

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.

11.1.9 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**.



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	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

from High Availability Pair counterpart.

11.1.10 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**.



The screenshot shows a web interface titled "Feature Activation". On the left, there is a label "Activation Key" next to a large, empty text input field for entering the activation key.

11.1.11 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.

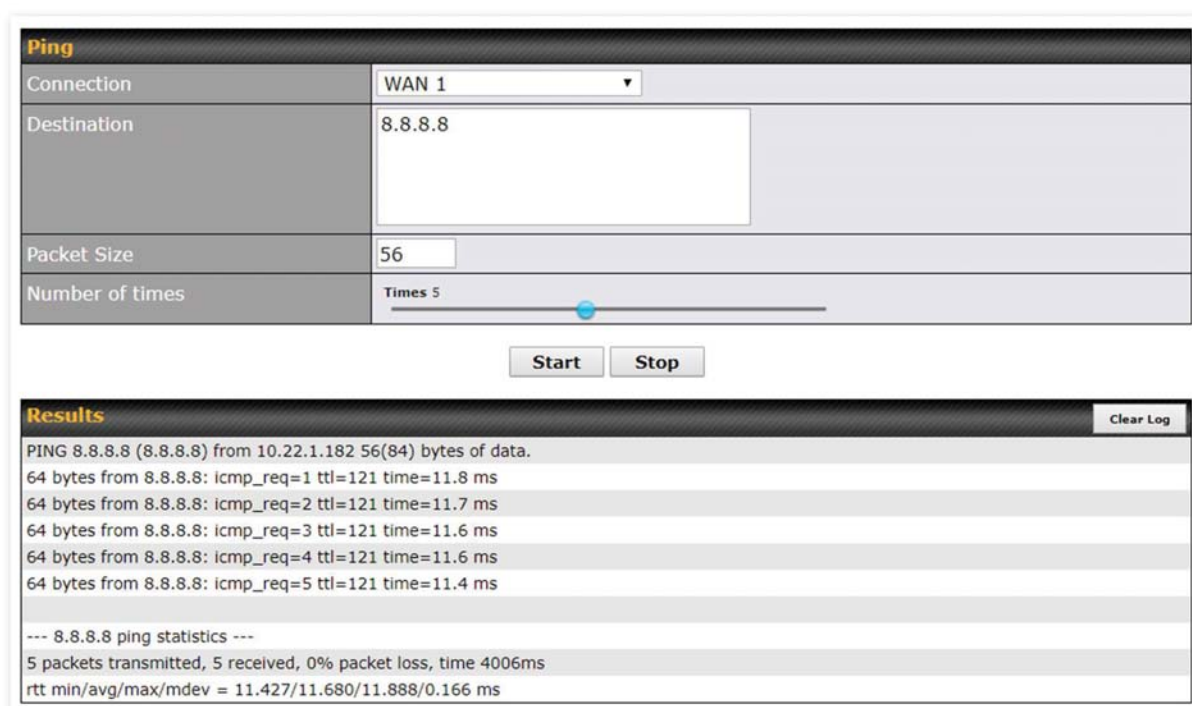


The screenshot shows a web interface titled "Reboot System" with a help icon (question mark) in the top right corner. Below the title bar, the text reads "Select the firmware you want to use to start up this device:". There are two radio button options: "Firmware 1: 8.0.0b03 build 2593 (Running)" which is selected, and "Firmware 2: 7.1.1 build 2460". At the bottom of the interface is a button labeled "Reboot".

11.2 Tools

11.3 Ping

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



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

Start Stop

Results		Clear Log
PING 8.8.8.8 (8.8.8.8) from 10.22.1.182 56(84) bytes of data.		
64 bytes from 8.8.8.8: icmp_req=1 ttl=121 time=11.8 ms		
64 bytes from 8.8.8.8: icmp_req=2 ttl=121 time=11.7 ms		
64 bytes from 8.8.8.8: icmp_req=3 ttl=121 time=11.6 ms		
64 bytes from 8.8.8.8: icmp_req=4 ttl=121 time=11.6 ms		
64 bytes from 8.8.8.8: icmp_req=5 ttl=121 time=11.4 ms		
--- 8.8.8.8 ping statistics ---		
5 packets transmitted, 5 received, 0% packet loss, time 4006ms		
rtt min/avg/max/mdev = 11.427/11.680/11.888/0.166 ms		

Tip

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

11.4 Traceroute

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

Traceroute

Connection	WAN 1
Destination	64.233.189.99

Results

```

1 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
2 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
3 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
4 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
5 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
6 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
7 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
8 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
9 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
10 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
11 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
12 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
13 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
14 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
15 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
16 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
17 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
18 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
19 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
20 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
21 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
22 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
23 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
24 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
25 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
26 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
27 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
28 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
29 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
30 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
31 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
32 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
33 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
34 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
35 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
36 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
37 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
38 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
39 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
40 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
41 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
42 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
43 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
44 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
45 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
46 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
47 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
48 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
49 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
50 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
51 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
52 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
53 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
54 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
55 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
56 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
57 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
58 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
59 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
60 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
61 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
62 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
63 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
64 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
65 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
66 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
67 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
68 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
69 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
70 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
71 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
72 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
73 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
74 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
75 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
76 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
77 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
78 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
79 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
80 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
81 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
82 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
83 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
84 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
85 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
86 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
87 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
88 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
89 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
90 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
91 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
92 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
93 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
94 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
95 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
96 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
97 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
98 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
99 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms
100 10.0.0.1 [10.0.0.1] 0.000 ms 0.000 ms 0.000 ms

```

Tip

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

11.5 Wake-on-LAN

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

Wake-on-LAN

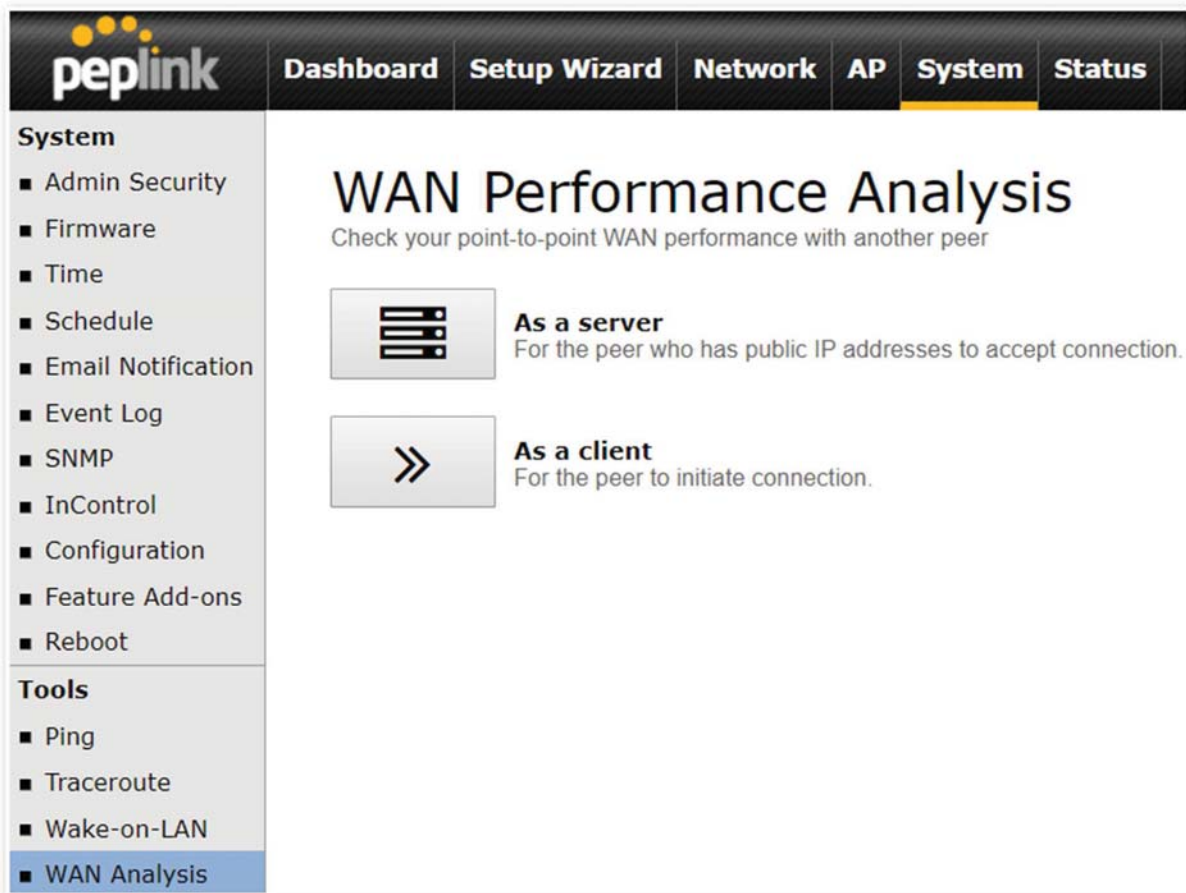
Wake-on-LAN Target	Custom MAC Address...	00:00:00:00:00:00	<input type="button" value="Send"/>
--------------------	-----------------------	-------------------	-------------------------------------

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

11.6 WAN Analysis

The WAN Analysis feature allows you to run a WAN to WAN speedtest between 2 Peplink devices .

You can set a device up as a **Server** or a **Client**. One device must be set up as a server to run the speed tests and the server must have a public IP address. T



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

System


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


Tools

- Ping
- Traceroute
- Wake-on-LAN
- WAN Analysis

WAN Performance Analysis

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

 **As a server**
For the peer who has public IP addresses to accept connection.

 **As a client**
For the peer to initiate connection.

The default port is 6000 and can be changed if required. The IP address of the WAN interface will be shown in the **WAN Connection Status** section.

peplink Dashboard Setup Wizard Network AP **System** Status Apply Changes

System

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

Tools

- Ping
- Traceroute
- Wake-on-LAN
- WAN Analysis

WAN Performance Analysis

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

Server Settings

Status	<input checked="" type="checkbox"/> Listening (Control Port: 6000)
Control Port	6000

Apply Stop

WAN Connection Status

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

The client side has a few more settings that can be changed. Make sure that the **Control Port** matches what's been entered on the server side. Select the WAN(s) that will be used for testing and enter the Servers WAN IP address. Once all of the options have been set, click the **Start Test** button.

peplink

Dashboard
Setup Wizard
Network
AP
System
Status
Apply Changes

System

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

Tools

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

WAN Performance Analysis

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

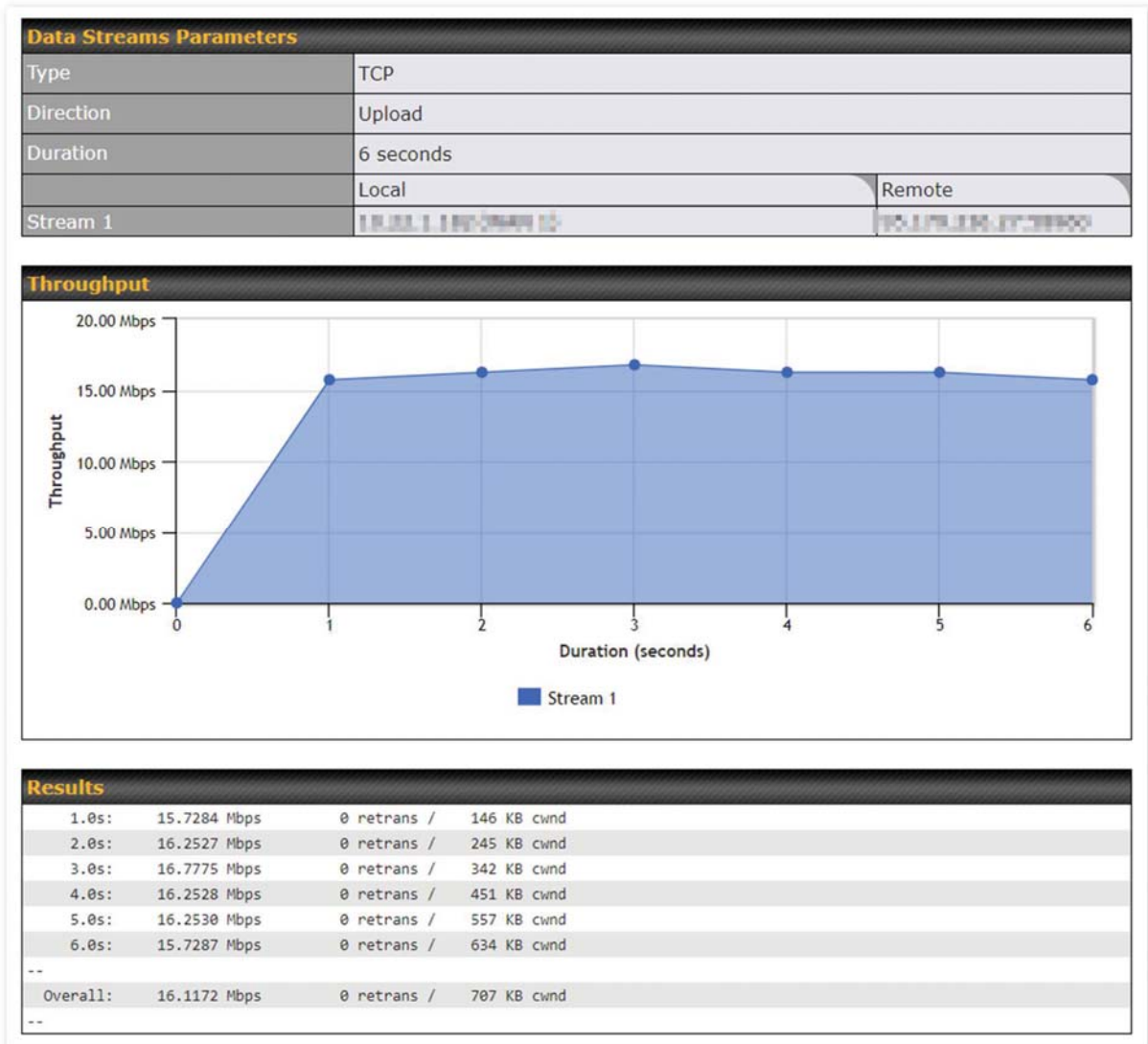
Client Settings

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

Data Streams

Local WAN Connection	Remote IP Address
1. -- Not Used --	
2. -- Not Used --	
3. -- Not Used --	
4. -- Not Used --	
5. -- Not Used --	
6. -- Not Used --	
7. -- Not Used --	
8. -- Not Used --	

The test output will show the **Data Streams Parameters**, the **Throughput** as a graph, and the **Results**.



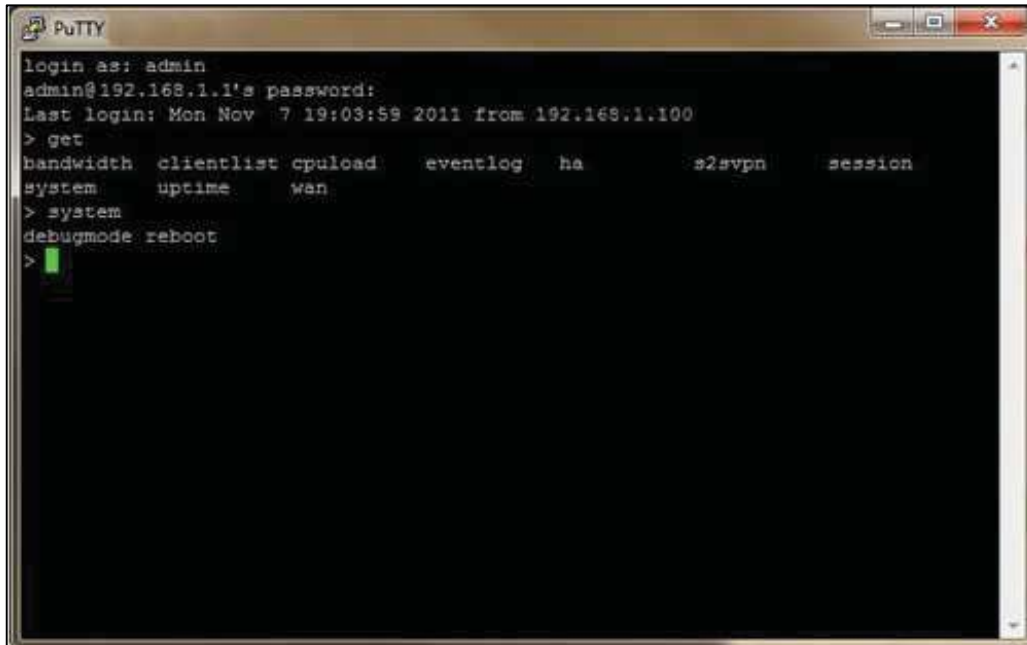
The test can be run again once it's complete by clicking the **Start** button or you can click **Close** and change the parameters for the test.

11.7 CLI (Command Line) Support

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

The serial console connector on other Peplink Balance units is a DB-9 male connector.

To access the serial console port, connect a null modem cable with a DB-9 connector on both ends to a terminal with the port setting of *115200,8N1*.



```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist  cpuload  eventlog  ha      s2svpn  session
system    uptime    wan
> system
debugmode  reboot
>
```

12 Status Tab

12.1 Status

12.1.1 Device

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

System Information	
Router Name	Mediafast
Model	Peplink MediaFast 500
Product Code	MFA-500-B
Hardware Revision	2
Serial Number	
Firmware	8.0.0b03 build 2593
PepVPN Version	8.0.0
Modem Support Version	1022 (Modem Support List)
Host Name	mediafast
Uptime	54 days 23 hours 7 minutes
System Time	Wed Apr 17 14:08:23 BST 2019
Content Filtering Database	Download (r20180514) Update
Diagnostic Report	Download
Remote Assistance	Turn On

MAC Address	
LAN	10:56:
WAN 1	10:56:
WAN 2	10:56:
WAN 3	10:56:
WAN 4	10:56:
WAN 5	10:56:

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 .

12.1.2 Active Sessions

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

Overview		Search	
Session data captured within one minute. Refresh			
Service	Inbound Sessions	Outbound Sessions	
DNS	0	51	
Facebook	0	1	
Google	0	33	
Google Ads	0	5	
HTTP	0	2	
IPsec	0	2	
QUIC	0	19	
SIP	0	8	
SSH	0	3	
SSL	1	136	
Skype	0	6	
Spotify	0	4	
Interface	Inbound Sessions	Outbound Sessions	
BT	1	360	
Virgin Media	0	0	
WAN_3	0	0	
WAN_4	0	6	
WAN_5	0	2	
WAN_6	0	0	
Top Clients			
Client IP Address	Total Sessions		
10.22.1.100	116		
10.22.1.101	90		
172.16.17.100	86		
10.22.1.102	83		
172.16.17.101	73		

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

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

Overview
Search

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

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

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
TCP	10.0.0.1:58827	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.0.0.1:58828	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.0.0.1:58784	35.186.224.47:443	SSL/Spotify	BT	00:00:10
TCP	10.0.0.1:65369	35.186.224.53:443	SSL/Spotify	BT	00:00:29

Total searched results: 4

Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Transit

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0







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

12.1.3 Client List

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

Clients can be imported into the DHCP reservation table by clicking the button on

the right. Further update the record after the import by going to **Network>LAN**.

Filter		<input type="checkbox"/> Online Clients Only	<input type="checkbox"/> DHCP Clients Only		
Client List					
IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
 192.168.167.10		0	0	10:56:56:168:167:10	
 192.168.167.11	U64-2-1	0	0	00:50:56:168:167:11A	
 192.168.167.12	U64-2-2	0	0	10:56:56:168:167:12	

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

12.1.4 WINS Clients

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

WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4

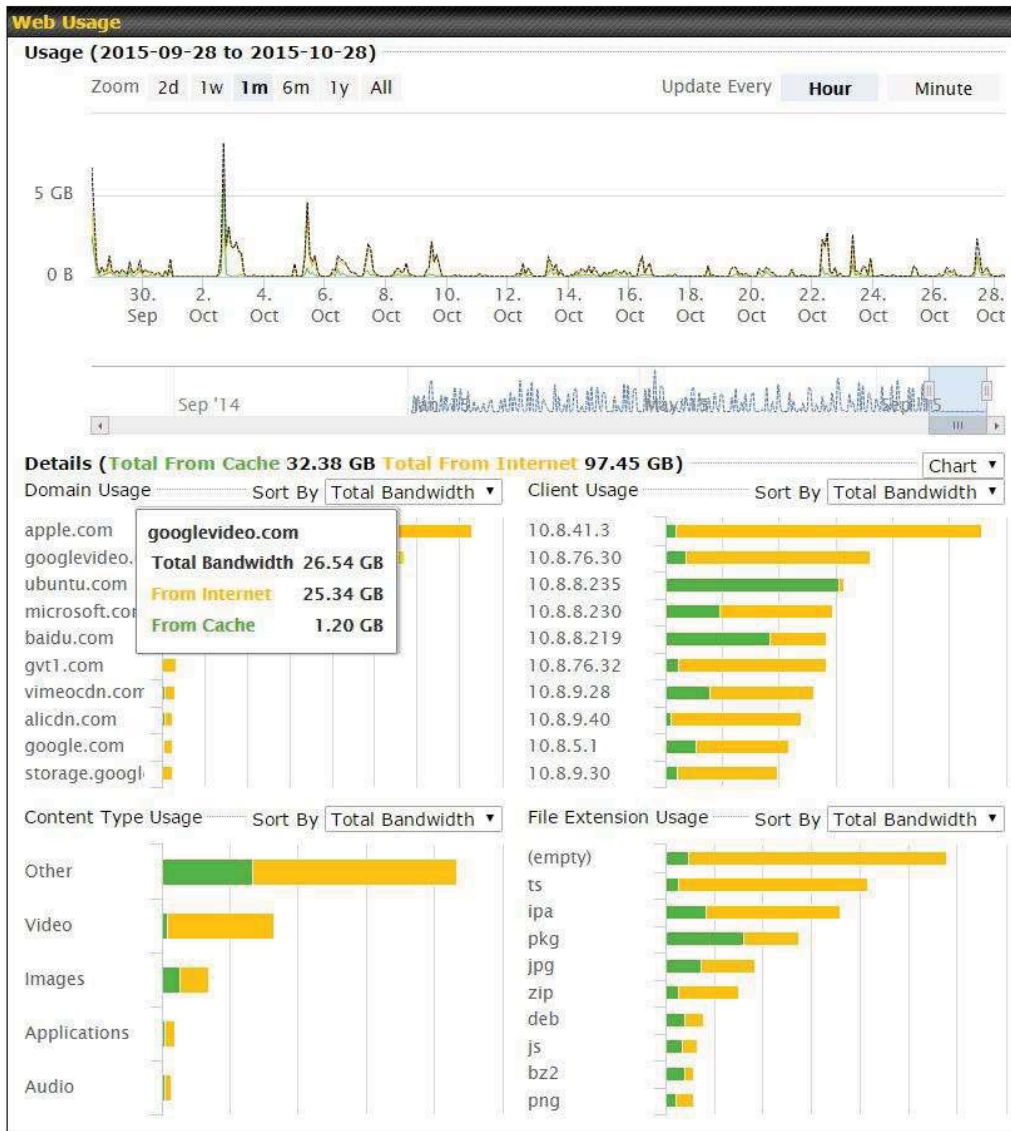
The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server. The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush All** to flush all WINS client records.

12.1.5 OSPF & RIPv2

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

12.1.6 MediaFast

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




12.1.7 SpeedFusion Status

Current SpeedFusion™ status information is located at **Status>SpeedFusion™**. Details about SpeedFusion™ connection peers appears as below:



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

Remote Peer	Profile	Information
FFFC-FFFC-FFFC	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
3ED2-3ED2-3ED2	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:

PepVPN Details ✕

Connection Information More information

Profile	BT		
Remote ID	192.168.1.1		
Router Name	192.168.1.1		
Serial Number	192.168.1.1		
Encapsulation Protocol	UDP		
Latency Difference Cutoff	500 ms		

WAN Statistics 📊

Remote Connections	<input type="checkbox"/> Show remote connections		
WAN Label	<input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port		
BT	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 18 ms
Virgin Media	Not available - WAN disabled		
WAN 3	Not available - WAN disabled		
WAN 4	Not available - link failure, no data received		
Registered via Speedfusion	Not available - link failure, no data received		
Speedfusion (Internet)	Not available - WAN down		
Total	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s

PepVPN Test Configuration ?

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

PepVPN Test Results

No information

The **connection information** shows the details of the selected PepVPN profile, consisting of the Profile name, **Router ID**, **Router Name** and **Serial Number** of the remote router

Advanced features for the PepVPN profile will also be shown when the **More Information** checkbox is selected.

The **WAN statistics** show information about the local and remote WAN connections (when **show Remote connections**) is selected.

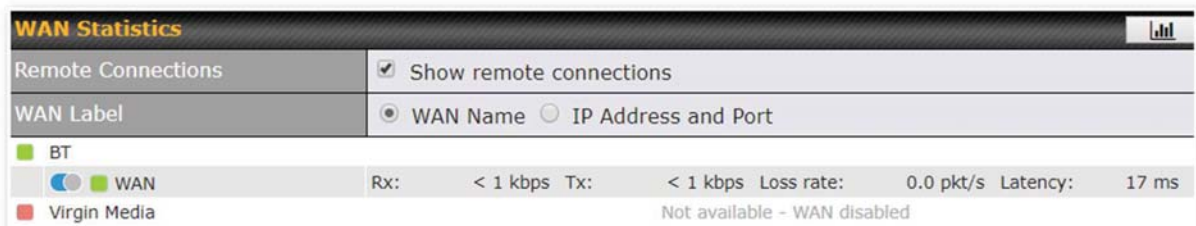
The available details are **WAN Name**, **IP address** and **port** used for the Speedfusion connection. **Rx and Tx rates**, **Loss rate** and **Latency**.



Connections can be temporarily disabled by sliding the switch button next to a WAN connection to the

left.

The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15 minutes without any action.

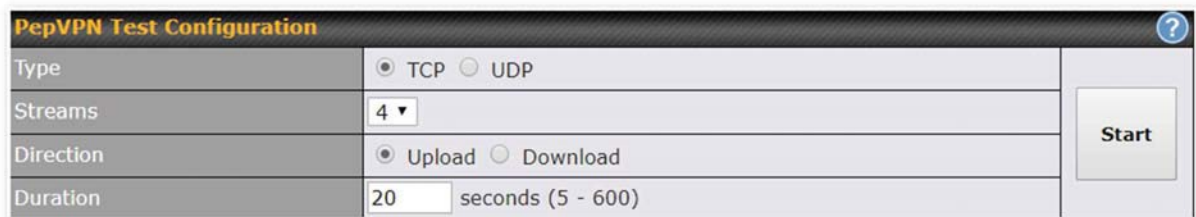
This can be used when testing the PepVPN speed between two locations to see if there is interference or network congestion between certain WAN connections.



WAN Statistics	
Remote Connections	<input checked="" type="checkbox"/> Show remote connections
WAN Label	<input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port
BT	
 WAN	Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 17 ms
 Virgin Media	Not available - WAN disabled

The PepVPN test configuration allows to configure and perform throughput tests.

This is usually done after the initial installation of the routers and in case there are problems with aggregation.



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

Press the Start button to perform throughput test according to the configured options.

If TCP is selected, 4 parallel streams will be generated to get the optimal results by default. This can be customized by selecting a different value of streams.

Using more streams will typically get better results if the latency of the tunnel is high.

PepVPN Test Results			
1.0s:	14.6724 Mbps	0 retrans /	323 KB cwnd
2.0s:	15.1620 Mbps	0 retrans /	416 KB cwnd
3.0s:	15.2438 Mbps	0 retrans /	513 KB cwnd
4.0s:	16.2522 Mbps	0 retrans /	609 KB cwnd
5.0s:	14.6811 Mbps	0 retrans /	699 KB cwnd
6.0s:	15.2058 Mbps	0 retrans /	804 KB cwnd
7.0s:	15.7294 Mbps	0 retrans /	935 KB cwnd
8.0s:	15.2053 Mbps	0 retrans /	1024 KB cwnd
9.0s:	15.6881 Mbps	0 retrans /	1045 KB cwnd
10.0s:	14.7147 Mbps	0 retrans /	1045 KB cwnd
--			
Stream 1:	4.0414 Mbps	0 retrans /	254 KB cwnd
Stream 2:	4.2783 Mbps	0 retrans /	253 KB cwnd
Stream 3:	2.8789 Mbps	0 retrans /	285 KB cwnd
Stream 4:	4.1534 Mbps	0 retrans /	253 KB cwnd
--			
Overall:	15.3520 Mbps	0 retrans /	1045 KB cwnd
--			
TEST DONE			

12.1.8 Event Log

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

Device Event Log

The screenshot shows the 'Device Event Log' interface. At the top, there are two tabs: 'Device Event Log' (selected) and 'ContentHub Event Log'. Below the tabs is a header for 'Device Event Log' with an 'Auto Refresh' checkbox checked. The log contains the following entries:

Apr 17 14:54:52	System: All user logins (successful & failed) for WAN-001 (IP: 193.174.252.40) are disabled.
Apr 17 14:39:44	System: All user logins (successful & failed) for WAN-001 (IP: 193.174.252.40) are disabled.
Apr 17 09:12:42	System: Changes applied.
Apr 17 09:07:33	Admin: Remote web console initiated from ipControl 2 by user@ipcontrol.com
Apr 16 10:01:13	System: System update (WAN-001-001) is available.
Apr 16 10:00:23	System: Changes applied.
Apr 16 09:59:04	System: Changes applied.
Apr 16 09:58:57	WAN: Single Mode (Disconnected) (Created)
Apr 16 09:57:10	System: System update (WAN-001-001) is available.
Apr 16 09:57:04	System: Changes applied.
Apr 16 09:56:16	WAN: Single Mode (Disconnected) (Created)
Apr 16 09:56:15	System: System update (WAN-001-001) is available.
Apr 16 09:56:15	System: System update (WAN-001-001) is available.
Apr 16 09:56:13	System: Changes applied.
Apr 16 09:54:41	Admin: Admin (s.d.s.s) login successful.
Apr 16 09:50:28	System: System update (WAN-001-001) is available.
Apr 16 09:50:28	System: System update (WAN-001-001) is available.

At the bottom left, there is a 'Clear Log' button. At the top right, there is an 'Auto Refresh' checkbox which is checked.

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

IPsec Event Log

The screenshot shows the 'IPsec VPN Event Log' interface. At the top, there are two tabs: 'Device Event Log' and 'IPsec VPN Event Log' (selected). Below the tabs is a header for 'IPsec VPN Event Log' with an 'Auto Refresh' checkbox checked. The log contains the following entries:

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...

At the bottom right, there is an 'End of log' message.

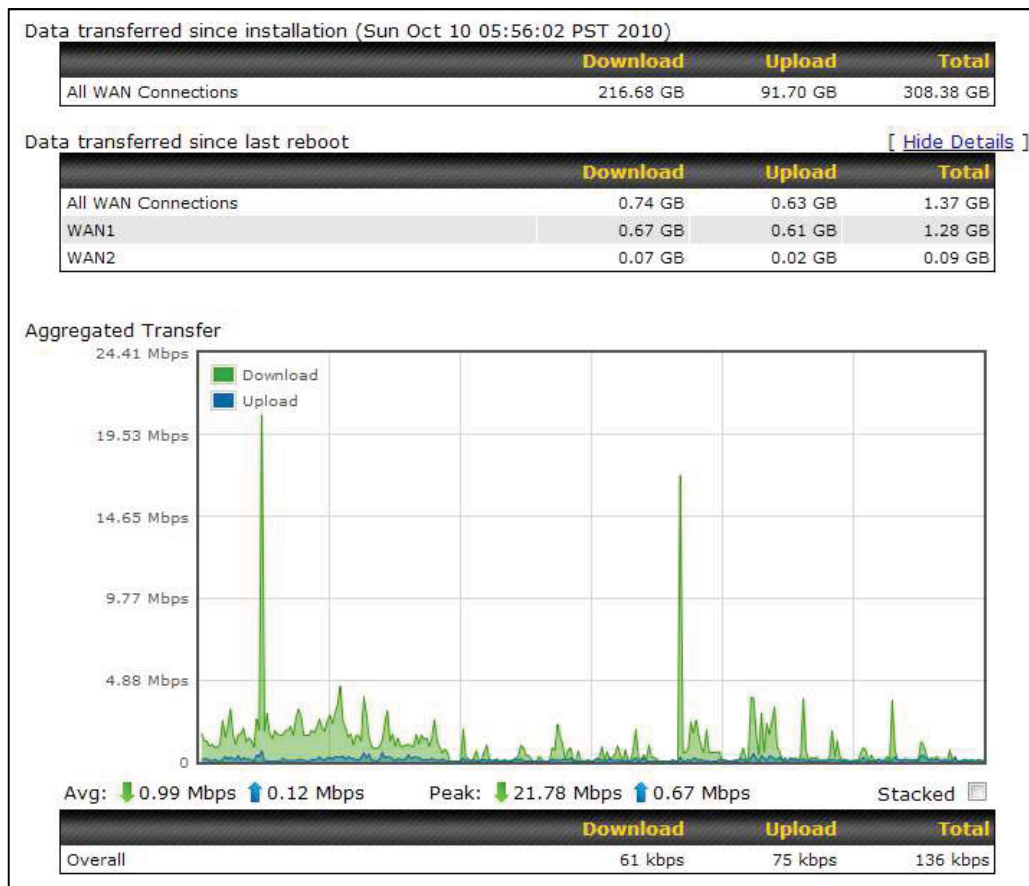
This section displays a list of events that have taken place within an IPsec VPN connection. Check the box next to **Auto Refresh** and the log will be refreshed automatically. For an AP event log, navigate to **AP>Info**.

12.2 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.

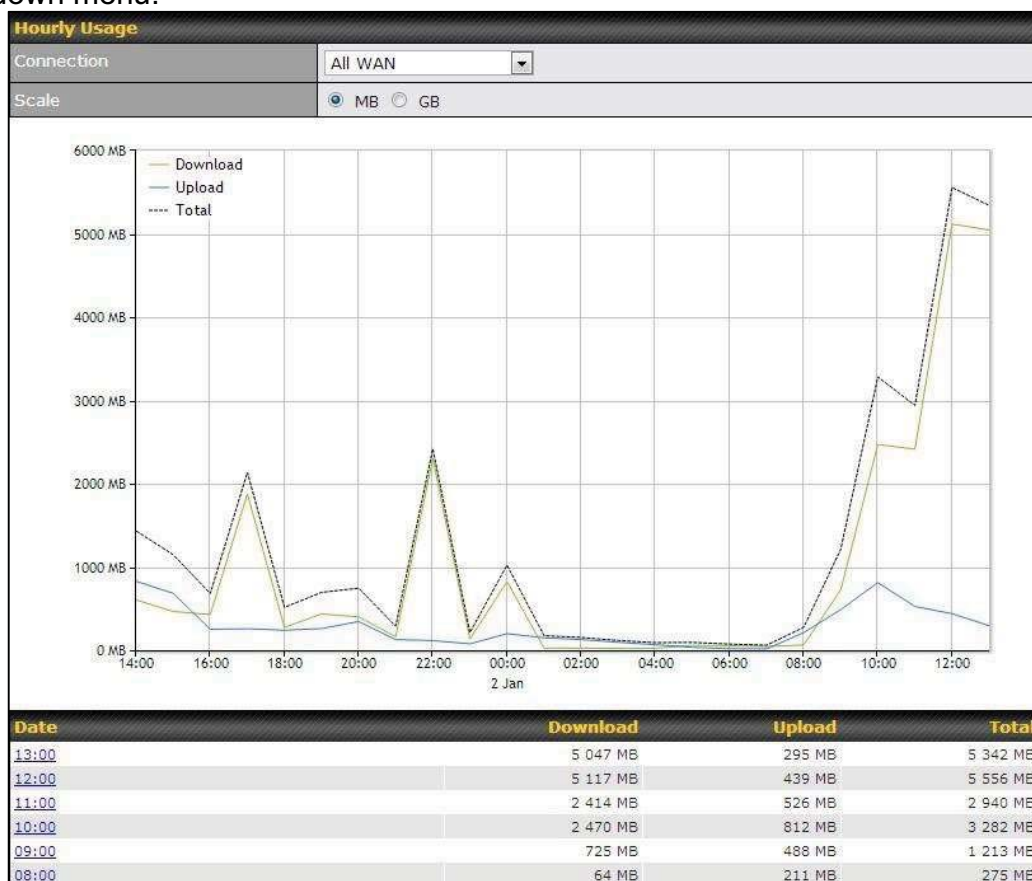
12.2.1 Real-Time

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.



12.2.2 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.

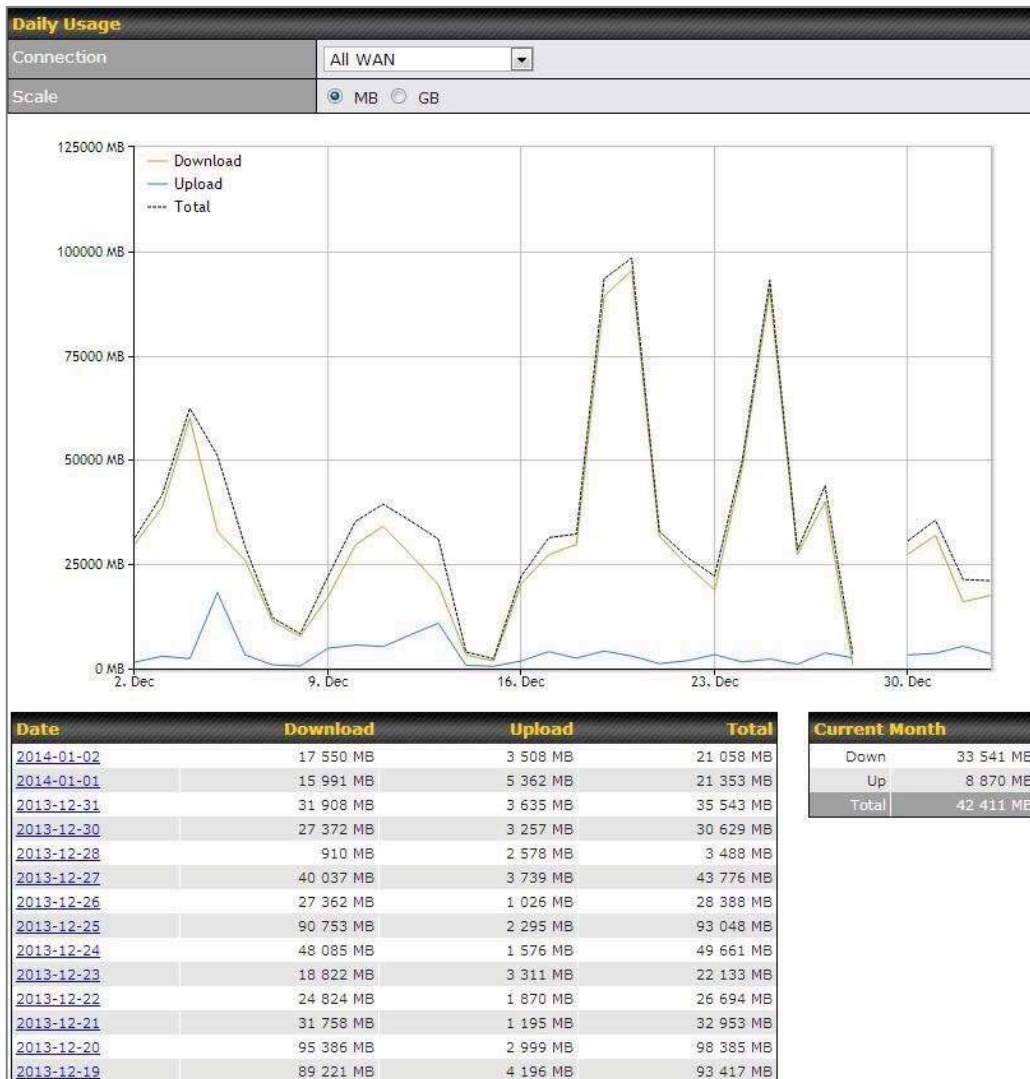


12.2.3 Daily

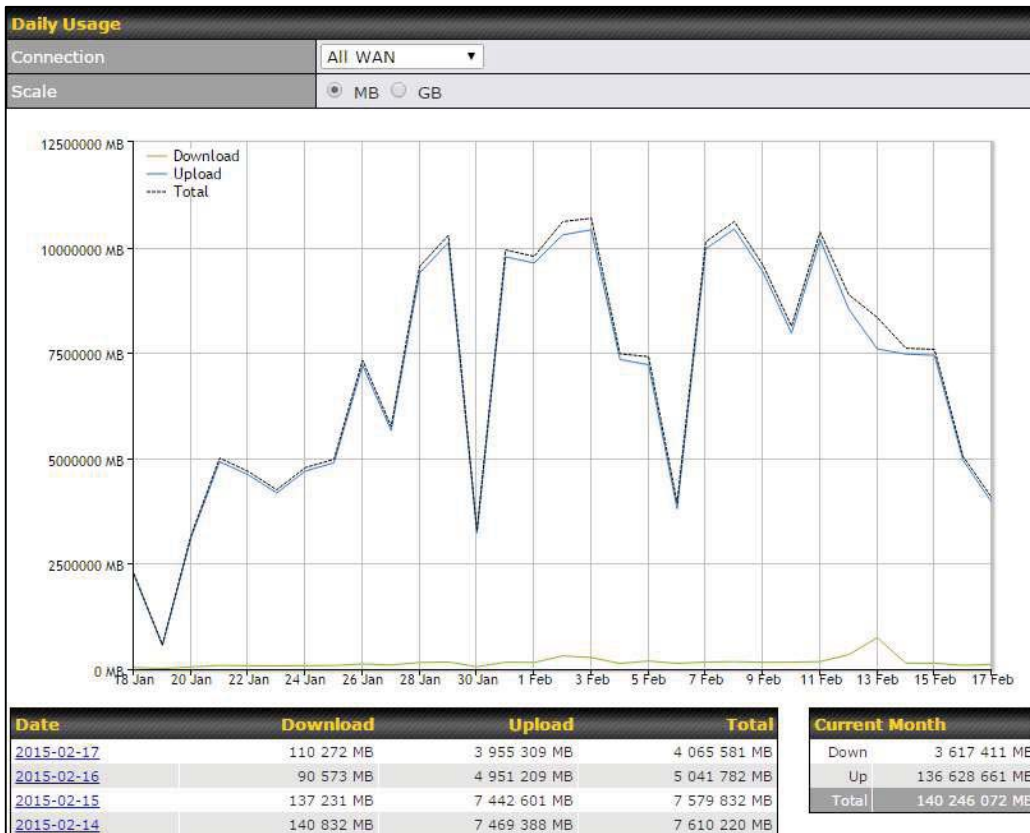
This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

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

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



Status



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

Client Bandwidth Usage (2015-02-15)

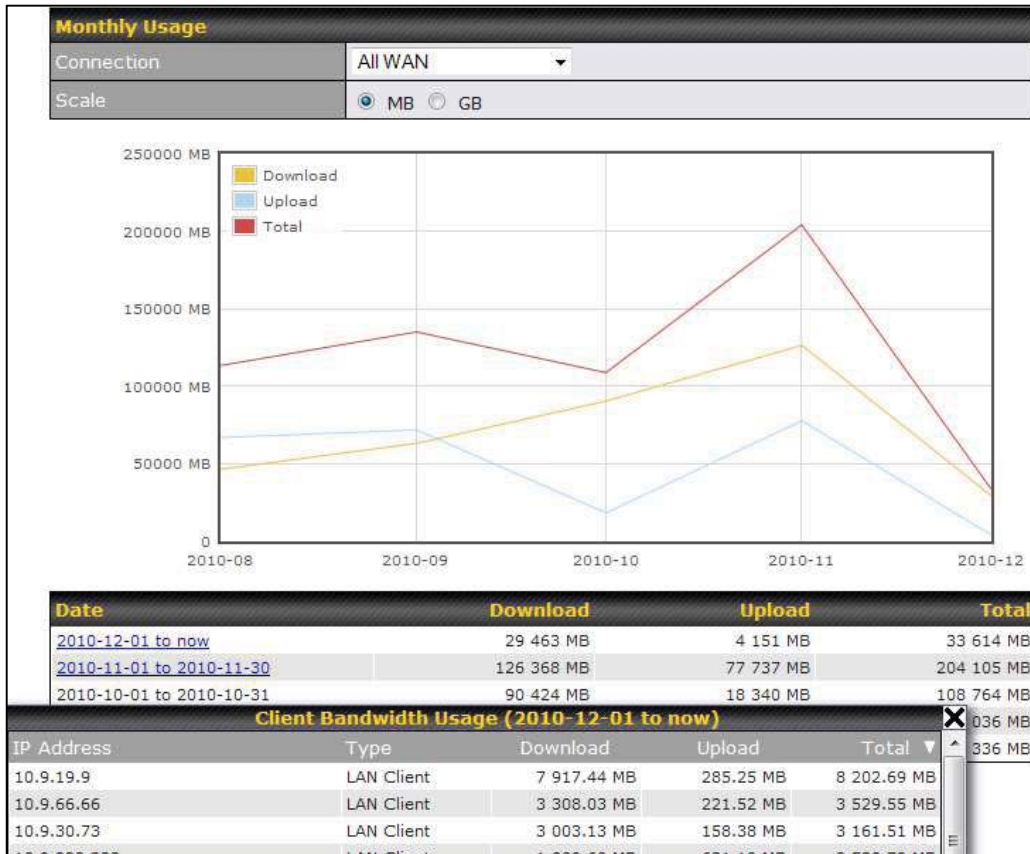
IP Address	Type	Download	Upload	Total
192.168.168.15	LAN Client	7 972.69 MB	1 217 122.81 MB	1 225 095.50 MB
192.168.168.14	LAN Client	7 432.25 MB	1 197 380.53 MB	1 204 812.79 MB
192.168.168.22	LAN Client	5 676.90 MB	617 109.49 MB	622 786.39 MB
192.168.168.21	LAN Client	5 693.38 MB	615 629.07 MB	621 322.46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

12.2.4 Monthly

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

enabled **Bandwidth Monitoring** feature as shown in **Section 13.4**, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

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



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

Appendix A. Restoration of Factory Defaults

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

For Balance models with a reset button:

1. Locate the reset button on the Peplink Balance unit.
2. With a paperclip, press and keep the reset button pressed.

Note: There is a dual function to the reset button.

Hold for 5-10 seconds for admin password reset (green status light starts blinking)

Hold for approximately 20 seconds for factory reset (all WAN/LAN port lights start blinking)

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 B. Routing under DHCP, Static IP, and PPPoE

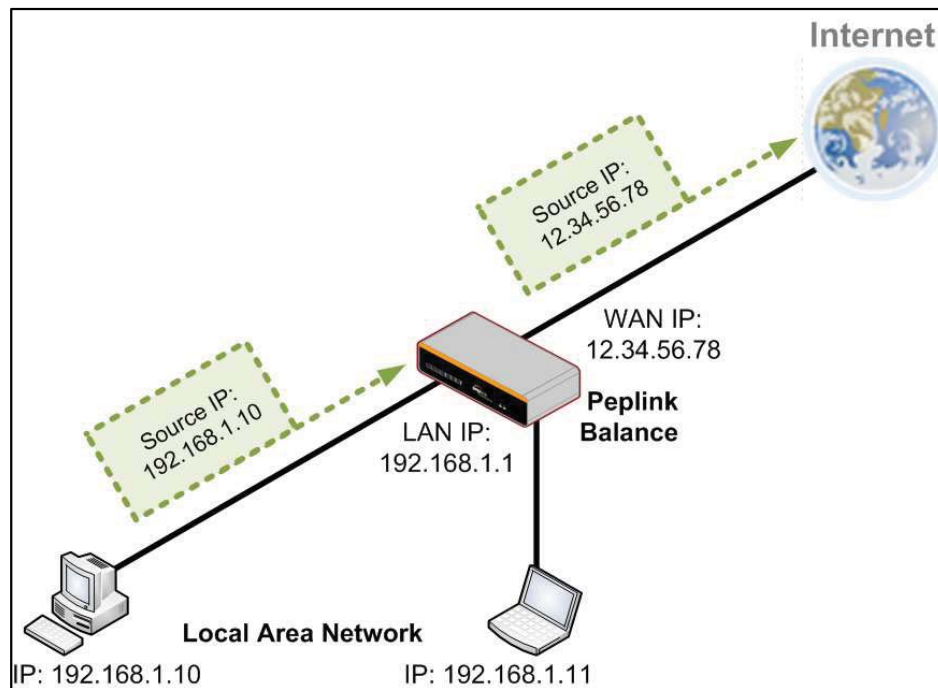
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

B.1 Routing Via Network Address Translation (NAT)

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

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

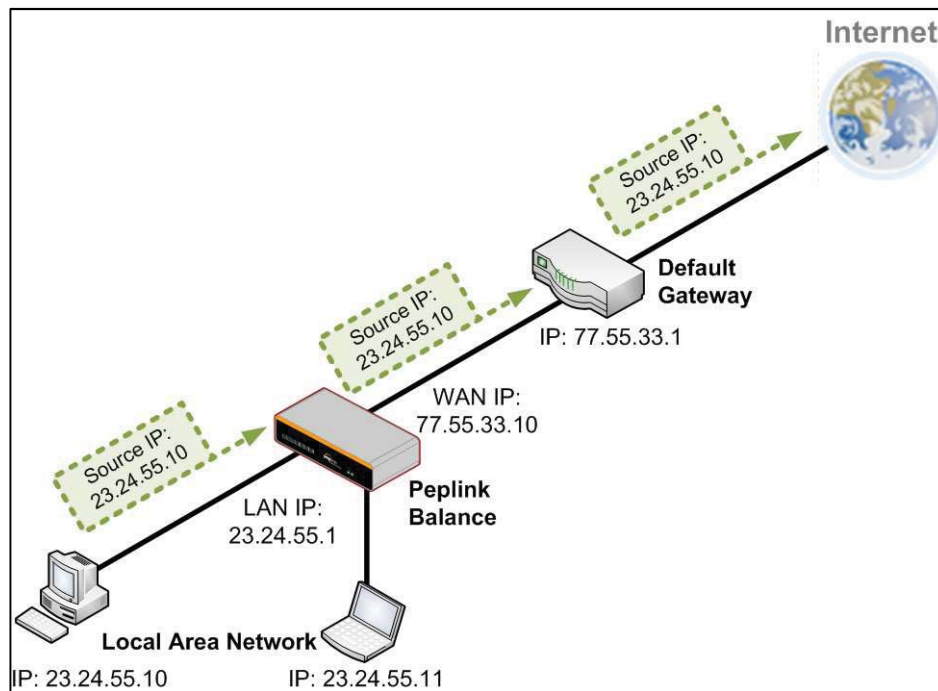
The following figure shows the packet flow in NAT mode:



B.2 Routing Via IP Forwarding

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

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



Appendix C. Case Studies

MPLS Alternative

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

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.

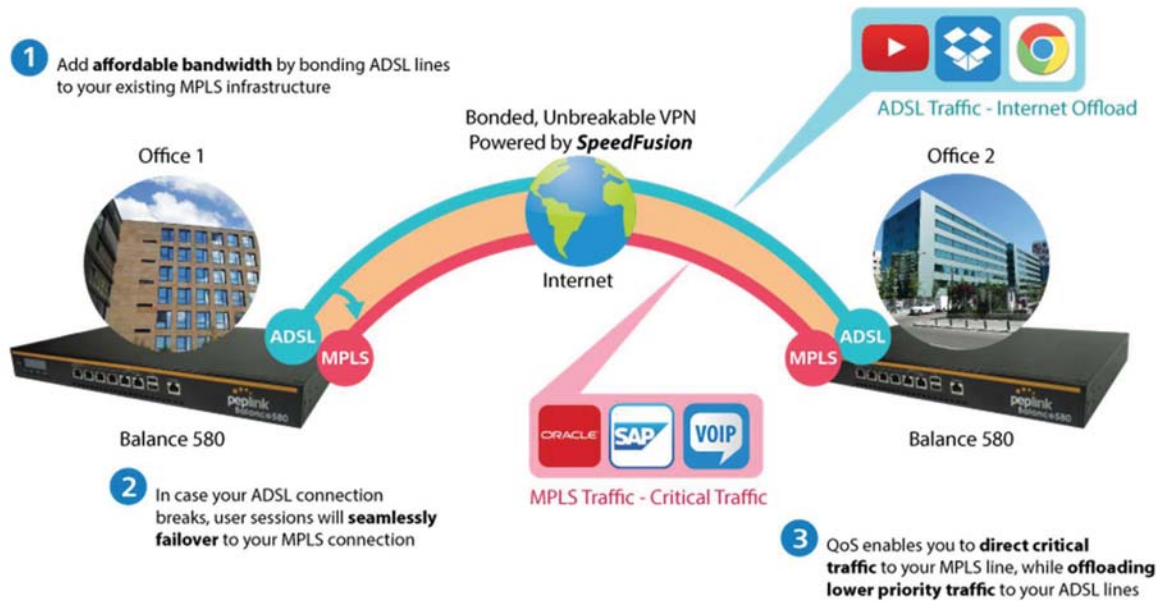
Special features of Balance 580: have high availability capability

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.

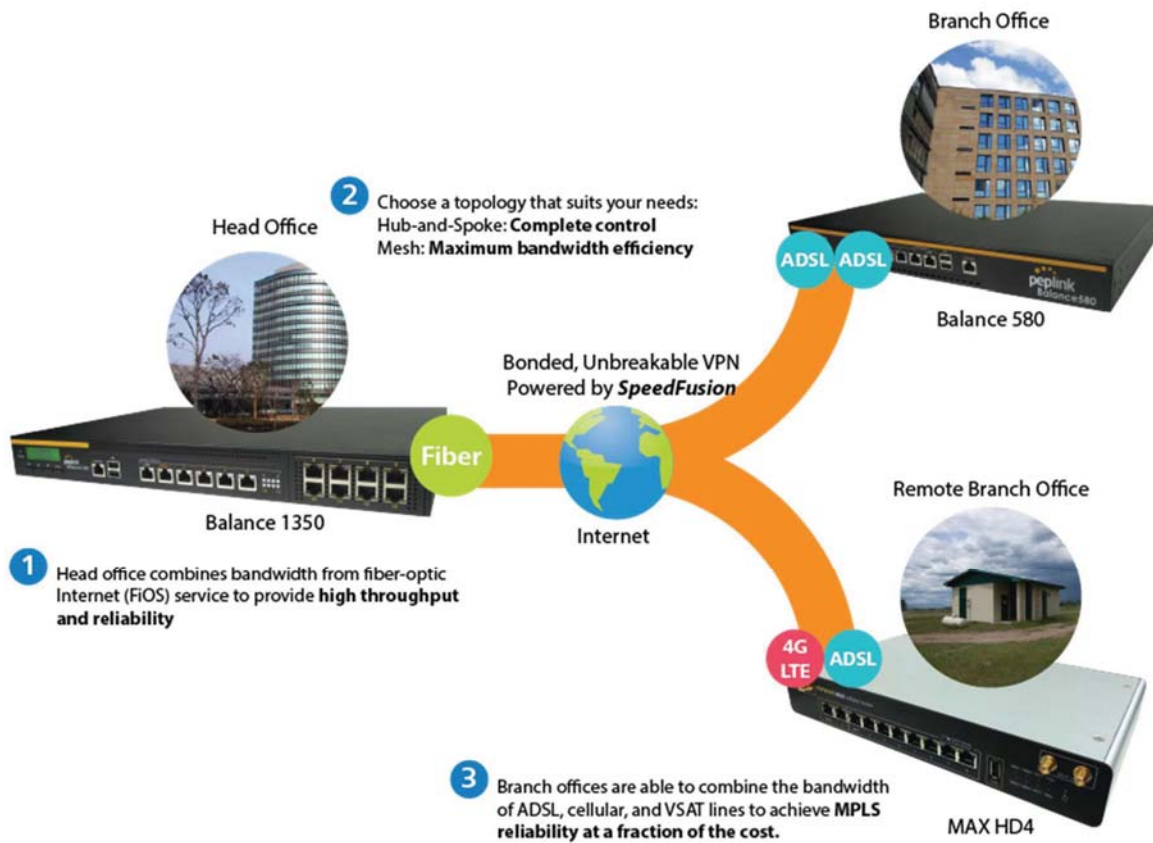
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement



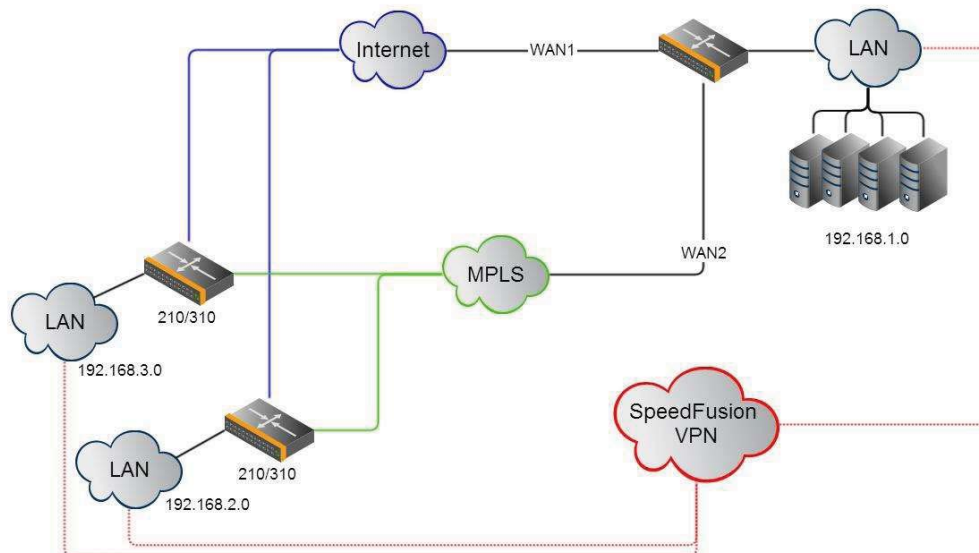
Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your 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 to supplement of existing Multi-Office MPLS network with DSL bonding through SpeedFusion using a Balance 580 at the headquarters and Balance 210/310 at branch offices.



Environment:

- This organization has one head office with 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 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

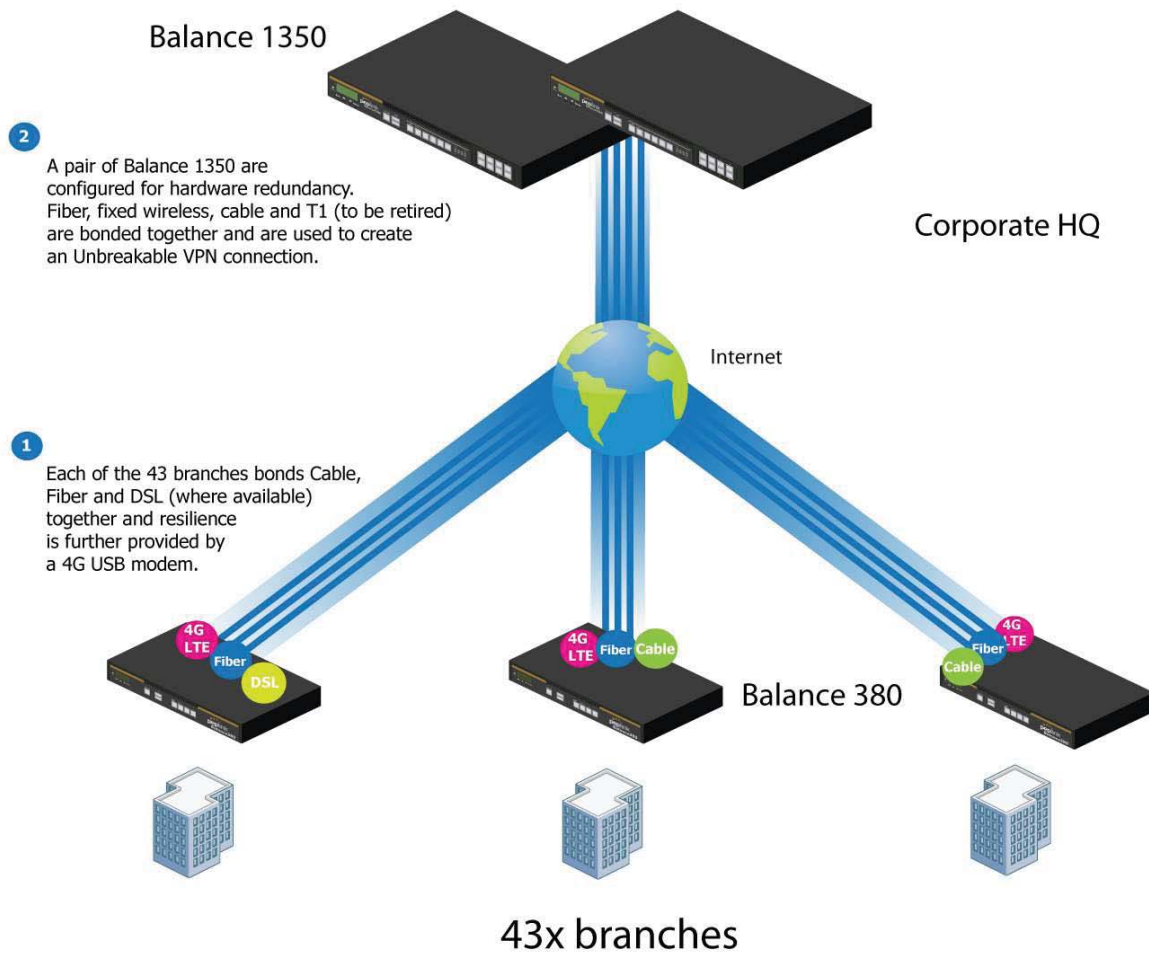
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

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.

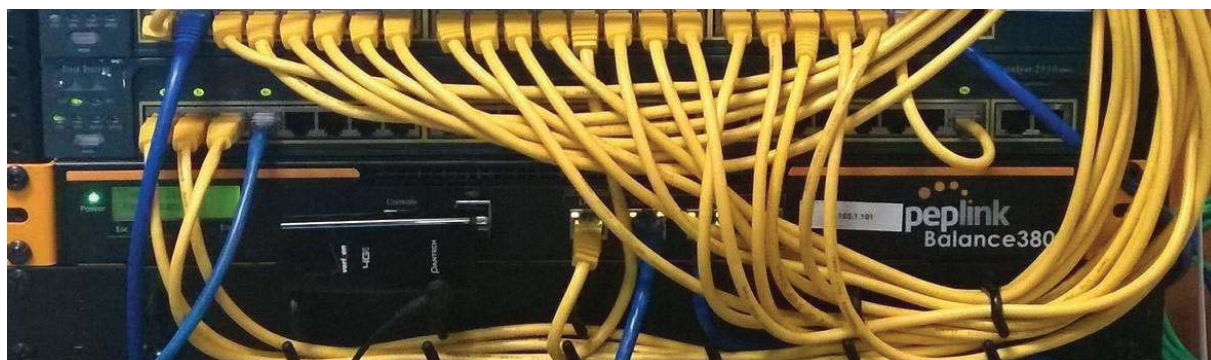
Quick Deployment and Unbreakable Connectivity

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

Adding to Life
pluss

400
USERS

VoIP 290
EndPoints

30+
SITES

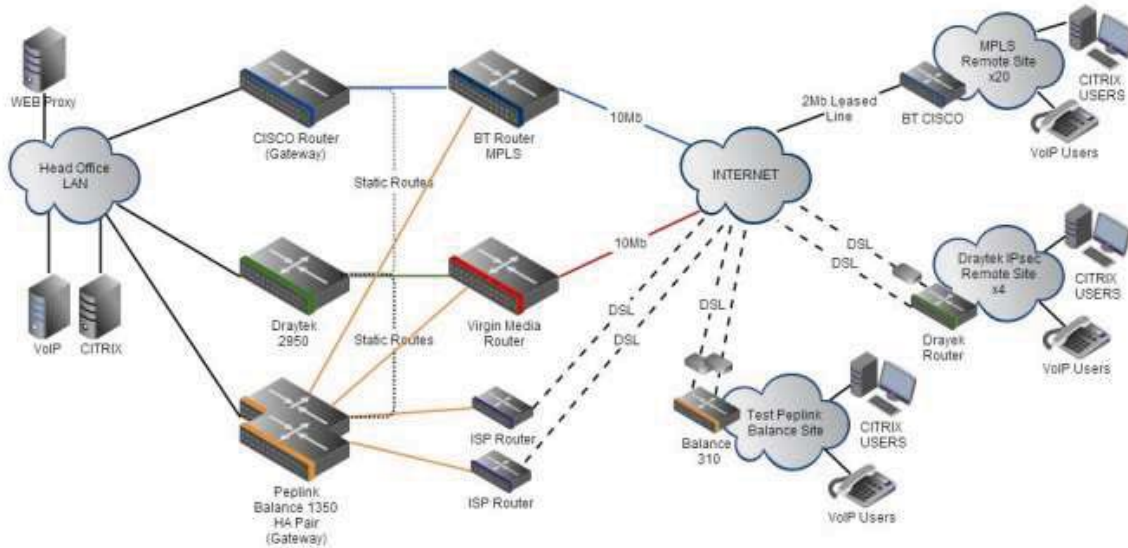
"It saves us money, is easy to manage and grows with us effortlessly."
Steve Taylor - Pluss

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.

Plus now powers its entire WAN infrastructure with simple-to-install, highly reliable, and cost-effective Peplink gear, which allows it to aggregate DSL and other commodity connections and replace expensive leased lines.



Colégio Next - Enabling eLearning



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

Despite being equipped with iPads, teachers and students alike were not making use of them. The reason for this was because of the slow network access speeds. Apps would

not download and course contents were inaccessible. Often, having more than a couple students connected to the same Wi-Fi access point was enough to bring it to its knees.

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

Requirements

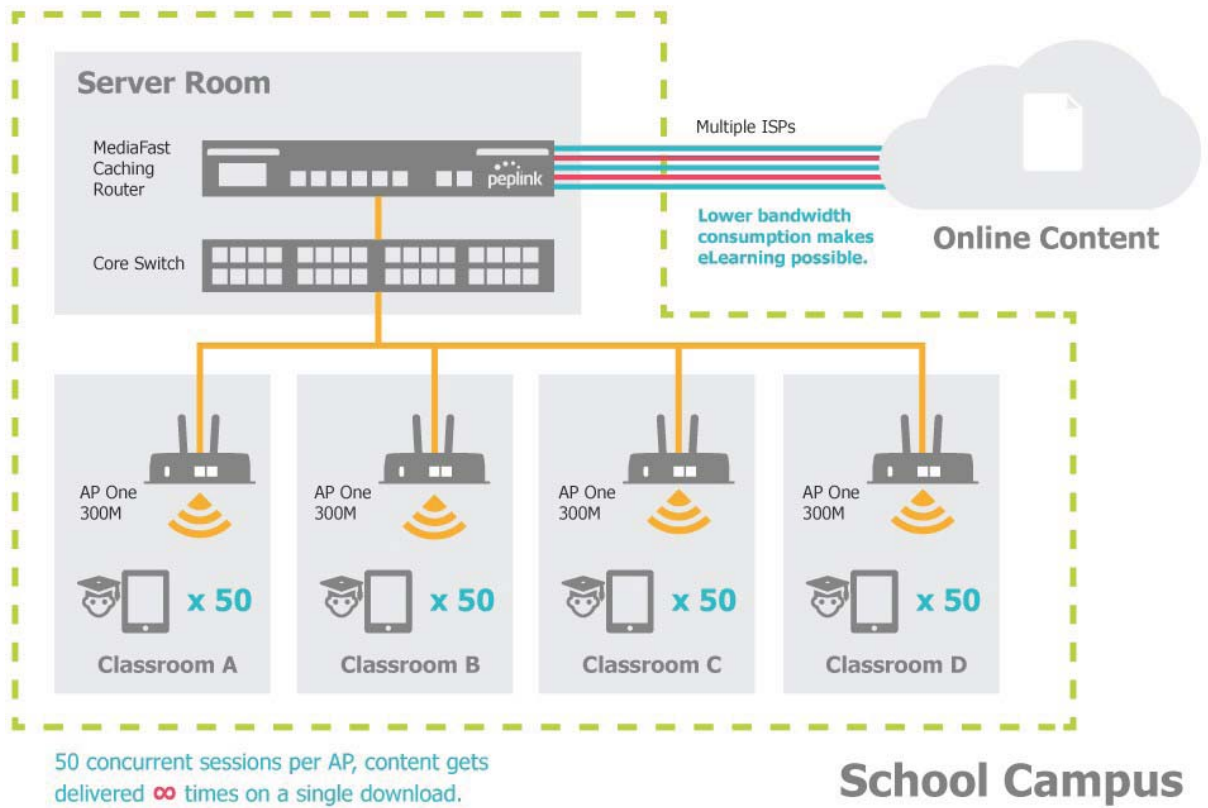
- Solve network congestion problem caused by 600 students over rural Internet connections
- Wi-Fi that can handle 50+ users per classroom
- An affordable network infrastructure that can provide simultaneous access to media-rich educational content

Solution

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

Benefits

- Instant, simultaneous access to media-rich educational content for 500+ iPads
- Wi-Fi connection stability for 50+ users per classroom, not achievable by other tested equipment
- Teachers, students and guests can be assigned access priority to available bandwidth, further preventing congestion
- iOS updates (often 2GB size) no longer congest the network as they are downloaded only once, cached on the MediaFast and then distributed to all iOS devices
- AP Controller makes MAC Address Filtering easy. Students are assigned to designated APs by their devices' MAC Address in order to prevent saturating any single AP.
- Flawless iPad AirPlay mirroring at all times
- iPads are used all day, reaching their full potential with a fast and stable network all the time
- Students are far more engaged and teachers rely on their iPads all day



Performance Optimization

Scenario

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

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

Solution

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

- Web browsing mainly downloads data; sending 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 30M/2M and 50M/50M, respectively. This will ensure that outbound traffic is more likely to be routed through WAN2.
- For HTTP, set the weight to 3:4.
- For SMTP, set the weight to 1:8, such that users will have a greater chance to be routed via WAN2 when sending e-mail.

Maintaining the Same IP Address Throughout a Session

Scenario

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

Solution

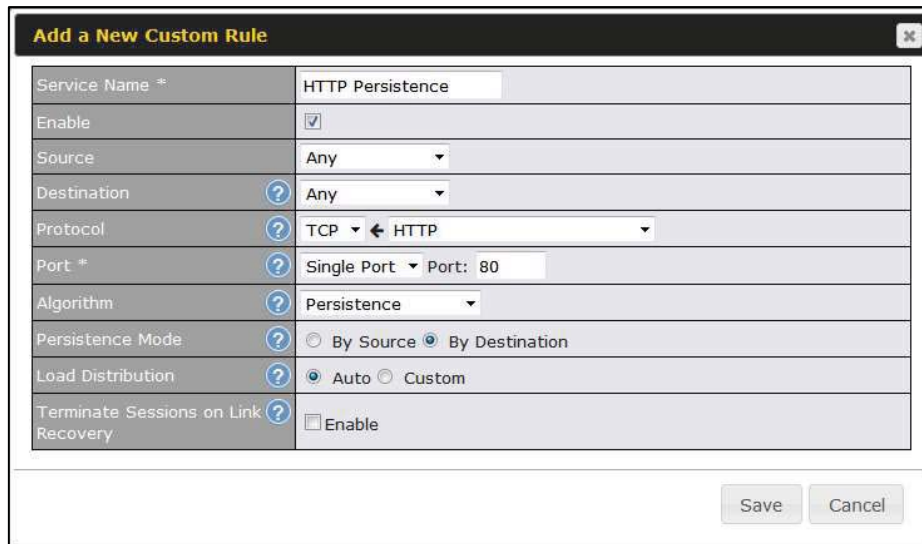
Make use of the persistence functionality of the Peplink Balance. With persistence configured and the **By Destination** option selected, the Peplink Balance will use a consistent WAN connection for source-destination pairs of IP addresses, preventing sessions from being dropped.

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

Settings

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

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



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

Tip

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

Bypassing the Firewall to Access Hosts on LAN

Scenario

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

Solution

The web admin interface can be used to add an inbound NAT mapping to a host and to bind the host to the WAN connection(s) of your choice. To begin, navigate to

Network>NAT Mappings.

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

LAN Client(s) ?	IP Address ▾
Address ?	192.168.1.102
Inbound Mappings ?	Connection / Inbound IP Address(es)
	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> 10.90.0.75 (Interface IP)
	<input type="checkbox"/> WAN 2
	<input type="checkbox"/> WAN 3
	<input type="checkbox"/> WAN 4
	<input type="checkbox"/> WAN 5
	<input type="checkbox"/> WAN 6
	<input type="checkbox"/> WAN 7
<input type="checkbox"/> Mobile Internet	
Outbound Mappings ?	Connection / Outbound IP Address
	WAN 1 10.90.0.75 (Interface IP) ▾
	WAN 2 10.90.0.76 (Interface IP) ▾
	WAN 3 Interface IP ▾
	WAN 4 Interface IP ▾
	WAN 5 Interface IP ▾
	WAN 6 Interface IP ▾
	WAN 7 Interface IP ▾
Mobile Internet Interface IP ▾	

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

Inbound Access Restriction

Scenario

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

Solution

Firewall functionality is built into the Peplink Balance. By default, inbound access is unrestricted. Enabling a basic level of protection involves setting up firewall rules. For example, in order to protect your private network from external access, you can set up a firewall rule between the Internet and your private network. To do so, navigate to **Network>Firewall>Access Rules**. Then click the **Add Rule** button in the **Inbound Firewall Rules** table and change the settings according to the following screenshot:

Add a New Inbound Firewall Rule
✕

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

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

Outbound Access Restriction

Scenario

For security reasons, it may be appropriate to restrict outbound access. For example, you may want to prevent LAN users from using ftp to transfer files to and from the Internet. This can easily be achieved by setting up an outbound firewall rule with the Peplink Balance.

Solution

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	<input type="text" value="No FTP access"/>
Enable	<input checked="" type="checkbox"/>
Protocol	TCP <input type="button" value="←"/> FTP
Source	Any Address Any Port
Destination	Any Address Single Port Port: 21
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

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

Appendix D. Troubleshooting

Problem 1

Outbound load is only distributed over one WAN connection.

Solution

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

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

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

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

For additional details, please refer to this FAQ:

<https://forum.peplink.com/t/speed-test-tool-for-combined-download-speed-in-multi-wan-environment/8457>

Problem 2

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

Solution

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

Problem 3

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

Solution

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

Problem 4

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

Solution

You can test the LAN connection using ping. For example, if you are using DOS/Windows, at the command prompt, type *ping 192.168.1.1*. This pings the Peplink Balance device (provided that Peplink Balance's IP is 192.168.1.1) to test whether the connection to the Peplink Balance is OK.

Problem 5

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

Solution

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

Appendix E. Declaration

CAUTION:

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

Federal Communication Commission Interference Statement

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide

reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

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

ISED Warning Statement

Industry Canada Statement

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:(1) This device may not cause interference; and(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

La bande 5150-5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Caution

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(iii) for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and

(iv) where applicable, antenna type(s), antenna model(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.

Mise en garde

(i) Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement à une utilisation en intérieur afin de réduire les risques d'interférence préjudiciables aux systèmes de satellites mobiles utilisant les mêmes canaux;

(iii) pour les dispositifs avec antenne(s) détachable(s), le gain d'antenne maximal autorisé pour les dispositifs dans la bande 5725-5850 MHz doit être tel que l'équipement soit toujours conforme à la norme e.i.r.p. limites, le cas échéant; et

(iv) le cas échéant, type(s) d'antenne, modèle(s) d'antenne et angle(s) d'inclinaison dans le cas le plus défavorable nécessaire pour rester conforme à l'e.i.r.p. L'exigence de masque d'altitude énoncée à la section 6.2.2.3 doit être clairement indiquée.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement respecte les limites d'exposition aux rayonnements IC définies pour un environnement non contrôlé. Cet équipement doit être installé et mis en marche à une distance minimale de 20 cm qui sépare l'élément rayonnant de votre corps.

This radio transmitter IC: 20682-P1AC8E has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio IC: 20682-P1AC8E a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

WLAN Antenna type: Replacement Antenna

WLAN Antenna gain: 2412~2462 GHz / 2.44 dBi ,

5150~5250 GHz / 4.10 dBi

5725~5850 GHz / 4.73 dBi

EU Declaration of Conformity

This device complies with the essential requirements of the Radio Equipment Directive 2014/53/EU.

The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the Radio Equipment Directive 2014/53/EU.

The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.1.1

EN 301 893 V2.1.1

EN 303 413 V1.1.1

EN 301 908-1 V11.1.1

EN 301 489-1 V2.2.0

EN 301 489-17 V3.2.0

EN 301 489-19 V2.1.0

EN 301 489-52 V1.1.0

EN 55032: 2015 + AC:2016

EN 61000-3-2: 2014

EN 61000-3-3: 2013

EN 55035: 2017

EN 62311: 2008

EN 62368-1:2014/AC:2015