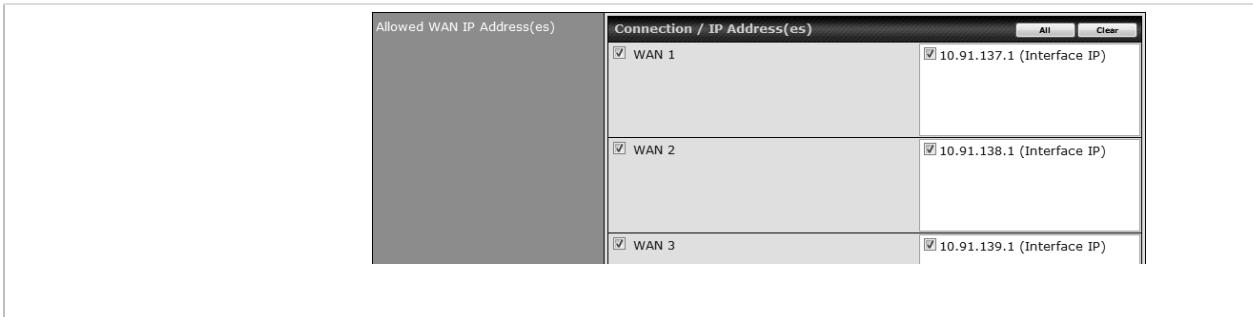
To define multiple subnets, separate each IP subnet, one per line. For example:

192.168.0.0/24

10.8.0.0/16

Allowed WAN IP Address(es)

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



26.2 Firmware

The firmware of Peplink Balance is upgradeable through the web admin interface. Firmware upgrade functionality is located at **System>Firmware**.

Firmware Upgrade

Current firmware version: 6.2.1
Firmware check pending

Check for Firmware

Manual Firmware Upgrade

Firmware Image No file chosen

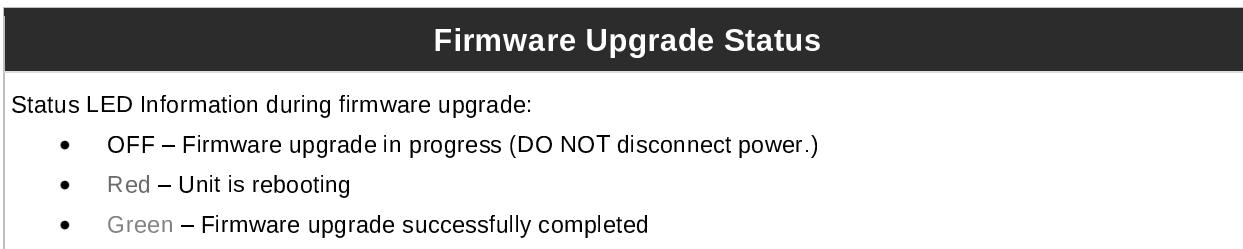
Manual Upgrade

There are two ways to upgrade the unit. The first method is through an online download. 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 **Choose File** 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.



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

26.3 Schedule

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

Enabled			<input checked="" type="checkbox"/>
Name	Time	Used by	
Weekdays Only	Weekdays only	-	<input type="button" value="X"/>

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

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

26.4 Time

The time server functionality enables the system clock of the Peplink Balance to be synchronized with a specified time server. The settings for time server configuration are located at **System>Time**.

Time Settings	
Time Zone	(GMT+07:00) Krasnoyarsk <input type="checkbox"/> Show all
Time Server	0.peplink.pool.ntp.org <input type="button" value="Default"/>
<input type="button" value="Save"/>	

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

26.5 Email Notification

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

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

Email Notification Settings	
Email Notification	This setting specifies whether or not to enable email notification. If Enable is checked, the Peplink Balance will send email messages to system administrators when the WAN status changes or when new firmware is available. If Enable is not checked, email notification is disabled and the Peplink Balance will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check Require authentication .
SSL Encryption	Check the box to enable SMTPS. When the box is checked, SMTP Port will be changed to 465 automatically.
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to 25 ; when SSL Encryption is checked, the default port number will be set to 465 . You may customize the port number by editing this field. Click Default to restore the number to its default setting.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if Require authentication is checked in the SMTP Server setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address which the Peplink Balance will use to send its reports.

Recipient's Email Address This setting specifies the email address(es) to which the Peplink Balance will send email notifications. For multiple recipients, separate each email using the enter key.

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

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

Send Test Notification **Cancel**

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

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

Test Result

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

26.6 Event Log

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

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

Remote Syslog Settings

Remote Syslog This setting specifies whether or not to log events at the specified remote syslog server.

Remote Syslog Host This setting specifies the IP address or hostname of the remote syslog server.

The Peplink Balance can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature.

Push Events



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

26.7 SNMP

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

SNMP Settings															
SNMP Device Name	Balance_0D84														
SNMP Port	161	Default													
SNMPv1	<input type="checkbox"/> Enable														
SNMPv2c	<input type="checkbox"/> Enable														
SNMPv3	<input type="checkbox"/> Enable														
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></td> </tr> <tr> <td colspan="4" style="text-align: center;">Add SNMP Community</td> </tr> </tbody> </table>				Community Name	Allowed Source Network	Access Mode		MyCompany	192.168.1.20/24	Read Only		Add SNMP Community			
Community Name	Allowed Source Network	Access Mode													
MyCompany	192.168.1.20/24	Read Only													
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>SHA / DES</td> <td>Read Only</td> <td></td> </tr> <tr> <td colspan="4" style="text-align: center;">Add SNMP User</td> </tr> </tbody> </table>				SNMPv3 User Name	Authentication / Privacy	Access Mode		SNMPUser	SHA / DES	Read Only		Add SNMP User			
SNMPv3 User Name	Authentication / Privacy	Access Mode													
SNMPUser	SHA / DES	Read Only													
Add SNMP User															
SNMP Settings															
SNMP Device Name	This field shows the router name defined at System>Admin Security .														
SNMP Port	This option specifies the port which SNMP will use. The default port is 161 .														
SNMPv1	This option allows you to enable SNMP version 1.														
SNMPv2	This option allows you to enable SNMP version 2.														
SNMPv3	This option allows you to enable SNMP version 3.														

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

SNMP Community	
Community Name	MyCompany
Allowed Network	192.168.1.25 / 255.255.255.0 (/24)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

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

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

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

26.8 InControl

InControl Management	
InControl Management	<input type="checkbox"/> Allow InControl Management
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/>

Save

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.

Alternately, you could also privately host InControl. Simply check the box beside the "Privately Host InControl" open, and enter the IP Address of your InControl Host.

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

26.9 Configuration

Backing up Peplink Balance settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Peplink Balance settings is found at **System>Configuration**.

The image contains four separate screenshots of the Peplink web admin interface, each showing a different configuration management function:

- Restore Configuration to Factory Settings:** A button labeled "Restore Factory Settings".
- Download Active Configurations:** A button labeled "Download".
- Upload Configurations:** A "Configuration File" input field with a "Browse..." button, showing "No file selected.", and a "Upload" button.
- Upload Configurations from High Availability Pair:** A "Configuration File" input field with a "Browse..." button, showing "No file selected.", and a "Upload" button.

Configuration	
Restore Configuration to Factory Settings	The Restore Factory Settings button is to reset the configuration to factory default settings. After clicking the button, you will need to click the Apply Changes button on the top right corner to make the settings effective.
Download Active Configurations	Click Download to backup the current active settings.
Upload Configurations	To restore or change settings based on a configuration file, click Choose File to locate the configuration file on the local computer, and then click Upload . The new settings can then be applied by clicking the Apply Changes button on the page header, or you can cancel the procedure by pressing discard on the main page of the web admin interface.
Upload Configurations from High Availability Pair	In a high availability (HA) configuration, the Balance unit can quickly load the configuration of its HA counterpart. To do so, click the Upload button. After loading the settings, configure the LAN IP address of the Peplink Balance unit so that it is different from the HA counterpart.

26.10 Feature Add-ons

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



26.11 Reboot

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

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



27 Tools

27.1 Ping

The ping test tool sends 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. **Packet Size** can be set to a maximum of 1472 bytes. The ping utility is located at **System>Tools>Ping**, illustrated below:

The screenshot shows two stacked windows. The top window is titled 'Ping' and contains four configuration fields: 'Connection' (set to 'WAN 1'), 'Destination' (set to '10.10.10.1'), 'Packet Size' (set to '56'), and 'Number of times' (set to '5'). Below these are two buttons: 'Start' and 'Stop'. The bottom window is titled 'Results' and displays the output of a ping command. It shows five successful ping responses from '10.10.10.1' to '10.91.137.1' with various round-trip times (rtt). It also shows the summary statistics: 5 packets transmitted, 5 received, 0% packet loss, and a total time of 4003ms.

Ping	
Connection	WAN 1
Destination	10.10.10.1
Packet Size	56
Number of times	Times 5

Results

```
PING 10.10.10.1 (10.91.137.1) 56(84) bytes of data.  
64 bytes from 10.10.10.1: icmp_req=1 ttl=59 time=28.5 ms  
64 bytes from 10.10.10.1: icmp_req=2 ttl=59 time=30.7 ms  
64 bytes from 10.10.10.1: icmp_req=3 ttl=59 time=29.3 ms  
64 bytes from 10.10.10.1: icmp_req=4 ttl=59 time=28.8 ms  
64 bytes from 10.10.10.1: icmp_req=5 ttl=59 time=29.2 ms  
  
--- 10.10.10.1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4003ms  
rtt min/avg/max/mdev = 28.536/29.357/30.781/0.792 ms
```

Tip

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

27.2 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**.

Traceroute	
Connection	WAN 1
Destination	64.233.189.99
	Start Stop
Results	Clear Log
<pre> traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 60 byte packets 1 10.96.137.204 (10.96.137.204) 3.708 ms 6.472 ms 9.207 ms 2 10.96.188.204 (10.96.188.204) 6.019 ms 3.080 ms 3.446 ms 3 10.96.188.1 (10.96.188.1) 1.075 ms 1.021 ms 3.066 ms 4 10.96.188.3 (10.96.188.3) 0.805 ms 0.805 ms 0.806 ms 5 10.96.188.2 (10.96.188.2) 0.806 ms 0.806 ms 0.806 ms 6 10.96.188.204 (10.96.188.204) 3.284 ms 3.191 ms 2.465.223 (3.191-2.465.223) 3.707 ms 11.813.98.204 (11.813.98.204) 3.473 ms 7 10.8.75.46 (10.8.75.46) 3.090 ms 3.089 ms 3.089 ms 10.8.95.229.46 (10.8.95.229.46) 3.293 ms 3.293 ms 8 209.120.1.198 (209.120.1.198) 0.301 ms 7.496 ms 7.496 ms 9 109.179.99.194 (109.179.99.194) 4.833 ms 2.005 ms 0.3 (109.179.99.194) 4.873 ms 106.70.199.149 (106.70.199.149) 4.246 ms 10 209.120.8.209 (209.120.8.209) 3.239 ms 72.14.194.246 (72.14.194.246) 6.491 ms 209.120.8.209 (209.120.8.209) 4.679 ms 11 72.14.209.205 (72.14.209.205) 9.840 ms 72.14.194.209 (72.14.194.209) 6.877 ms 72.14.209.205 (72.14.209.205) 9.888 ms 12 72.14.209.205 (72.14.209.205) 8.984 ms 209.89.202.181 (209.89.202.181) 7.315 ms 209.89.245.39 (209.89.245.39) 6.489 ms 13 209.89.202.203 (209.89.202.203) 14.973 ms 209.89.245.183 (209.89.245.183) 6.899 ms 6.3889 ms 14 209.89.202.203 (209.89.202.203) 8.982 ms * 7.289 ms 15 64.233.189.99 (64.233.189.99) 8.279 ms 8.244 ms 8.289 ms </pre>	

Tip

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

27.3 Wake-on-LAN

Peplink routers can send special “magic packets” to any client specified from the Web UI.

To access this feature, navigate to **System > Tools > Wake-on-LAN**

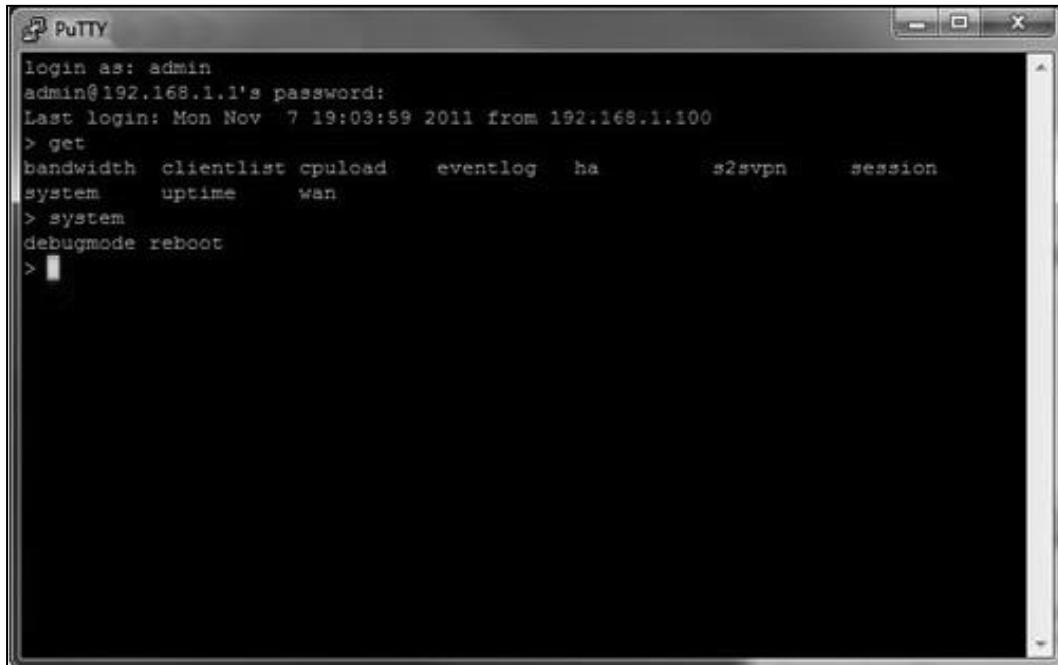
Wake-on-LAN Target	<input type="text" value="Surf_SOHO (00:90:0B:36:3C:8C)"/>	<input type="button" value="Send"/>
--------------------	--	-------------------------------------

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

27.4 CLI (Command Line Interface) Support

The serial console connector on some Peplink Balance units is RJ-45. To access the serial console port, prepare a RJ-45 to DB-9 console cable. Connect the RJ-45 end to the unit's console port and the DB-9 end to a terminal's serial port. The port setting will be 115200,8N1.

The serial console connector on other Peplink Balance units is a DB-9 male connector. To access the serial console port, connect a null modem cable with a DB-9 connector on both ends to a terminal with the port setting of 115200,8N1.



The screenshot shows a PuTTY terminal window with the title "PUTTY". The session has been titled "Peplink". The window displays a command-line interface for a Peplink Balance device. The user has logged in as "admin" and entered the password. The system information includes the last login date (Mon Nov 7 19:03:59 2011) and IP address (192.168.1.100). The user has run several commands: "get", which lists bandwidth, clientlist, cpupload, eventlog, ha, s2vpn, and session; "system", which lists uptime and wan; and "debugmode reboot". The prompt ">" indicates the user can enter more commands.

```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist  cpupload  eventlog  ha      s2vpn    session
system     uptime       wan
> system
debugmode reboot
>
```

28 Status

28.1 Device

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

System Information	
Router Name	1824-6C65-DDB9
Model	Peplink Balance 30
Hardware Revision	2
Serial Number	1824-6C65-DDB9
Firmware	6.2.1 build 2977
PepVPN Version	4.0.0
Modem Support Version	1018 (Modem Support List)
Host Name	1824-6c65-ddb9
Uptime	8 days 1 hour 12 minutes
System Time	Sun Jun 21 07:51:07 WET 2015
Diagnostic Report	Download
Remote Assistance	Turn on

Interface	MAC Address
LAN	10:56:CA:04:64:BC
WAN 1	10:56:CA:04:64:BD
WAN 2	10:56:CA:04:64:BE
WAN 3	10:56:CA:04:64:BF

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

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

Important Note

If you encounter issues and would like to contact the Peplink Support Team (<http://www.peplink.com/contact/>), please download the diagnostic report file and attach it along with a description of your issue. In Firmware 5.1 or before, the diagnostic report file can be obtained at **System>Reboot**.

28.2 Active Sessions

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

Session data captured within one minute. Refresh		
Service	Inbound Sessions	Outbound Sessions
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 listing for additional information. This screen also indicates the number of sessions initiated by each WAN port. Finally, you can see which clients are initiating the most sessions.

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

Overview Search

Session data captured 1 min ago. [Refresh](#)

IP / Subnet	<input type="text"/> Source or Destination ▾	/ 255.255.255.255 (/32) ▾
Port	<input type="text"/> Source or Destination ▾	
Protocol / Service	<input type="text"/> SSL ▾	
Interface	<input type="checkbox"/> 1 WAN 1 <input type="checkbox"/> 2 WAN 2 <input type="checkbox"/> 3 WAN 3 <input type="checkbox"/> 4 WAN 4 <input type="checkbox"/> 5 WAN 5 <input type="checkbox"/> 6 WAN 6 <input type="checkbox"/> 7 WAN 7 <input type="checkbox"/> 8 WAN 8 <input type="checkbox"/> 9 WAN 9 <input type="checkbox"/> 10 WAN 10 <input type="checkbox"/> 11 WAN 11 <input type="checkbox"/> 12 WAN 12 <input type="checkbox"/> Mobile Internet <input type="checkbox"/> VPN	

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Transit

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

This **Active Sessions** section displays the active inbound / outbound sessions of each WAN connection on the Peplink Balance. A filter is available to help sort out the active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering.

28.3 Client List

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

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

Filter	<input type="checkbox"/> Online Clients Only	<input type="checkbox"/> DHCP Clients Only			
Client List					
IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
 192.168.167.10		0	0	10:56:CA:0A:56:58	
 192.168.167.11	PogoU64-2-1	0	0	00:50:56:99:49:1A	
 192.168.167.12	PogoU64-2-2	0	0	00:50:56:99:32:75	

If the PPTP server (see **Section Error! Reference source not found.**), SpeedFusion™ see **Section 12.1**), or AP controller (see **Section 20**) is enabled, you may see the corresponding connection name listed in the **Name** field.

28.4 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
Flush All	

The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server (see **Section 10**). The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush All** to flush all WINS client records.

28.5 OSPF & RIPv2

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

28.6 SpeedFusion™ Status

Current SpeedFusion™ status information is located at **Status>SpeedFusion™**.

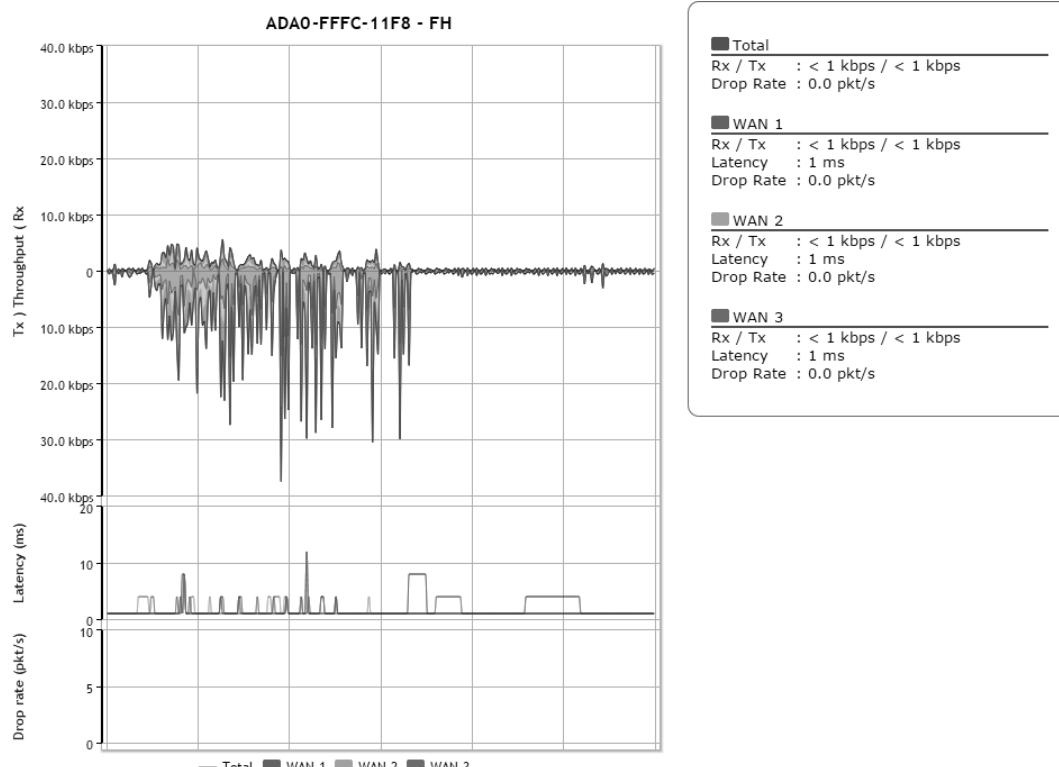
Details about SpeedFusion™ connection peers appears as below:

PepVPN with SpeedFusion - Remote Peer Details			Show disconnected profiles
Remote Peer ▲	Profile	Information	
🔒 ▶ ADA0-FFFC-11F8	FH	192.168.77.0/24	 
🔒 ▶ 3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24	 

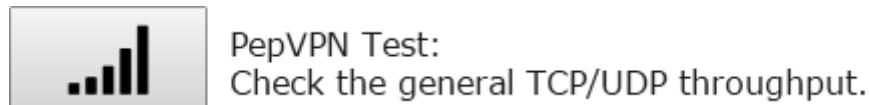
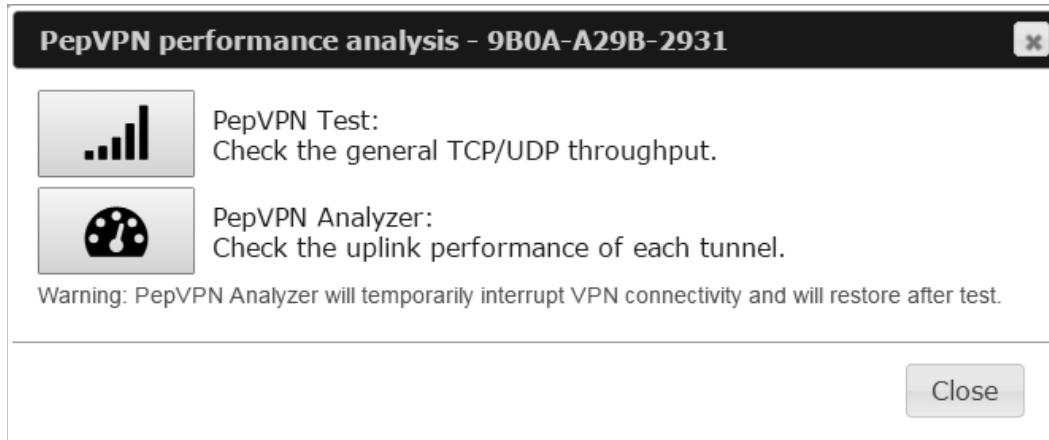
Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.

Remote Peer ▲	Profile	Information	
🔒 ▶ ADA0-FFFC-11F8	FH	192.168.77.0/24	 
▢ WAN 1	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms	
▢ WAN 2	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms	
▢ WAN 3	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 1 ms	
Total	Rx: < 1 kbps Tx: 1.1 kbps	Drop rate: 0.0 pkt/s	
🔒 ▶ 3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24	 
▢ WAN 1	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms	
▢ WAN 2	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms	
▢ WAN 3	Rx: < 1 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s Latency: 4 ms	
Total	Rx: 1.6 kbps Tx: < 1 kbps	Drop rate: 0.0 pkt/s	

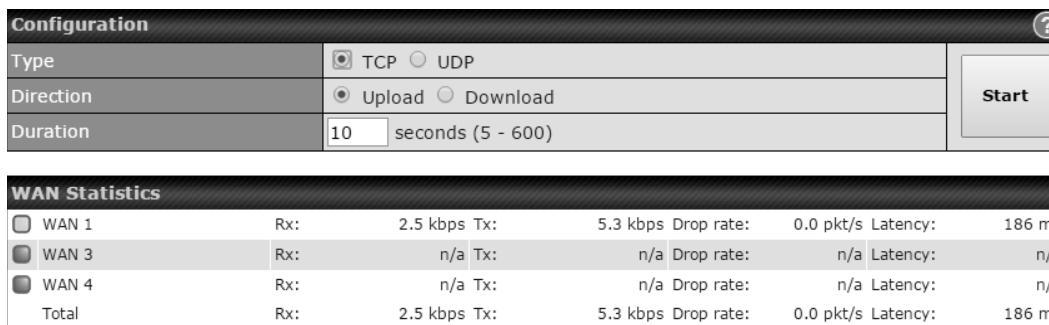
Click the  button for a chart displaying real-time throughput, latency, and drop-rate information for each WAN connection.



When pressing the  button, the following menu will appear:



After clicking the icon, the following menu appears:



The screenshot shows a configuration interface with sections for "Configuration" and "WAN Statistics".
Configuration:
Type: TCP UDP
Direction: Upload Download
Duration: 10 seconds (5 - 600)
Start button
WAN Statistics:
WAN 1: Rx: 2.5 kbps Tx: 5.3 kbps Drop rate: 0.0 pkt/s Latency: 186 ms
WAN 3: Rx: n/a Tx: n/a Drop rate: n/a Latency: n/a
WAN 4: Rx: n/a Tx: n/a Drop rate: n/a Latency: n/a
Total: Rx: 2.5 kbps Tx: 5.3 kbps Drop rate: 0.0 pkt/s Latency: 186 ms

Select the L2 protocol (TCP/UDP), direction, and duration and click the **Start** button to begin the general throughput test.

Results	
0.1250 MB / 1.00 sec =	1.0485 Mbps
1.0000 MB / 1.00 sec =	8.3888 Mbps
1.3125 MB / 1.00 sec =	11.0098 Mbps
3.0000 MB / 1.00 sec =	25.1465 Mbps
5.6875 MB / 1.00 sec =	47.7473 Mbps
6.0625 MB / 1.00 sec =	50.8562 Mbps
4.9375 MB / 1.00 sec =	41.4188 Mbps
4.5000 MB / 1.00 sec =	37.7487 Mbps
5.0000 MB / 1.00 sec =	41.9438 Mbps
5.6875 MB / 1.00 sec =	47.7099 Mbps
 37.3167 MB / 10.05 sec = 31.1504 Mbps 8 %TX 9 %RX 47 retrans 132.62 msRTT	
TEST DONE	



PepVPN Analyzer:
Check the uplink performance of each tunnel.

The bandwidth bonding 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. **Please note that the PepVPN Analyzer will temporarily interrupt VPN connectivity and will restore after test.**

After clicking the icon, the analyzer will require several minutes to perform its analysis depending the number of WAN links in the SpeedFusion™ Tunnel. Once the test the complete, the report will appear:

Results							
Estimated time: 150 s							
Time remaining: 0 s							
100%							
Local WAN1 > Remote WAN3	Local WAN1 > Remote WAN4	Local WAN1 > Remote WAN5	Local WAN1 > Remote WAN6	Tx Avg. (Mbps)	Tx Max. (Mbps)	Packet loss (%)	RTT (ms)
O	O	O	O	5.87	16.95	0.76	420.51
				20.72	26.39	1.59	29.89
		O	O	30.10	43.69	2.24	29.61
			O	45.01	55.93	2.16	28.24
O	O	O	O	24.87	33.56	0.86	49.86
O	O	O	O	19.30	31.28	0.01	49.78
O	O	O	O	18.59	30.41	2.08	39.78
O	O	O	O	20.56	34.60	0.00	38.11
O	O	O	O	36.70	59.16	2.64	42.06
	O	O	O	19.98	30.40	4.40	38.01
O	O	O	O	31.63	42.99	0.72	37.99
		O	O	36.88	55.78	2.60	33.89
O	O	O	O	38.30	47.89	0.01	29.98
	O	O	O	33.21	55.23	2.69	30.48
O	O	O	O	30.02	46.66	3.77	28.68

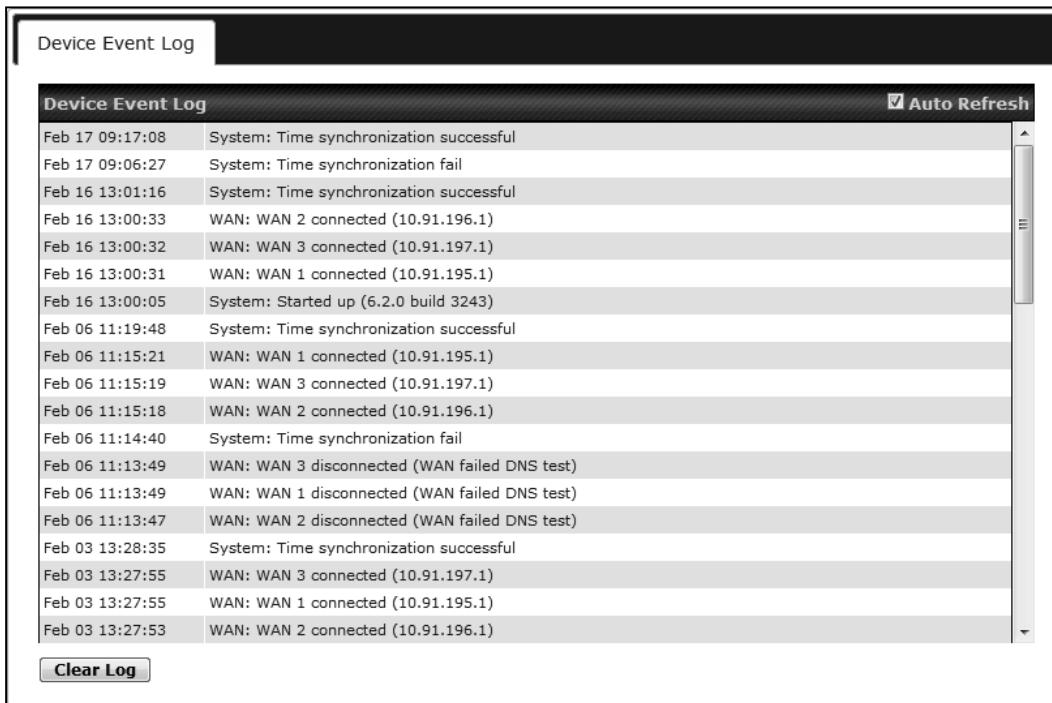
"O" indicates that specific WAN / Tunnel is active for that particular test.

"Tx Avg." is the averaged throughput across the full 10 seconds time, while "Tx Max." is the averaged throughput of the fastest 30% of time.

28.7 Event Log

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

28.7.1 Device Event Log



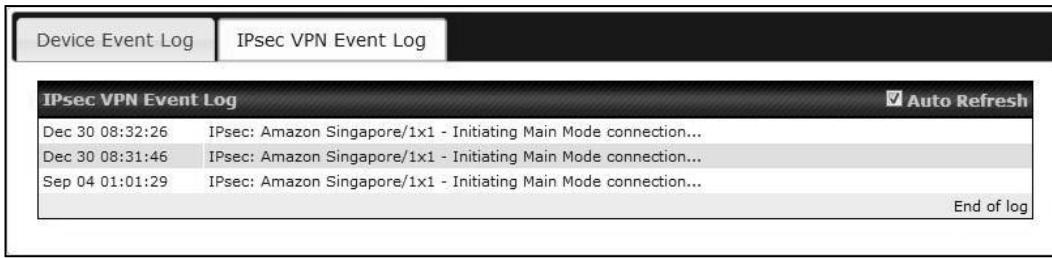
The screenshot shows the 'Device Event Log' section. At the top right is a checked checkbox labeled 'Auto Refresh'. Below the header is a scrollable list of log entries. The entries include various system and WAN connection events. At the bottom left is a 'Clear Log' button.

Date	Event Description
Feb 17 09:17:08	System: Time synchronization successful
Feb 17 09:06:27	System: Time synchronization fail
Feb 16 13:01:16	System: Time synchronization successful
Feb 16 13:00:33	WAN: WAN 2 connected (10.91.196.1)
Feb 16 13:00:32	WAN: WAN 3 connected (10.91.197.1)
Feb 16 13:00:31	WAN: WAN 1 connected (10.91.195.1)
Feb 16 13:00:05	System: Started up (6.2.0 build 3243)
Feb 06 11:19:48	System: Time synchronization successful
Feb 06 11:15:21	WAN: WAN 1 connected (10.91.195.1)
Feb 06 11:15:19	WAN: WAN 3 connected (10.91.197.1)
Feb 06 11:15:18	WAN: WAN 2 connected (10.91.196.1)
Feb 06 11:14:40	System: Time synchronization fail
Feb 06 11:13:49	WAN: WAN 3 disconnected (WAN failed DNS test)
Feb 06 11:13:49	WAN: WAN 1 disconnected (WAN failed DNS test)
Feb 06 11:13:47	WAN: WAN 2 disconnected (WAN failed DNS test)
Feb 03 13:28:35	System: Time synchronization successful
Feb 03 13:27:55	WAN: WAN 3 connected (10.91.197.1)
Feb 03 13:27:55	WAN: WAN 1 connected (10.91.195.1)
Feb 03 13:27:53	WAN: WAN 2 connected (10.91.196.1)

Clear Log

The log section displays a list of events that has taken place on the Peplink Balance unit. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

28.7.2 IPsec Event Log



The screenshot shows the 'IPsec VPN Event Log' section. At the top right is a checked checkbox labeled 'Auto Refresh'. Below the header is a scrollable list of log entries. The entries show IPsec connections being initiated. At the bottom right is the text 'End of log'.

Date	Event Description
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

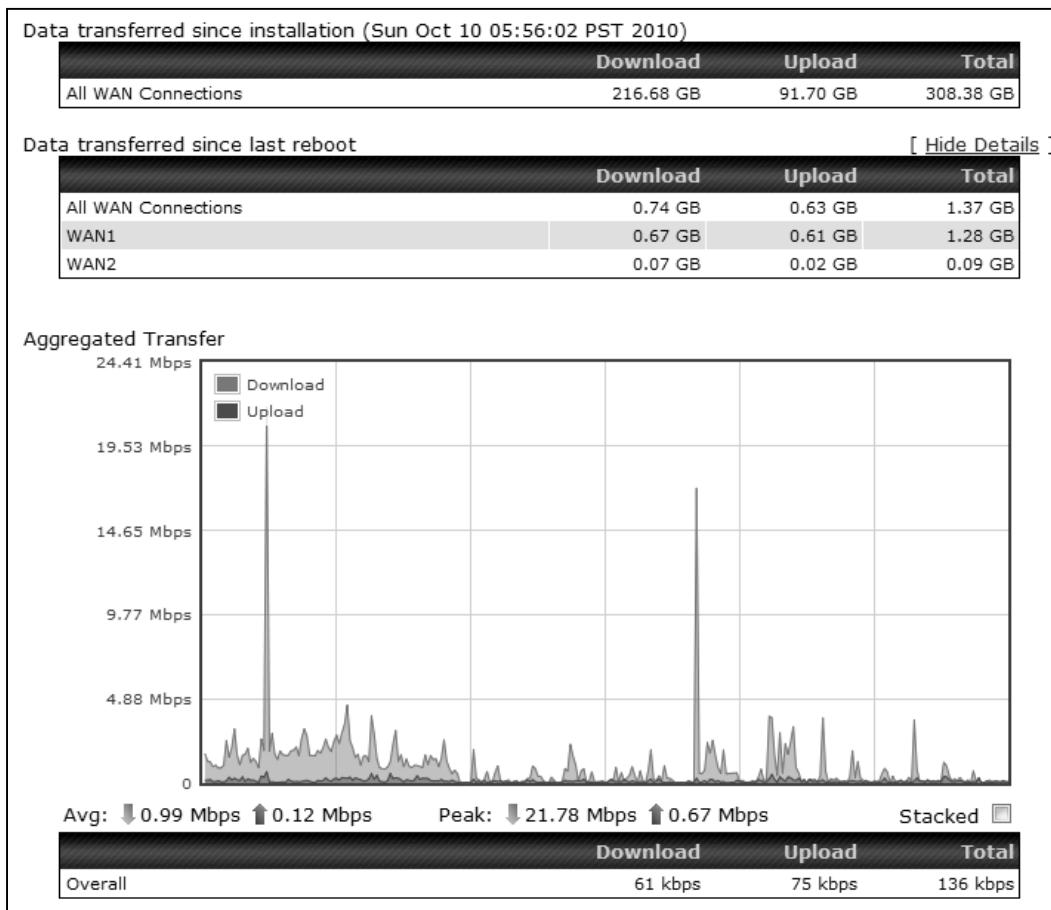
This section displays a list of events that has taken place within an IPsec VPN connection. Check the box next to **Auto Refresh** and the log will be refreshed automatically. For an AP event log, navigate to **AP>Info**.

28.8 Bandwidth

This section shows the bandwidth usage statistics, located at **Status>Bandwidth**. Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

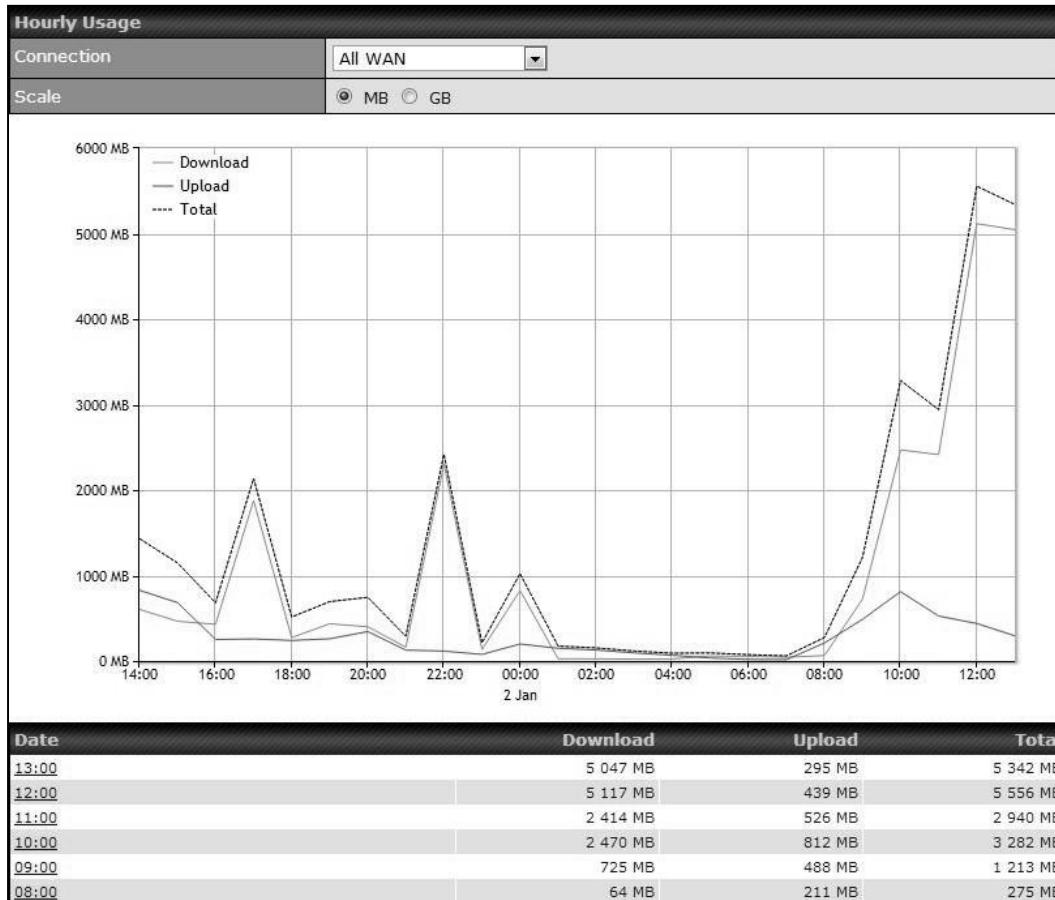
28.8.1 Real-Time

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



28.8.2 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.

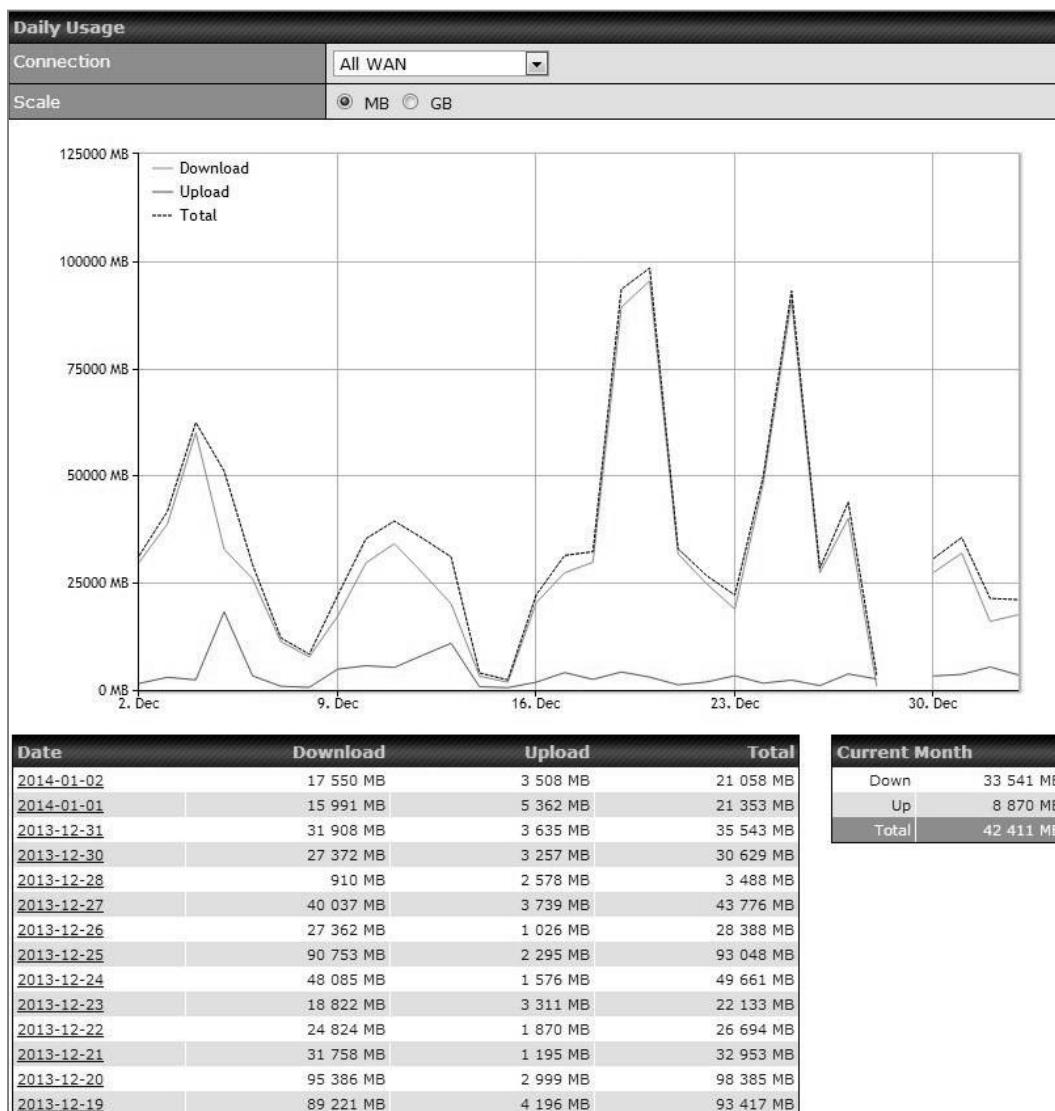


28.8.3 Daily

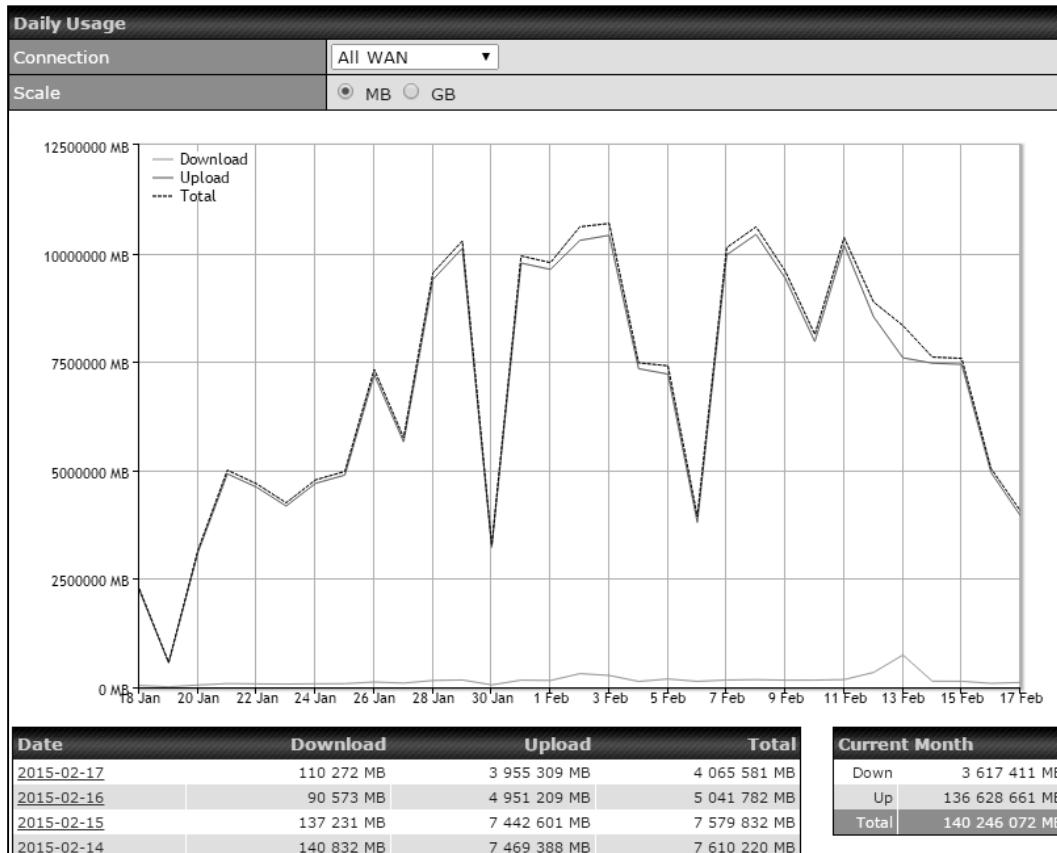
This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature as shown in **Section 14.4**, the **Current Billing Cycle** table for that WAN connection will be displayed.

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



Status



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

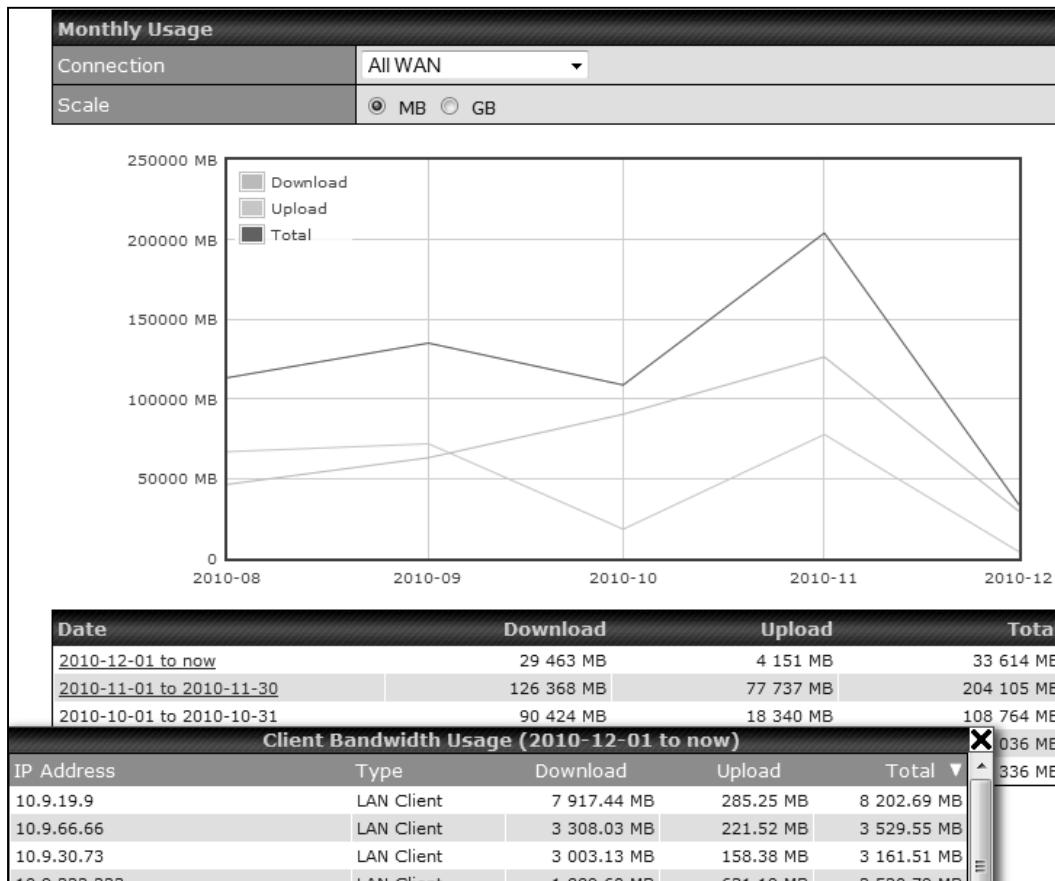
Client Bandwidth Usage (2015-02-15)

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

28.8.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection. If you have enabled **Bandwidth Monitoring** feature as shown in **Section 14.4**, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

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



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

Appendix A. Restoration of Factory Defaults

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

For Balance models with a reset button:

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

For Balance/MediaFast models with an LCD menu:

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

Afterwards, the factory default settings will be restored.

Important Note

All user settings will be lost after restoring the factory default settings. Regular backup of configuration parameters is strongly recommended.

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

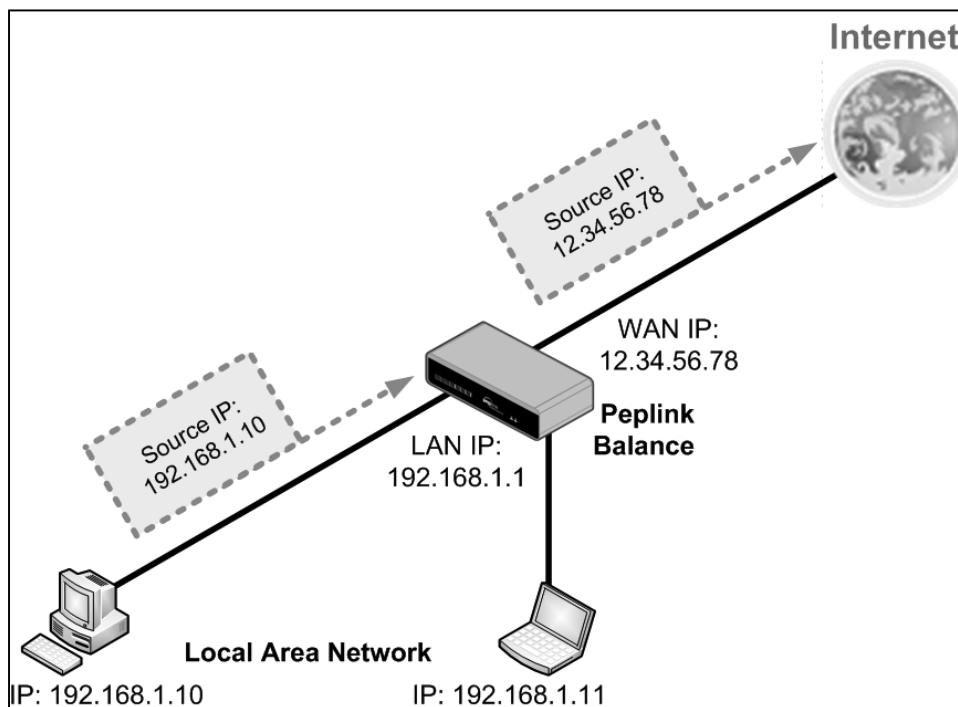
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

C.1 Routing Via Network Address Translation (NAT)

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

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

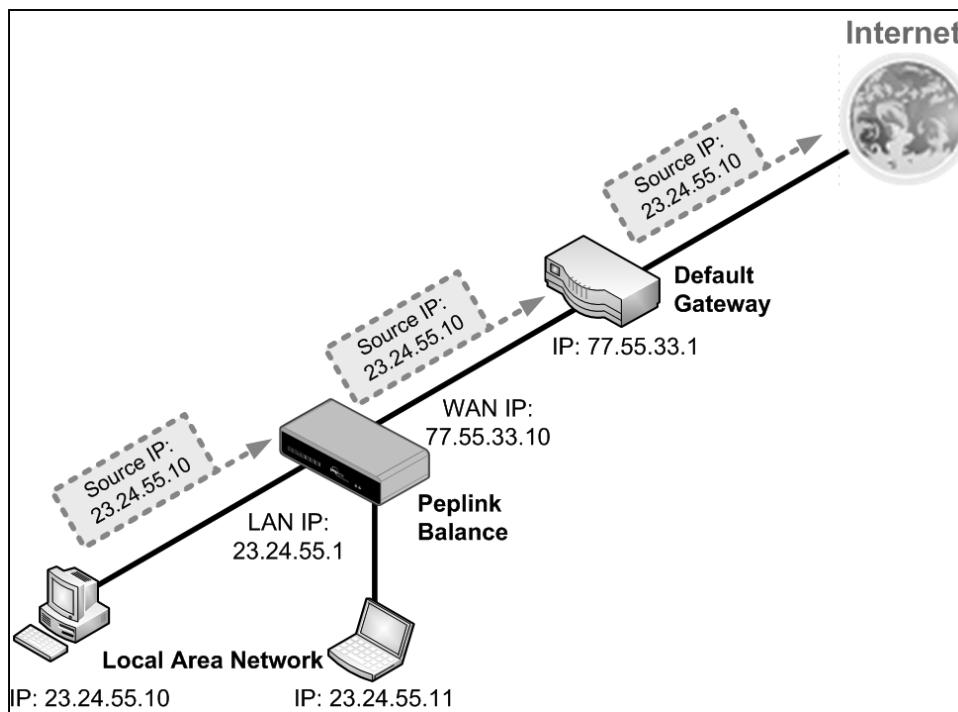
The following figure shows the packet flow in NAT mode:



C.2 Routing Via IP Forwarding

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

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



Appendix D. Case Studies

D.1 MPLS Alternative

Our SpeedFusion enabled routers can be used to bond multiple low-cost/commodity Internet connections to replace an expensive managed business Internet connection, private leased line, MPLS, and frame relay without sacrificing reliability and availability.

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

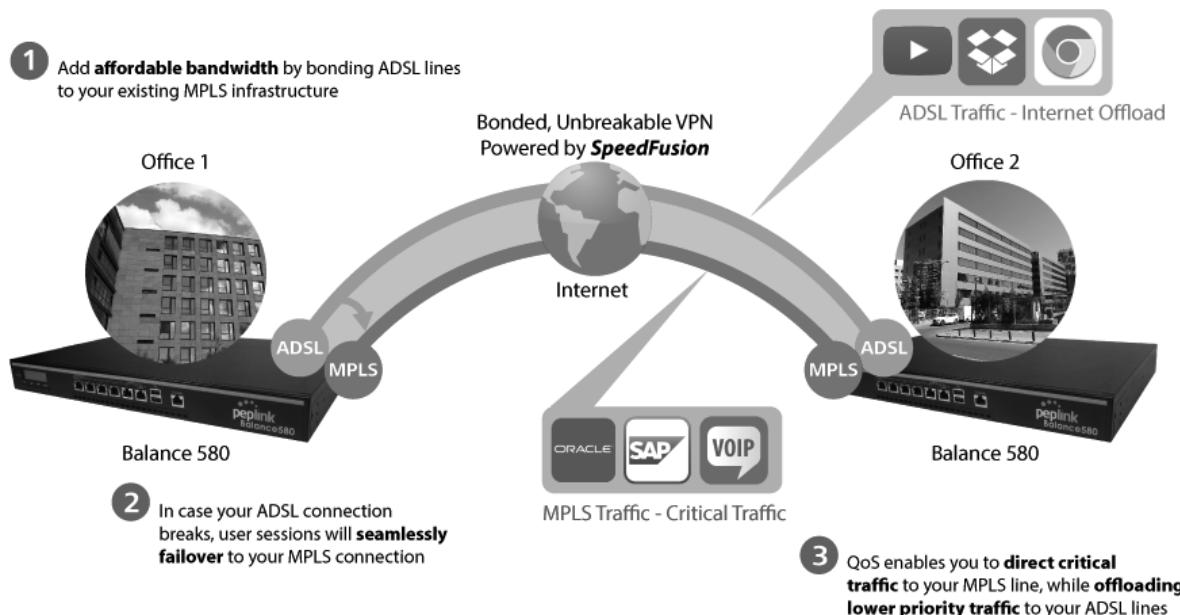
Special features of Balance 580: have high availability capability

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

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

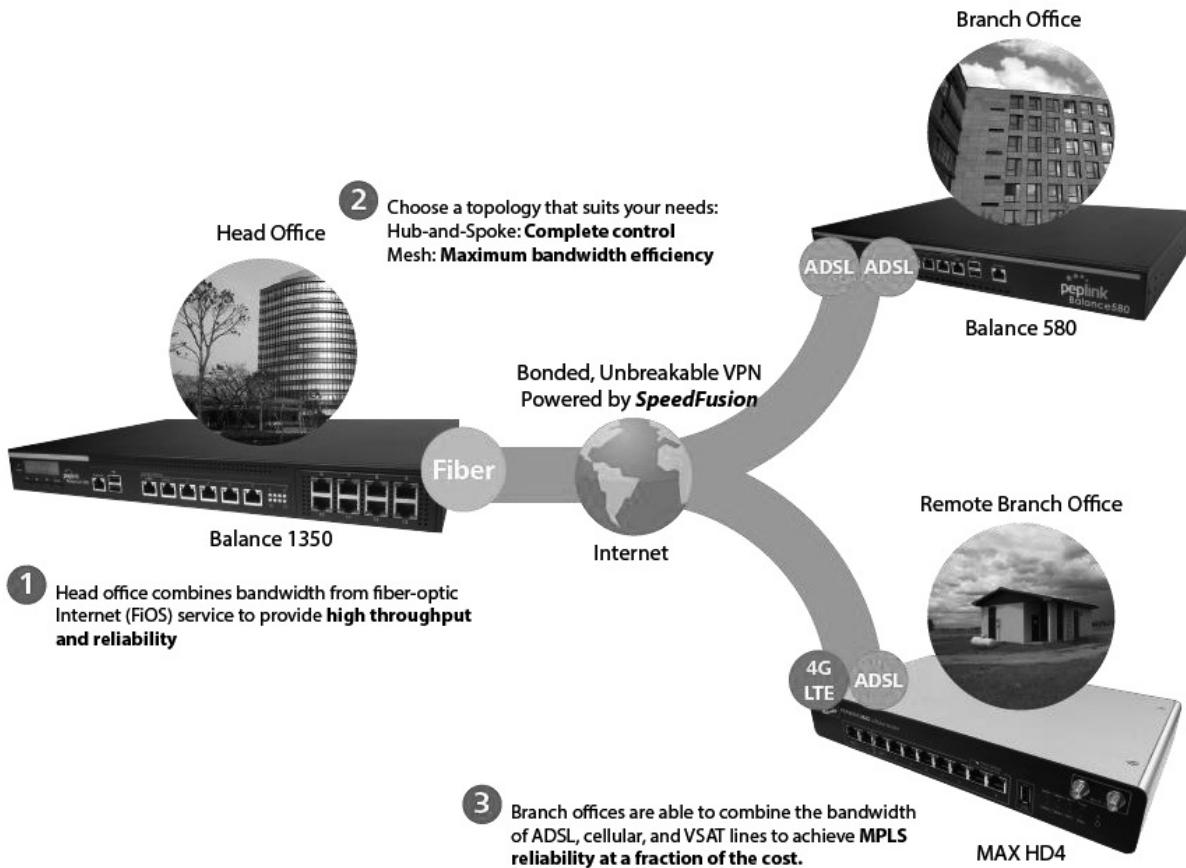
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement



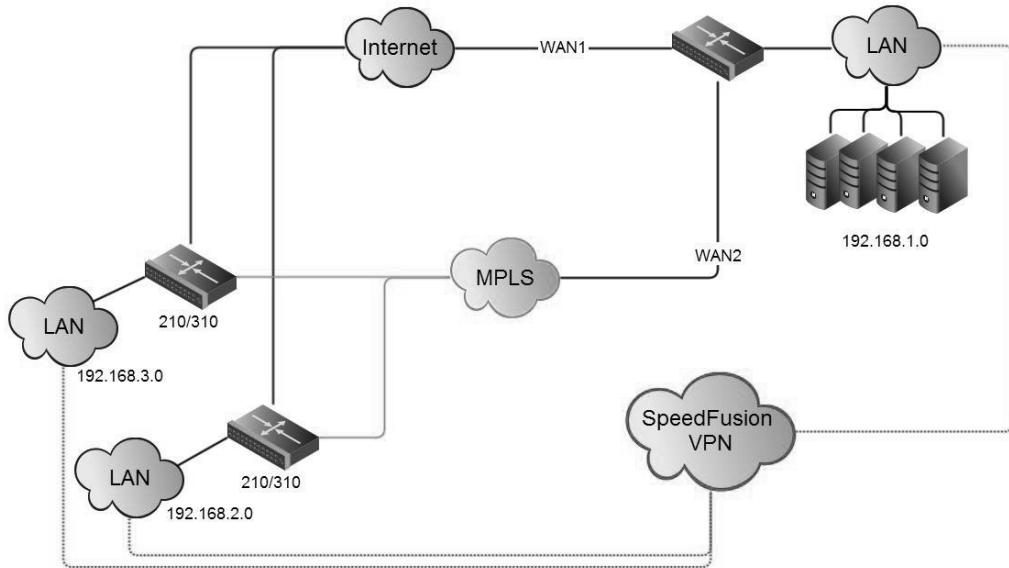
Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your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

Option 2: MPLS Alternative



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

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



Environment:

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

Requirement:

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

Recommended Solution:

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

Devices Deployed: Balance 210, Balance 310, Balance 580

Harrington Industrial Plastics



Overview

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

Requirements

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

Solution

- Peplink Balance 1350
- Peplink Balance 380
- Unbreakable VPN

Benefits

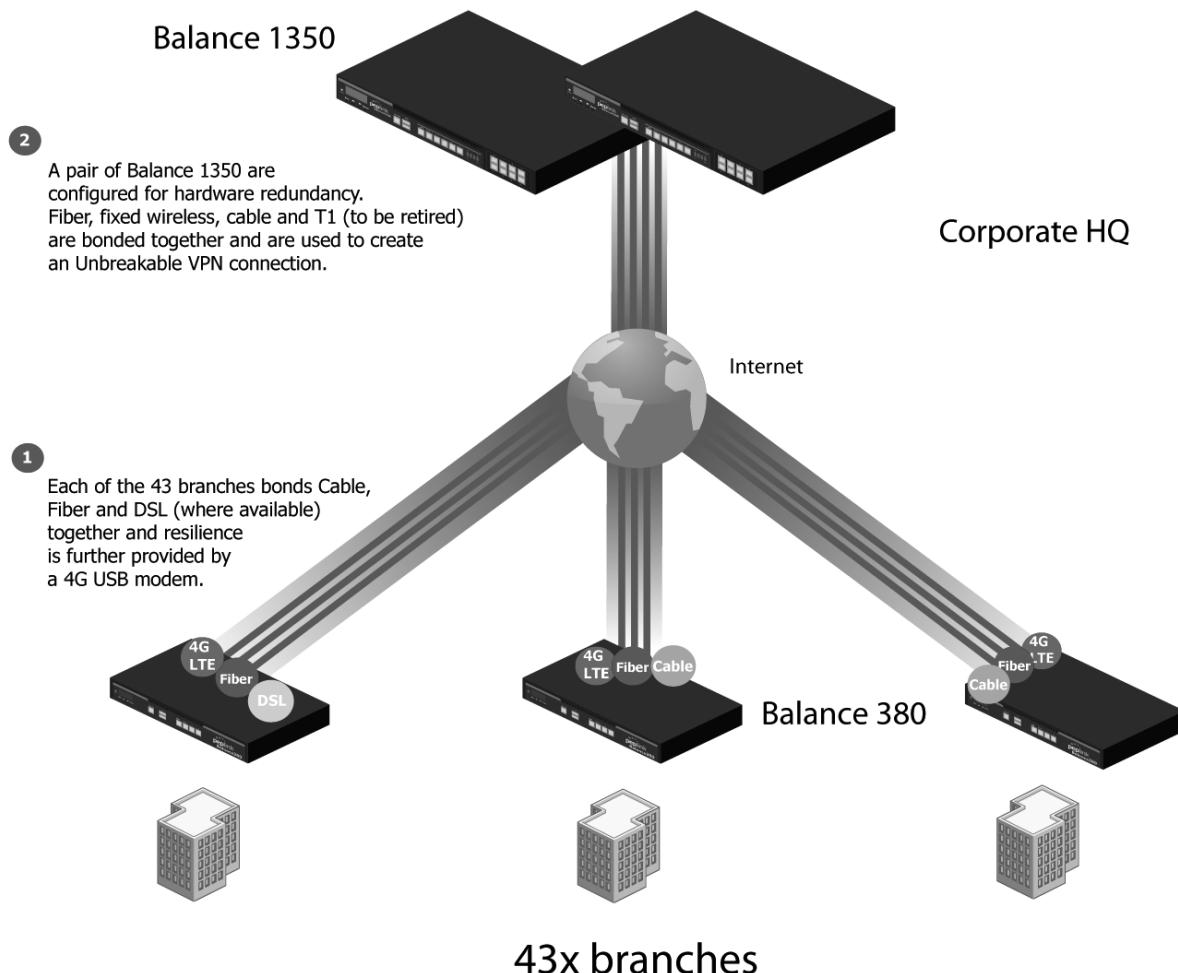
- Extreme savings of \$100,000 per year
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

Time For An Upgrade

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

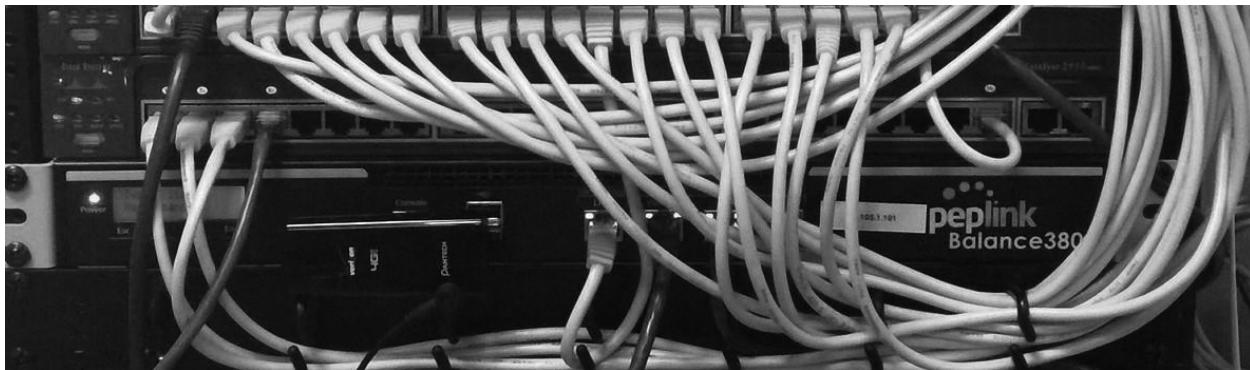
Quick Deployment and Unbreakable Connectivity

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



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

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



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

PLUSS

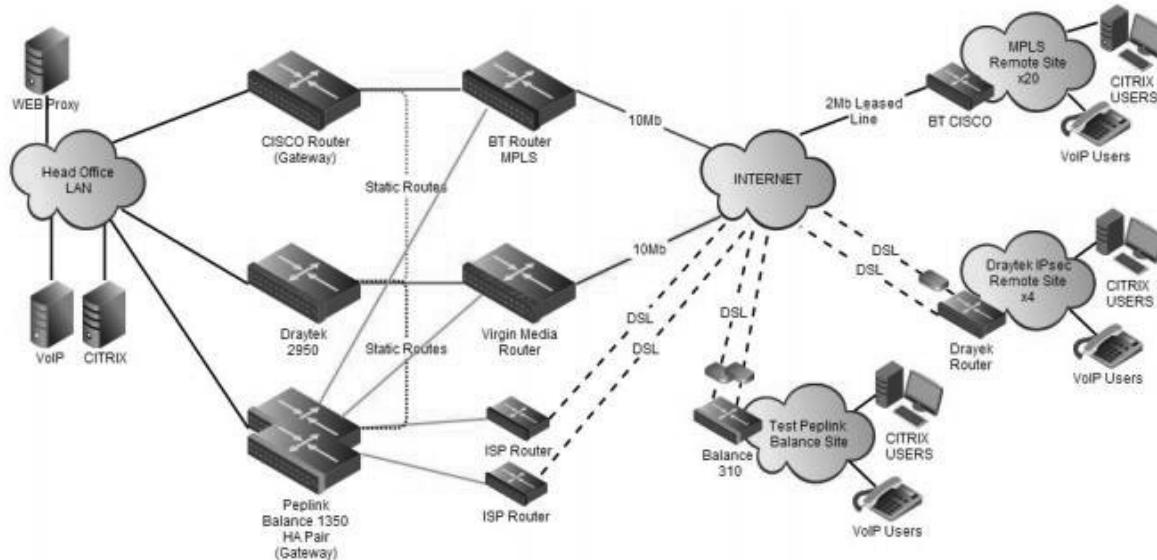
Peplink + Citrix + VoIP Adds Up to Fast, Cost-Effective WAN for Pluss



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

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

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



D.2 Colégio Next - Enabling eLearning



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

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

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

Requirements

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

Solution

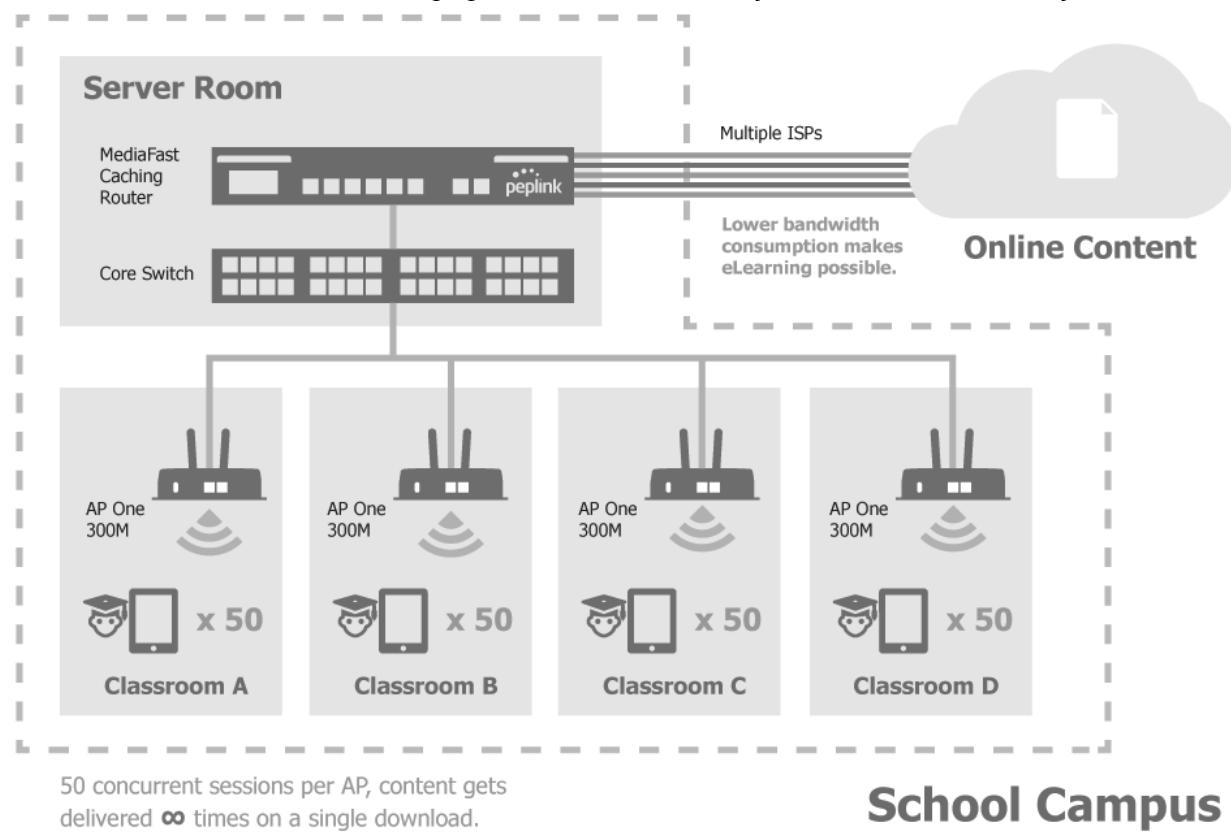
- Peplink MediaFast
- Multi-WAN Content-caching router, tailor-made for Education networking.
- AP One 300M
- Enterprise grade AP, 5GHz Wi-Fi, up to 60 concurrent users.

Benefits

- Instant, simultaneous access to media-rich educational content for 500+ iPads
- Wi-Fi connection stability for 50+ users per classroom, not achievable by other tested

equipment

- Teachers, students and guests can be assigned access priority to available bandwidth, further preventing congestion
- iOS updates (often 2GB size) no longer congest the network as they are downloaded only once, cached on the MediaFast and then distributed to all iOS devices
- AP Controller makes MAC Address Filtering easy. Students are assigned to designated APs by their devices' MAC Address in order to prevent saturating any single AP.
- Flawless iPad AirPlay mirroring at all times
- iPads are used all day, reaching their full potential with a fast and stable network all the time
- Students are far more engaged and teachers rely on their iPads all day



D.3 Performance Optimization

D.3.1 Scenario

In this scenario, email and web browsing are the two main Internet services used by LAN users.

The mail server is external to the network. The connections are ADSL (WAN1, with slow uplink and fast downlink) and Metro Ethernet (WAN2, symmetric).

D.3.2 Solution

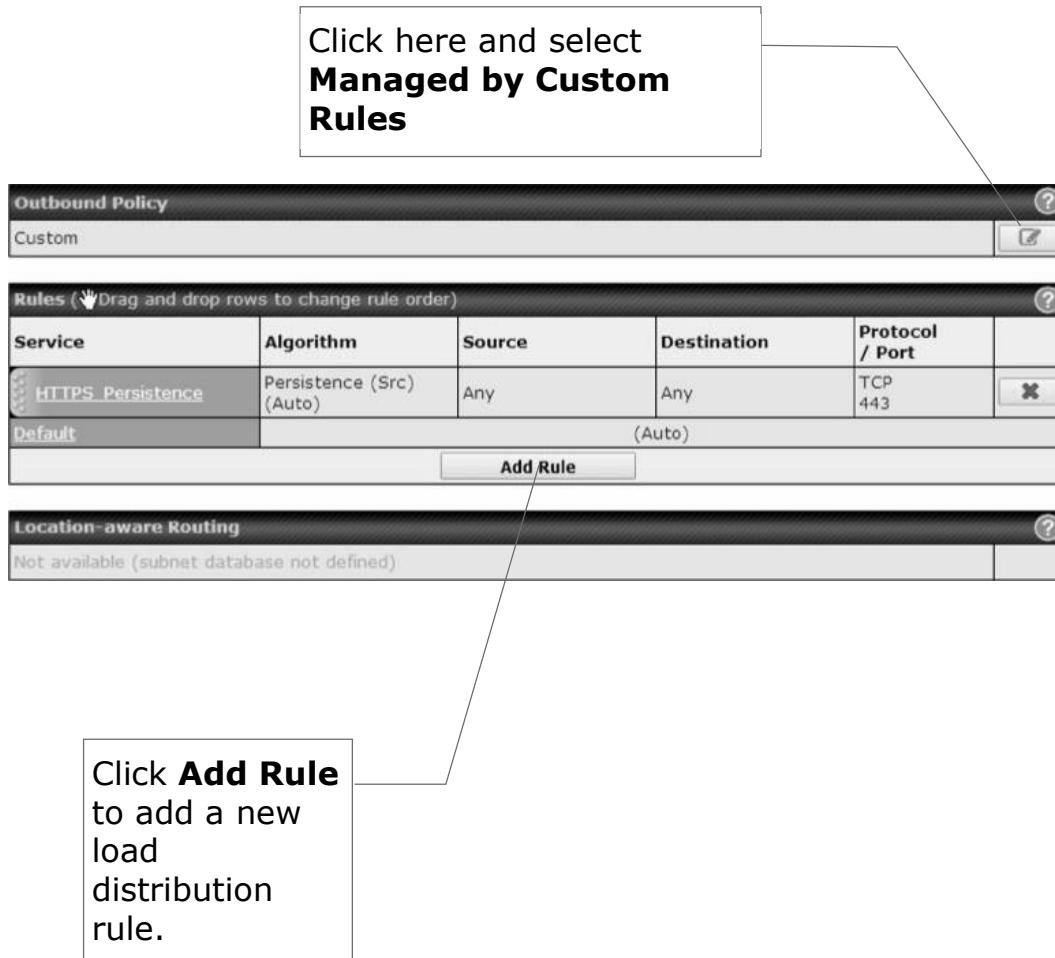
For optimal performance with this configuration, individually set the WAN load balance according to the characteristics of each service.

- Web browsing mainly downloads data; sending e-mails mainly consumes upload bandwidth.
- Both connections 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.

D.3.3 Settings

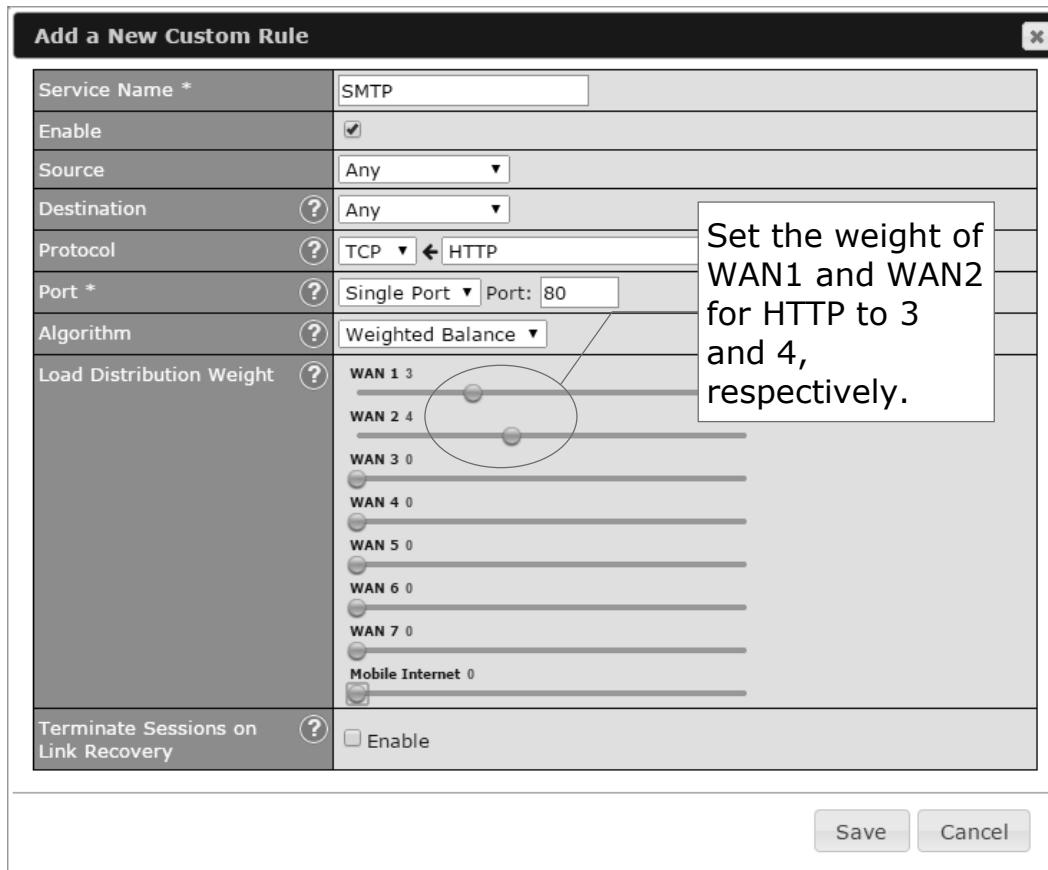
1. Add a new outbound traffic rule for HTTP.
2. Add a new outbound traffic rule for SMTP.

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



Settings for HTTP:

Add a New Custom Rule

Service Name *	SMTP
Enable	<input checked="" type="checkbox"/>
Source	Any ▾
Destination	Any ▾
Protocol	TCP ▾ HTTP
Port *	Single Port ▾ Port: 80
Algorithm	Weighted Balance ▾
Load Distribution Weight	<p>WAN 1 3 WAN 2 4 WAN 3 0 WAN 4 0 WAN 5 0 WAN 6 0 WAN 7 0 Mobile Internet 0</p>  <p>Set the weight of WAN1 and WAN2 for HTTP to 3 and 4, respectively.</p>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

Save Cancel

Settings for SMTP:

Add a New Custom Rule

Service Name *	SMTP
Enable	<input checked="" type="checkbox"/>
Source	Any ▾
Destination	Any ▾
Protocol	TCP ▾ ← SMTP ▾
Port *	Single Port ▾ Port: 25
Algorithm	Weighted Balance ▾
Load Distribution Weight	<p>WAN 1 1 WAN 2 8 WAN 3 10 WAN 4 10 WAN 5 10 WAN 6 10 WAN 7 10 Mobile Internet 10</p> <p>Set the weight of WAN1 and WAN2 for SMTP to 1 and 8, respectively.</p>
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

Save Cancel

D.4 Maintaining the Same IP Address Throughout a Session

D.4.1 Scenario

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

D.4.2 Solution

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

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

D.4.3 Settings

Set persistence in at **Advanced>Outbound Policy**.

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

Add a New Custom Rule

Service Name *	HTTP Persistence
Enable	<input checked="" type="checkbox"/>
Source	Any
Destination	Any
Protocol	TCP ▾ ↳ HTTP
Port *	Single Port ▾ Port: 80
Algorithm	Persistence
Persistence Mode	<input type="radio"/> By Source <input checked="" type="radio"/> By Destination
Load Distribution	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

Save **Cancel**

Tip

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

D.5 Bypassing the Firewall to Access Hosts on LAN

D.5.1 Scenario

There are times when remote access to computers on the LAN is desirable; for example, when hosting web sites, online businesses, FTP download and upload areas, etc. In such cases, it may be appropriate to create an inbound NAT mapping for the network to allow some hosts on the LAN to be accessible from outside of the firewall.

D.5.2 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**.

In this example, the host with an IP address of 192.168.1.102 is bound to 10.90.0.75 of WAN1:

The screenshot shows the 'NAT Mappings' configuration page. A table lists a single entry for a LAN client with IP 192.168.1.102. The 'Inbound Mappings' section shows a connection to WAN1 and an external IP of 10.90.0.75. The 'Outbound Mappings' section lists various WAN connections, each with its corresponding external IP set to 'Interface IP'. At the bottom are 'Save' and 'Cancel' buttons.

LAN Client(s)	Address	IP Address
	192.168.1.102	

Connection / Inbound IP Address(es)	
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.90.0.75 (Interface IP)
<input type="checkbox"/> WAN 2	
<input type="checkbox"/> WAN 3	
<input type="checkbox"/> WAN 4	
<input type="checkbox"/> WAN 5	
<input type="checkbox"/> WAN 6	
<input type="checkbox"/> WAN 7	
<input type="checkbox"/> Mobile Internet	

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

Save **Cancel**

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

D.6 Inbound Access Restriction

D.6.1 Scenario

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

D.6.2 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 **Advanced>Firewall>Access Rules**. Then click the **Add Rule** button in the **Inbound Firewall Rules** table and change the settings according to the following screenshot:

The screenshot shows a configuration dialog titled "Add a New Inbound Firewall Rule". It contains a table with the following fields and values:

New Firewall Rule	
Rule Name	Inbound Firewall rule Ex
Enable	<input checked="" type="checkbox"/>
WAN Connection	Any
Protocol	TCP < HTTP
Source IP & Port	Any Address Any Port
Destination IP & Port	Any Address Single Port Port: 80
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

At the bottom right are "Save" and "Cancel" buttons.

After the fields have been entered as in the screenshot, click **Save** to add the rule. Afterwards, change the default inbound rule to **Deny** by clicking the **default** rule in the **Inbound Firewall Rules** table. Click **Apply Changes** on the top right corner to complete the process.

D.7 Outbound Access Restriction

D.7.1 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 the Peplink Balance.

D.7.2 Solution

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

The screenshot shows a configuration dialog titled "Add a New Outbound Firewall Rule". It contains the following fields:

New Firewall Rule	
Rule Name	No FTP Access
Enable	<input checked="" type="checkbox"/>
Protocol	TCP < HTTP
Source IP & Port	Any Address Any Port
Destination IP & Port	Any Address Single Port Port: 21
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

At the bottom right are "Save" and "Cancel" buttons.

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

Appendix E. Troubleshooting

Problem 1

Outbound load is only distributed over one WAN connection.

Solution

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

For a single user, download management applications are recommended. The applications can split a file into pieces and download the pieces simultaneously.

Examples include: DownThemAll (Firefox Extension), iGetter (Mac), etc.

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

For additional details, please refer to this FAQ:

<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.). Why is the download speed still only that of a single link?

Solution

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

Problem 3

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

Solution

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

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's IP is 192.168.1.1) to test whether the connection to the Peplink Balance is OK.

Problem 5

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

Solution

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

Problem 6

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

Solution

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

Additional troubleshooting resources:

Peplink Knowledgebase: <http://www.peplink.com/knowledgebase/>

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

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 equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

5.15 ~ 5.25GHZ is for indoor user only.

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 20cm between the radiator & your body.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination.

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

Appendix G: Product Datasheets

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/>