

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

DSL/Cable Optimization

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

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

13.11 Firewall

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

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

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)
- Internal Network (VLAN to VLAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

13.11.1 Access Rules

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

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

Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any		
Default	Any	Any	Any		

Add Rule

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☒ Always on
Protocol	Any :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save **Cancel**

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

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

Rule	Protocol	WAN	Source	Destination	Action	
test	Any	Any	Any	Any		
Default	Any	Any	Any	Any		

Add Rule

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

Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☒ Always on
WAN Connection	Any
Protocol	Any :: Protocol Selection Tool
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save
Cancel

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

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

Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any		
Default	Any	Any	Any		

Add Rule

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

Add a New Internal Network Firewall Rule

New Firewall Rule

Rule Name	
Enable	☒ Always on
Protocol	Any :: Protocol Selection
Source	Any Address
Destination	Any Address
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save
Cancel

Inbound / Outbound / Internal Network 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. 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.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: • Any • TCP • UDP • ICMP • DSCP • IP 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.
Source and Port	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:  In addition, a single port, or a range of ports, can be specified for the Source settings.
Destination and Port	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:  In addition, a single port, or a range of ports, can be specified for the settings.

Action

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

- 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).

Event Logging

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

- **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	TCP	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 Outbound, Inbound and Internal Network access.

Tip

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

Intrusion Detection and DoS Prevention



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

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

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

13.11.2 Content Blocking

Application Blocking
?

Please Select Application...
+

Web Blocking
?

Preset Category

☐ High
☐ Moderate
☐ Low
☒ Custom

☐ Adware
☐ Dating
☐ P2P/File sharing
☐ Malware
☐ Social Networking
☐ Violence
☐ Aggressive
☐ Drugs
☐ Gambling
☒ Pornography
☐ Contraband
☐ Weapons
☐ Audio-Video
☐ File Hosting
☐ Games
☒ Proxy/Anonymizer
☐ Update Sites

Content Filtering Database Auto Update
?
☐

Customized Domains
?

+

Exempted Domains from Web Blocking
?

+

Exempted User Groups
?

Manager	☐ Exempt
Staff	☐ Exempt
Guest	☐ Exempt

Exempted Subnets
?

Network	Subnet Mask
	255.255.255.0 (/24) +

URL Logging

Enable
☐

Log Server Host
Port: 514

Application Blocking

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

Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for

those on the Exempted User Groups or Exempted Subnets defined below.

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

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

The device will inspect and look for blocked domain names on all HTTP and HTTPS traffic.

Customized Domains

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

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

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

Exempted User Groups

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

Exempted Subnets

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

URL Logging

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

13.12 Routing Protocols

13.12.1 OSPF & RIPv2

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

OSPF								
Router ID	LAN IP Address							
Area	Interfaces							
0.0.0.0	Untagged LAN (192.168.112.1/24), WAN 4 (192.168.254.10/24)							
Add								
RIPv2								
No RIPv2 Defined.								
OSPF & RIPv2 Route Advertisement								
PepVPN Route Isolation	 ☐ Enable							
Network Advertising	 --- 							
All LAN/VLAN networks will be advertised when no network advertising is chosen.								
Static Route Advertising	 ☒ Enable							
	<table border="1"> <thead> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>255.255.255.0 (/24) </td> <td></td> </tr> </tbody> </table>	Excluded Networks	Subnet Mask			255.255.255.0 (/24) 		
Excluded Networks	Subnet Mask							
	255.255.255.0 (/24) 							
Save								

OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the WAN IP address. If you want to specify your own ID, enter it into the Custom field.
Area	This is an overview of the OSPF areas that you have defined. Clicking on the name under Area allows you to configure the connection. To define a new area, click Add. To delete an existing area, click on the  .

OSPF settings

Area ID

0.0.0.0

Link Type

☒ Broadcast
 ☐ Point-to-Point

Authentication

None

Interfaces

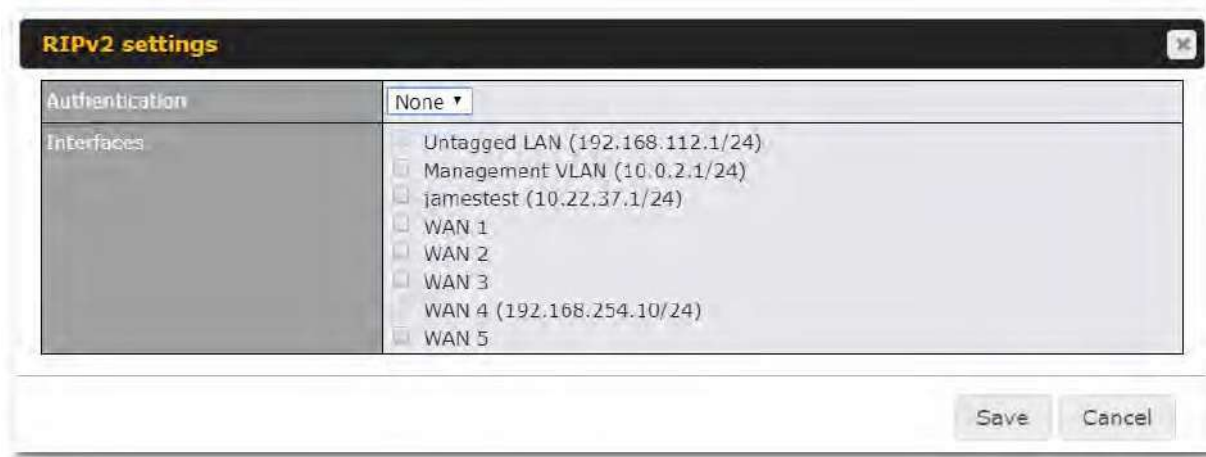
☒ Untagged LAN (192.168.112.1/24)
☐ Management VLAN (10.0.2.1/24)
☐ jamestest (10.22.37.1/24)
☐ WAN 1
☐ WAN 2
☐ WAN 3
☒ WAN 4 (192.168.254.10/24)
☐ WAN 5

Save

Cancel

OSPF Settings	
Area ID	Assign a name to be applied to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore them.
Link Type	Choose the type of network that this area will use.
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are MD5 and Text . Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver OSPF packets.

To access RIPv2 settings, click on .



The RIPv2 settings dialog box has a title bar 'RIPv2 settings' with a close button. It contains two main sections: 'Authentication' and 'Interfaces'. The 'Authentication' section has a dropdown menu currently set to 'None'. The 'Interfaces' section is a list box containing the following items: 'Untagged LAN (192.168.112.1/24)', 'Management VLAN (10.0.2.1/24)', 'jamestest (10.22.37.1/24)', 'WAN 1', 'WAN 2', 'WAN 3', 'WAN 4 (192.168.254.10/24)', and 'WAN 5'. At the bottom right, there are 'Save' and 'Cancel' buttons.

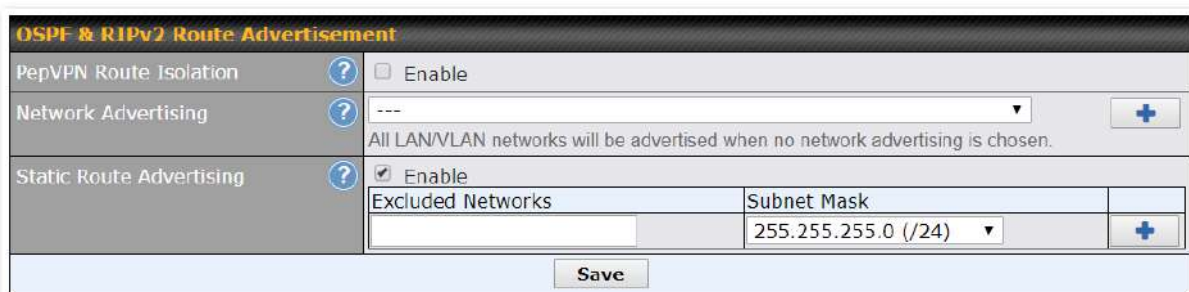
RIPv2 Settings

Authentication

If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.

Interfaces

Select the interface(s) that this area will use to listen to and deliver RIPv2 packets.



The OSPF & RIPv2 Route Advertisement dialog box has a title bar 'OSPF & RIPv2 Route Advertisement'. It contains three main sections: 'PepVPN Route Isolation' with an 'Enable' checkbox; 'Network Advertising' with a dropdown menu and a '+' button; and 'Static Route Advertising' with an 'Enable' checkbox. Below the 'Static Route Advertising' section is a table with two columns: 'Excluded Networks' and 'Subnet Mask'. The first row in the table shows '255.255.255.0 (/24)' in the 'Subnet Mask' column. At the bottom, there is a 'Save' button.

OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation

Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption..

Network Advertising

Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.

Static Route Advertising

Enabling OSPF & RIPv2 Route Advertising allows it to advertise LAN static routes over OSPF & RIPv2. Static routes on the Excluded Networks table will not be advertised.

13.12.2 BGP

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

BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	
Add			

Click the "x" to delete a BGP profile.

Click "Add" to create a new BGP profile.

BGP Profile

BGP Profile

Profile Name:

Enable

☒

Interface

WAN

Router ID

☒ WAN IP Address
☐ Custom:

Autonomous System

Neighbor

IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
		disable			

Hold Time

240

Next Hop Self

☐

IBGP Local Preference

100

BFD

☐ Enable

BGP	
Name	This field specifies the name that represents this profile.
Enable	When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.
Interface	The interface in which the BGP neighbor is located.
Autonomous System	The Autonomous System Number (ASN) assigned to this profile.
Neighbor	BGP Neighbors and their details.

IP address	The IP address of the Neighbor.
Autonomous System	The Neighbor's ASN.
Multihop/TTL	This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255.
Password	(Optional) Assign a password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received routes.
Hold Time	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
Next Hop Self	Enable this option to advertise your own source address as the next hop when propagating routes.
iBGP Local Preference	This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100
BFD	Enable this option to add Bidirectional Forwarding Detection for path failure. All directly connected Neighbors that use the same physical interface share the same BFD settings. All multihop Neighbors share the same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.

Route Advertisement			
Network Advertising	?	--- +	
Static Route Advertising	?	☒ Enable	
		Excluded Networks	Subnet Mask
			255.255.255.0 (/24) +
Custom Route Advertising	?	Networks	Subnet Mask
			255.255.255.0 (/24) +
Advertise OSPF Route	?	☐	
Set Community	?	Community	Route Prefix
			+

Route Advertisement	
Network Advertising	Select the Networks that will be advertised to the BGP Neighbor.
Static Route Advertising	Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised.
Custom Route Advertising	Additional routes to be advertised to the BGP Neighbor.
Advertise OSPF Route	When this box is checked, every learnt OSPF route will be advertised.
Set Community	Assign a prefix to a Community Community: Two numbers in new-format. e.g. 65000:21344 Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284 Route Prefix: Comma separated networks. e.g. 172.168.1.0/24,192.168.1.0/28

Route Import			
Filter Mode	Accept ▼		
Restricted Networks	Network	Subnet Mask	Exact Match
		255.255.255.0 (/24) ▼	☐
		+	

Route Import Settings	
Filter Mode	This field allows for the selection of the filter mode for route import. None: All BGP routes will be accepted. Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. Reject: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted	This field specifies the network(s) in the "route import" entry.

Networks

Exact Match: When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.

Route Export				
Filter Mode	Accept ▼			
Restricted Networks	Network	Subnet Mask	Exact Match	
		255.255.255.0 (/24) ▼	☐	+
Export to other BGP Profile	☐			
Export to OSPF	☐			

Filter Mode

This field allows for the selection of the filter mode for route export.

None: All BGP routes will be accepted.

Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.

Reject: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.

Restricted Networks

This field specifies the network(s) in the "route export" entry.

Exact Match: When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.

Export to other BGP Profile

When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.

Export to OSPF

When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.

13.13 Remote User Access

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

13.13.1 L2TP with IPsec

Remote User Access Settings	
Enable	☒
VPN Type	☒ L2TP with IPsec ☐ PPTP ☐ OpenVPN
Preshared Key	☒ Hide Characters

L2TP with IPsec Remote User Access Settings	
Pre-shared Key	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
Listen On	This setting is for specifying the WAN IP addresses that allow remote user access.
Disable Weak Ciphers	Click the  button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.

Continue to configure the authentication method.

13.13.2 OpenVPN

Remote User Access Settings	
Enable	☒
VPN Type	☐ L2TP with IPsec ☐ PPTP ☒ OpenVPN You can obtain the OpenVPN client profile from the status page

Select OpenVPN and continue to configure the authentication method.

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

OpenVPN Client Profile	Route all traffic Split tunnel
------------------------	--

You have a choice between 2 different OpenVPN Client profiles:

Option 1: "Route all traffic" profile
Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel

Option 2: "Split tunnel" profile
Using this profile, VPN clients will ONLY send those traffic designated to the untagged LAN and VLAN segment through the OpenVPN tunnel.

13.13.3 PPTP

Remote User Access Settings	
Enable	☒
VPN Type	☐ L2TP with IPsec ☒ PPTP ☐ OpenVPN

No additional configuration required.

The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well known security issues

Continue to configure authentication methods.

13.13.4 Authentication Methods

Connect to Network	Untagged LAN	
Authentication	Local User Accounts	
User Accounts	Username	Password
+		

Authentication Method	
Connect to Network	Select the VLAN network for remote users to enable remote user access on.
Authentication	Determine the method of authenticating remote users

User accounts:

This setting allows you to define the Remote 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.

Note:

The username must contain lowercase letters, numerics, underscore(_), dash(-), at sign(@), and period(.) only.

The password must be between 8 and 12 characters long.

LDAP Server:

Connect to Network	 Untagged LAN ▾
Authentication	LDAP Server ▾
LDAP Server	Port 389 Default ☐ Use DN/Password to bind to LDAP Server
Base DN	
Base Filter	

Enter the matching LDAP server details to allow for LDAP server authentication.

Radius Server:

Authentication	RADIUS Server ▾
Auth Protocol	MS-CHAP v2 ▾
Auth Server	Port 1812 Default
Auth Server Secret	☒ Hide Characters
Accounting Server	Port 1813 Default
Accounting Server Secret	☒ Hide Characters

Enter the matching Radius server details to allow for Radius server authentication.

Active Directory:

Connect to Network	 Untagged LAN ▾
Authentication	Active Directory ▾
Server Hostname	
Domain	
Admin Username	
Admin Password	☒ Hide Characters

Enter the matching Active Directory details to allow for Active Directory server authentication.

13.14 Misc. Settings

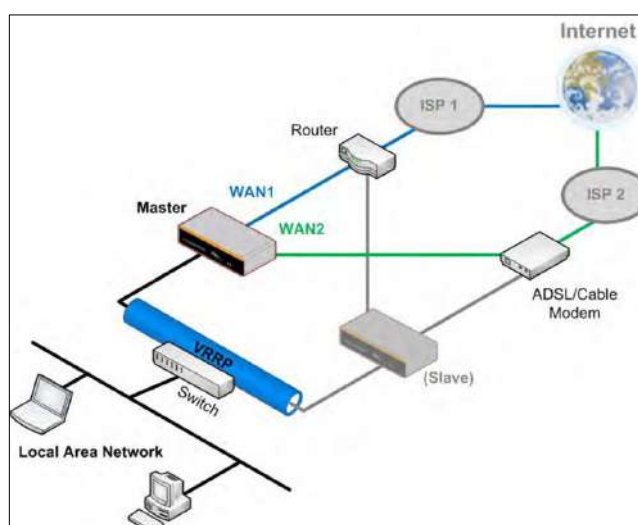
13.14.1 High Availability

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	
Enable	☒
Group Number	5
Preferred Role	☒ Master ☐ Slave
Resume Master Role Upon Recovery	☒
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

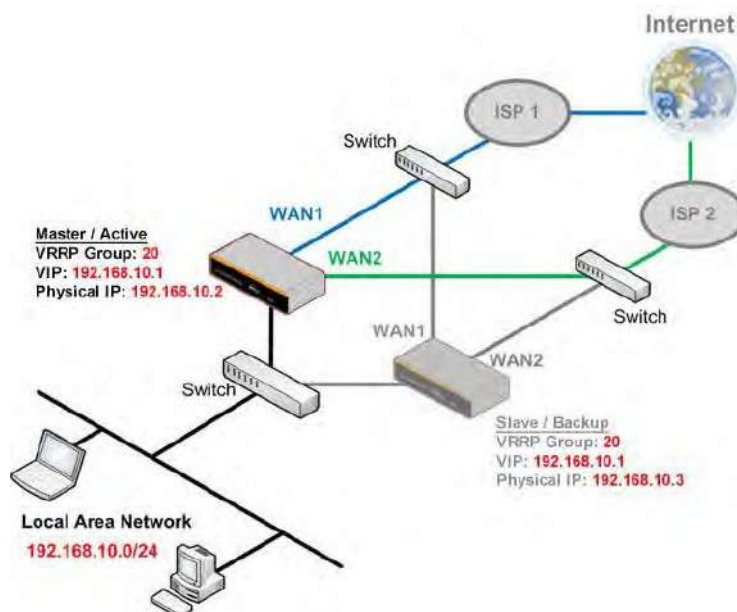
Interface for Slave Router

High Availability	
Enable	☒
Group Number	5
Preferred Role	☐ Master ☒ Slave
Configuration Sync.	☒ Master Serial Number: 5454-5454-5454
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

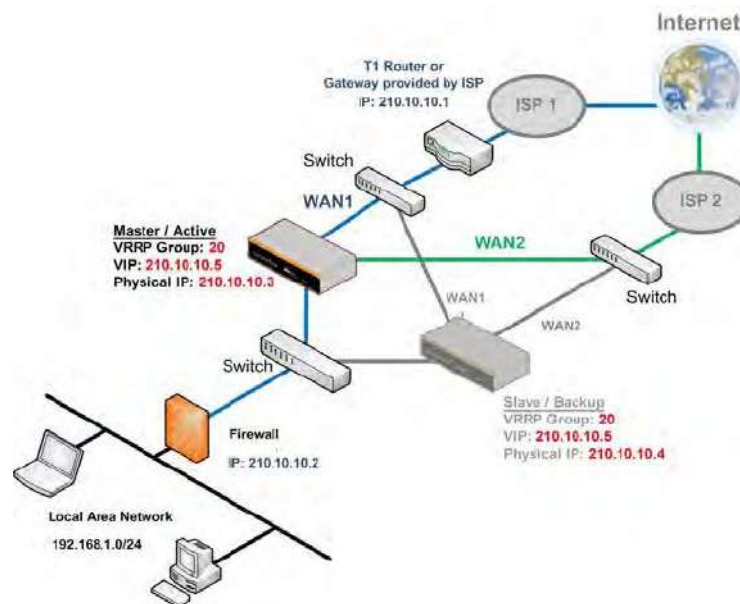
High Availability	
Enable	Checking this box specifies that the Peplink Balance unit is part of a high availability configuration.
Group Number	This number identifies a pair of Peplink Balance units operating in a high availability configuration. The two Peplink Balance units in the pair must have the 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.

13.14.2 Certificate Manager

Certificate		
VPN Certificate	No Certificate	
Web Admin SSL Certificate	Default Certificate is in use	
Captive Portal SSL Certificate	Default Certificate is in use	
MediaFast Root CA Certificate	Default Certificate is in use	
OpenVPN Root CA Certificate	Default Certificate is in use	

ContentHub Certificate	
No Certificates defined	
Add Certificate	

Wi-Fi WAN Client Certificate	
No Certificates defined	
Add Certificate	

Wi-Fi WAN CA Certificate	
No Certificates defined	
Add Certificate	

This section allows you to assign certificates for the local VPN, OpenVPN, Captive Portal, Mediafast, ContentHub, Wi-Fi WAN (Client and CA) and web admin SSL for extra security.

Read the following knowledgebase article for full instructions on how to create and import a self-signed certificate: <https://forum.peplink.com/t/how-to-create-a-self-signed-certificate-and-import-it-to-a-peplink-product/>

13.14.3 Service Forwarding

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

SMTP Forwarding Setup ?	
SMTP Forwarding	☐ Enable
Web Proxy Forwarding Setup ?	
Web Proxy Forwarding	☐ Enable
DNS Forwarding Setup ?	
Forward Outgoing DNS Requests to Local DNS Proxy	☐ Enable
Custom Service Forwarding Setup	
Custom Service Forwarding	☐ 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.

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		☒ Enable	
Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	☐		
WAN 2	☒	22.2.2.2	25
WAN 3	☒	33.3.3.2	25
WAN 4	☐		

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 16.1**).

Web Proxy Forwarding

Web Proxy Forwarding Setup			
Web Proxy Forwarding		☒ Enable	
Web Proxy Interception Settings			
Proxy Server		IP Address 123.123.11.22 Port 8080 (Current settings in users' browser)	
Connection	Enable Forwarding?	Proxy Server IP Address : Port	
WAN 1	☐		
WAN 2	☒	22.2.2.2 : 8765	
WAN 3	☒	33.3.3.2 : 8080	
WAN 4	☐		

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.

DNS Forwarding

DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	☒ Enable

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

Custom Service Forwarding

Custom Service Forwarding Setup			
Custom Service Forwarding	☒ Enable		
Settings	TCP Port	Server IP Address	Server Port
			+

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.

13.14.4 Service Passthrough

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

Service Passthrough Support	
SIP	☒ Standard Mode ☐ Compatibility Mode ☒ Define custom signal ports 1. 2. 3.
H.323	☒ Enable
FTP	☒ Enable ☒ Define custom control ports 1. 2. 3.
TFTP	☒ Enable
IPsec NAT-T	☒ Enable ☒ Define custom ports 1. 2. 3. ☒ 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 correctly in NAT mode. Such passthrough support is always enabled and there are two modes for selection: Standard Mode and Compatibility Mode. 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.
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.

13.14.5 NTP Server

Peplink routers can now serve as a local NTP server. Upon start up, it is now able to provide connected devices with the accurate time, precise UTC from either an external NTP server or via GPS and ensuring that connected devices always receive the correct time.

NTP Server setting can be found via: **Network>Misc. Settings>NTP Server**

NTP Server	
Enable	☐

Save

Time Settings can be found at **System>Time>Time Settings**

Time Settings	
Time Zone	(GMT) Casablanca ☐ Show all
Time Sync	Time Server
Time Server	0.peplink.pool.ntp.org

Save

13.14.6 Grouped Networks

Grouped Networks	
Name	Networks
Add Group	

Using “Grouped Networks” you can group and name a range of IP addresses, which can then be used to define firewall rules or outbound policies.

Start by clicking on “add group” then fill in the appropriate field. In this example we’ll create a group “accounting”. Click save when you have finished adding the required networks.

Grouped Networks			
Name	Accounting		
Networks	Network	Subnet Mask	
	192.168.50.192	255.255.255.224 (/27)	X
		255.255.255.255 (/32)	+

The grouped network “accounting” can now be used to configure a group policy or firewall rule.

The screenshot shows the Peplink web interface with the 'Network' tab selected. The left sidebar contains a menu with 'WAN', 'LAN', 'VPN', 'Outbound Policy' (highlighted), and 'Inbound Access'. The main content area is titled 'Outbound Policy' and shows a 'Custom' policy selected. Below this is a section titled 'Add a New Custom Rule' with a form containing the following fields:

Service Name		
Enable	☒ Always on ▼	
Source	Grouped Networ ▼	Accounting ▼

13.14.7 Remote SIM Management

Remote SIM management is accessible via **Network > Misc Settings > Remote SIM Management**. By default, this feature is disabled.

Please note that a limited number of Pepwave routers support the SIM Injector, may refer to the link: <https://www.peplink.com/products/sim-injector/> or Appendix C for more details on FusionSIM Manual.

The screenshot shows the 'Remote SIM Host' settings page. It features a header 'Remote SIM Host' and a status bar indicating 'Remote SIM is disabled' with a red icon on the right.

Remote SIM Host Settings

Remote SIM Host Settings

Auto LAN Discovery

☐

Remote SIM Host

Save

Remote SIM Host Settings	
Active LAN Discovery	Check this box to enable Auto LAN discovery of the remote SIM server.
Remote SIM Host	Enter the public IP address of the SIM Injector. If you enter IP addresses here, it is not necessary to tick the "Auto LAN Discovery" box above.

Remote SIM Host

192.168.1.10



Remote SIM Management

Server

Slot

No Remote SIM Defined.

Add Remote SIM

You may define the Remote SIM information by clicking the **"Add Remote SIM"**. Here, you can enable **Data Roaming** and **custom APN** for your SIM cards.

Add Remote SIM

Remote SIM	
SIM Server	New SIM Server... ▼
SIM Server - Serial Number	
SIM Server - Name	Optional
SIM Slot	1 ▼
SIM Slot - Name	Optional
Data Roaming	☐
Operator Settings (for LTE/HSPA/EDGE/GPRS only)	☒ Auto ☐ Custom Mobile Operator Settings
SIM PIN (Optional)	(Confirm)

Save

Add Remote SIM Settings	
SIM Server	Add a new SIM Server
SIM Server - Serial Number	Enter the serial number of SIM Server
SIM Server - Name	This optional field allows you define a name for the SIM Server
SIM Slot	Click the drop-down menu and choose which SIM slot you want to connect.
SIM Slot - Name	This optional field allows you define a name for the SIM slot.
Data Roaming	Enables data roaming on this particular SIM card.
Operator Settings (for LTE/HSPA/EDGE/GPRS Only)	This setting allows you to configure the APN settings of your connection. If Auto is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making a connection, you may select Custom to enter your carrier's APN, Username and Password settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto.

13.14.8 SIM Toolkit

The SIM Toolkit can be found via **Networks > Misc Settings > SIM Toolkit**. This supports two functionalities, USSD and SMS.

USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by mobile phones to communicate with their service provider's computers. One of the most common uses is to query the available balance.

SIM Status	
WAN Connection	Cellular ▼
SIM Card	1
IMSI	856195002108538
Tool	USSD ▼

USSD	
USSD Code	Submit

Enter your USSD code under the **USSD Code** text field and click **Submit**.

SIM Status	
WAN Connection	Cellular ▼
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
Receive SMS	Get

You will receive a confirmation. To check the SMS response, click **Get**.

SIM Status	
WAN Connection	Cellular ▼
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
USSD Status	Request is sent successfully
Receive SMS	Get

After a few minutes you will receive a response to your USSD code

Received SMS	
May 27 20:02	PCX As of May 27th Account Balance: \$ 0.00 Amount Unbilled Voice Calls: 0 minutes Video Calls: 0 minutes SMS (Roaming): 0 SMS (Within Network): 0 MMS (Roaming): 0 MMS (Within Network): 0 Data Usage: 7384KB (For reference only, please refer to bill)
Aug 8 , 2013 14:51	PCX iPhone & Android users need to make sure "PCX" is entered as the APN under "Settings" > "Mobile network setting" for web browsing and mobile data service. Other handset models will receive handset settings via SMS shortly (PIN: 1234) (Consumer Service Hotline: 1000 / Business Customer Hotline 10088)

SMS

The SMS option allows you to read SMS (text) messages that have been sent to the SIM in your Peplink router.

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	724041100000000
Tool	SMS

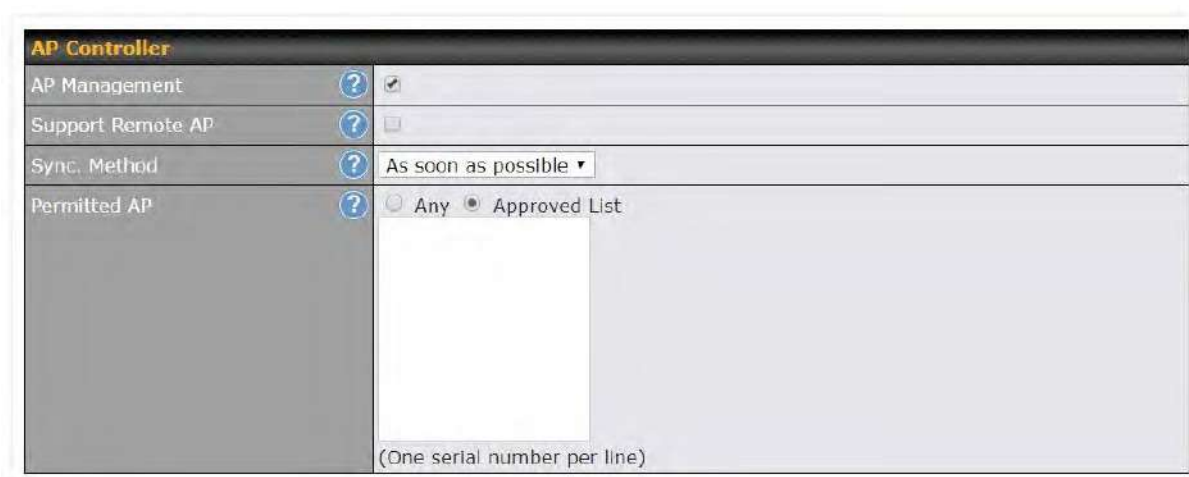
SMS		Refresh
Jun 21, 2017 18:00	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖
May 06, 2017 12:23	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖
Mar 15, 2017 10:03	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖
Mar 06, 2017 14:50	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖
Dec 28, 2016 09:53	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖
Dec 06, 2016 13:09	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖
Nov 08, 2016 11:29	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖
Sep 07, 2016 17:05	From: [redacted] Hello, you are now logged in to the system. You can change this when you first login to the system.	✖

14 AP Tab

14.1 AP

14.1.1 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	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. The DHCP server and/or local DNS server of the remote AP's network should be configured in the DNS Proxy Settings menu under Network>LAN. The procedure is as follows: 1. Define an extended DHCP option, CAPWAP Access Controller addresses (field 138), in the DHCP server, where the values are the AP controller's public IP addresses; and/or 2. Create a local DNS record for the AP controller with a value corresponding to the AP controller's public IP address.

DNS Proxy Settings					
Enable	☒				
DNS Caching	☐				
Include Google Public DNS Servers	☐				
Local DNS Records	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td>wlancontroller</td> <td>10.10.10.1</td> </tr> </tbody> </table>	Host Name	IP Address	wlancontroller	10.10.10.1
Host Name	IP Address				
wlancontroller	10.10.10.1				

Sync. Method	Select the required option to synchronize the managed AP's. Options are: - As soon as possible (default) - Progressively (synchronize AP's in groups) - One at a time (synchronize one AP at a time)
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.

14.1.2 Wireless SSID

SSID	Security Policy
No SSID Defined	
Add	

Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model. The below settings show a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).

The screenshot shows a window titled 'SSID' with a question mark icon in the top right corner. A help dialog box is open, displaying the text: 'Help To set SSID advanced settings, please click [here](#). Close'.

SSID

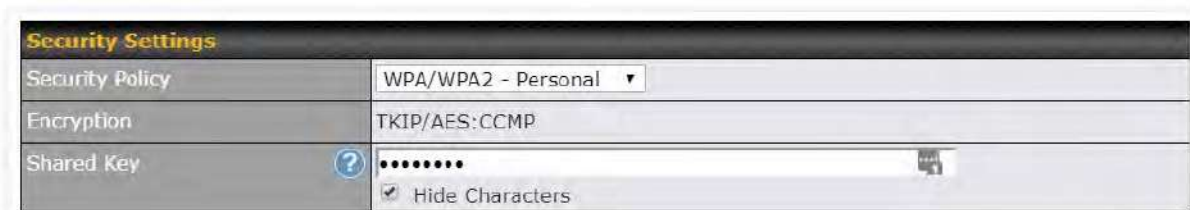
SSID Settings

SSID	PEPLINK_63E6
Enable	Always on
VLAN	0 (0: Untagged) ☐ Use VLAN Pool
Broadcast SSID	☒
Data Rate	☒ Auto ☐ Fixed
Multicast Filter	☐
Multicast Rate	MCS0/6M
IGMP Snooping	☐
DHCP Relay	☐
DHCP Option 82	☐
Network Priority (QoS)	Gold
Layer 2 Isolation	☐
Maximum number of clients	2.4 GHz: 0 5 GHz: 0 (0: Unlimited)
Band Steering	☐ Disable

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Enable	Click the drop-down menu to apply a time schedule to this interface
VLAN	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). Use of a VLAN pool is enabled by selecting the checkbox.
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 Pepwave router 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 Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
DHCP Relay	Put the address of the DHCP server in this field.. DHCP requests will be relayed to this DHCP server
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.
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.
Maximum Number of Clients	Indicate the maximum number of clients that should be able to connect to each frequency.
Band Steering	To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency. Choose between: Force - Clients capable of 5 GHz operation are only offered with 5 GHz frequency. Prefer - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered. Disable - Default

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



The screenshot shows the 'Security Settings' section of a web interface. It contains three rows: 'Security Policy' with a dropdown menu set to 'WPA/WPA2 - Personal', 'Encryption' with a dropdown menu set to 'TKIP/AES:CCMP', and 'Shared Key' with a text input field containing several dots and a 'Hide Characters' checkbox checked. A blue question mark icon is visible next to the Shared Key field.

Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options: • Open (No Encryption) • WPA3 -Personal (AES:CCMP) • WPA2/WPA3 -Personal (AES:CCMP)

- **WPA2 -Personal** (AES:CCMP)
- **WPA2 – Enterprise**
- **WPA/WPA2 - Personal** (TKIP/AES: CCMP)
- **WPA/WPA2 – Enterprise**

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.

NOTE:

When **WPA2/WPA3- Personal** is configured, if a managed AP which is NOT WPA3 PSK capable, the AP Controller will not push those WPA3 and WPA2/WPA3 SSID to that AP.

Access Control Settings	
Restricted Mode	Deny all except listed ▼
MAC Address List	?

Access Control

Restricted Mode

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

MAC Address List

Connections coming from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field.

If more than one MAC address needs to be entered, you can use a carriage return to separate them.

RADIUS Server Settings	Primary Server	Secondary Server
Host		
Secret	 ☒ Hide Characters	 ☒ Hide Characters
Authentication Port	1812 Default	1812 Default
Accounting Port	1813 Default	1813 Default
NAS-Identifier	Device Name ▼	

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 the field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the Default button to enter 1812 .
Accounting Port	In the field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the Default button to enter 1813 .
NAS-Identifier	Choose between Device Name , LAN MAC address , Device Serial Number and Custom Value

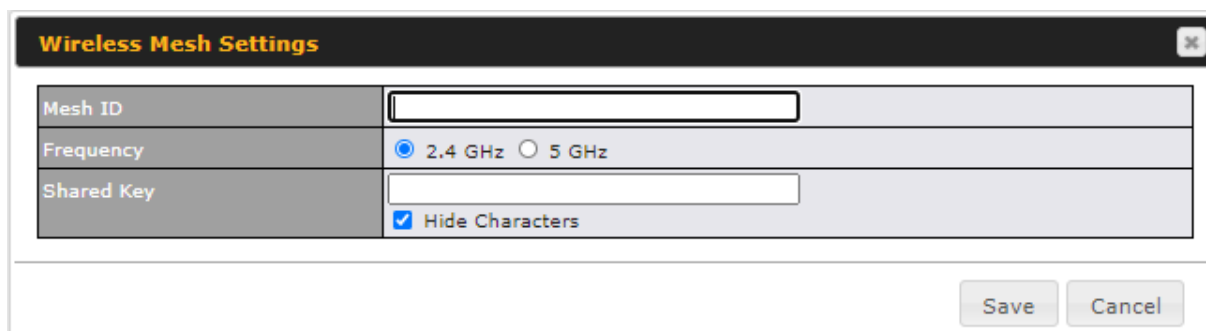
14.1.3 Wireless Mesh



The screenshot shows the 'Wireless Mesh' configuration page. At the top, there are tabs for 'Wireless Mesh' and 'Frequency Band'. Below the tabs, a message states 'No Wireless Mesh Defined'. At the bottom, there is an 'Add' button.

Wireless Mesh Support is available on devices running 802.11ac (Wi-Fi 5) and above. Along with the AP Controller, mesh network extensions can be established, which can expand network coverage. Note that the Wireless Mesh settings need to match the Mesh ID and Shared Key of the other devices on the same selected frequency band.

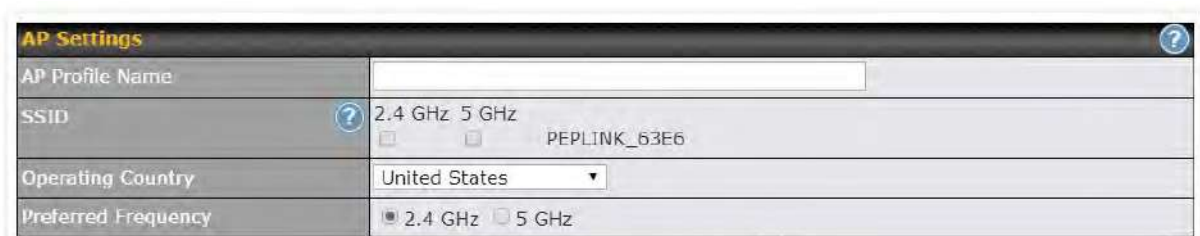
To create a new Wireless Mesh profile, go to **AP > Wireless Mesh**, and click **Add**.



The screenshot shows the 'Wireless Mesh Settings' dialog box. It has a title bar with 'Wireless Mesh Settings' and a close button. The dialog contains three main sections: 'Mesh ID' with a text input field, 'Frequency' with radio buttons for '2.4 GHz' (selected) and '5 GHz', and 'Shared Key' with a text input field and a checked 'Hide Characters' checkbox. At the bottom right, there are 'Save' and 'Cancel' buttons.

Wireless Mesh Settings	
Mesh ID	Enter a name to represent the Mesh profile.
Frequency	Select the 2.4GHz or 5GHz frequency to be used.
Shared Key	Enter the shared key in the text field. Please note that it needs to match the shared keys of the other APs in the Wireless Mesh settings. Click Hide / Show Characters to toggle visibility.

14.1.4 AP > Profiles



The screenshot shows the 'AP Settings' window with the following fields:

- AP Profile Name:** A text input field.
- SSID:** A dropdown menu showing '2.4 GHz' and '5 GHz' options, with a radio button selected for '2.4 GHz'. The SSID value 'PEPLINK_63E6' is displayed.
- Operating Country:** A dropdown menu showing 'United States'.
- Preferred Frequency:** Radio buttons for '2.4 GHz' (selected) and '5 GHz'.

AP Settings	
AP Profile Name	Ap Profile name
SSID	You can select the wireless networks for 2.4 GHz or 5 GHz separately for each SSID.
Operating Country	This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow. - 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). NOTE: Users are required to choose an option suitable to local laws and regulations.
Preferred Frequency	Indicate the preferred frequency to use for clients to connect.

Important Note
Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.

	2.4 GHz	5 GHz
Protocol	802.11ng	802.11n/ac
Channel Width	Auto ▼	Auto ▼
Channel	Auto ▼ Edit Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto ▼ Edit Channels: 36 40 44 48 149 153 157 161 165
Auto Channel Update	Daily at 03 ▼ :00 ☒ Wait until no active client associated	Daily at 03 ▼ :00 ☒ Wait until no active client associated
Output Power	Fixed: Max ▼ ☐ Boost	Fixed: Max ▼ ☐ Boost
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)	0 (0: Unlimited)

AP Settings (part 2)

Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are 802.11ng and 802.11na . By default, 802.11ng is selected.
Channel Width	Available options are 20 MHz , 40 MHz , and Auto (20/40 MHz) . Default is Auto (20/40 MHz) , which allows both widths to be used simultaneously.
Channel	This option allows you to select which 802.11 RF channel will be utilized. Channel 1 (2.412 GHz) is selected by default.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – Max , High , Mid , and Low . The actual output power will be bound by the regulatory limits of the selected country.
Client Signal Strength Threshold	This setting determines the maximum strength at which the Wi-Fi AP can broadcast
Maximum number of clients	This setting determines the maximum number of clients that can connect to this Wi-Fi frequency.

Advanced Wi-Fi AP settings can be displayed by clicking the  on the top right-hand corner of the **Wi-Fi AP Settings** section, which can be found at **AP>Settings**. Other models will display a separate section called **Wi-Fi AP Advanced Settings**, which can be found at **Advanced>Wi-Fi Settings**.

Management VLAN ID	0 (0: Untagged)
Operating Schedule	Always on ▼
Beacon Rate	1 Mbps ▼
Beacon Interval	100 ms ▼
DTIM	1 Default
RTS Threshold	0 Default
Fragmentation Threshold	0 (0: Disable) Default
Distance / Time Converter	4050 m Note: Input distance for recommended values
Slot Time	☐ Auto ☒ Custom 9 μ s Default
ACK Timeout	48 μ s Default
Frame Aggregation	☒
Aggregation Length	50000 Default

Advanced AP Settings

Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as communication traffic between the AP and the AP Controller. The value is zero by default, which means 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.
Operating Schedule	Choose from the schedules that you have defined in System>Schedule. Select the schedule for the integrated AP to follow from the drop-down menu.
Beacon Rate ^A	This option is for setting the transmit bit rate for sending a beacon. By default, 1Mbps is selected.
Beacon Interval ^A	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM ^A	This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to 1 ms.
RTS Threshold ^A	The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500.
Fragmentation Threshold ^A	This setting determines the maximum size of a packet before it gets fragmented into multiple pieces.
Distance / Time	Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout.

Convertor	
Slot Time ^A	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to 9 μs .
ACK Timeout ^A	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 μs .
Frame Aggregation ^A	This option allows you to enable frame aggregation to increase transmission throughput.

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



The screenshot shows the 'Web Administration Settings' window. It includes a table with the following fields and values:

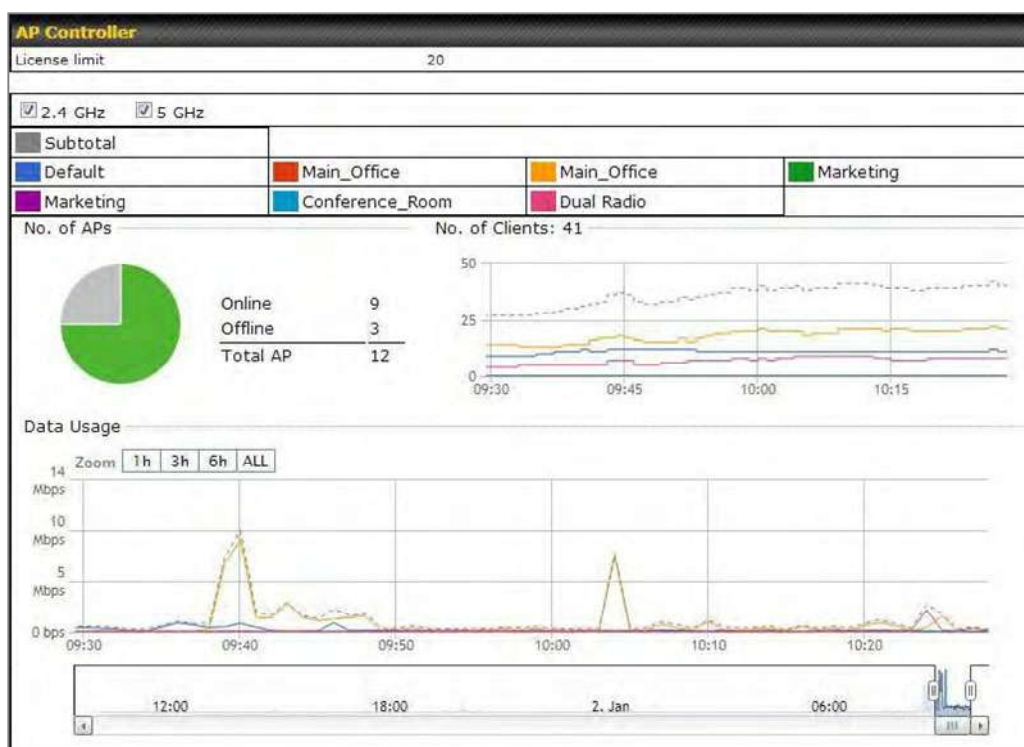
Web Administration Settings	
Enable	☒
Web Access Protocol	☐ HTTP ☒ HTTPS
Management Port	443
HTTP to HTTPS Redirection	☒
Admin Username	admin
Admin Password	 Generate ☒ Hide Characters

Web Administration Settings	
Enable	Ticking this box enables web admin access for APs located on the WAN.
Web Access Protocol	Determines whether the web admin portal can be accessed through HTTP or HTTPS
Management Port	Determines the port at which the management UI can be accessed.
HTTP to HTTPS redirection	Redirects HTTP request to HTTPS
Admin Username	Determines the username to be used for logging into the web admin portal
Admin Password	Determines the password for the web admin portal on external AP.

14.2 AP Controller Status

14.2.1 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.

14.2.2 Access Points (Usage)

A detailed breakdown of data usage for each AP is available at **AP> Access Point**.

Search Filter						
AP Name / Serial Number / SSID	All					
	☐ Include Offline APs					
Search Result						

Managed APs						
						Expand Collapse
Name	IP Address	MAC	Location	Firmware Pack ID	Configuration	
Default (8/9 online)						
10.8.82.11	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** **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:

Managed Wireless Devices

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	36.25 MB
c4:6e:b7:bf:d7:15	10.5.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.25 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
18:00:12d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB

Click the  icon to configure each client

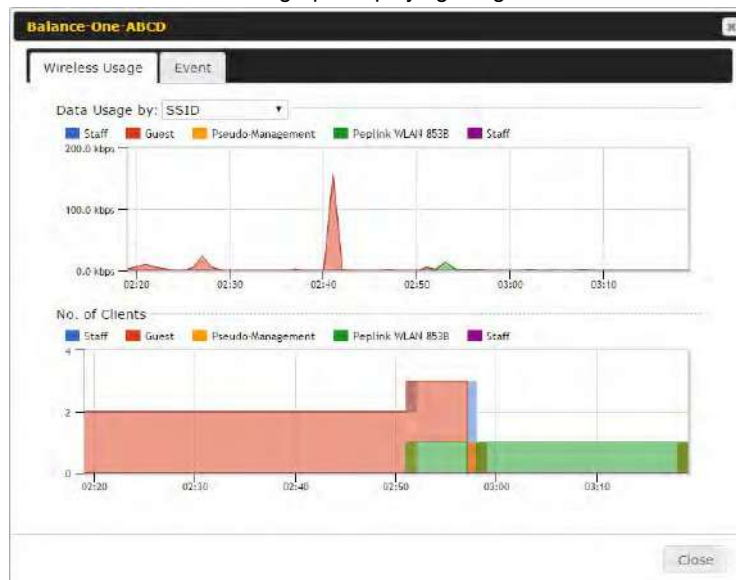
AP Details

Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:ED
Product Name	Pepwave AP Pro Duo
Name	
Location	
Firmware Version	3.5.2
Firmware Pack	Default (None) ▼
AP Client Limit	☒ Follow AP Profile ☐ Custom
2.4 GHz SSID List	T40pen
5 GHz SSID List	T40pen
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: Follow AP Profile ▼ 5 GHz: Follow AP Profile ▼
Output Power	2.4 GHz: Follow AP Profile ▼ 5 GHz: 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

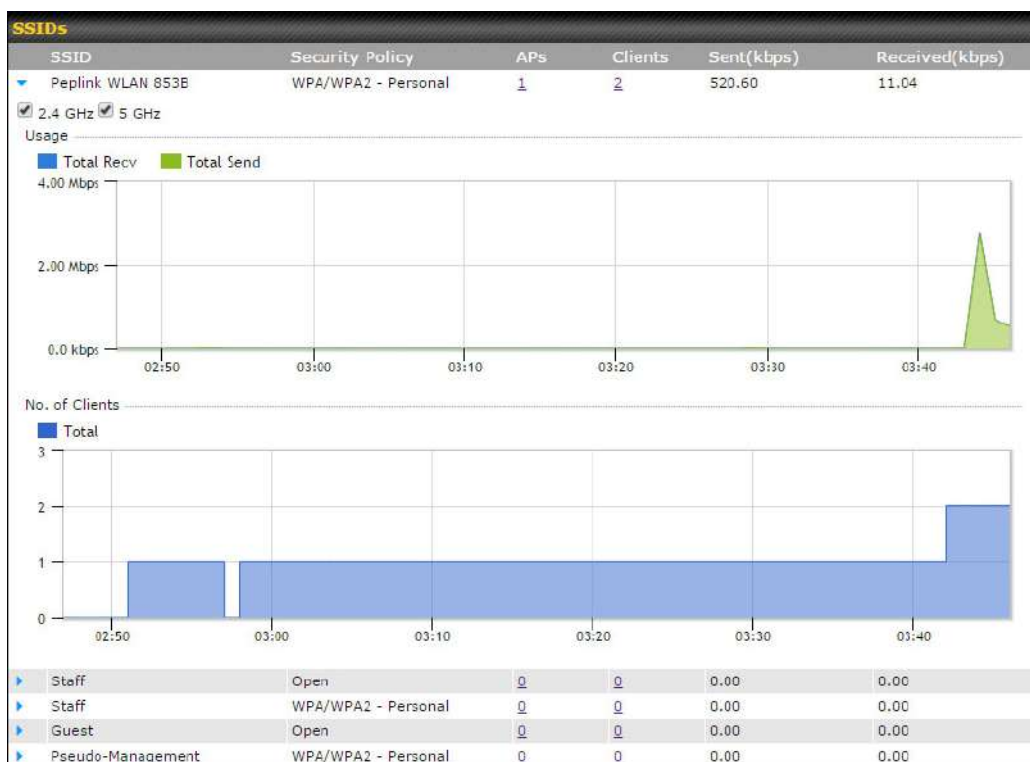
information by SSID or by AP send/receive rate.

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 00:26:8B: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 A8:8B:CF:E1:0F:1E disassociated from Balance_11a
Jan 2 11:11:54	Client A8:8B: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:FD 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 00:26:8B:08:AC:FD disassociated from Wireless_11a
Jan 2 09:52:46	Client 00:26:8B: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	

14.2.3 Wireless SSID

In-depth wireless SSID reports are available under **AP > Wireless SSID**.



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

14.2.4 Wireless Client

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

Search Filter	
Client MAC / SSID / AP Serial Number	
Maximum Result (1-256)	50
Search Result	
Search	

Top 10 Clients of last hour (Updated at 03:00)		
Client MAC Address	Upload	Download
C0:EE:FB:20:13:36	53.5 KB	101.4 KB

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:

Client C0:EE:FB:20:13:36
✕

Information	
Status	Associated
Access Point	1111-2222-3333
SSID	Peplink WLAN 853B
IP Address	192.168.1.34
Duration	00:27:31
Usage (Upload / Download)	141.28 MB / 4.35 MB
RSSI	-48
Rate (Upload / Download)	150M / 48M
Type	802.11na

Download
Upload

SSID	AP	From	To	Upload	Download
Peplink WLAN 853B	192C-1835-642F	Nov 23 03:43:04	-	141.28 MB	4.35 MB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:58:36	Nov 23 03:47:52	173.7 KB	94.2 KB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:52:15	Nov 23 02:58:15	105.9 KB	62.5 KB

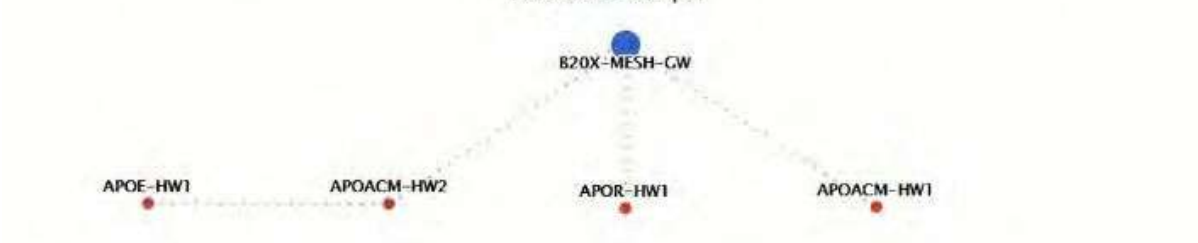
Close

14.2.5 Mesh / WDS

Mesh / WDS allows you to monitor the status of your wireless distribution system (WDS) or Mesh, and track activity by MAC address by navigating to **AP > Controller Status > Mesh / WDS**. This table shows the detailed information of each AP, including protocol, transmit rate (sent / received), signal strength, and duration.

Type	Peer MAC	Protocol	Rate (Send)	Rate (Receive)	Signal (dBm)	Duration
APOACM-HW1/						
Mesh ()		802.11ac	325M	650M	-56	19:13:35
APOACM-HW2/						
Mesh ()		802.11ac	650M	351M	-63	00:49:20
Mesh ()		802.11ac	390M	325M	-67	01:35:09
APOE-HW1/						
Mesh ()		802.11ac	58.5M	130M	-69	00:45:22
APOR-HW1/						
Mesh ()		802.11ac	325M	866.7M	-53	19:14:44
B20X-MESH-GW/						
Mesh ()		802.11ac	433M	650M	-69	19:14:44
Mesh ()		802.11ac	325M	390M	-66	01:35:42
Mesh ()		802.11ac	351M	650M	-70	19:13:45
Mesh ()		802.11ac	130M	117M	-88	00:45:52

Network Graph



14.2.6 Nearby Device

A listing of near devices can be accessed by navigating to **AP > Controller Status > Nearby Device**.

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

Nearby 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.

14.2.7 Event Log

You can access the AP Controller Event log by navigating to **AP > Controller Status > Event Log**.

Filter	
Search key	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name
Time	From hh:mm to hh:mm
Alerts only	☐
Search	

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:11:AA:28:89:A4 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 68:67:20:24:66:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:11:AA:28:89:A4 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:3D:3D:4E:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:3D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 33:8F:40:8F:78:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:11:AA:28:89:A4 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 5C:34:2B:1D:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A0:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A0:2D:A0:D5 associated with Marketing_11a	
		More...

Events

This event log displays all activity on your AP network, down to the client level. Use to filter box to search by MAC address, SSID, AP Serial Number, or AP Profile name. Click **View Alerts** to see only alerts, and click the **More...** link for additional records.

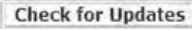
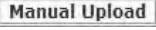
14.3 Toolbox

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								
<table border="1"> <thead> <tr> <th>Pack ID</th> <th>Release Date</th> <th>Details</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>1126</td> <td>2013-08-26</td> <td></td> <td></td> </tr> </tbody> </table>			Pack ID	Release Date	Details	Action	1126	2013-08-26		
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.

15 System Tab

15.1 System

15.1.1 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 administrative 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.

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 log out before closing the browser. The **default** is 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	hostname: ⚙️ This configuration is being managed by InControl .
Admin User Name	admin
Admin Password	
Confirm Admin Password	
Read-only User Name	user
User Password	
Confirm User Password	
Front Panel Passcode	☐
Web Session Timeout	4 Hours 0 Minutes
Authentication by RADIUS	☐ Enable
CLI SSH & Console	☐ Enable
Security	HTTP / HTTPS ▾ ☒ Redirect HTTP to HTTPS
Web Admin Access	HTTP: LAN Only HTTPS: LAN Only ▾
Web Admin Port	HTTP: 80 HTTPS: 443

LAN Connection Access Settings	
Allowed LAN Networks	☒ Any ☐ Allow this network only

Admin Settings	
Router Name	This field allows you to define a name for this Pepwave router. By default, Router Name is set as MAX_XXXX , where XXXX refers to the last 4 digits of the unit's serial number.
Admin User Name	Admin User Name is set as <i>admin</i> 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 <i>user</i> 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 Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router 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.
CLI SSH	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to Section 15.3 .
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:

	• HTTP • HTTPS • HTTP/HTTPS HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.
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.



LAN Connection Access Settings

Allowed LAN Networks ☐ Any ☒ Allow this network only Public (10) ▼

LAN Connection Access Settings	
Allowed LAN Networks	This field allows you to permit only specific networks or VLANs to access the Web UI.



WAN Connection Access Settings

Allowed Source IP Subnets ☐ Any ☒ Allow access from the following IP subnets only

Allowed WAN IP Address(es)

Connection / IP Address(es)	All	Clear
☒ WAN 1	☒ 10.98.3.158 (Interface IP)	
☐ WAN 2		
☐ Wi-Fi WAN		
☐ Cellular 1		
☐ Cellular 2		
☐ USB		

WAN Connection Access Settings	
Allowed Source IP	This field allows you to restrict web admin access only from defined IP subnets. • Any - Allow web admin accesses to be from anywhere, without IP address

Subnets	restriction. • Allow access from the following IP subnets only - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath: The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of <i>w.x.y.z/m</i>, where <i>w.x.y.z</i> is an IP address (e.g., <i>192.168.0.0</i>), and <i>m</i> is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, <i>192.168.0.0/24</i>). To define multiple subnets, separate each IP subnet one in a 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.

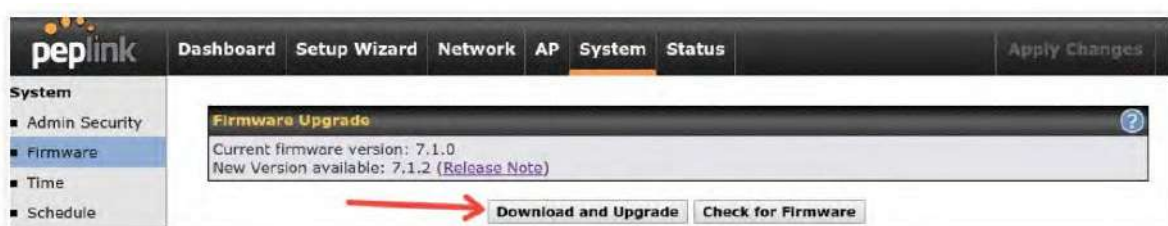
15.1.2 Firmware

Upgrading firmware can be done in one of three ways. Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

The automatic upgrade can be done from **System > Firmware**.



If an update is found the buttons will change to allow you to **Download and Update** the firmware.



Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

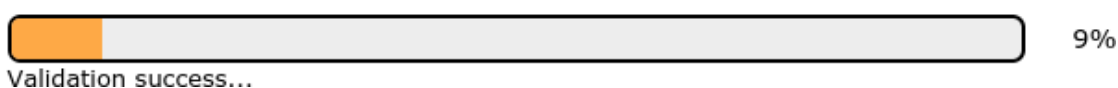
The router will download and then apply the firmware. The time that this process takes will depend on your internet connection's speed.



The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will also depend on the router that's being upgraded.

Firmware Upgrade

It may take up to 8 minutes.



*Upgrading the firmware will cause the router to reboot.

Web admin interface: install updates manually

In some cases, a special build may be provided via a ticket or it may be found in the forum. Upgrading to the special build can be done using this method, or using IC2 if you are using that to manage your firmware upgrades. A manual upgrade using the GA firmware posted on the site may also be recommended or required for a couple of reasons.

All of the Peplink/Pepwave GA firmware can be found [here](#). Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the Balance line.

Balance						
Product ▼		Search:				
Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual	
Balance 1350	HW2	7.1.2	Download	PDF	PDF	
Balance 1350	HW1	6.3.4	Download	PDF	PDF	
Balance 20	HW1-6	7.1.2	Download	PDF	PDF	
Balance 210	HW4	7.1.2	Download	PDF	PDF	

If the device has more than one firmware version the current hardware revision will be required to know what firmware to download.

Navigate to System > Firmware and click the Choose File button under the Manual Firmware Upgrade section. Navigate to the location that the firmware was downloaded to select the ".img" file and click the Open button.

Click on the Manual Upgrade button to start the upgrade process.

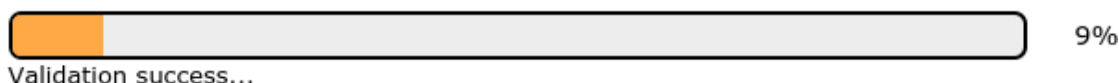


The screenshot shows a web interface titled "Manual Firmware Upgrade". It features a "Firmware Image" section with a "Choose File" button and a text field displaying "No file chosen". Below this is a "Manual Upgrade" button.

A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the Ok button to start the upgrade process. The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will depend on the router that's being upgraded.

Firmware Upgrade

It may take up to 8 minutes.



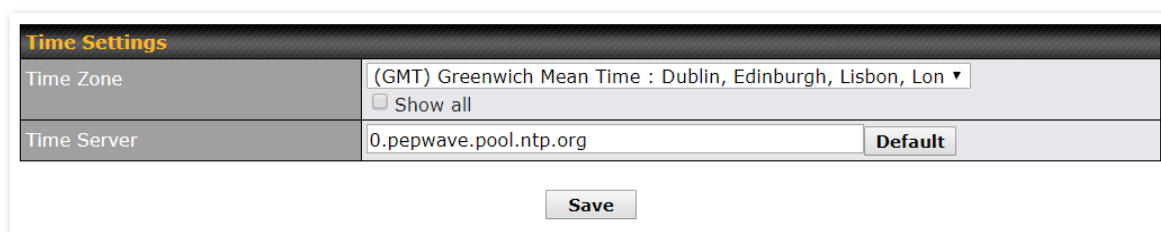
*Upgrading the firmware will cause the router to reboot.

The InControl method

[Described in this knowledgebase article on our forum.](#)

15.1.3 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**.



The screenshot shows the "Time Settings" configuration page. It includes a "Time Zone" dropdown menu set to "(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon" with a "Show all" link below it. The "Time Server" field is set to "0.pepwave.pool.ntp.org" with a "Default" button next to it. A "Save" button is located at the bottom.

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.

15.1.4 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**

Schedule			
Enabled			
Name	Time	Used by	
Weekdays Only	Weekdays only	-	
New Schedule			

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

Edit schedule profile							
Schedule Settings							
Enable	☒	The schedule function of those associated features will be lost if profile is disabled.					
Name	Weekdays Only						
Schedule	Weekdays only						
Used by	You may go to supported feature settings page and set this profile as scheduler.						
Schedule Map							
	Midnight	4am	8am	Noon	4pm	8pm	
Sunday	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x
Monday	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
Tuesday	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
Wednesday	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
Thursday	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
Friday	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
Saturday	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x	x x x x x x x x
		Save		Cancel			

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.

15.1.5 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 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 .
Connection Security	This setting specifies via a drop-down menu one of the following valid Connection Security: • None • STARTTLS • SSL/TLS
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to 25. If Connection Security is selected "STARTTLS", the default port number will be set to 587. If Connection Security is selected "SSL/TLS", the default port number will be set to 465. You may customize the port number by editing this field.
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

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

Test email sent.
(NOTE: Settings are not saved. To confirm the update, click 'Save' button.)

Email Notification Setup	
Email Notification	☒ Enable
SMTP Server	☒ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	
SMTP Password	
Confirm SMTP Password	
Sender's Email Address	
Recipient's Email Address	

Test Email Notification **Save**

Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
[<-] 220 smtp.gmail.com ESMTP h11sm3907691pjg.46 - gsmtp
[->] EHLO balance.peplink.com
[<-] 250-smtp.gmail.com at your service, [14.192.209.255]
[<-] 250-SIZE 35882577
[<-] 250-8BITMIME
[<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
[<-] 250-ENHANCEDSTATUSCODES
[<-] 250-PIPELINING
[<-] 250-CHUNKING
[<-] 250 SMTPUTF8
[->] AUTH PLAIN AGdwc2djbjk0QGdtYVwlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

15.1.6 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	☐
Remote Syslog Host	
Port:	514

Push Events to Mobile Devices	
Push Events	☒

URL Logging	
Enable	☒
Log Server Host	
Port:	514

Session Logging	
Enable	☒
Log Server Host	
Port:	514

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.
Push Events	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.
URL Logging	This setting is to enable event logging at the specified log server.
URL Logging Host	This setting specifies the IP address or hostname of the URL log server.
Session Logging	This setting is to enable event logging at the specified log server.
Session	This setting specifies the IP address or hostname of the Session log server.

Logging Host



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

15.1.7 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_OD84		
SNMP Port	161	Default	
SNMPv1	☐ Enable		
SNMPv2c	☐ Enable		
SNMPv3	☐ Enable		
Save			

Community Name	Allowed Source Network	Access Mode	
MyCompany	192.168.1.20/24	Read Only	X
Add SNMP Community			

SNMPv3 User Name	Authentication / Privacy	Access Mode	
SNMPUser	SHA / DES	Read Only	X
Add SNMP User			

SNMP Settings

SNMP Device Name This field shows the router name defined at **System>Admin Security**.

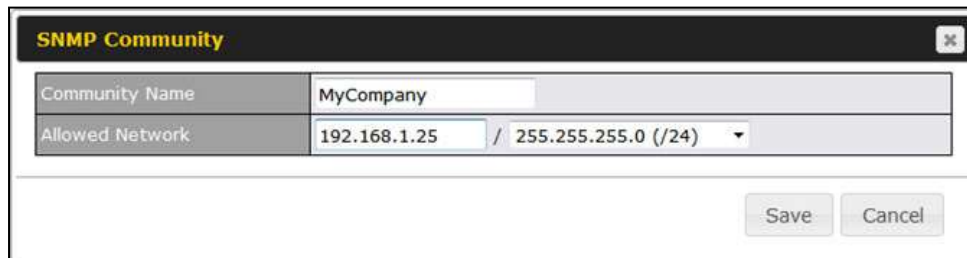
SNMP Port This option specifies the port which SNMP will use. The default port is **161**.

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:



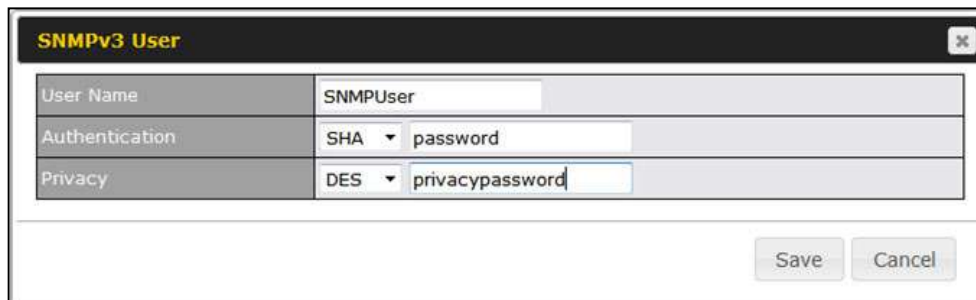
SNMP Community

Community Name	MyCompany
Allowed Network	192.168.1.25 / 255.255.255.0 (/24)

Save 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 password
Privacy	DES privacypassword

Save 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: - 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: NONE

- DES

When DES is selected, an entry field will appear for the password.

15.1.8 SMS Control

SMS Control allows the user to control the device using SMS even if the modem does not have a data connection. The settings for configuring the SMS Control can be found at **System>SMS Control**.

Note: Supported Models

- **Balance/MAX:** *-LTE-E, *-LTEA-W, *-LTEA-P, *-LTE-MX
- **EPX:** *-LW*, *-LP*

The screenshot shows the 'SMS Control' settings page. The 'Enable' checkbox is currently unchecked. There is a question mark icon next to the checkbox.

When this box is checked, the device will be allowed to take actions according to received commands via SMS.

Make sure your mobile plan supports SMS, and note that some plans may incur additional charges for this.

SMS Control can reboot devices and configure cellular settings over signalling channels, even if the modem does not have an active data connection.

For details of supported SMS command sets, please refer to our [knowledge base](#).

The screenshot shows the 'SMS Control' settings page with the 'Enable' checkbox checked. The 'Password' field is visible with a 'Hide Characters' checkbox checked. The 'White List' section has a 'Phone Number' input field and a '+' button to add more numbers. A 'Save' button is at the bottom.

SMS Control Settings	
Enable	Click the checkbox to enable the SMS Control.
Password	This setting sets the password for authentication - maximum of 32 characters, which cannot include semicolon (;).
White List	Optionally, you can add phone number(s) to the whitelist. Only matching phone numbers are allowed to issue SMS commands. Phone numbers must be in the E.164 International Phone Numbers format.

15.1.9 InControl



Controller Management Settings	
Controller	InControl ☐ Restricted to Status Reporting Only
Privately Host InControl	☒
InControl Host	 ☐ Fail over to InControl in the cloud.
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 checkbox 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.

When the box **Restricted to Status Reporting Only** is ticked, the router will only report its status, but can't be managed or configured by InControl.

Alternatively, you can 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.

15.1.10 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 screenshot shows the 'Configuration' page with the following sections:

- Restore Configuration to Factory Settings**: A button labeled 'Restore Factory Settings'.
- Download Active Configurations**: A button labeled 'Download'.
- Upload Configurations**: A section with a 'Configuration File' label, a 'Choose File' button, and a 'No file chosen' text. Below this is an 'Upload' button.
- Upload Configurations from High Availability Pair**: A section with a 'Configuration File' label, a 'Choose File' button, and a 'No file chosen' text. Below this is an '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.

15.1.11 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**.

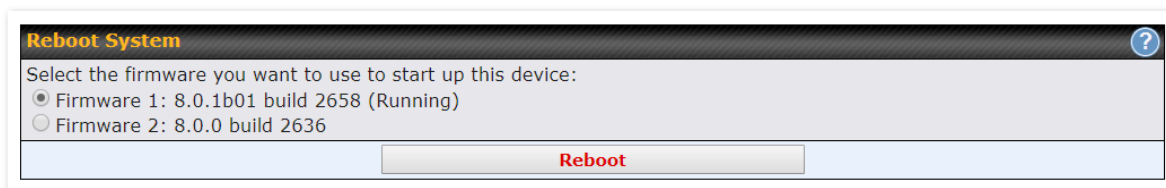


The 'Feature Activation' form has a title bar with the text 'Feature Activation'. Below the title bar, there is a label 'Activation Key' on the left side of a large, empty rectangular input field.

15.1.12 Reboot

This page provides a reboot button for restarting the system. For maximum reliability, the Peplink Balance Series can be equipped 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.

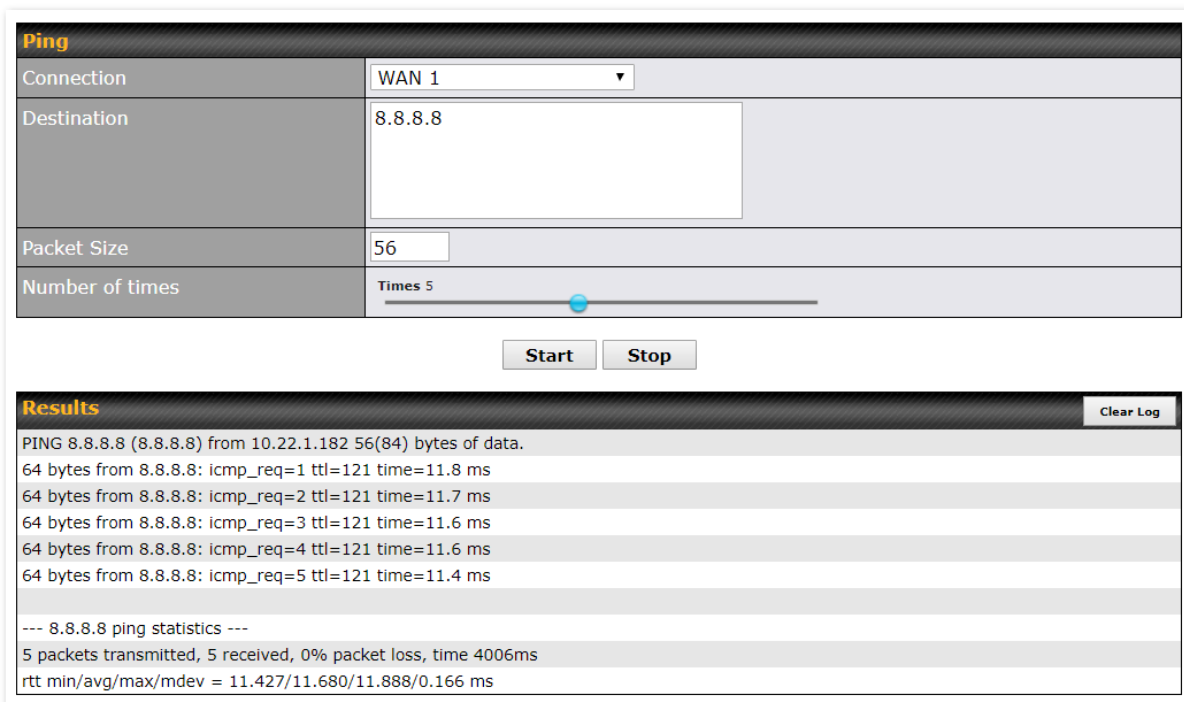


The 'Reboot System' form has a title bar with the text 'Reboot System' and a help icon (question mark in a circle) on the right. Below the title bar, the text 'Select the firmware you want to use to start up this device:' is followed by two radio button options: 'Firmware 1: 8.0.1b01 build 2658 (Running)' (which is selected) and 'Firmware 2: 8.0.0 build 2636'. At the bottom of the form is a button labeled 'Reboot' in red text.

15.2 Tools

15.2.1 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.

15.2.2 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

Start Stop

Results Clear Log

Tracerouting to 64.233.189.99 (64.233.189.99), 30 Traces (max), 30 Traces available

1 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

2 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

3 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

4 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

5 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

6 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

7 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

8 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

9 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

10 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

11 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

12 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

13 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

14 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

15 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

16 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

17 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

18 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

19 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

20 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

21 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

22 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

23 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

24 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

25 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

26 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

27 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

28 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

29 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

30 100.64.1.1 (100.64.1.1) 0.000 hop 0.000 hop 0.000 hop

Tip

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

15.2.3 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

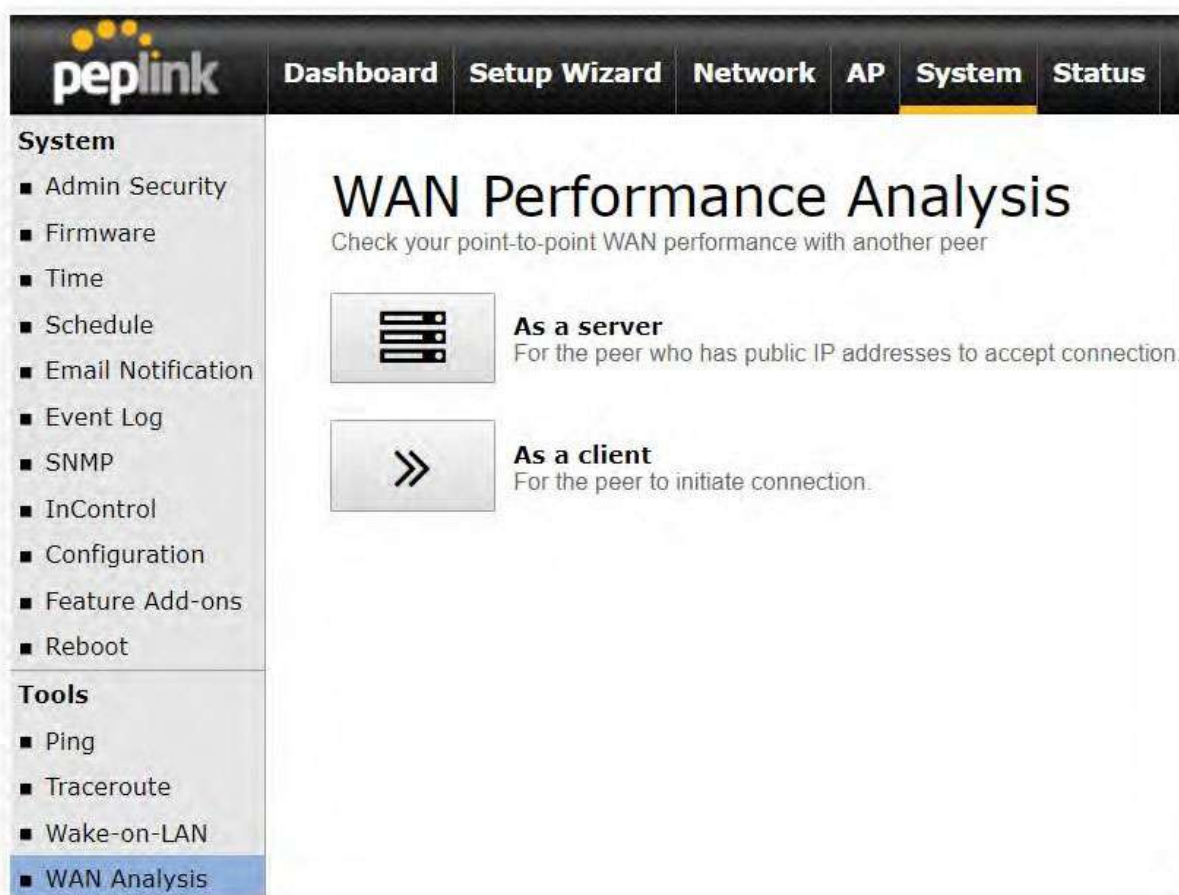
Wake-on-LAN Target: Custom MAC Address... 00:00:00:00:00:00 Send

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

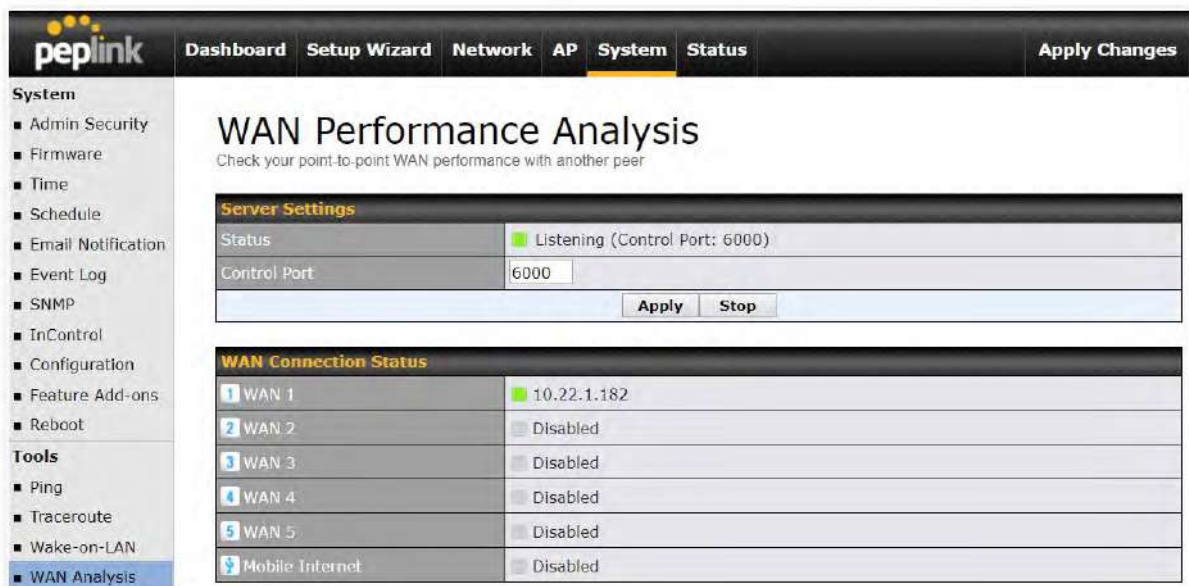
15.2.4 WAN Analysis

The WAN Analysis feature allows you to run a WAN to WAN speed test 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.



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.



The screenshot shows the Peplink System configuration interface. The top navigation bar includes links for Dashboard, Setup Wizard, Network, AP, System (selected), and Status. A right-hand button says 'Apply Changes'. The left sidebar lists various system settings under 'System' and 'Tools'. The main content area is titled 'WAN Performance Analysis' with a subtitle 'Check your point-to-point WAN performance with another peer'.

Server Settings

Status	☒ Listening (Control Port: 6000)
Control Port	6000

Buttons: Apply, Stop

WAN Connection Status

1 WAN 1	☒ 10.22.1.182
2 WAN 2	☐ Disabled
3 WAN 3	☐ Disabled
4 WAN 4	☐ Disabled
5 WAN 5	☐ Disabled
Mobile Internet	☐ 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.



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

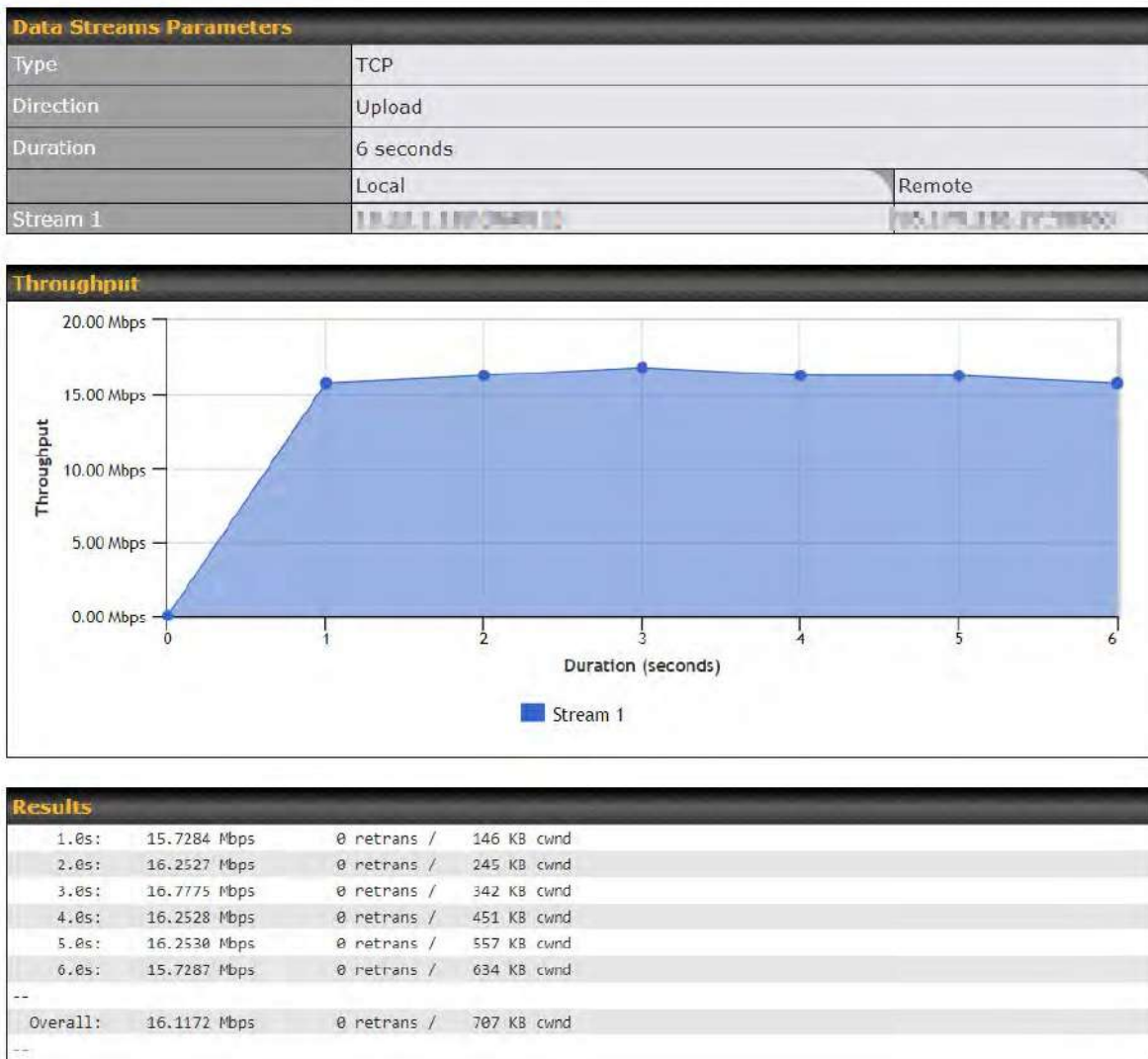
Control Port	6000
Data Port	57280 - 57287
Type	☒ TCP ☐ UDP
Direction	☒ Upload ☐ Download
Duration	20 seconds (5 - 600)

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 --	

Start Test

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

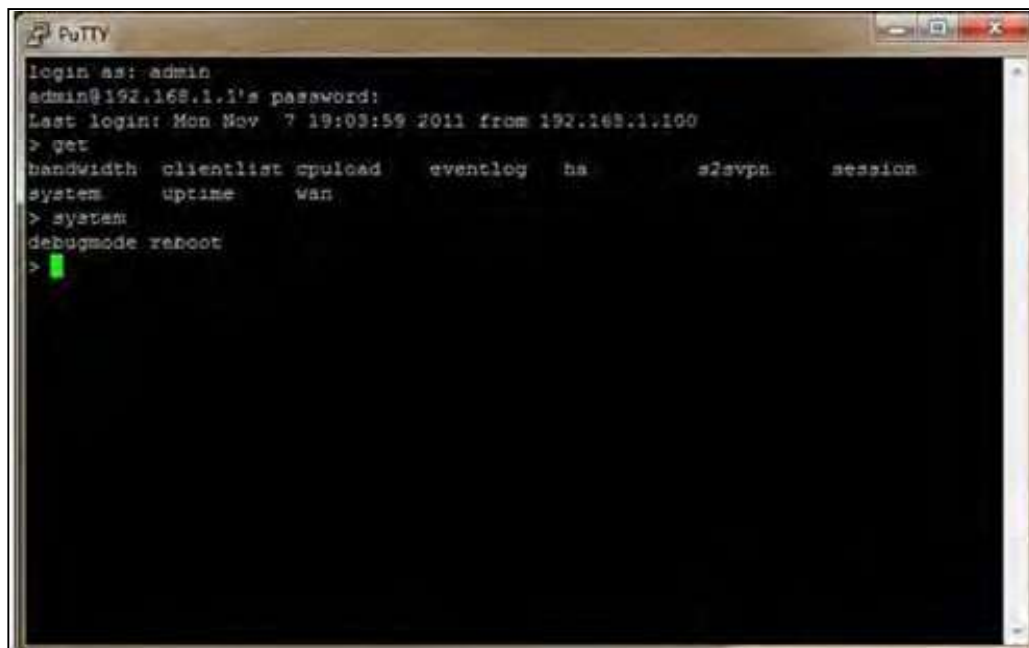


The test can be run again once it's complete by clicking the **Start** button or you can click **Close** and change the parameters for the test.

15.3 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
>
```

16 Status Tab

16.1 Status

16.1.1 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	10:56:00:00:00:00
WAN 1	10:56:00:00:00:00
WAN 2	10:56:00:00:00:00
WAN 3	10:56:00:00:00:00
WAN 4	10:56:00:00:00:00
WAN 5	10:56:00:00:00:00

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.

16.1.2 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 1	0	2
WAN 2	0	0

Top Clients	
Client IP Address	Total Sessions
10.22.1.1	116
10.22.1.2	90
172.16.17.1	86
10.22.1.3	83
172.16.17.2	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 ▾	/ 255.255.255.255 (/32) ▾
Port	Source or Destination ▾	
Protocol / Service	Spotify ▾	
Interface	☐ 1 BT ☐ 2 Virgin Media ☐ 3 WAN 3 ☐ 4 WAN 4 ☐ 5 Peplink HK Net... ☐ Mobile Internet ☐ VPN	
Search		

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.

16.1.3 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

☐ Online Clients Only
 ☐ DHCP Clients Only

Client List

IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
192.168.167.10		0	0	10:56:56:56:56:56	
192.168.167.11	U64-2-1	0	0	00:50:56:56:56:14	
192.168.167.12	U64-2-2	0	0	10:56:56:56:56:75	

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

In the client list table, there is a “Ban Client” feature which is used to disconnect the Wi-Fi and Remote User Access clients by clicking the  button on the right.

Filter

☐ Online Clients Only
☐ DHCP Clients Only

Client List

IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)	
		0	0				
		0	0			-37	

There is a blocklist on the same page after you banned the Wi-Fi or Remote User Access clients.

Filter

☐ Online Clients Only

☐ DHCP Clients Only

Access restriction in action, some clients are currently banned

Client List

IP Address	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)
------------	------	-----------------	---------------	-------------	---------------------	--------------

You may also unblock the Wi-Fi or Remote User Access clients when the client devices need to reconnect the network by clicking  the button on the right.



16.1.4 WINS Clients

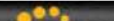
The WINS client list table is located at **Status>WINS Client**.

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

16.1.5 OSPF & RIPv2

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



Dashboard

Setup Wizard

Network

AP

System

Status

Apply Changes

Status

■ Device

■ Active Sessions

■ Client List

■ OSPF & RIPv2

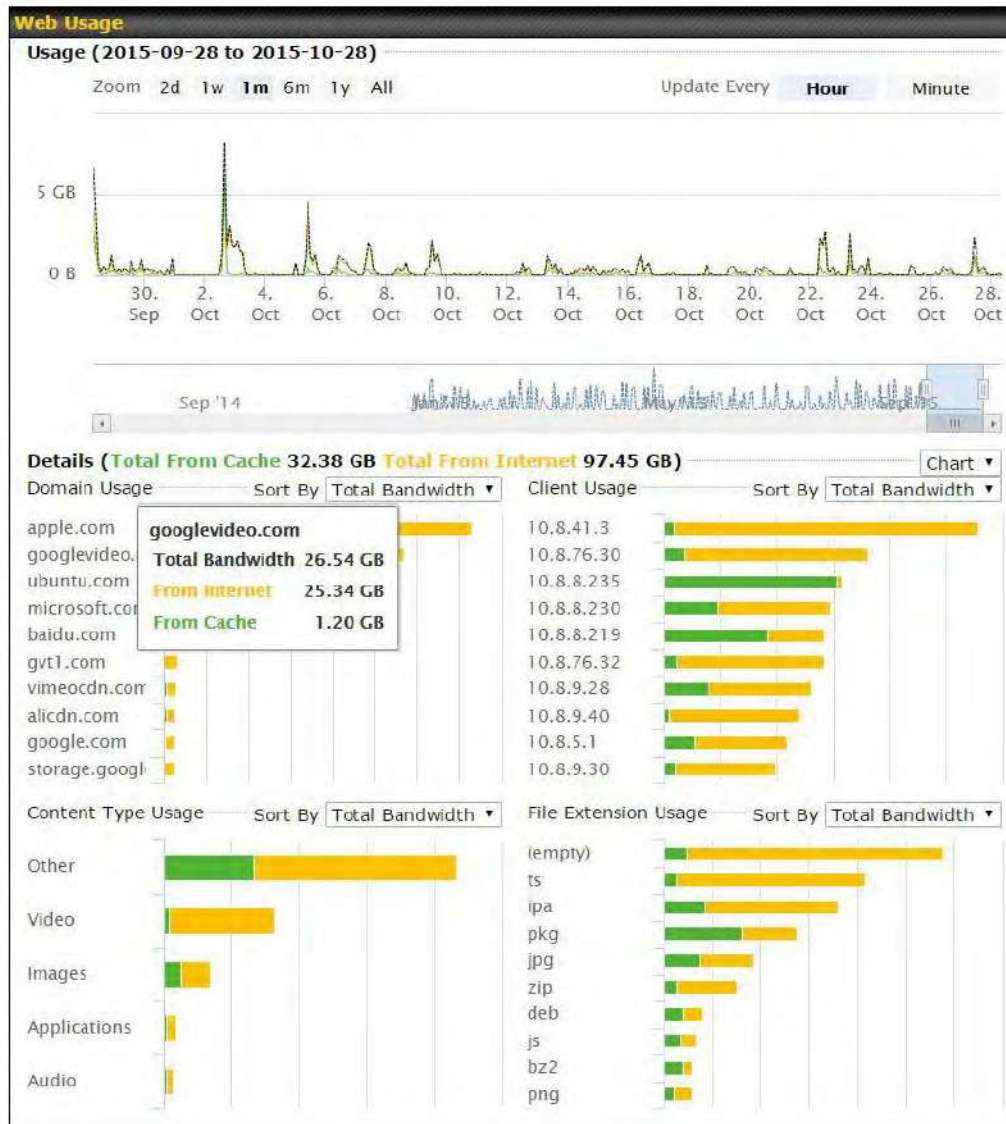
■ BGP

OSPF & RIPv2

Area	Remote Networks
0.0.0.0	
PepVPN	10.0.2.0/24 10.0.3.0/24 192.168.63.0/24 10.0.100.0/24 192.168.100.0/24 192.168.162.0/24

16.1.6 MediaFast

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



16.1.7 PepVPN / SpeedFusion Status

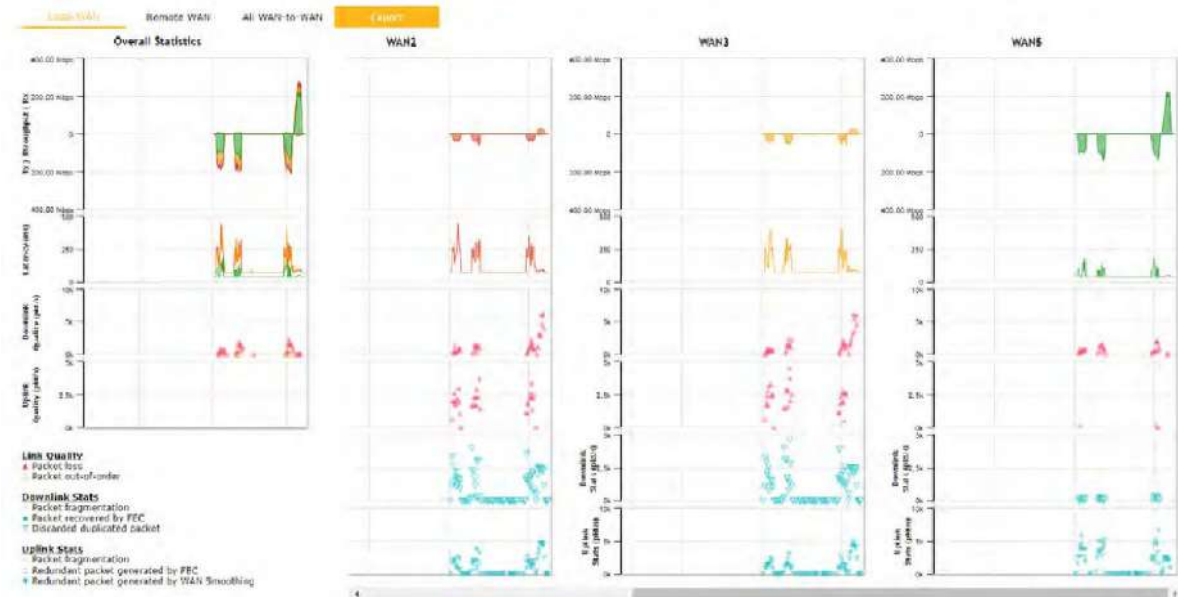
PepVPN/SpeedFusion Status shows the current connection status of each connection profile and is displayed at **Status> PepVPN/SpeedFusion**.

PepVPN with SpeedFusion - Remote Peer			Show all profiles
Search			
Remote Peer ▲	Profile	Information	
MAX-BR1-XXXX (XXXX-XXXX-XXXX-XXXX-XXXX-XXXX)	XXXX	XXXX-XXXX-XXXX-XXXX-XXXX-XXXX XXXX-XXXX-XXXX-XXXX-XXXX-XXXX XXXX-XXXX-XXXX-XXXX-XXXX-XXXX XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	 >
MAX-BR1-XXXX (XXXX-XXXX-XXXX-XXXX-XXXX-XXXX)	XXXX	XXXX-XXXX-XXXX-XXXX-XXXX-XXXX XXXX-XXXX-XXXX-XXXX-XXXX-XXXX XXXX-XXXX-XXXX-XXXX-XXXX-XXXX XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	 >

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

PepVPN with SpeedFusion - Remote Peer			Show all profiles
Search		SFC	
Remote Peer ▲	Profile	Information	
SFC-SIN-001 (SFC-SIN-001)	SFC	SpeedFusion Cloud	 >
WAN1	Rx:	< 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 42 ms	
WAN2	Rx:	< 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 42 ms	
WAN3	Rx:	< 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 42 ms	
WAN4	Rx:	Not available - WAN disabled	
WAN5	Rx:	< 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 10 ms	
Mobile Internet	Rx:	< 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 32 ms	
Total	Rx:	< 1 kbps Tx: 1.1 kbps Loss rate: 0.0 pkt/s	

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



When pressing the  button for a PepVPN/SpeedFusion Tunnel Bandwidth Test Tool, the following menu will appear:

PepVPN Details

Connection Information

More information

Profile	SFC
Remote ID	SFC-SIN-001
Device Name	SFC-SIN-001
Serial Number	1197-A047-2E3D

WAN Statistics

Show remote connections

WAN Label

WAN Name
IP Address and Port

WAN1	Not available - WAN disabled				
WAN2	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 43 ms	
WAN3	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 44 ms	
WAN4	Not available - WAN disabled				
WAN5	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 10 ms	
Mobile Internet	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 42 ms	
Total	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s		

PepVPN Test Configuration

Type
TCP
UDP

Streams
4

Direction
Upload
Download

Duration
20 seconds (5 - 600)

Start

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	☒ Show remote connections
WAN Label	☒ WAN Name ☐ IP Address and Port
BT WAN Virgin Media	
Rx:	< 1 kbps
Tx:	< 1 kbps
Loss rate:	0.0 pkt/s
Latency:	17 ms
Not available - WAN disabled	

The PepVPN/SpeedFusion test configuration allows us to configure and perform thorough tests. This is usually done after the initial installation of the routers and in case there are problems with aggregation.

PepVPN Test Configuration	
Type	☒ TCP ☐ UDP
Streams	4 ▼
Direction	☒ Upload ☐ Download
Duration	20 seconds (5 - 600)
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:	2.0709 Mbps	0 retrans /	205 KB cwnd
Stream 4:	4.1534 Mbps	0 retrans /	253 KB cwnd
--			
Overall:	15.3520 Mbps	0 retrans /	1045 KB cwnd
--			
TEST DONE			

16.1.8 Event Log

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

Device Event Log

The screenshot shows the 'Device Event Log' section of the Peplink management interface. It features a tabbed interface with 'Device Event Log' and 'ContentHub Event Log'. The 'Device Event Log' tab is active, displaying a list of events. Each event entry includes a timestamp (e.g., 'Apr 17 14:54:52') and a description (e.g., 'System: Changes applied'). An 'Auto Refresh' checkbox is checked in the top right corner of the log area. A 'Clear Log' button is located at the bottom left of the log area.

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.

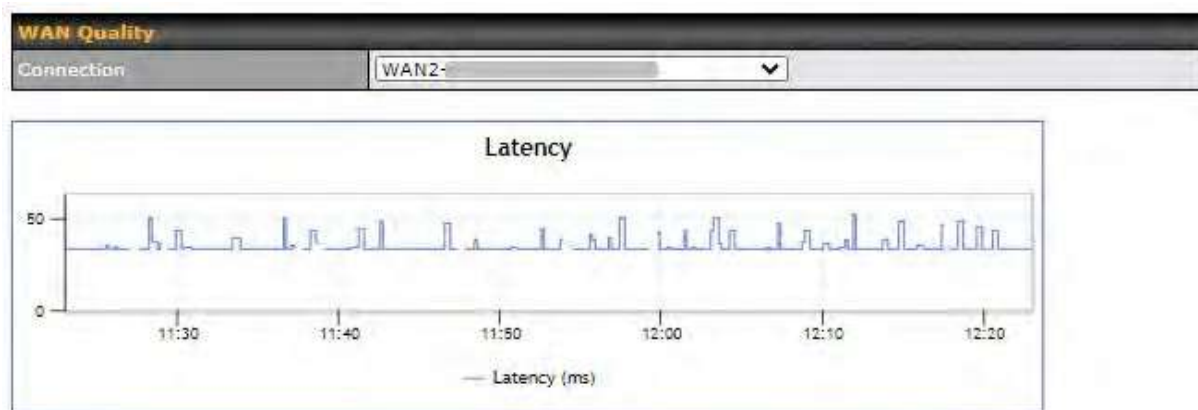
IPsec Event Log

The screenshot shows the 'IPsec VPN Event Log' section of the Peplink management interface. It features a tabbed interface with 'Device Event Log' and 'IPsec VPN Event Log'. The 'IPsec VPN Event Log' tab is active, displaying a list of events. Each event entry includes a timestamp (e.g., 'Dec 30 08:32:26') and a description (e.g., 'IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...'). An 'Auto Refresh' checkbox is checked in the top right corner of the log area. An 'End of log' message is visible at the bottom right of the log area.

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**.

16.2 WAN Quality



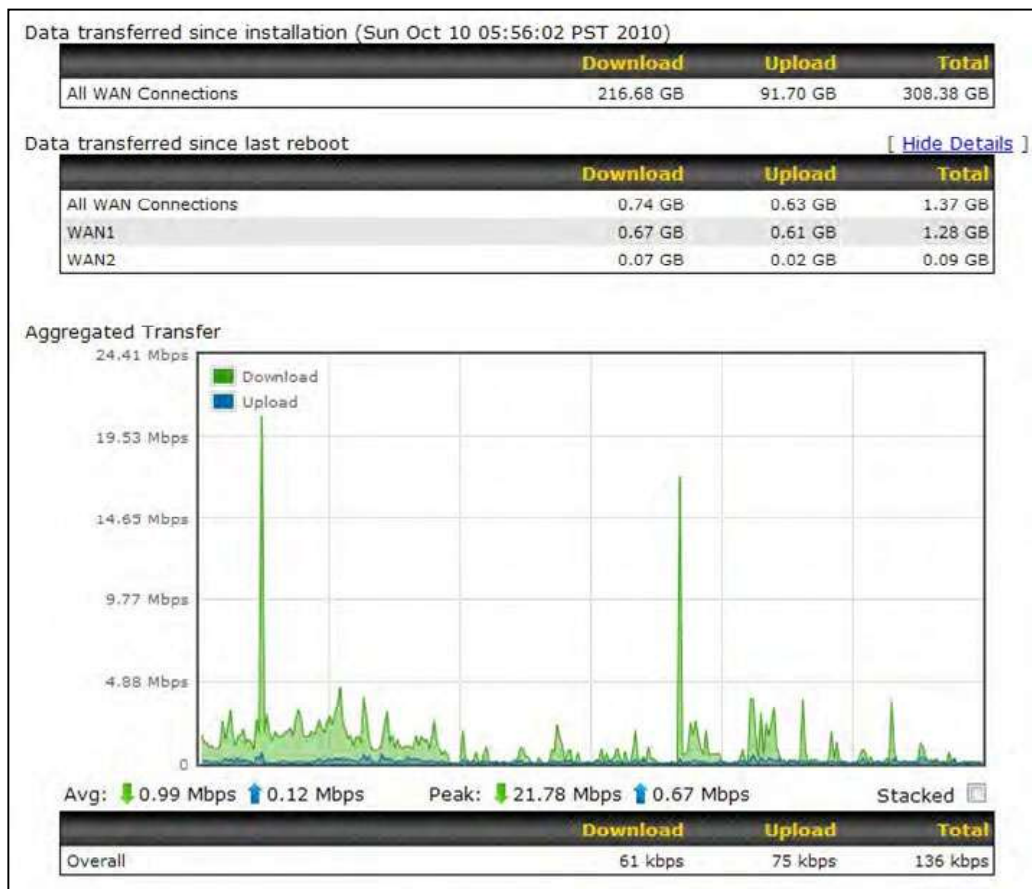
The **Status > WAN Quality** allows to show detailed information about each connected WAN connection.

16.3 Usage Reports

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.

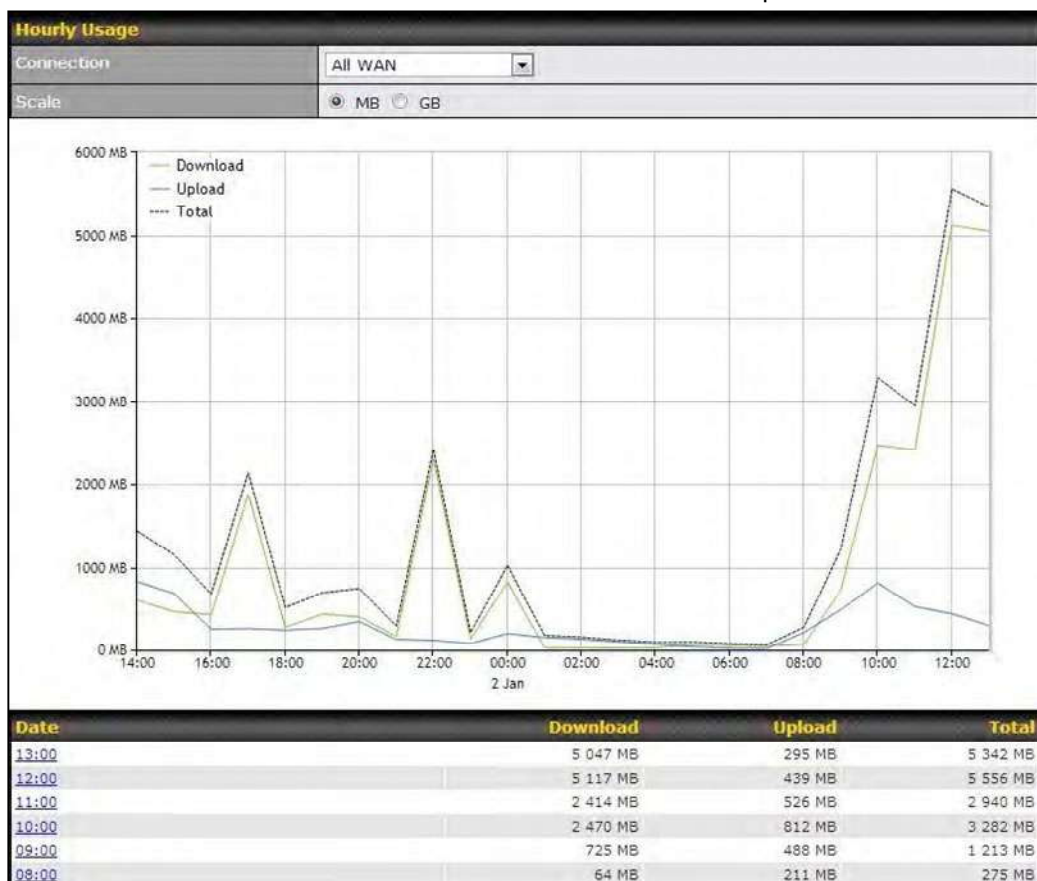
16.3.1 Real-Time

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.



16.3.2 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.



16.3.3 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.

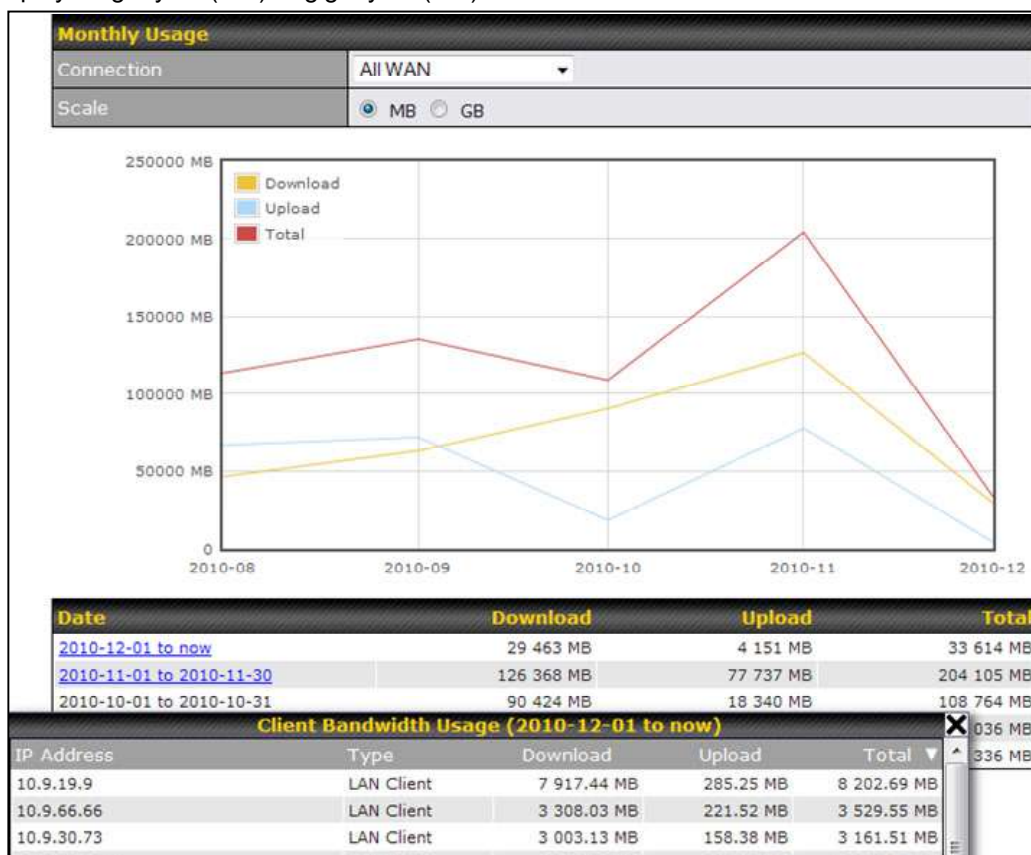
Client Bandwidth Usage (2015-02-15)

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

16.3.4 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

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.

Hold for 5-10 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

Hold for approximately 20 seconds for factory reset (Note: The LED status light blinks in RED 3 times and release the button, all WAN/LAN port lights start blinking)

After the Peplink Balance router finishes rebooting, the factory default settings will be restored.

For Balance/MediaFast models with an LCD menu:

- Use the buttons on the 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 previous configurations and bandwidth usage data will be lost after restoring factory default settings. Regular backup of configuration settings is strongly recommended.

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

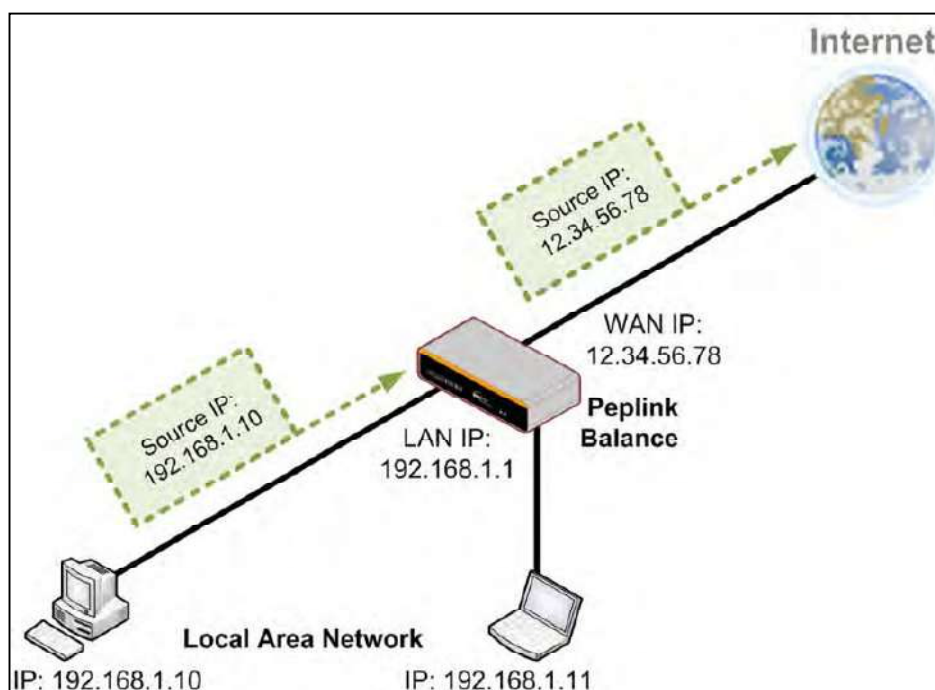
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

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.

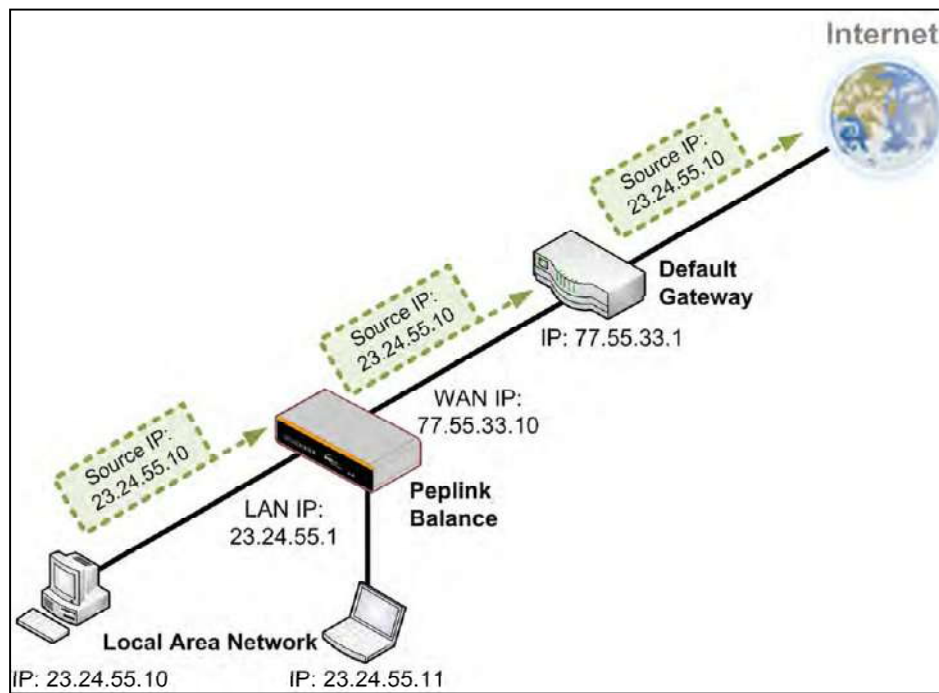
The following figure shows the packet flow in NAT mode:



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. FusionSIM Manual

Peplink has developed a unique technology called FusionSIM, which allows SIM cards to remotely link to a cellular router. This can be done via cloud or within the same physical network. There are a few key scenarios to fit certain applications.

The purpose of this manual is to provide an introduction on where to start and how to set up for the most common scenarios and uses.

Requirements

1. A Cellular router that supports FusionSIM technology
2. SIM Injector
3. SIM card

Notes:

- Always check for the latest [Firmware version](#) for both the cellular router and the SIM Injector. You can also check for the latest Firmware version on the device's WEB configuration page.
- A list of products that support FusionSIM can be found on the SIM Injector [WEB page](#). Please check under the section **Supported models**.

SIM Injector reset and login details

How to reset a SIM Injector:

- Hold the reset button for 5-10 seconds. Once the LED status light turns RED, the reset button can be released. SIM Injector will reboot and start with the factory default settings.

The default WEB login settings:

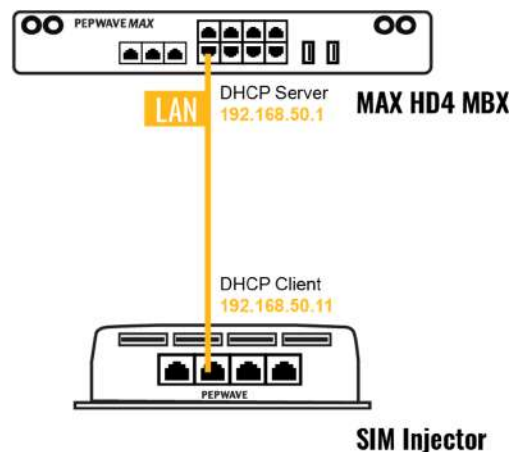
- **User:** admin
- **Password:** admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

Notes:

- The SIM Injector can be monitored via InControl 2. Configuration is not supported.

Scenario 1: SIM Injector in LAN of Cellular Router

Setup topology



This is the most basic scenario in which the SIM Injector is connected directly to the cellular router's LAN port via an ethernet cable. This allows for the cellular router to be positioned for the best possible signal. Meanwhile, the SIM cards can be conveniently located in other locations such as the office, passenger area, or the bridge of a ship. The SIM Injector allows for easily swapping SIM cards without needing to access a cellular router.

IMPORTANT: Cellular WAN will not fallback to the local SIM if it is configured to use the SIM Injector.

Configuring the SIM Injector

1. Connect the SIM Injector to the LAN port of the cellular router.
2. Insert SIM cards into the SIM Injector. The SIM cards will be automatically detected.

IMPORTANT: SIM cards inserted into SIM Injector must not have a PIN code.

Note 1: The SIM Injector gets its IP address via DHCP and doesn't have a static IP address. To find it's address, please check the DHCP lease on the cellular router.

Configuring the Cellular Router

Step 1. Enable the SIM Injector communication protocol.

- 1a. If you are using a Balance cellular router, go to the **Network** tab (top navigation bar).
- 1b. If you are using a MAX cellular router, go to the **Advanced** tab (top navigation bar).

2. Under **Misc. settings** (left navigation bar) find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.



4. Check the **Auto LAN discovery** checkbox and click **Save** and **Apply Changes**.



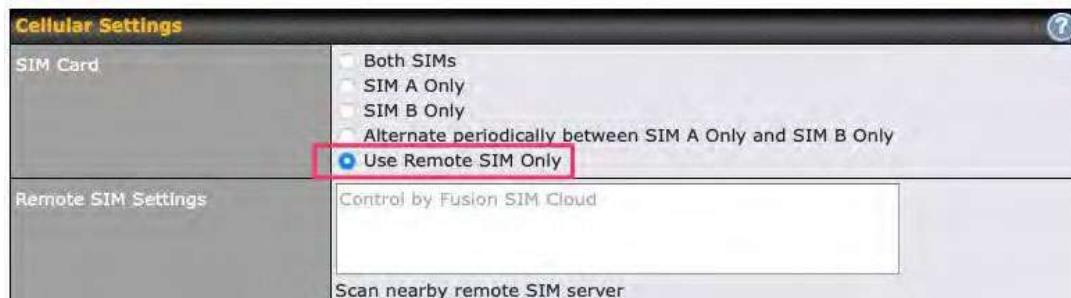
5. Click **Save** and then **Apply Changes**.

Step 2. Enable RemoteSIM for the selected Cellular interface.

1. Go to **Network** (top navigation bar), then **WAN** (left navigation bar) and click **Details** for a selected cellular WAN. This will open the WAN Connection Settings page.



2. Scroll down to **Cellular settings**.
3. In the **SIM Card** section, select **Use Remote SIM Only**.

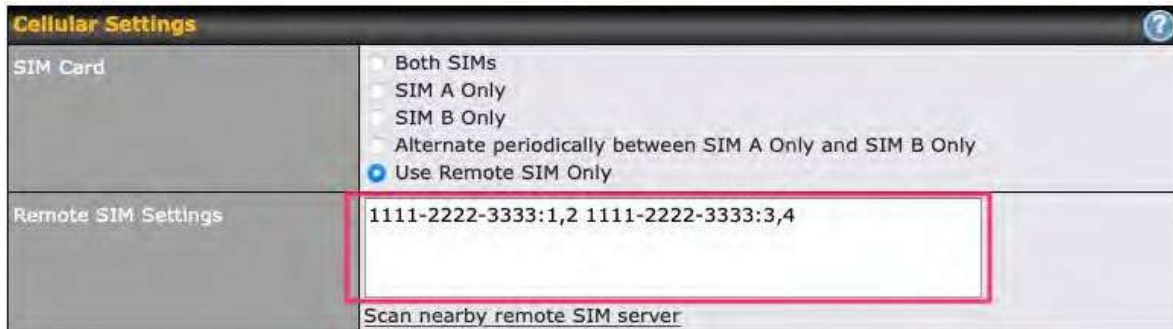


4. Enter configuration settings in **Remote SIM Settings** section. Click on **Scan nearby remote SIM server** to show the serial number(s) of the connected SIM Injector(s). Available configuration options for cellular interface are shown below:

- A. Defining SIM Injector(s)
 - Format: <S/N>
 - Example 1: 1111-2222-3333
 - Example 2: 1111-2222-3333 4444-5555-6666

B. Defining SIM Injector(s) SIM slot(s):

- Format: <S/N:slot number>
- Example 1: 1111-2222-3333:7,5 (the Cellular Interface will use SIM in slot 7, then 5)
- Example 2: 1111-2222-3333:1,2 1111-2222-3333:3,4 (the cellular Interface will use SIM in slot 1, then in 2 from the first SIM Injector, and then it will use 3 and 4 from the second SIM Injector).



Note: It is recommended to use different SIM slots for each cellular interface.

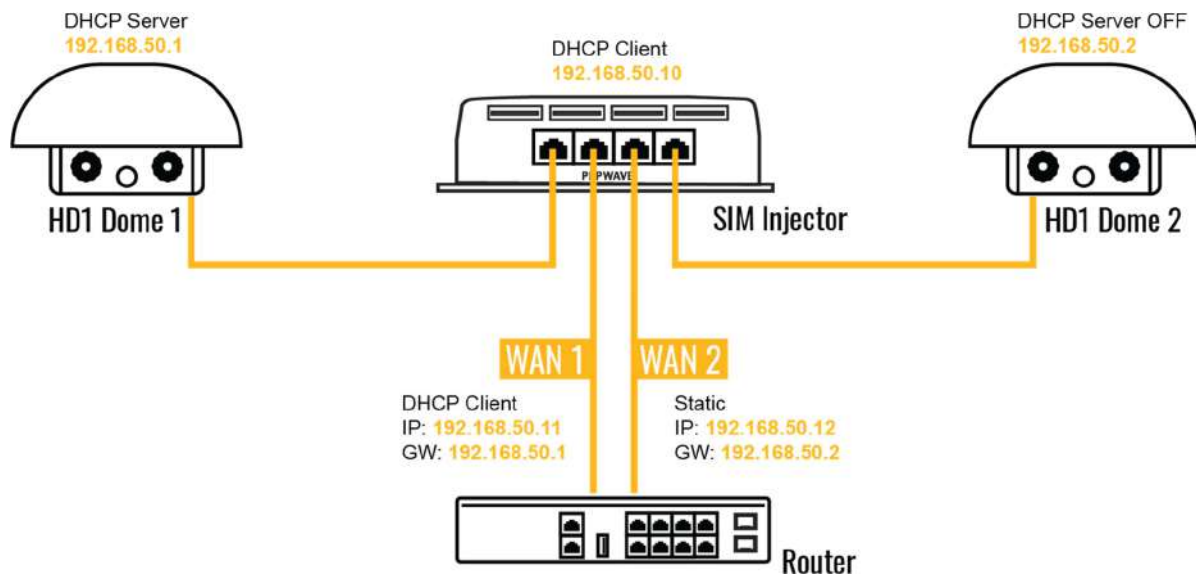
5. Click **Save** and **Apply Changes**.

Step 3. (Optional) Custom SIM cards settings.

- 1a. For a Balance router, go to the **Network** (Top tab). 1b. For a MAX router, go to the **Advanced** (Top tab).
2. Under **Misc. settings** (Left-side tab) find **Remote SIM Management**.
3. Click on the **Add Remote SIM** button, fill in all the required info and click **Save**. This section allows defining custom requirements for a SIM card located in a certain SIM slot:
 - Enable/Disable roaming (by default roaming is disabled).
 - Add Custom mobile operator settings (APN, user name, password).
4. Repeat configuration for all SIM cards which need custom settings.
5. Click **Apply Changes** to take effect.

Scenario 2: SIM Injector in WAN of main Router and multiple Cellular Routers

Setup topology



In this scenario, each HD Dome creates a WAN connection to the main router. A single SIM Injector is used to provide SIM cards for each HD Dome. The HD Dome can be replaced with any Peplink cellular router supporting RemoteSIM technology.

This scenario requires the completion of the configuration steps shown in Scenario 1 in addition to the configuration steps explained below.

Additional configurations for Cellular Routers

Step 1. Disable the DHCP server.

- HD Dome 1 should act as a DHCP server.
- HD Dome 2 should be configured to have a static IP address with DHCP disabled.
- Both routers should be in the same subnet (e.g. 192.168.50.1 and 192.168.50.2).

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **Untagged LAN**. This will open up the LAN settings page.
2. Change the IP address to 192.168.50.2.
3. In the **DHCP Server** section, uncheck the checkbox to disable DHCP Server.
4. Click **Save** and **Apply Changes**.

Step 2. Ethernet port configuration

The Ethernet port must be set to **ACCESS** mode for each HD Dome. To do this, dummy VLANs need to be created first.

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **New LAN**. This will open the settings page to create a dummy VLAN.
2. The image below shows the values that need to be changed to create a new VLAN:

LAN

IP Settings

IP Address: 192.168.10.1 (255.255.255.0 (/24))

Network Settings

Name: VLAN10

VLAN ID: 10

Inter-VLAN routing: ☒

Captive Portal: ☐

DHCP Server

DHCP Server: ☐ Enable

DHCP Server Logging: ☐

IP Range: 255.255.255.0 (/24)

Note: set different IP addresses for each HD dome (e.g. 192.168.10.1 and 192.168.10.2).

3. Click Save and **Apply Changes**.
4. Go to **Network** (Top tab), then **Port Settings** (Left-side tab).
5. Set the Port Type to **Access** and set VLAN to **Untagged LAN** (see picture below).

Port Settings

	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port 1	☒	100	100	Access	Untagged

6. Click **Save** and **Apply Changes**.

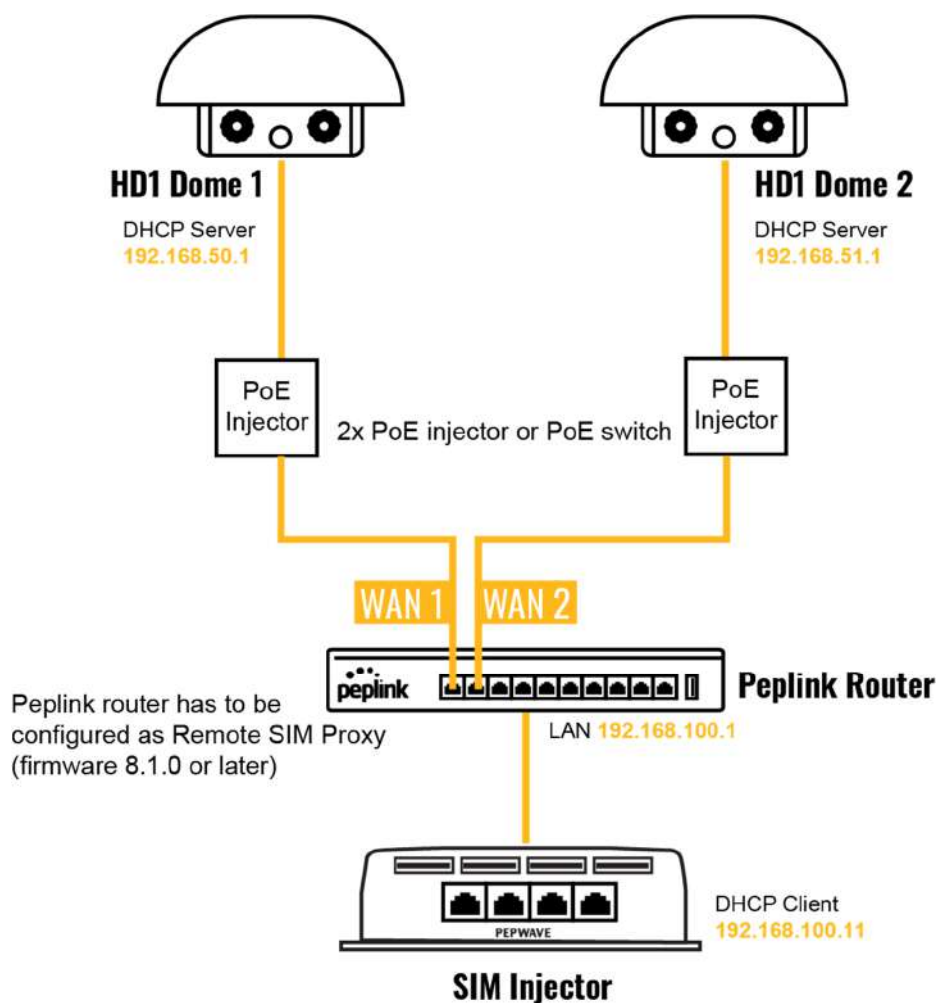
Configuration requirements for the main Router

Requirements for the main router are:

- Configure **WAN 1** as a DHCP client.
- **WAN 1** will automatically get the Gateway IP address from HD Dome 1.
- Configure **WAN 2** as a Static IP and set it to 192.168.50.12.
- Configure **WAN 2** Gateway to 192.168.50.2. Same as the HD Dome 2's IP address.

Scenario 3: SIM Injector in LAN of main Router and multiple Cellular Routers

Setup topology



In this scenario, SIMs are provided to the HD Domes via the main router. In this example, the **Remote SIM Proxy** functionality needs to be enabled on the main router.

Notes:

- HD Dome can be replaced with any other cellular router that supports RemoteSIM.
- It is recommended to use Peplink [Balance series](#) or [X series](#) routers as the main router.

This scenario requires the completion of the configuration steps for the cellular router and the SIM Injector as in Scenario 1. The configuration for the main router is explained below.

Main Router configuration

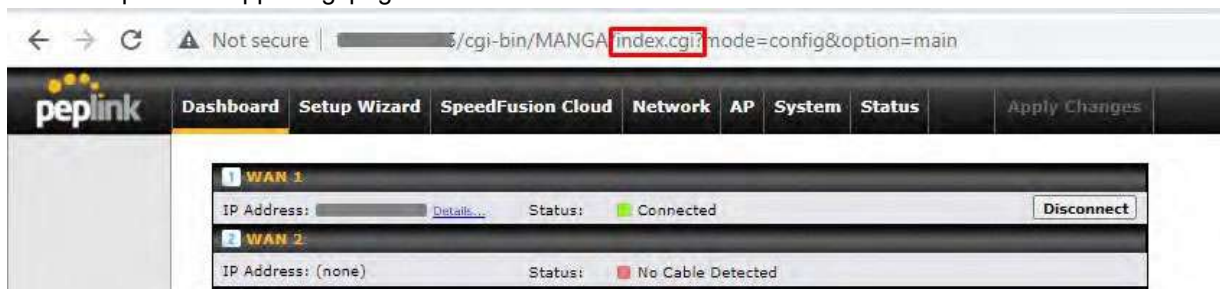
IMPORTANT: Main router LAN side and Cellular Routers must be configured using different subnets, e.g. 192.168.**50**.1/24 and 192.168.**100**.1/24.

Note: please make sure the Peplink router is running Firmware 8.1.0 or above.

1. Open the main router WEB interface and change:

From <IP address>/cgi-bin/MANGA/**index.cgi** to <IP address>/cgi-bin/MANGA/**support.cgi**.

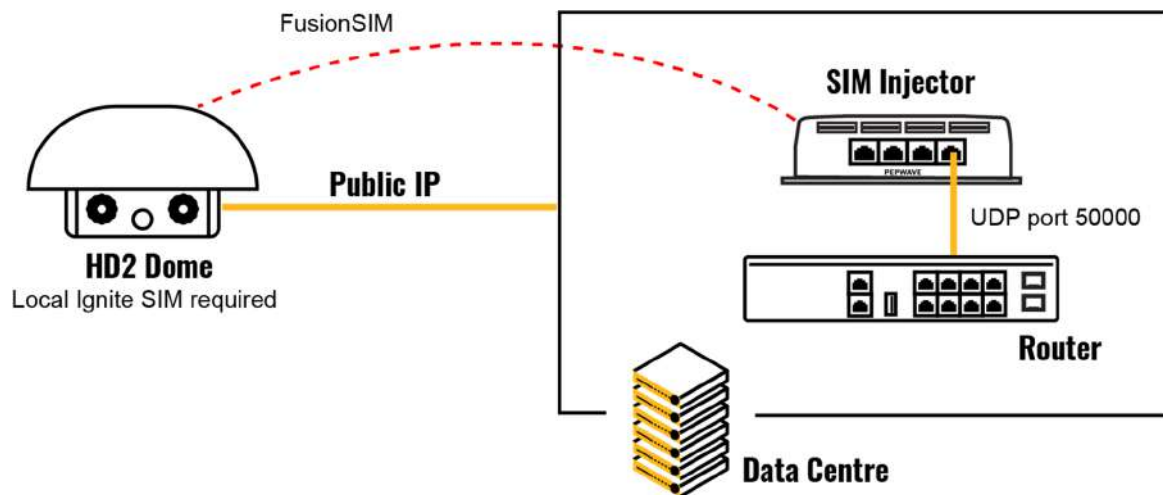
This will open the support.cgi page.



2. Scroll down to find **Remote SIM Proxy** and click on **[click to configure]** that is located next to it.
3. Check the **Enable** checkbox.
4. Click on **Save**.
5. Go back to the index.cgi page and click on **Apply Changes**.

Scenario 4: SIM Injector in a remote location

Setup topology



Requirements for installing a SIM Injector in a remote location:

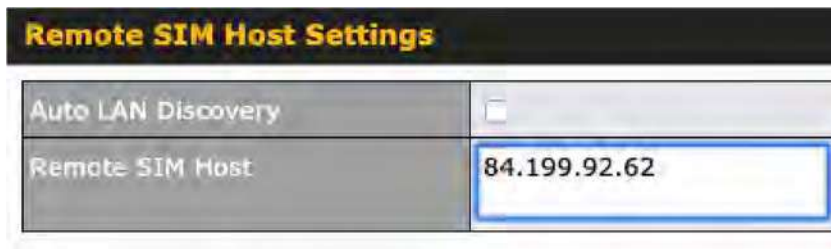
- Cellular router communicates with the SIM Injector via UDP port 50000. Therefore this port must be reachable via public IP over the Internet.
- The one way latency between the cellular router and the SIM Injector should be **up to 250 ms**. A higher latency may lead to stability issues.
- The cellular router must have Internet connection to connect to the SIM Injector. It can be another Internet connection via Ethernet or Fiber if possible, or a secondary cellular interface with a local SIM (Ignite SIM).
- Due to its high latency, it is not recommended to use satellite WAN for connecting to a SIM Injector in remote locations.

SIM Injector configuration is the same as in Scenario 1.

Cellular Router configuration

Step 1. Enable the SIM Injector communication protocol.

- 1a. For a Balance cellular router, go to the **Network** (Top tab).
- 1b. For a MAX cellular router, go to the **Advanced** (Top tab).
2. Under **Misc. settings** (Left-side tab), find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.
4. Enter the public IP of the SIM Injector and click **Save** and **Apply Changes**.



Remote SIM Host Settings	
Auto LAN Discovery	☐
Remote SIM Host	84.199.92.62

Notes:

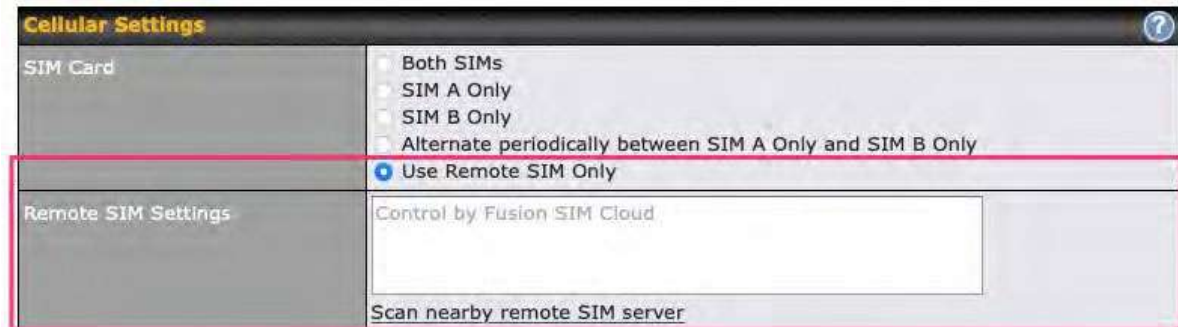
- Do NOT check **Auto LAN Discovery**.
- Adding a SIM Injector serial number to the **Remote SIM Host** field is a mistake!

Step 2. RemoteSIM and custom SIM card settings configurations are the same as in Scenario 1.

How to check if a Pepwave Cellular Router supports Remote SIM

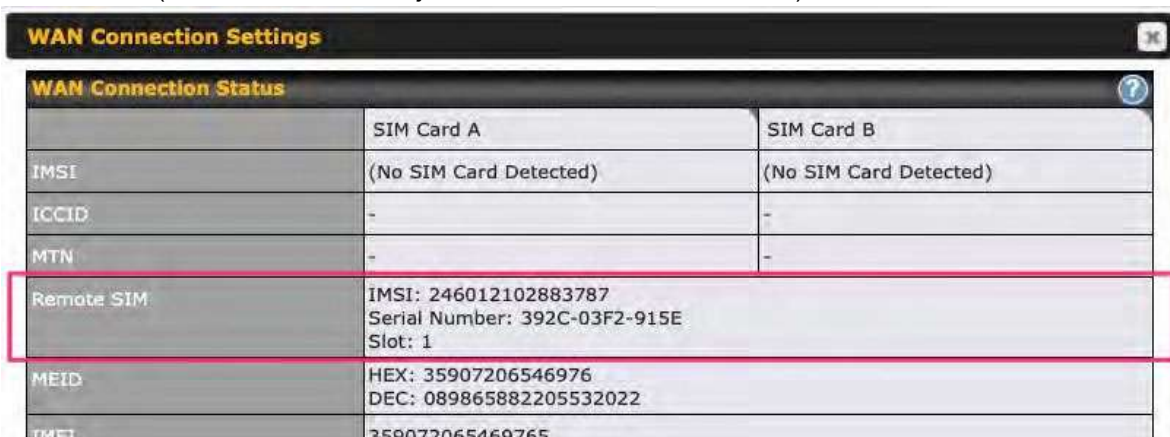
1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on any cellular WAN. This will open the WAN Connection Settings page.
2. Scroll down to **Cellular settings**.

If you can see the **Remote SIM Settings** section, then the cellular router supports RemoteSIM.



Monitor the status of the Remote SIM

1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on the cellular WAN which was configured to use RemoteSIM.
2. Check the **WAN Connection Status** section. Within the cell WAN details, there is a section for **Remote SIM** (SIM card IMSI, SIM Injector serial number and SIM slot).



Appendix D. 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.

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

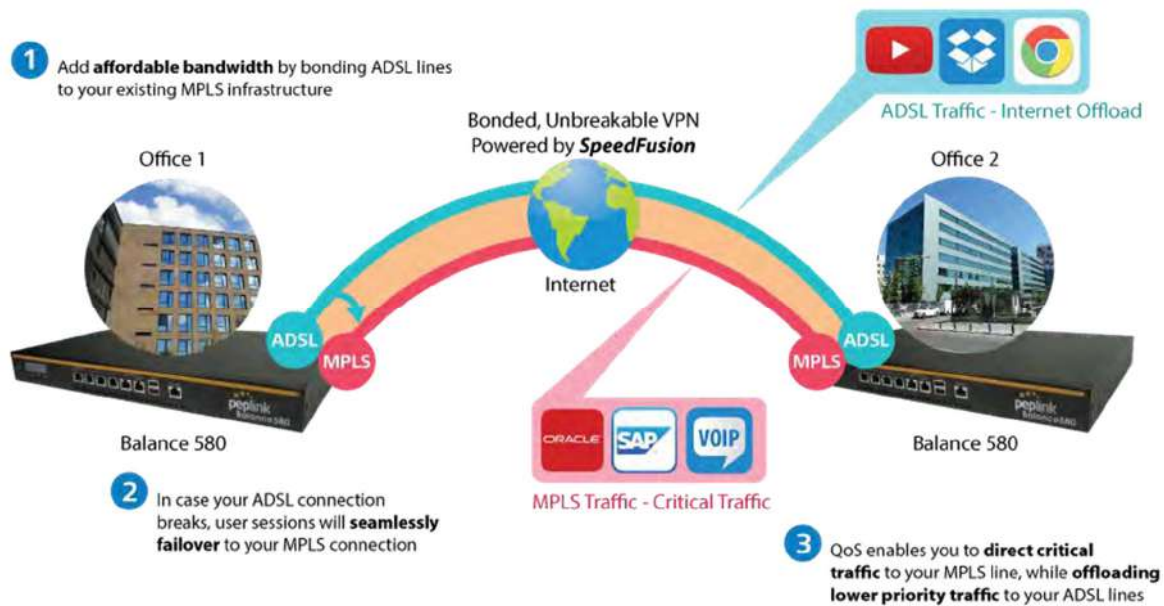
Special features of Balance 580: have high availability capability

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.

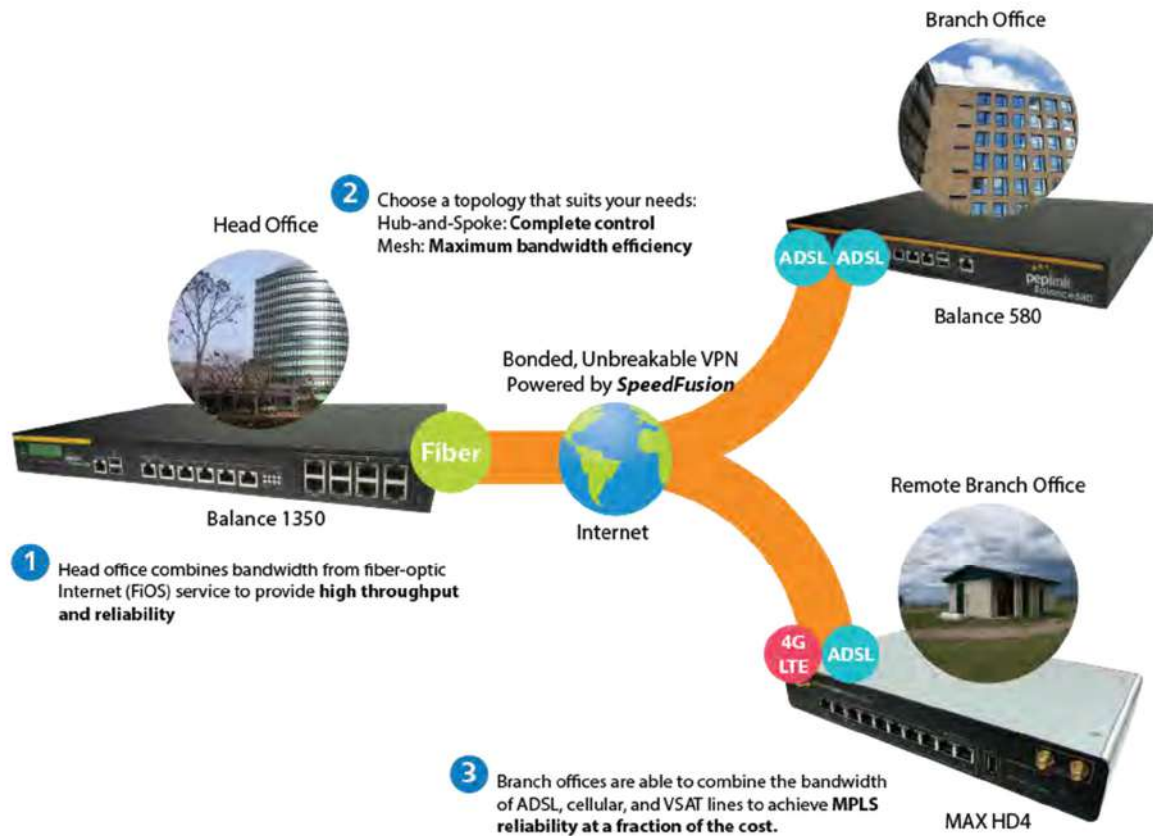
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement



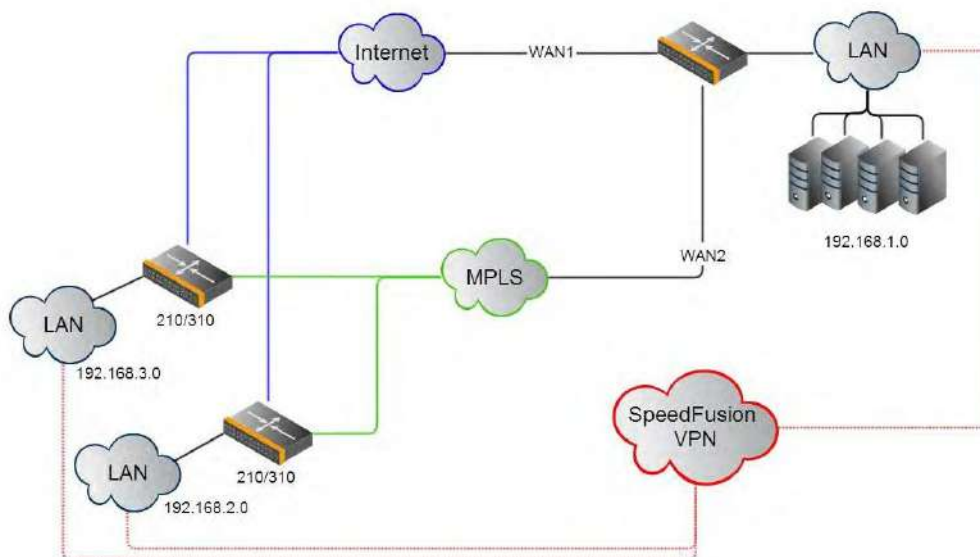
Affordably increase your bandwidth by adding commodity ADSL links to your MPLS connection. SpeedFusion technology bonds all your connections together, enabling session-persistent, user-transparent hot failover. QoS support, bandwidth control, and traffic prioritization gives you total control over your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

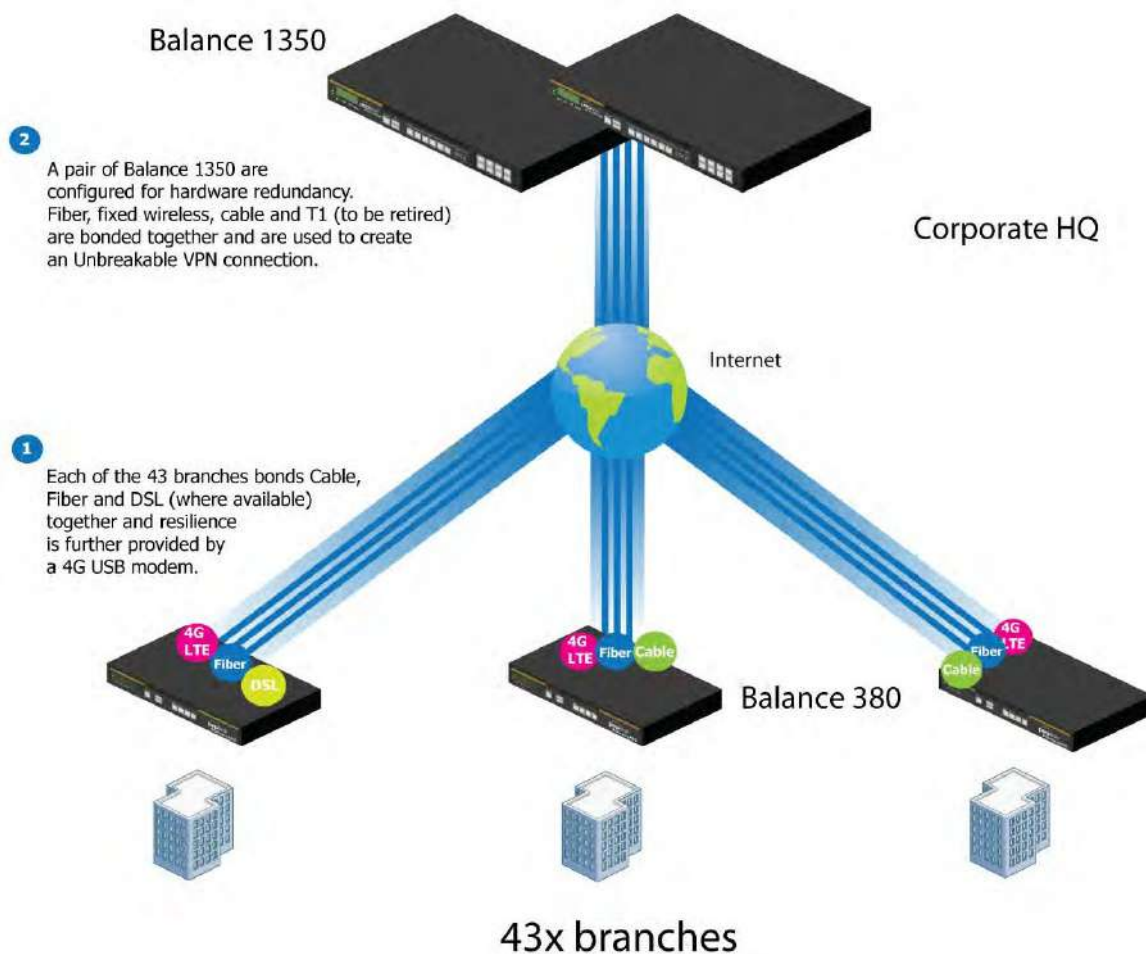
- Extreme savings of \$100,000 per year
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

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

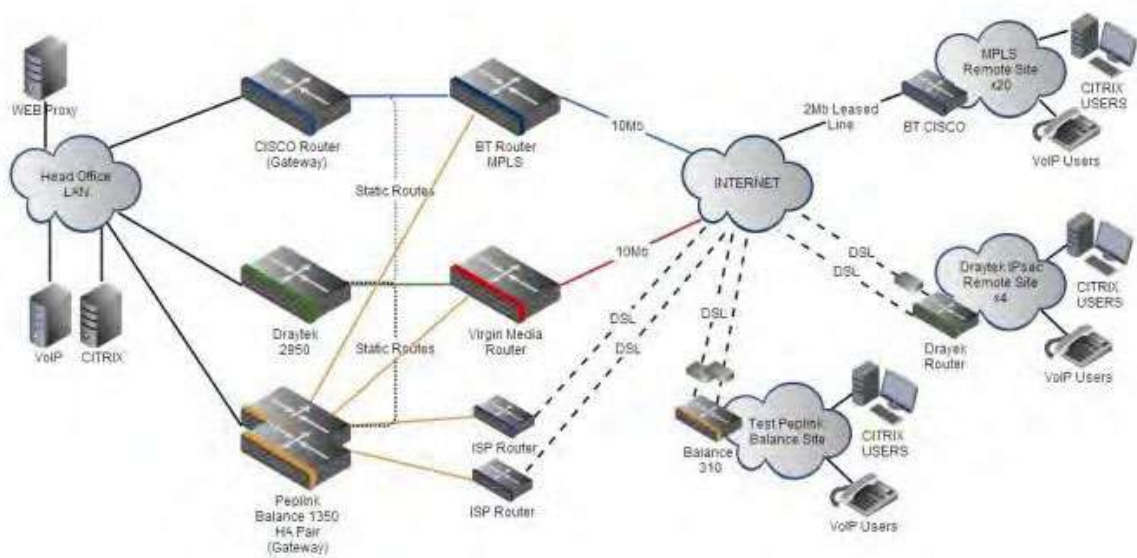
Peplink + Citrix + VoIP Adds Up to Fast, Cost-Effective WAN for Pluss

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.



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

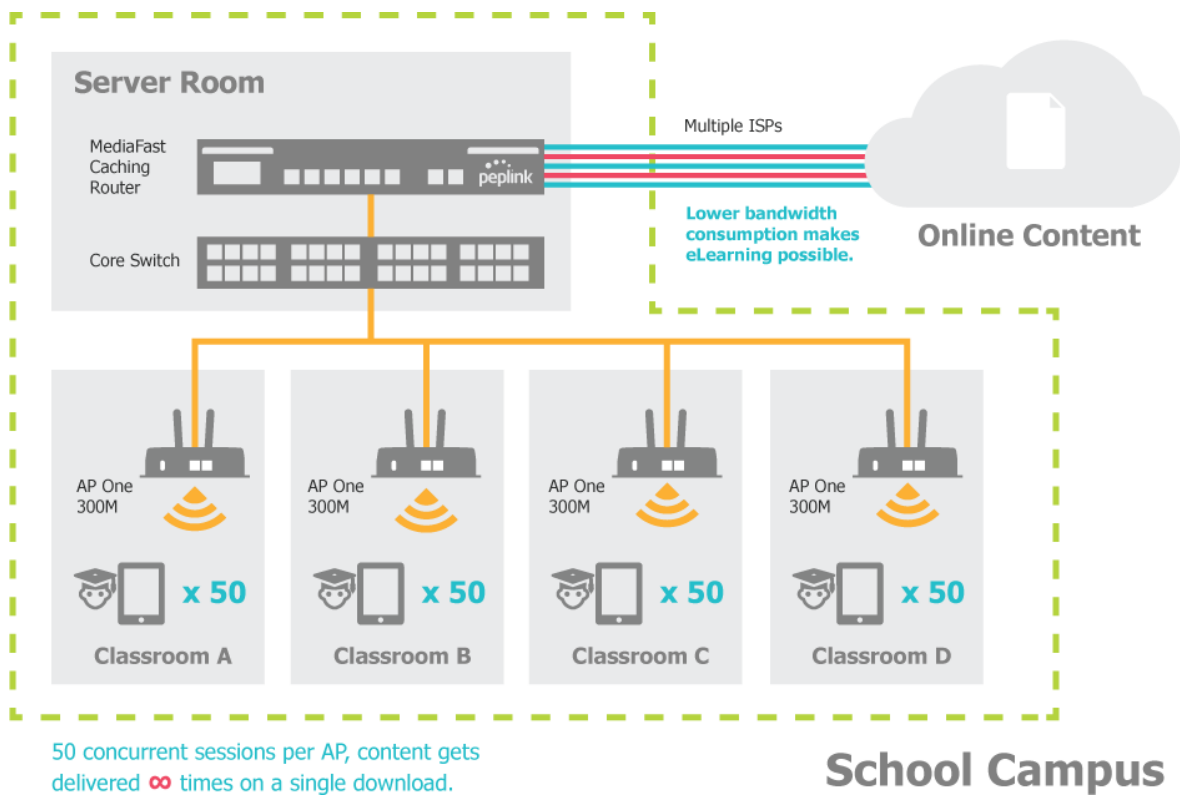
- Solve network congestion problem caused by 600 students over rural Internet connections
- Wi-Fi that can handle 50+ users per classroom
- An affordable network infrastructure that can provide simultaneous access to media-rich educational content

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 emails 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 email.

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	☒
Source	Any
Destination	Any
Protocol	TCP ← HTTP
Port *	Single Port Port: 80
Algorithm	Persistence
Persistence Mode	☐ By Source ☒ By Destination
Load Distribution	☒ Auto ☐ Custom
Terminate Sessions on Link Recovery	☐ Enable

Save
Cancel

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) <table border="1"> <tr> <td>☒ WAN 1</td> <td>☒ 10.90.0.75 (Interface IP)</td> </tr> <tr> <td>☐ WAN 2</td> <td></td> </tr> <tr> <td>☐ WAN 3</td> <td></td> </tr> <tr> <td>☐ WAN 4</td> <td></td> </tr> <tr> <td>☐ WAN 5</td> <td></td> </tr> <tr> <td>☐ WAN 6</td> <td></td> </tr> <tr> <td>☐ WAN 7</td> <td></td> </tr> <tr> <td>☐ Mobile Internet</td> <td></td> </tr> </table>	☒ WAN 1	☒ 10.90.0.75 (Interface IP)	☐ WAN 2		☐ WAN 3		☐ WAN 4		☐ WAN 5		☐ WAN 6		☐ WAN 7		☐ Mobile Internet	
☒ WAN 1	☒ 10.90.0.75 (Interface IP)																
☐ WAN 2																	
☐ WAN 3																	
☐ WAN 4																	
☐ WAN 5																	
☐ WAN 6																	
☐ WAN 7																	
☐ Mobile Internet																	
Outbound Mappings	Connection / Outbound IP Address <table border="1"> <tr> <td>WAN 1</td> <td>10.90.0.75 (Interface IP)</td> </tr> <tr> <td>WAN 2</td> <td>10.90.0.76 (Interface IP)</td> </tr> <tr> <td>WAN 3</td> <td>Interface IP</td> </tr> <tr> <td>WAN 4</td> <td>Interface IP</td> </tr> <tr> <td>WAN 5</td> <td>Interface IP</td> </tr> <tr> <td>WAN 6</td> <td>Interface IP</td> </tr> <tr> <td>WAN 7</td> <td>Interface IP</td> </tr> <tr> <td>Mobile Internet</td> <td>Interface IP</td> </tr> </table>	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
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.

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:

New Firewall Rule	
Rule Name	Inbound Firewall Rule Exce
Enable	☒
WAN Connection	Any
Protocol	TCP HTTP
Source	Any Address Any Port
Destination	Any Address Single Port Port: 80
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save Cancel

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	No FTP access		
Enable	☒		
Protocol	<input <input="" tcp="" type="button" value="←"/> FTP		
Source	<input <="" address="" any="" td="" type="button" value="?"/> <td colspan="2">Any Port</td>	Any Port	
Destination	<input <="" address="" any="" td="" type="button" value="?"/> <td colspan="2">Single Port Port: 21</td>	Single Port Port: 21	
Action	<input <input="" type="radio" value="?"/> Allow ☒ Deny		
Event Logging	<input <input="" checked="" type="checkbox" value="?"/> Enable		

Save
Cancel

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:

<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 the 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 the problem still persists, change the size to progressively 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 F.

FCC Requirements for Operation in the United States Federal Communications Commission (FCC) Compliance Notice:

For Balance 310 Fiber 5G

FCC 15.21:

The changes or modifications not expressly approved by the party responsible for

compliance could void the user's authority to operate the equipment.

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.

Industry Canada Statement

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

French:

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.