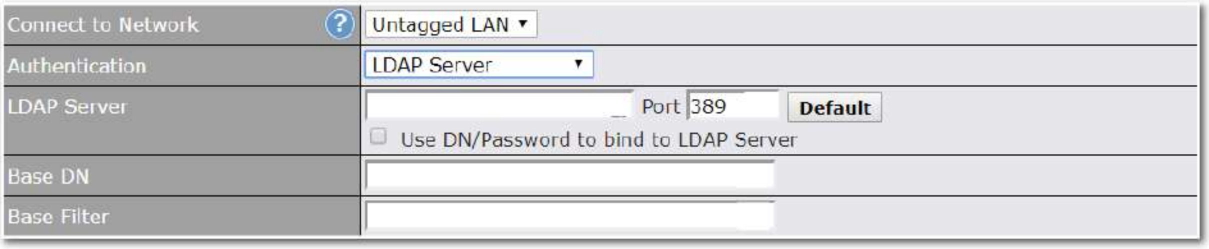
The password must be between 8 and 12 characters long.

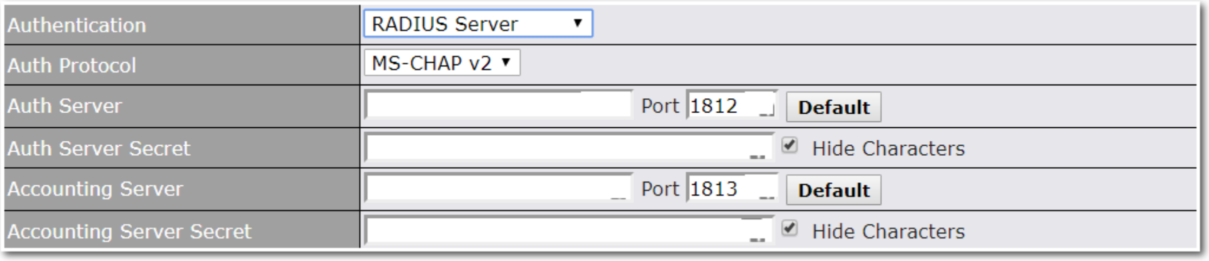
LDAP Server:



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.

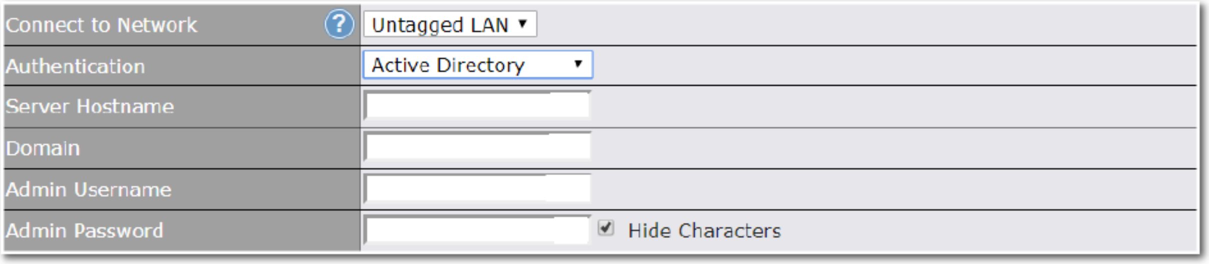
Radius Server:



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.

10.14 Misc. Settings

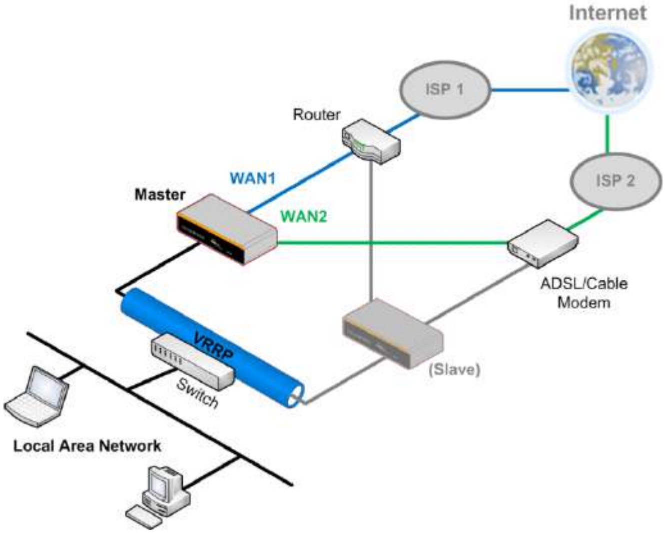
10.14.1 High Availability

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:



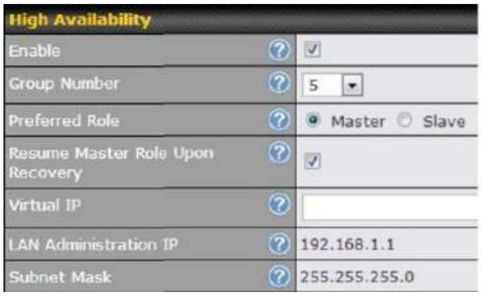
In the diagram, the WAN ports of each Peplink Balance unit connect to the router and to the modem. Both Peplink Balance units connect to the same LAN switch via a LAN port.

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

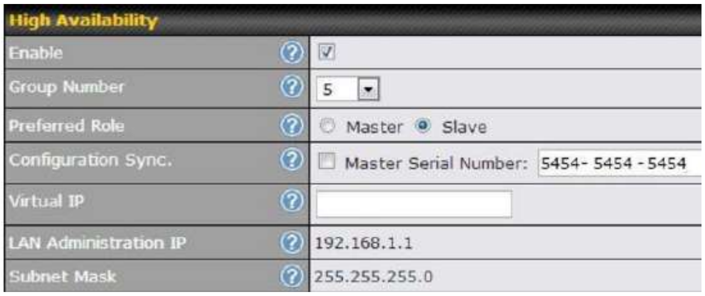
- In an HA configuration, the two Peplink Balance units communicate with each other using VRRP over the LAN.
- The two Peplink Balance units broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the master Peplink Balance 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	Interface for Slave 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

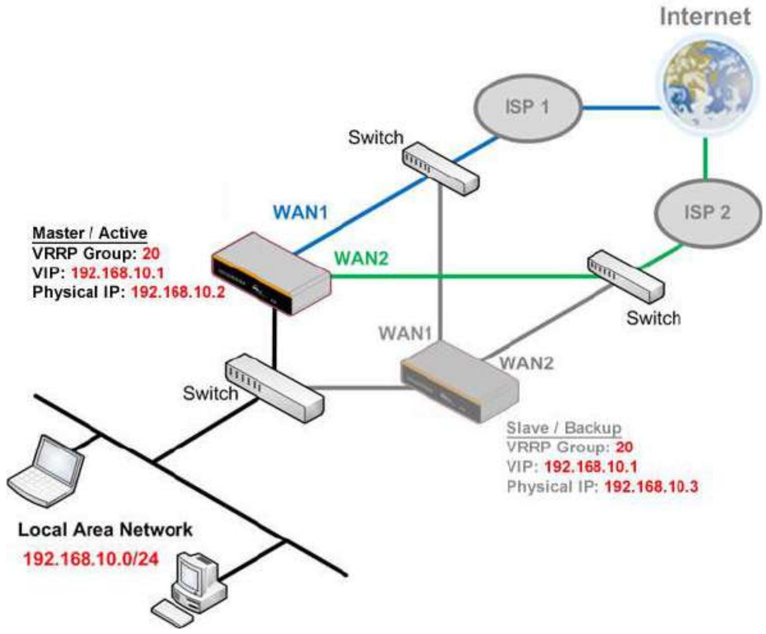


High Availability	
Enable	☑
Group Number	5
Preferred Role	○ Master ● Slave
Configuration Sync.	□ Master Serial Number: 5454- 5454 -5454
Virtual IP	
LAN Administration IP	192.168.1.1
Subnet Mask	255.255.255.0

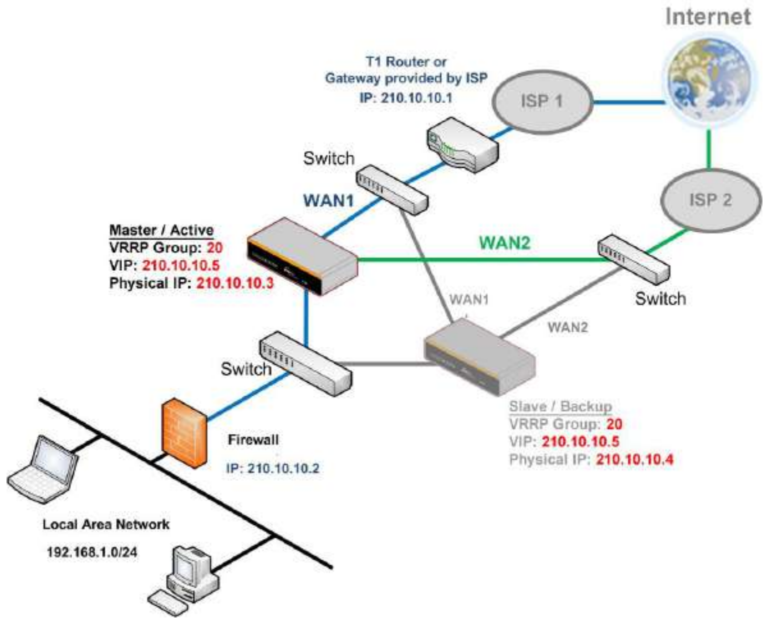
High Availability	
Enable	Checking this box specifies that the Peplink Balance unit is part of a high availability configuration.
Group Number	This number identifies a pair of Peplink Balance units operating in a high availability configuration. The two Peplink Balance units in the pair must have the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

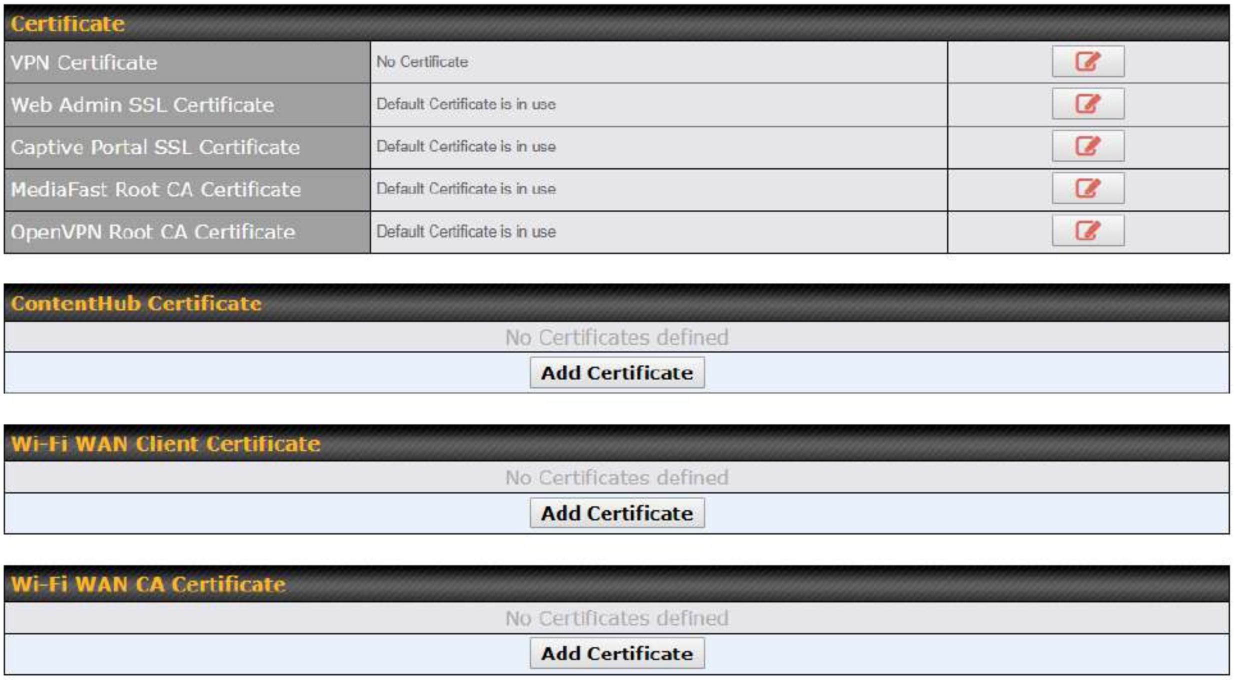


In drop-in mode, no other configuration needs to be set.



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

10.14.2 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

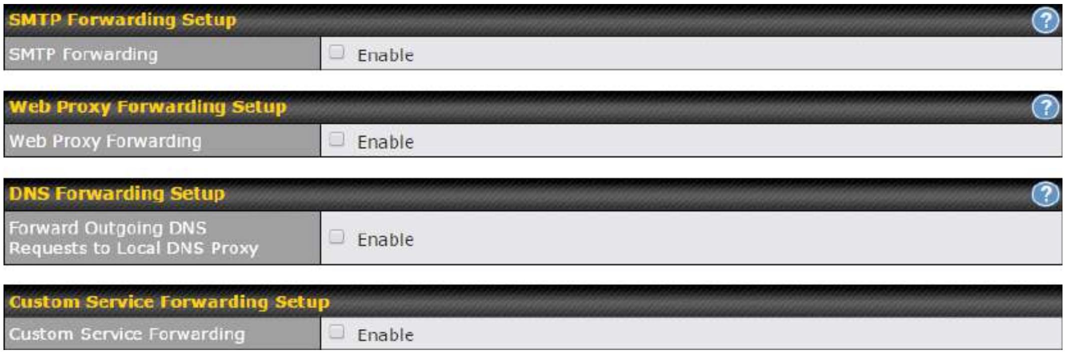
Wi-Fi WAN CA Certificate
No Certificates defined
Add Certificate

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/

10.14.3 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

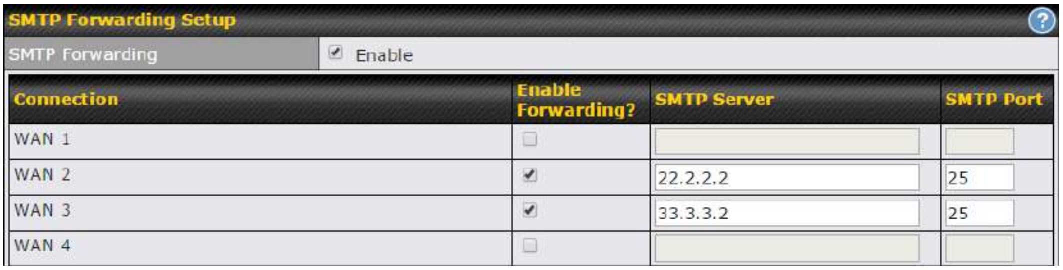
DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	□ Enable

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	□		

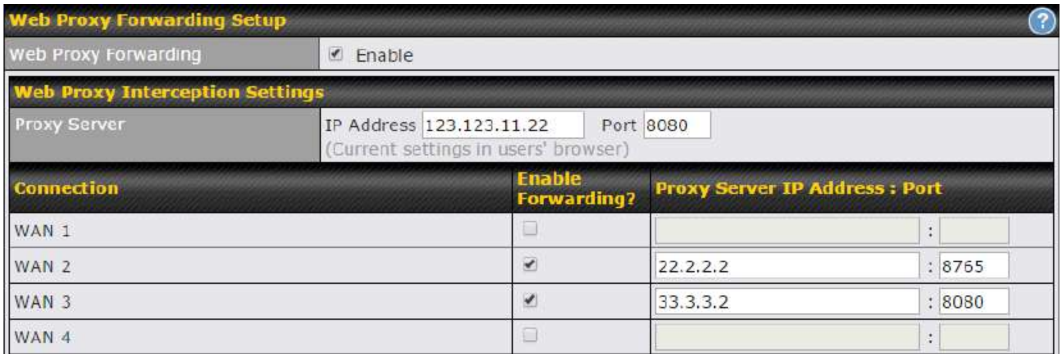
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

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

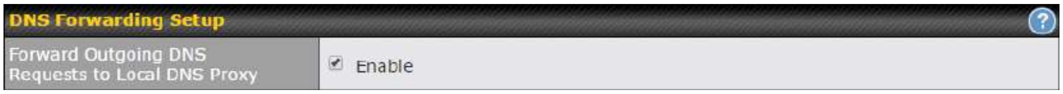
Web Proxy Interception Settings

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.

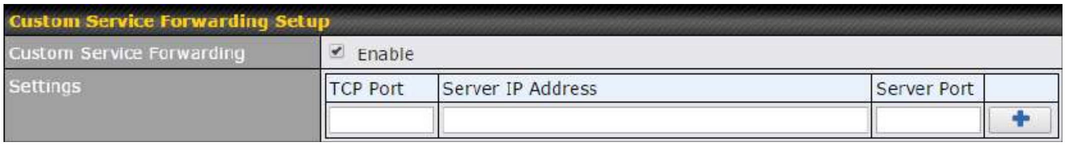
DNS Forwarding



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

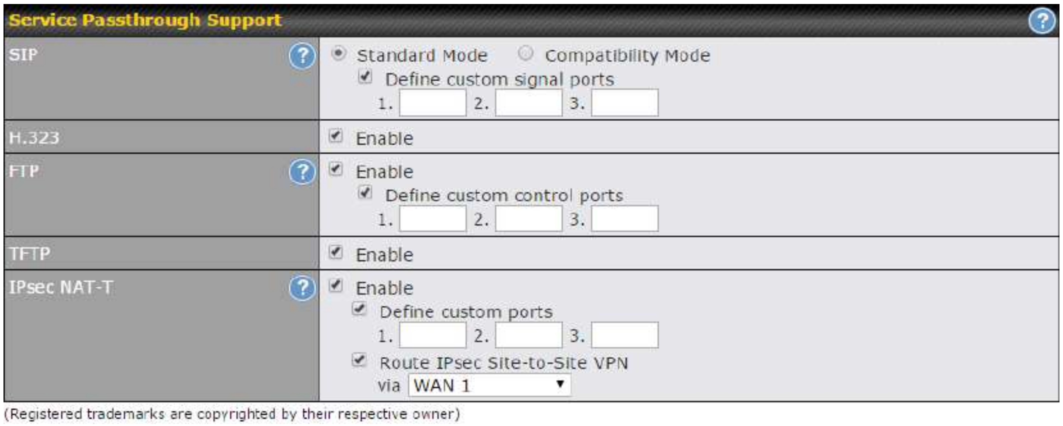


Custom Service Forwarding Setup	
Custom Service Forwarding	☑ Enable
Settings	TCP Port / Server IP Address / Server Port / +

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.

10.14.4 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)

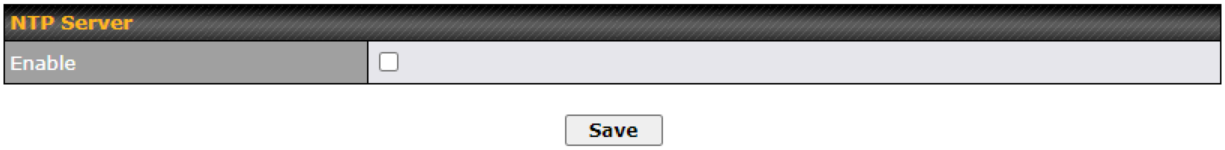
Some Internet services need to be specially handled in a multi-WAN environment. The Peplink Balance can handle these services such that Internet applications do not notice it is behind a multi-WAN router. Settings for service passthrough support are available here.

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.

10.14.5 NTP Server

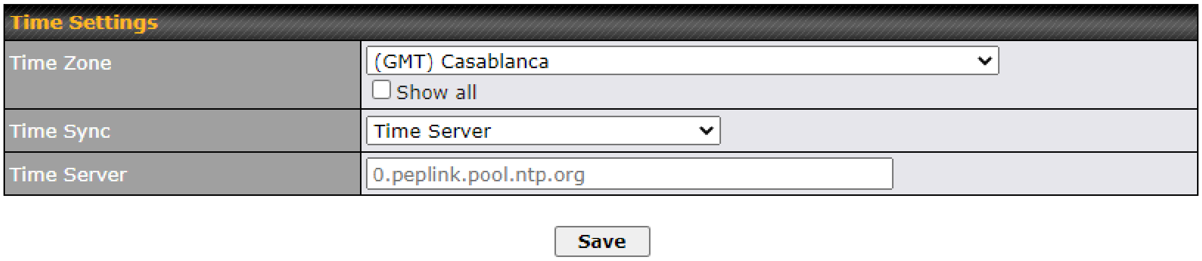
Peplink routers can now serve as a local NTP server. Upon start up, it is now able to provide connected devices with the accurate time, precise UTC from either an external NTP server or via GPS and ensuring that connected devices always receive the correct time.

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



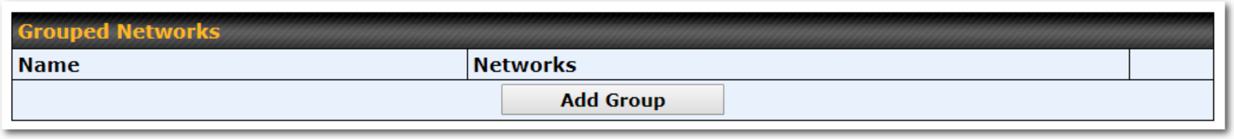
NTP Server	
Enable	□

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

10.14.6 Grouped Networks

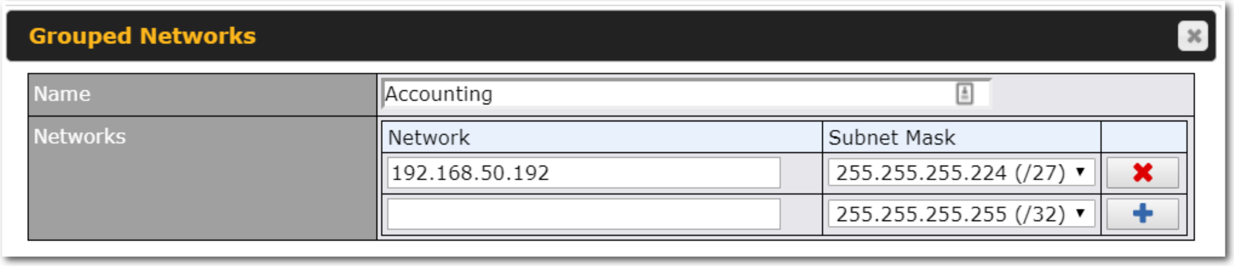


Grouped Networks

Name	Networks	

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.

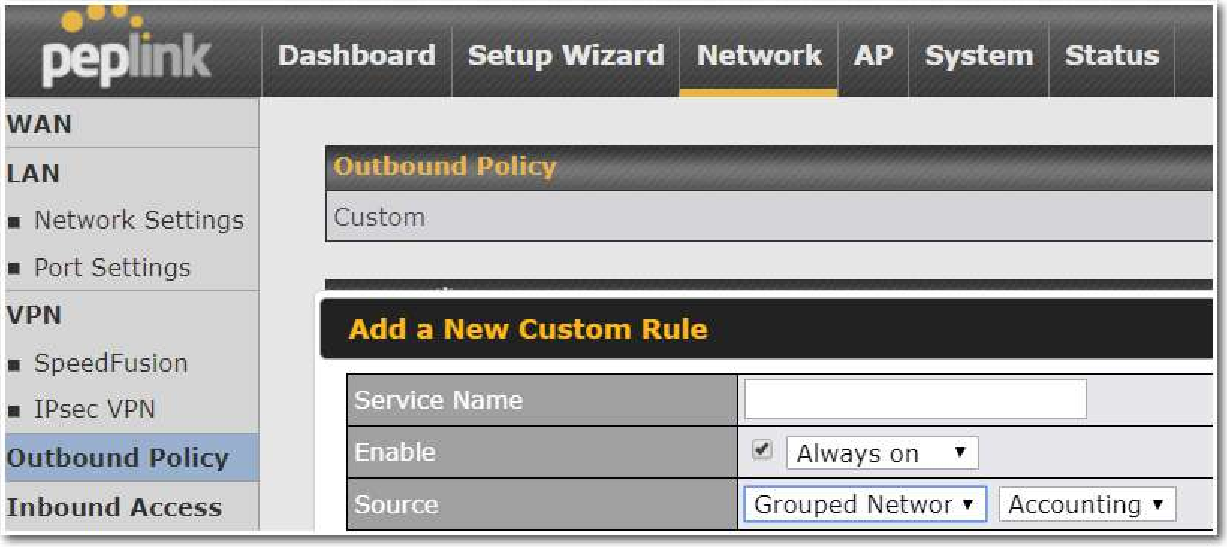
Start by clicking on "add group" then fill in the appropriate field.
In this example we'll create a group "accounting"
Click save when you have finished adding the required networks.



Grouped Networks

Name	Accounting
Networks	Network: 192.168.50.192 — Subnet Mask: 255.255.255.224 (/27) ✖ Network: — Subnet Mask: 255.255.255.255 (/32) ✚

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



Outbound Policy

Custom

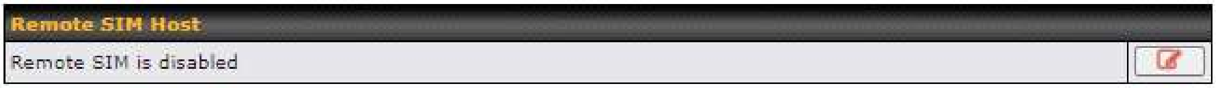
Add a New Custom Rule

Service Name	
Enable	☑ Always on ▾
Source	Grouped Networ ▾ Accounting ▾

10.14.7 Remote SIM Management

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

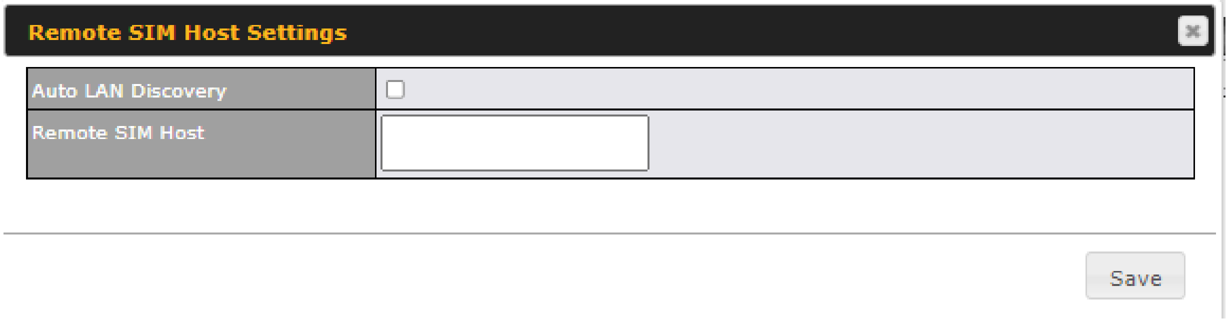
Please note that a limited number of Pepwave routers support the SIM Injector, may refer to the link: https://www.peplink.com/products/sim-injector/ or Appendix C for more details on FusionSIM Manual.



Remote SIM Host

Remote SIM is disabled

Remote SIM Host Settings

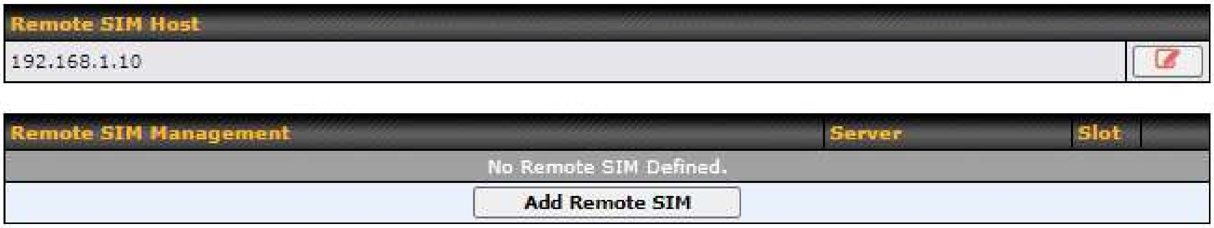


Remote SIM Host Settings

Auto LAN Discovery	☐
Remote SIM Host	

Remote SIM Host Settings	
Active LAN Discovery	Check this box to enable Auto LAN discovery of the remote SIM server.

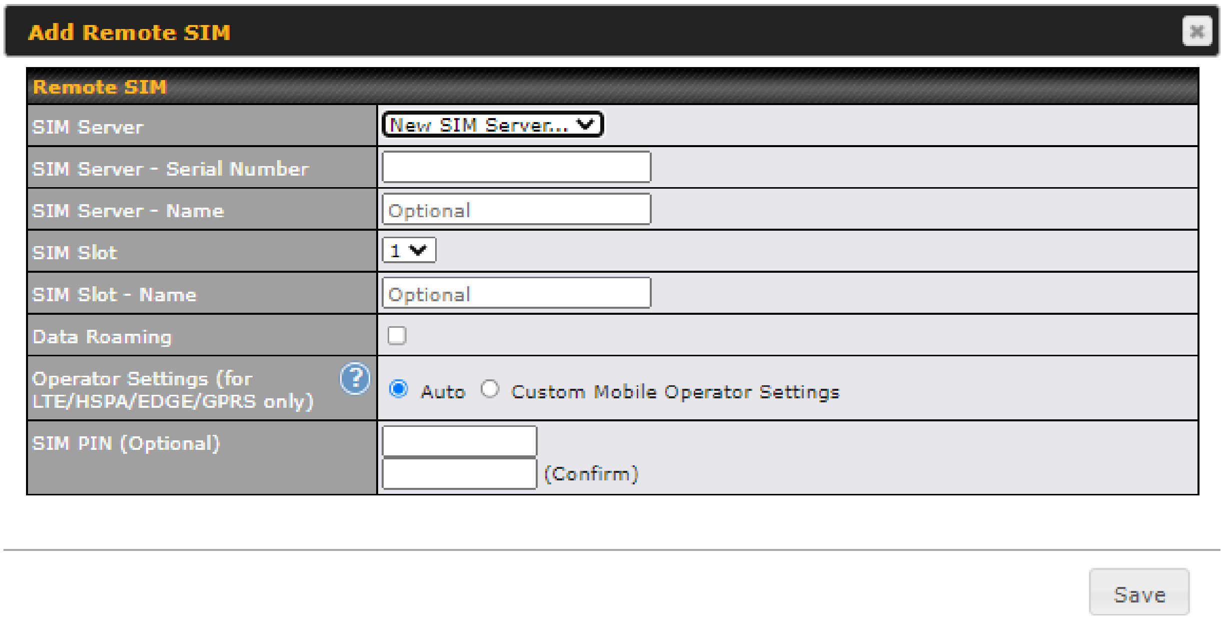
Remote SIM Host	Enter the public IP address of the SIM Injector. If you enter IP addresses here, it is not necessary to tick the "**Auto LAN Discovery**" box above.



Remote SIM Host	
192.168.1.10	

Remote SIM Management	Server	Slot
No Remote SIM Defined.		

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)

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.

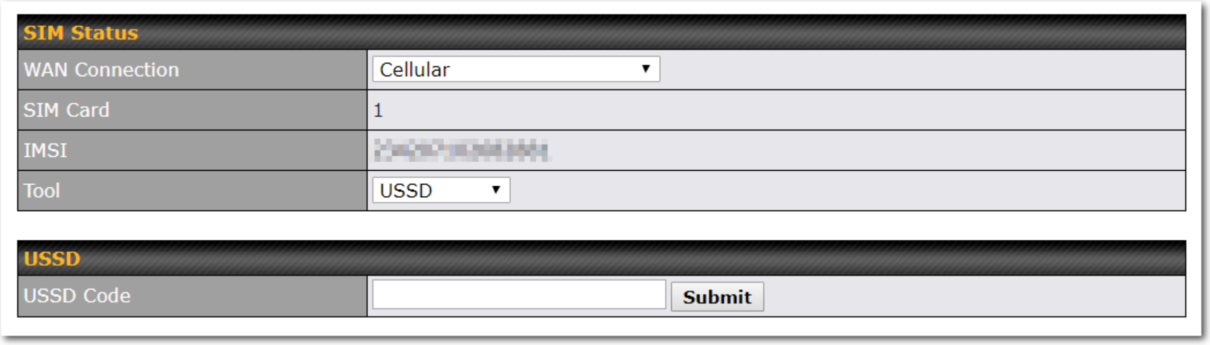
Data Roaming	Enables data roaming on this particular SIM card.
Operator Settings (for LTE//HSPA/EDGE/GPRS Only)	This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured 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.

10.14.8 SIM Toolkit

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

USSD

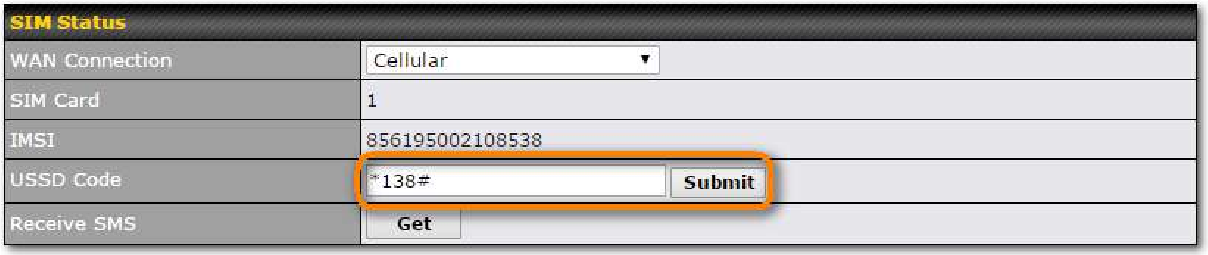
Unstructured Supplementary Service Data (USSD) is a protocol used by mobile phones to communicate with their service provider's computers. One of the most common uses is to query the available balance.



SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	[redacted]
Tool	USSD ▾

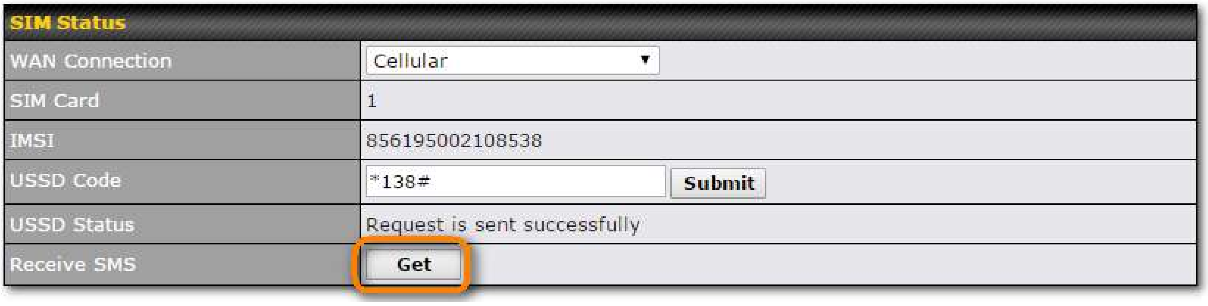
USSD	
USSD Code	Submit

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



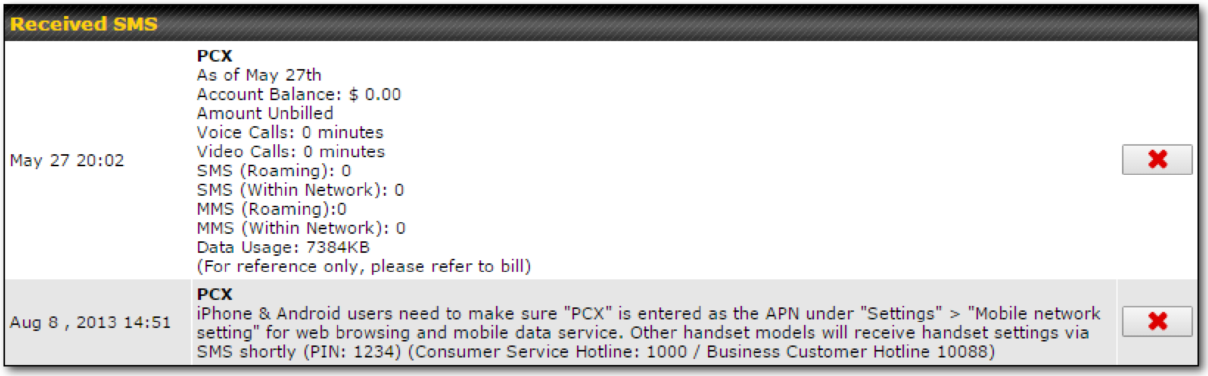
SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
Receive SMS	Get

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

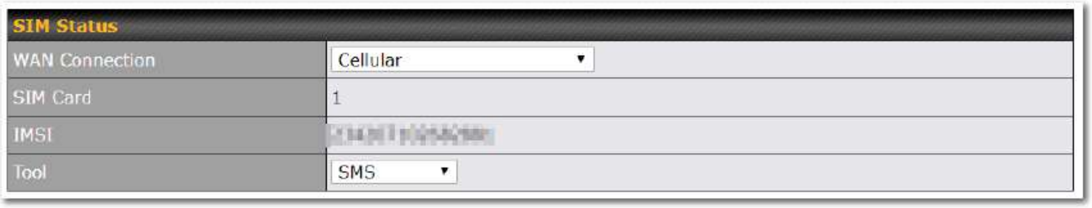


Received SMS

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)	✖

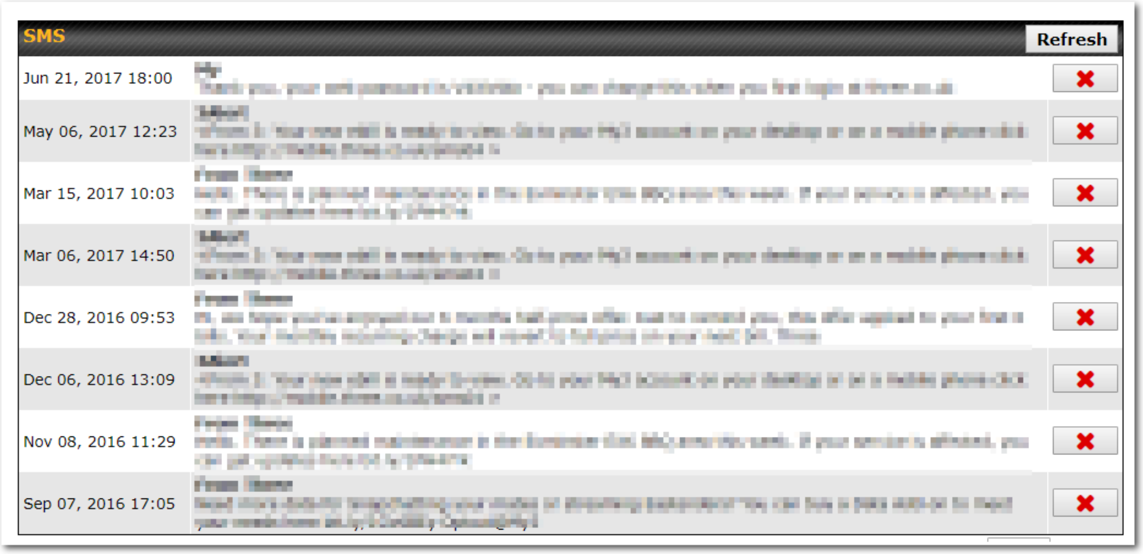
SMS

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	[illegible]
Tool	SMS ▾



SMS Refresh

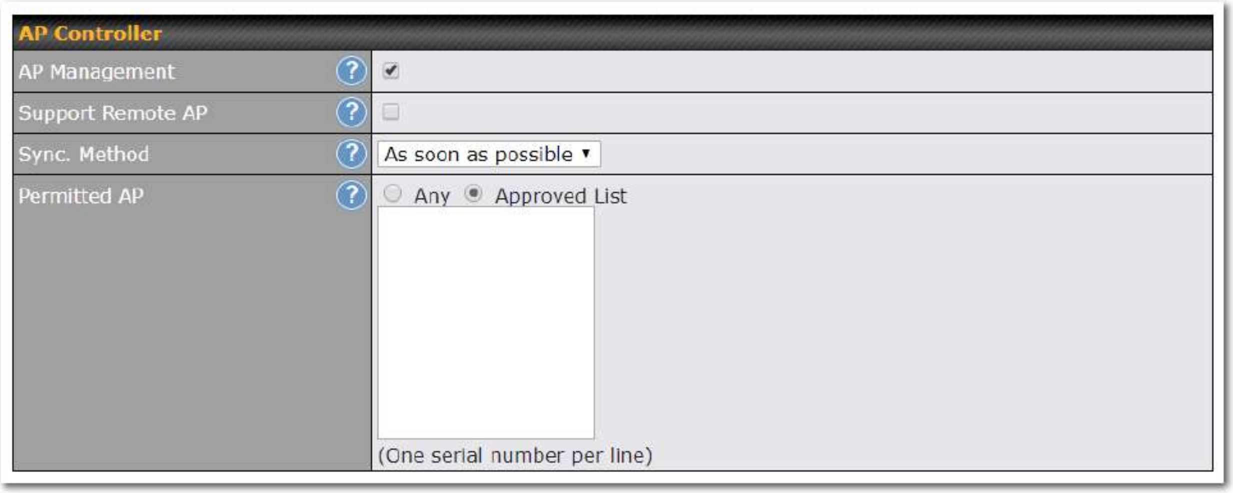
Jun 21, 2017 18:00	[illegible]	✖
May 06, 2017 12:23	[illegible]	✖
Mar 15, 2017 10:03	[illegible]	✖
Mar 06, 2017 14:50	[illegible]	✖
Dec 28, 2016 09:53	[illegible]	✖
Dec 06, 2016 13:09	[illegible]	✖
Nov 08, 2016 11:29	[illegible]	✖
Sep 07, 2016 17:05	[illegible]	✖

11 AP Tab

11.1 AP

11.1.1 AP Controller

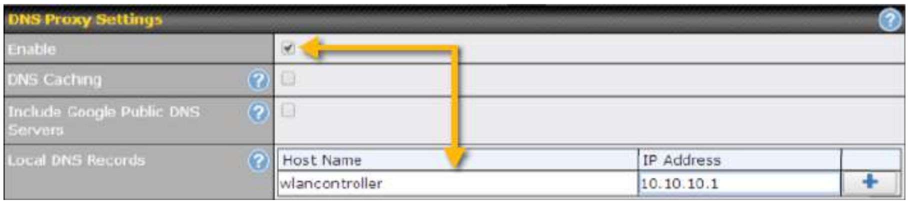
Clicking on the **AP** tab will default to this menu, where you can view basic AP management options:



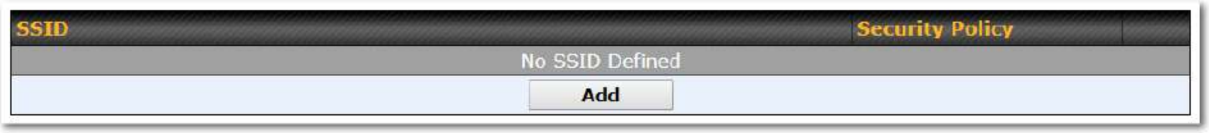
AP Controller

AP Management	☑
Support Remote AP	□
Sync. Method	As soon as possible ▾
Permitted AP	○ Any ● Approved List (One serial number per line)

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: Host Name: wlancontroller, IP Address: 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.

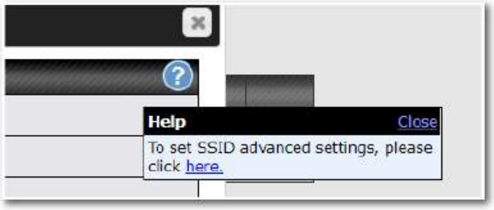
11.1.2 Wireless SSID



SSID	Security Policy
No SSID Defined	

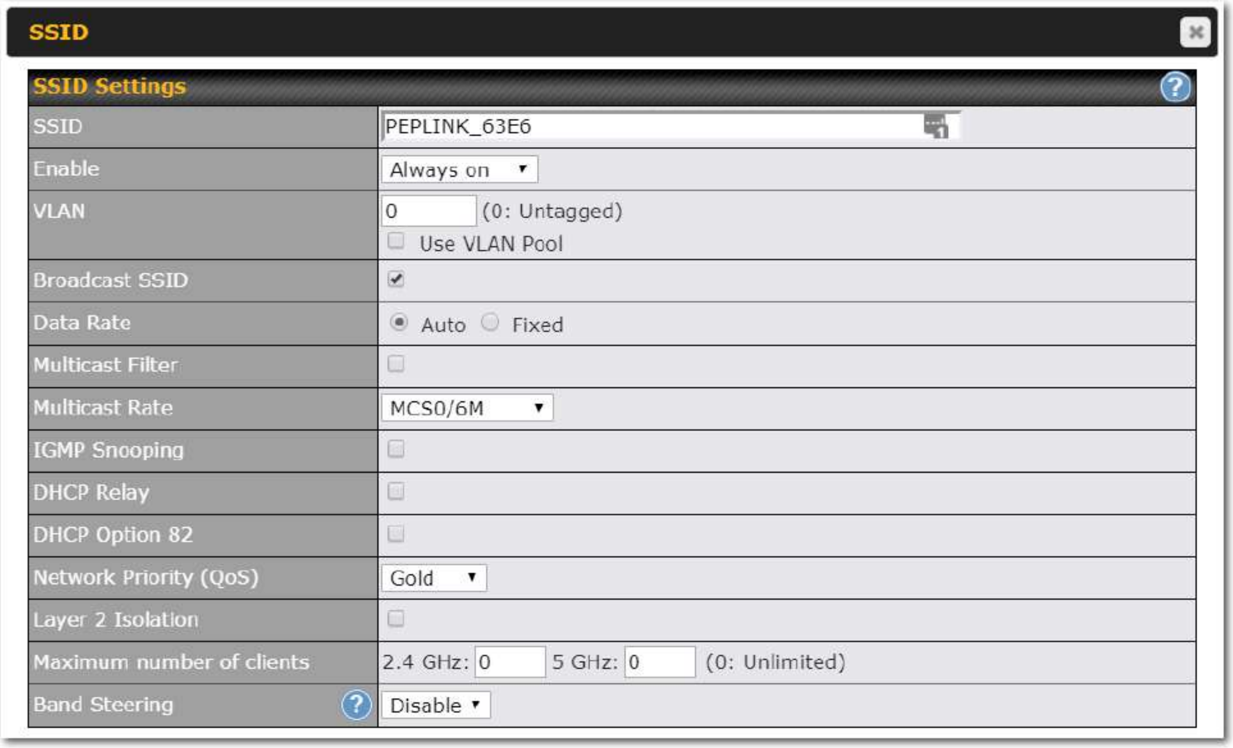
Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model.

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).



Help

To set SSID advanced settings, please click here.



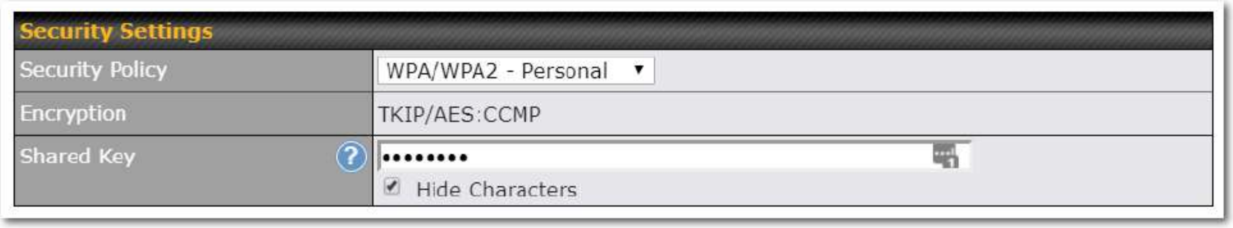
SSID

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

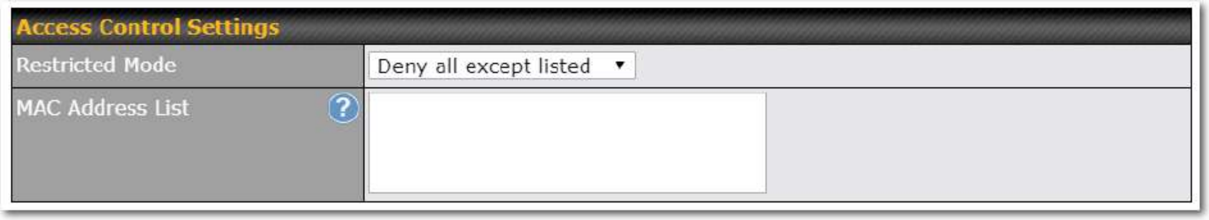
[A] - Advanced feature. Click the ? button on the top right-hand corner to activate.



Security Settings	
Security Policy	WPA/WPA2 - Personal ▾
Encryption	TKIP/AES:CCMP
Shared Key ?	•••••••• ☑ Hide Characters

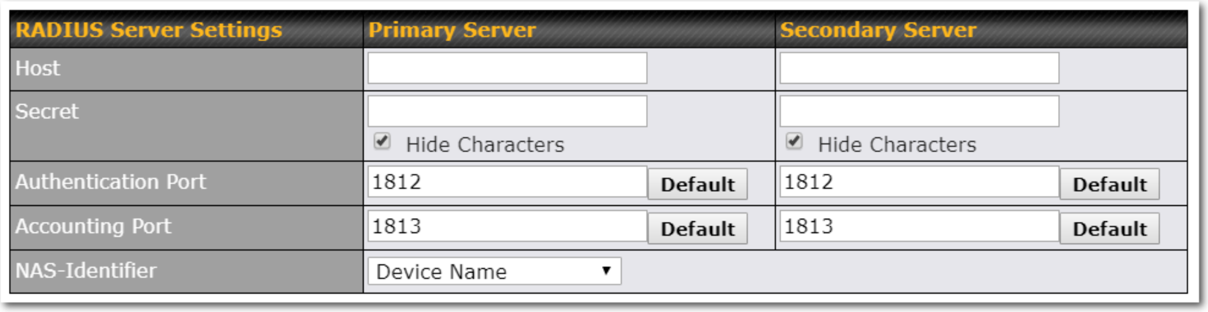
Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options: ● **Open (**No Encryption) ● **Enhanced Open** (OWE) ● **WPA3 -Personal** (AES:CCMP) ● **WPA2/WPA3 -Personal** (AES:CCMP) ● **WPA2 -Personal** (AES:CCMP) ● **WPA2 – Enterprise** ● **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 ?	

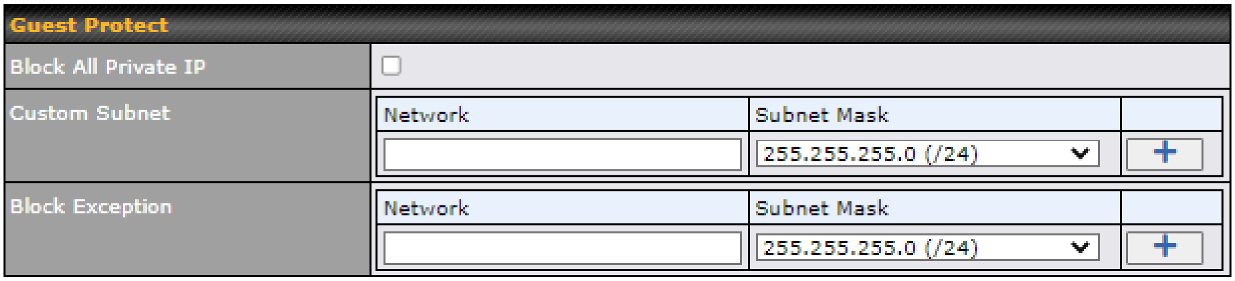
Access Control Settings	
Restricted Mode	The settings allow the administrator to control access using MAC address filtering. Available options are **None**, **Deny all except listed**, **Accept all except listed** and **Radius MAC Authentication.**
MAC Address List	Connections coming from the MAC addresses 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 ▾			

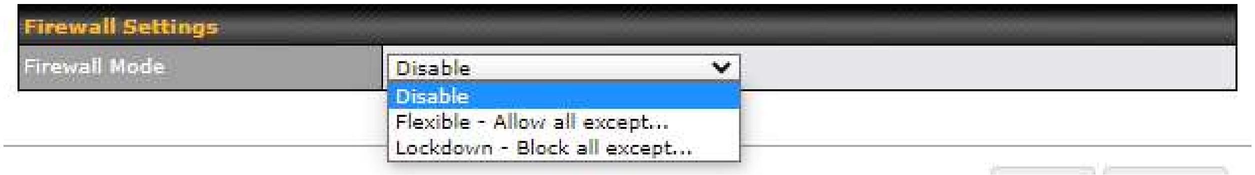
RADIUS Server Settings	
Host	Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.
Secret	Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
Authentication Port	In the field, enter the UDP authentication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

Port	**Default** button to enter **1813**.
NAS-Identifier	Choose between **Device Name**, **LAN MAC address**, **Device Serial Number** and **Custom Value**



Guest Protect	
Block All Private IP	□
Custom Subnet	Network: ␣ Subnet Mask: 255.255.255.0 (/24) +
Block Exception	Network: ␣ Subnet Mask: 255.255.255.0 (/24) +

Guest Protect	
Block All Private IP	Check this box to deny all connection attempts by private IP addresses.
Custom Subnet	To create a custom subnet for guest access, enter the IP address and choose a subnet mask from the drop-down menu.
Block Exception	To block access from a particular subnet, enter the IP address and choose a subnet mask from the drop-down menu.



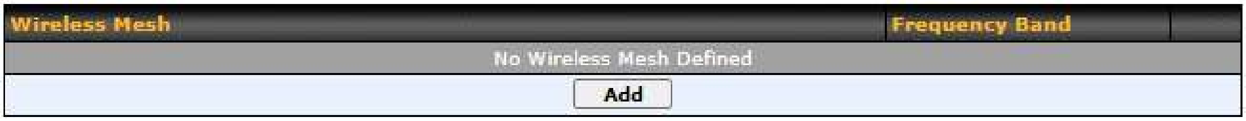
Firewall Settings

Firewall Mode: Disable

Disable
Flexible - Allow all except...
Lockdown - Block all except...

Firewall Settings	
Firewall Mode	The settings allow administrators to control access to the SSID based on Firewall Rules. Available options are **Disable,Lockdown - Block all except...** and **Flexible -Allow all except...**
Firewall Exceptions	Create Firewall Rules based on **Port, IP Network, MAC address** or **Domain Name**

11.1.3 Wireless Mesh

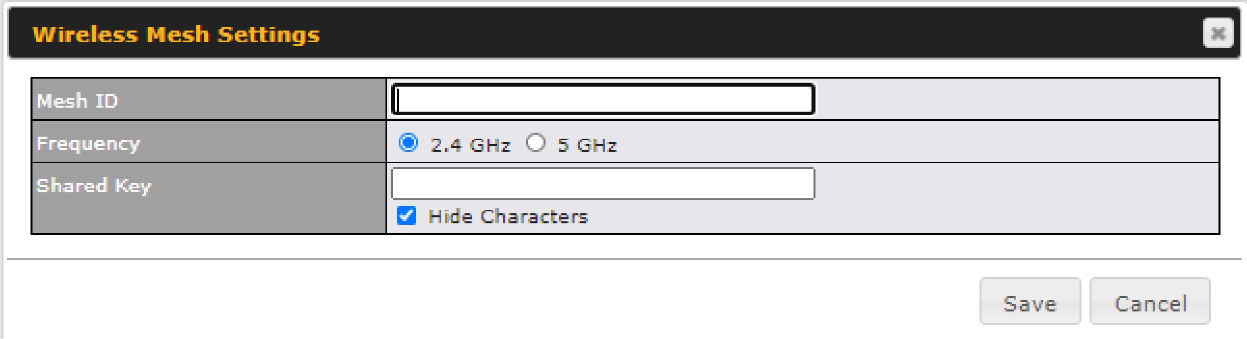


Wireless Mesh	Frequency Band	
No Wireless Mesh Defined		

Add

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**.

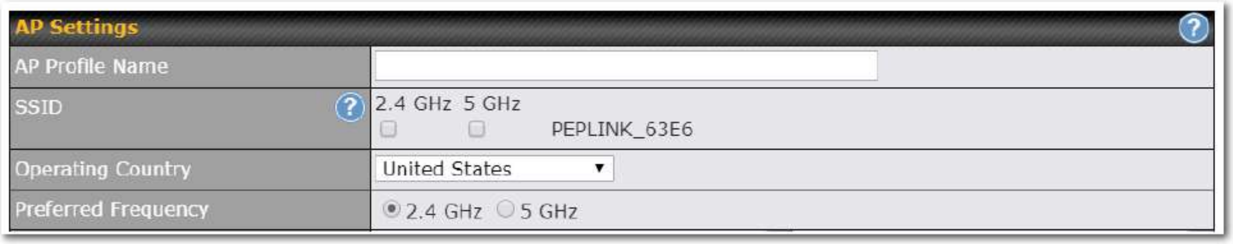


Wireless Mesh Settings

Mesh ID	
Frequency	● 2.4 GHz ○ 5 GHz
Shared Key	☑ Hide Characters

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.

11.1.4 AP > Profiles



AP Settings

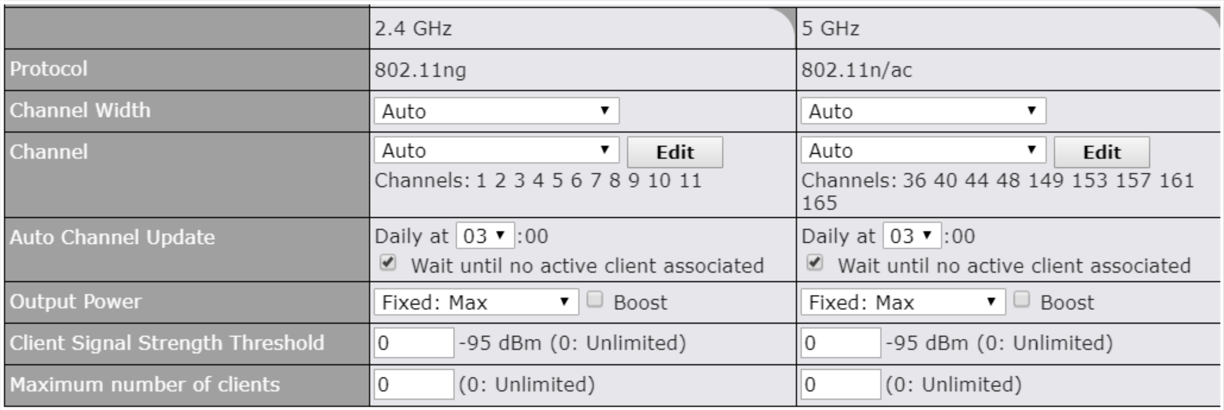
AP Profile Name	
SSID	2.4 GHz 5 GHz □ □ PEPLINK_63E6
Operating Country	United States
Preferred Frequency	● 2.4 GHz ○ 5 GHz

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.

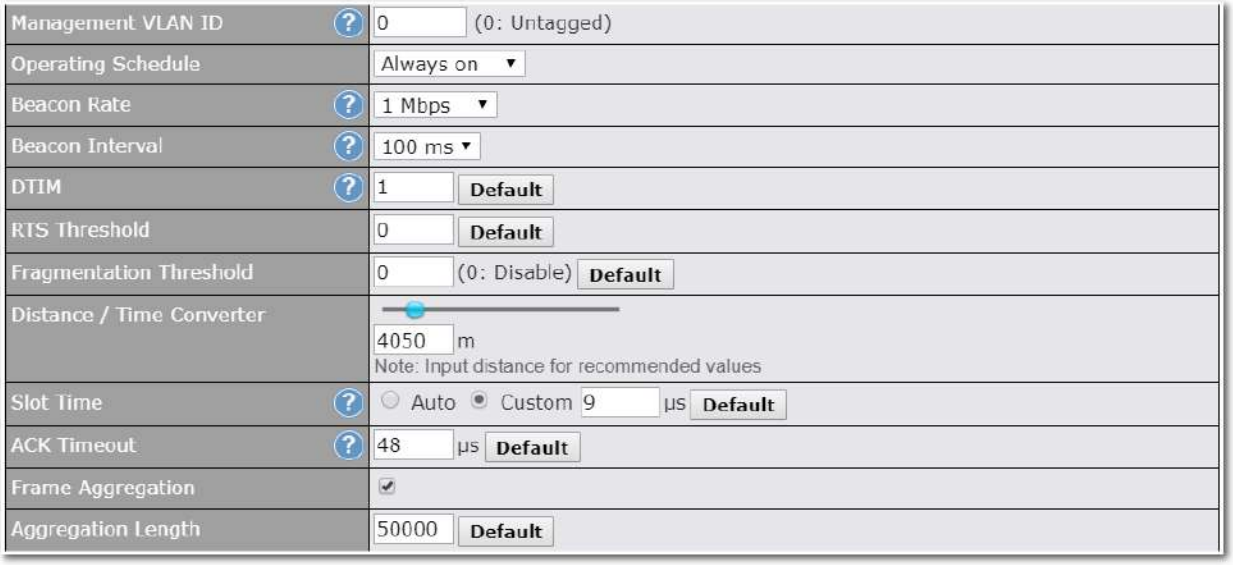


	2.4 GHz	5 GHz
Protocol	802.11ng	802.11n/ac
Channel Width	Auto ▾	Auto ▾
Channel	Auto ▾ Edit Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto ▾ Edit Channels: 36 40 44 48 149 153 157 161 165
Auto Channel Update	Daily at 03 ▾ :00 ☑ Wait until no active client associated	Daily at 03 ▾ :00 ☑ Wait until no active client 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	Clients with signal strength lower than this value will not be allowed to connect.

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**.

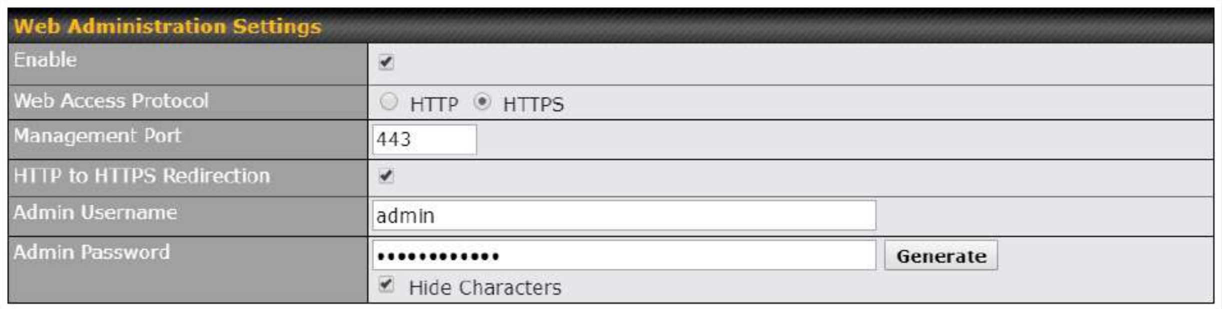


Management VLAN ID ?	0 (0: Untagged)
Operating Schedule	Always on ▾
Beacon Rate ?	1 Mbps ▾
Beacon Interval ?	100 ms ▾
DTIM ?	1 Default
RTS Threshold	0 Default
Fragmentation Threshold	0 (0: Disable) Default
Distance / Time Converter	4050 m Note: Input distance for recommended values
Slot Time ?	○ Auto ● Custom 9 μs Default
ACK Timeout ?	48 μs 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 Convertor	Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout.
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.



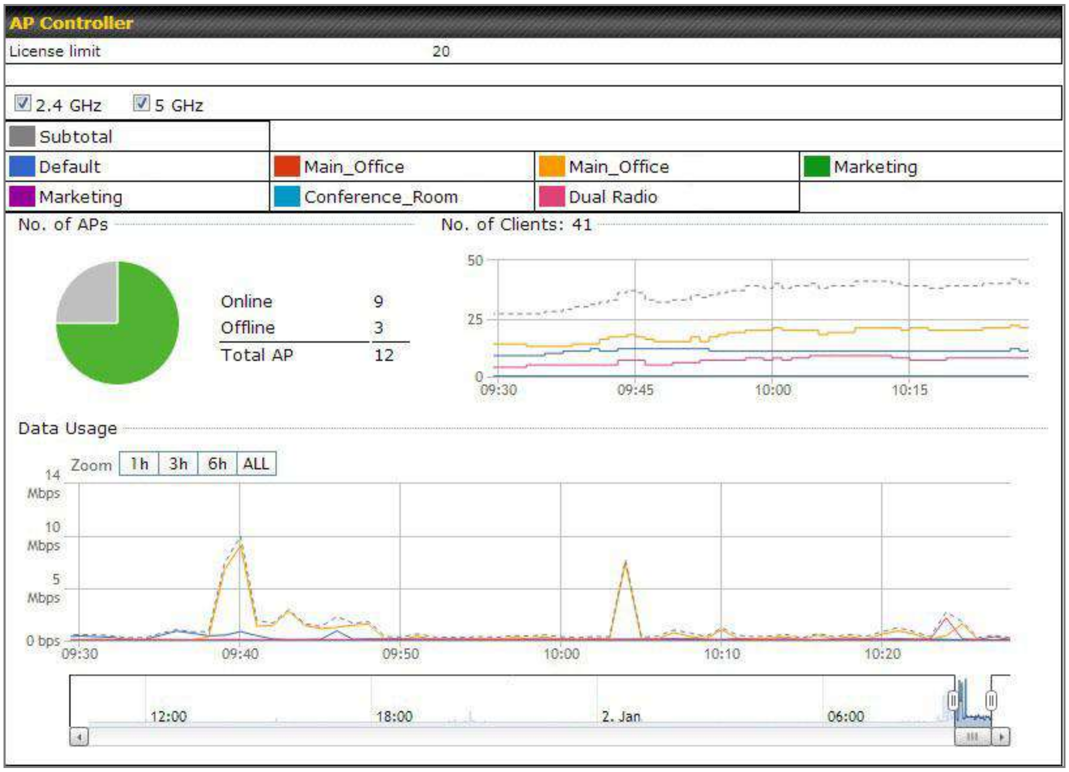
Web Administration Settings	
Enable	☑
Web Access Protocol	○ HTTP ● HTTPS
Management Port	443
HTTP to HTTPS Redirection	☑
Admin Username	admin
Admin Password	•••••••••••• Generate ☑ Hide Characters

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.

11.2 AP Controller Status

11.2.1 Info

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



AP Controller

License limit	20

☑ 2.4 GHz ☑ 5 GHz

No. of APs	
Online	9
Offline	3
Total AP	12

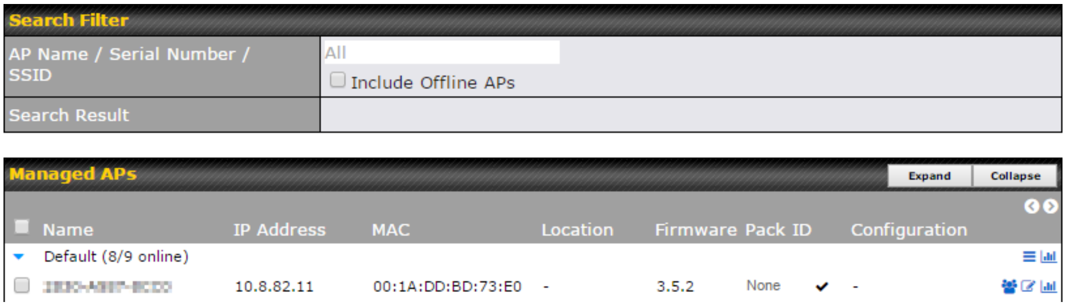
No. of Clients: 41

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.

11.2.2 Access Points (Usage)

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

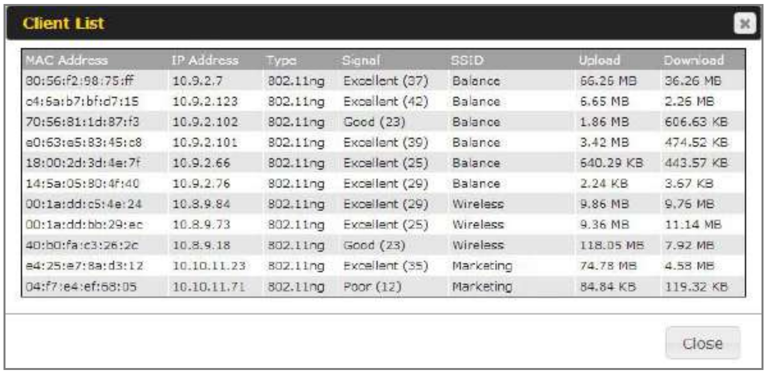


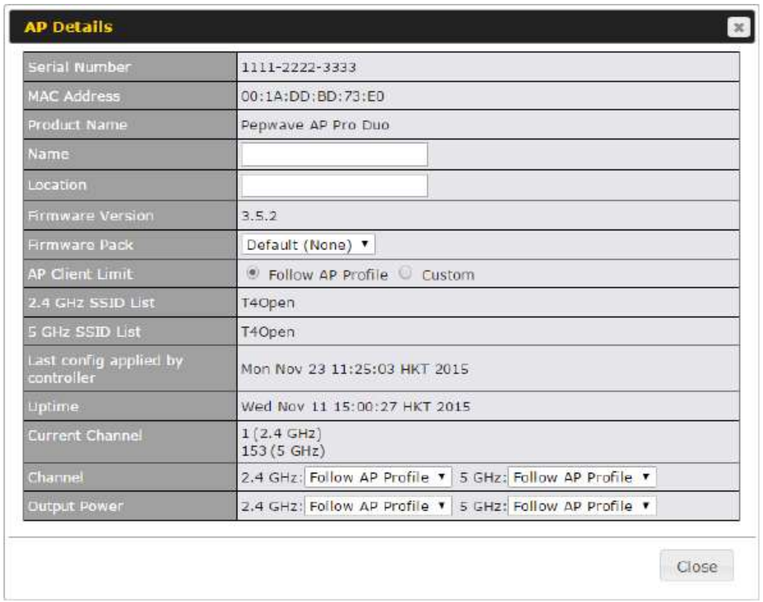
Search Filter

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)							
□	[redacted]	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None	✔	-

<table>
<tr><th colspan="2">Usage</th></tr>
<tr><td><b>AP Name/Serial Number</b></td><td>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.</td></tr>
<tr><td><b>Online Status</b></td><td>This button toggles whether your search will include offline devices.</td></tr>
<tr><td><b>Managed Wireless Devices</b></td><td>
<p>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.</p>
<p>On the right of the table, you will see the following icons: 👥 📝 📊 .</p>
<p>Click the 👥 icon to see a usage table for each client:</p>

<p><b>Client List</b></p>
<table>
<tr><th>MAC Address</th><th>IP Address</th><th>Type</th><th>Signal</th><th>SSID</th><th>Upload</th><th>Download</th></tr>
<tr><td>30:56:f2:98:75:ff</td><td>10.9.2.7</td><td>802.11ng</td><td>Excellent (37)</td><td>Balance</td><td>56.26 MB</td><td>36.26 MB</td></tr>
<tr><td>c4:6a:b7:bf:d7:15</td><td>10.9.2.123</td><td>802.11ng</td><td>Excellent (42)</td><td>Balance</td><td>6.65 MB</td><td>2.26 MB</td></tr>
<tr><td>70:56:81:1d:87:f3</td><td>10.9.2.102</td><td>802.11ng</td><td>Good (23)</td><td>Balance</td><td>1.86 MB</td><td>606.63 KB</td></tr>
<tr><td>e0:63:e5:83:45:c8</td><td>10.9.2.101</td><td>802.11ng</td><td>Excellent (39)</td><td>Balance</td><td>3.42 MB</td><td>474.52 KB</td></tr>
<tr><td>18:00:2d:3d:4e:7f</td><td>10.9.2.66</td><td>802.11ng</td><td>Excellent (25)</td><td>Balance</td><td>640.29 KB</td><td>443.57 KB</td></tr>
<tr><td>14:5a:05:80:4f:40</td><td>10.9.2.76</td><td>802.11ng</td><td>Excellent (29)</td><td>Balance</td><td>2.24 KB</td><td>3.67 KB</td></tr>
<tr><td>00:1a:dd:c5:4e:24</td><td>10.8.9.84</td><td>802.11ng</td><td>Excellent (29)</td><td>Wireless</td><td>9.86 MB</td><td>9.76 MB</td></tr>
<tr><td>00:1a:dd:bb:29:ec</td><td>10.8.9.73</td><td>802.11ng</td><td>Excellent (25)</td><td>Wireless</td><td>9.36 MB</td><td>11.14 MB</td></tr>
<tr><td>40:b0:fa:c3:26:2c</td><td>10.8.9.18</td><td>802.11ng</td><td>Good (23)</td><td>Wireless</td><td>118.05 MB</td><td>7.92 MB</td></tr>
<tr><td>e4:25:e7:8a:d3:12</td><td>10.10.11.23</td><td>802.11ng</td><td>Excellent (35)</td><td>Marketing</td><td>74.78 MB</td><td>4.58 MB</td></tr>
<tr><td>04:f7:e4:ef:68:05</td><td>10.10.11.71</td><td>802.11ng</td><td>Poor (12)</td><td>Marketing</td><td>84.84 KB</td><td>119.32 KB</td></tr>
</table>
<p>Close</p>
<p>Click the 📝 icon to configure each client</p>
</td></tr>
</table>

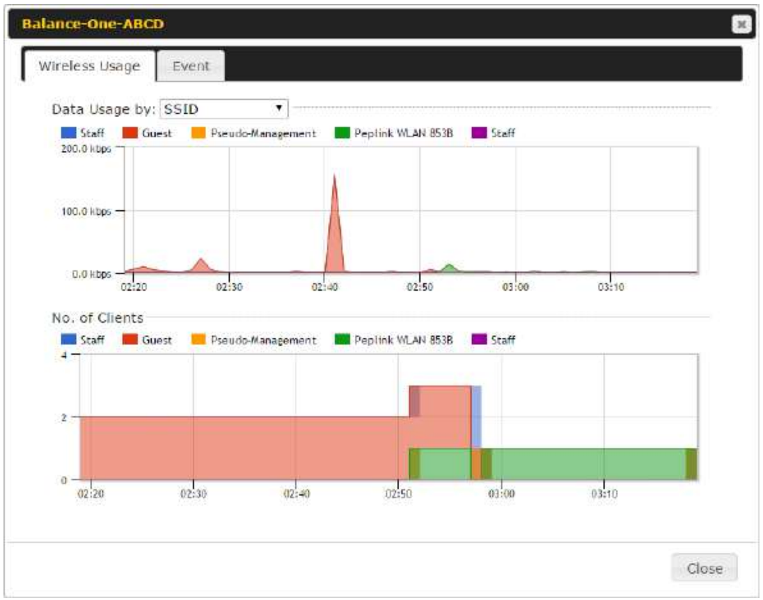


AP Details

Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:E0
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	T4Open
5 GHz SSID List	T4Open
Last config applied by controller	Mon Nov 23 11:25:03 HKT 2015
Uptime	Wed Nov 11 15:00:27 HKT 2015
Current Channel	1 (2.4 GHz) 153 (5 GHz)
Channel	2.4 GHz: Follow AP Profile ▾ 5 GHz: Follow AP Profile ▾
Output Power	2.4 GHz: Follow AP Profile ▾ 5 GHz: Follow AP Profile ▾

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:

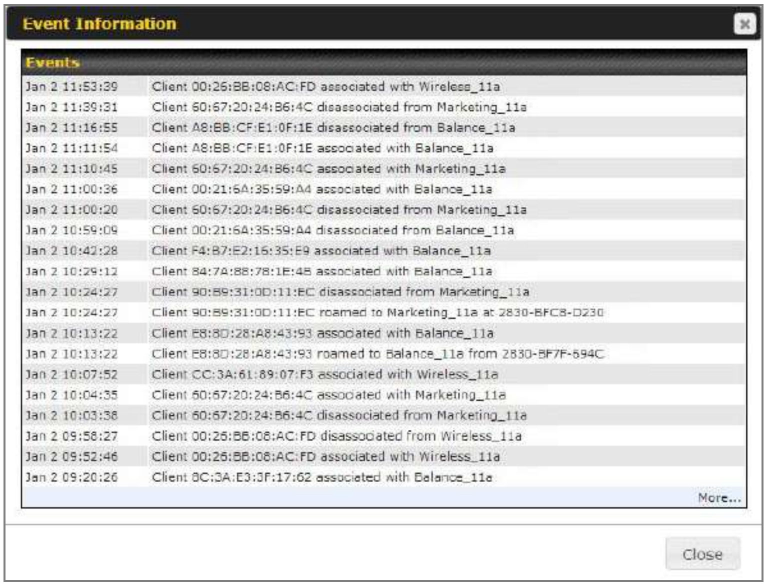


Balance-One-ABCD

Data Usage by: SSID ▾

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.

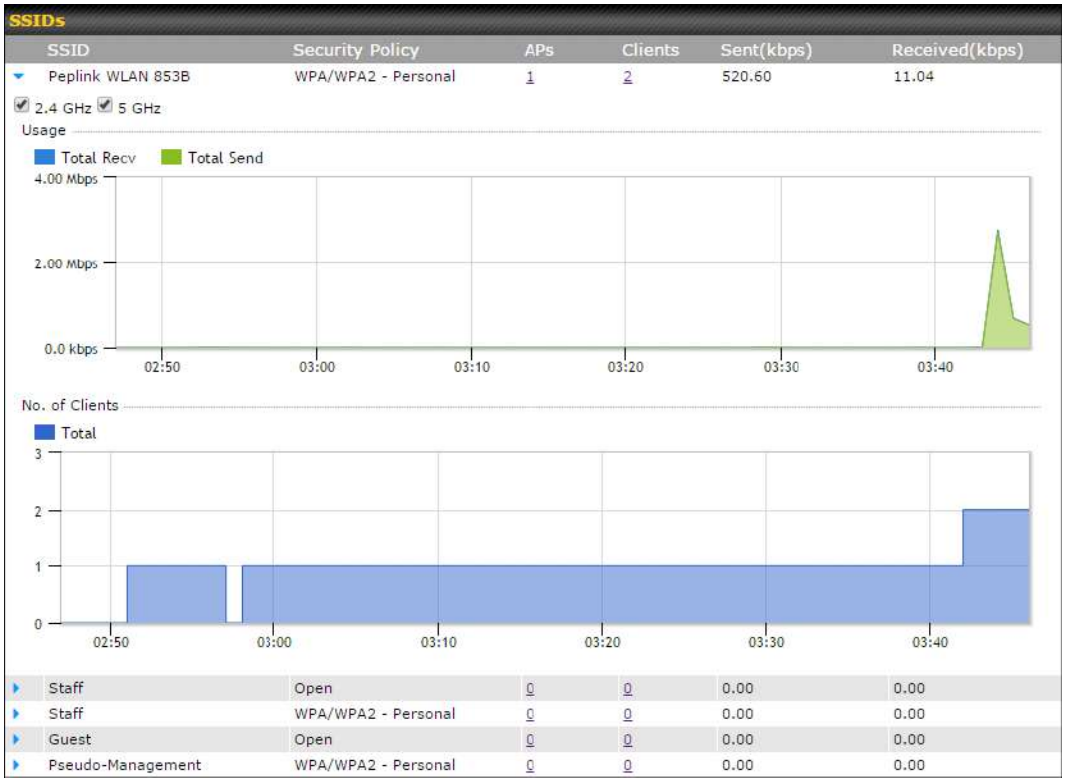
Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:



```
Jan 2 11:53:39    Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 11:39:31    Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:16:55    Client A8:BB:CF:E1:0F:1E disassociated from Balance_11a
Jan 2 11:11:54    Client A8:BB:CF:E1:0F:1E associated with Balance_11a
Jan 2 11:10:45    Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 11:00:36    Client 00:21:6A:35:59:A4 associated with Balance_11a
Jan 2 11:00:20    Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 10:59:09    Client 00:21:6A:35:59:A4 disassociated from Balance_11a
Jan 2 10:42:28    Client F4:B7:E2:16:35:E9 associated with Balance_11a
Jan 2 10:29:12    Client 84:7A:88:78:1E:48 associated with Balance_11a
Jan 2 10:24:27    Client 90:B9:31:0D:11:EC disassociated from Marketing_11a
Jan 2 10:24:27    Client 90:B9:31:0D:11:EC roamed to Marketing_11a at 2830-BFC8-D230
Jan 2 10:13:22    Client E8:8D:28:A8:43:93 associated with Balance_11a
Jan 2 10:13:22    Client E8:8D:28:A8:43:93 roamed to Balance_11a from 2830-BF7F-694C
Jan 2 10:07:52    Client CC:3A:61:89:07:F3 associated with Wireless_11a
Jan 2 10:04:35    Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 10:03:38    Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 09:58:27    Client 00:26:BB:08:AC:FD disassociated from Wireless_11a
Jan 2 09:52:46    Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 09:20:26    Client 8C:3A:E3:3F:17:62 associated with Balance_11a
```

11.2.3 Wireless SSID

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



SSIDs

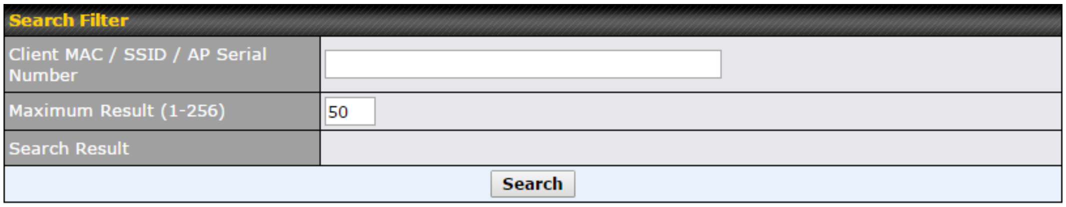
	SSID	Security Policy	APs	Clients	Sent(kbps)	Received(kbps)
▼	Peplink WLAN 853B	WPA/WPA2 - Personal	1	2	520.60	11.04
▶	Staff	Open	0	0	0.00	0.00
▶	Staff	WPA/WPA2 - Personal	0	0	0.00	0.00
▶	Guest	Open	0	0	0.00	0.00
▶	Pseudo-Management	WPA/WPA2 - Personal	0	0	0.00	0.00

☑ 2.4 GHz ☑ 5 GHz

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

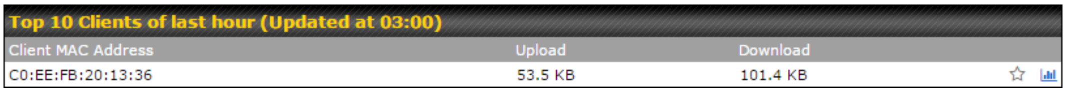
11.2.4 Wireless Client

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



Search Filter

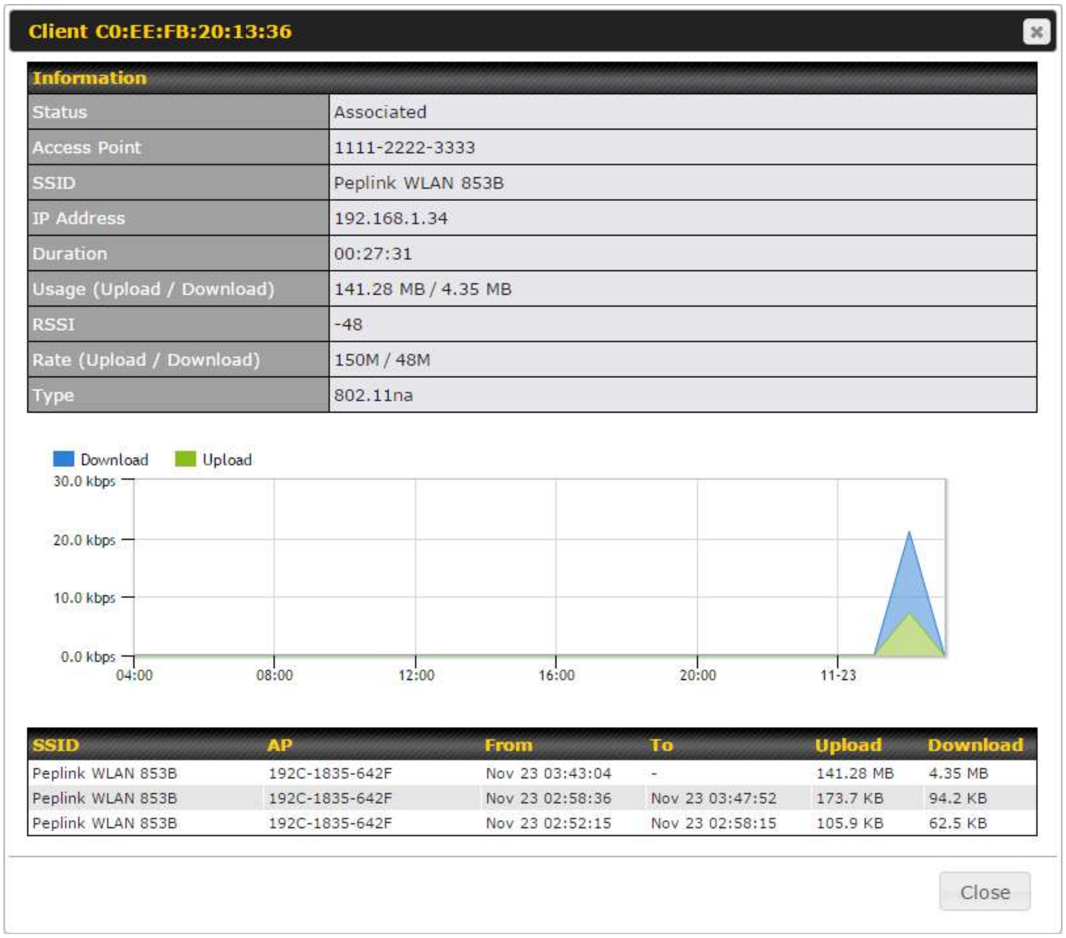
Client MAC / SSID / AP Serial Number	
Maximum Result (1-256)	50
Search Result	



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:



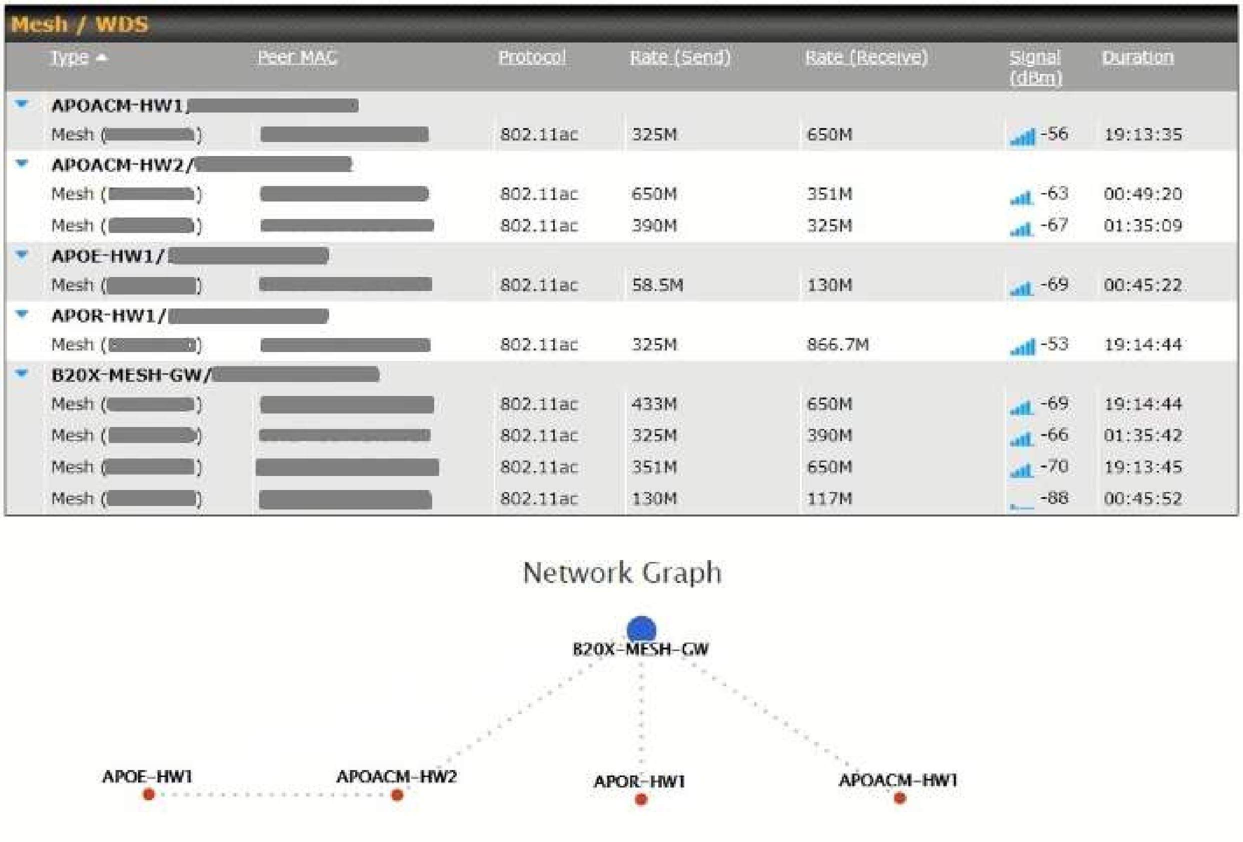
Client C0:EE:FB:20:13:36

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

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

11.2.5 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.



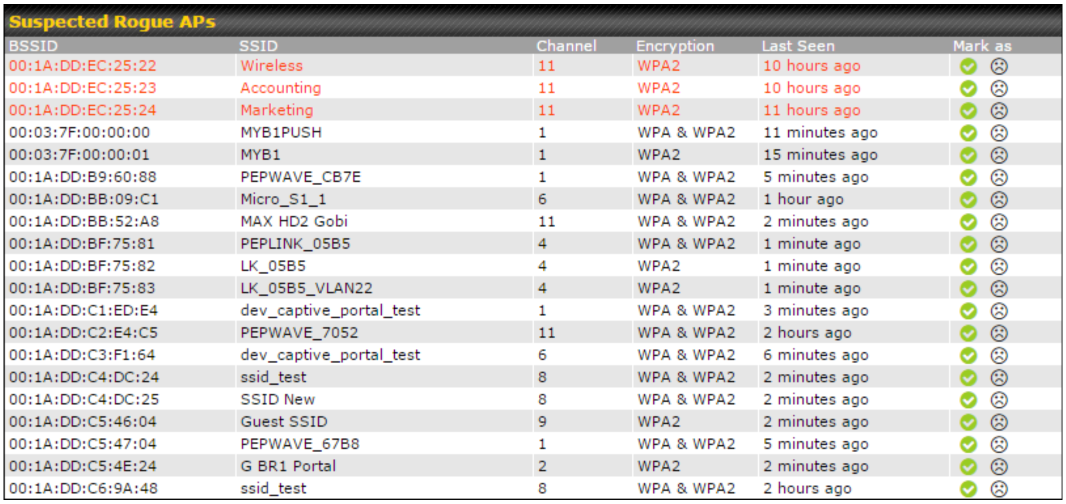
Mesh / WDS

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

Network Graph

11.2.6 Nearby Device

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



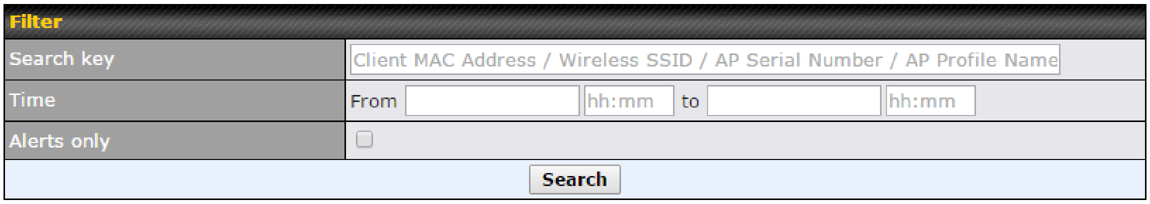
Suspected Rogue APs

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.

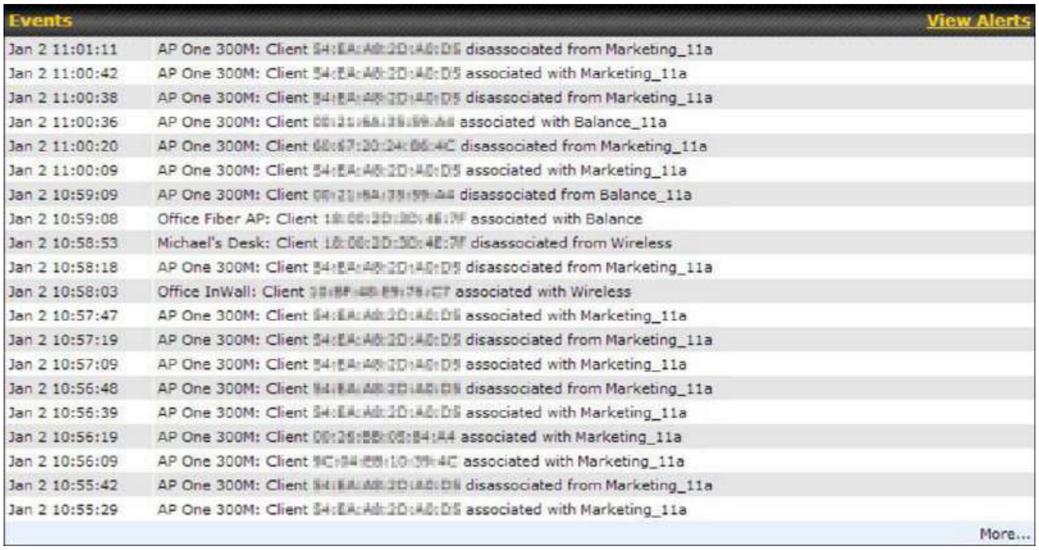
11.2.7 Event Log

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	□

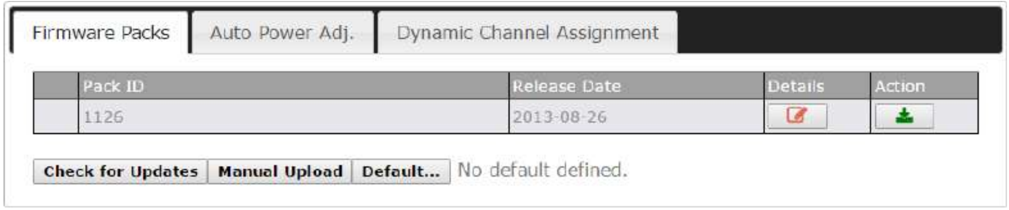


```
Events                                                                          View Alerts
Jan 2 11:01:11   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:42   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 11:00:38   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:36   AP One 300M: Client [redacted] associated with Balance_11a
Jan 2 11:00:20   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:59:09   AP One 300M: Client [redacted] disassociated from Balance_11a
Jan 2 10:59:08   Office Fiber AP: Client [redacted] associated with Balance
Jan 2 10:58:53   Michael's Desk: Client [redacted] disassociated from Wireless
Jan 2 10:58:18   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:58:03   Office InWall: Client [redacted] associated with Wireless
Jan 2 10:57:47   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:57:19   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:57:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:48   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:56:39   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:19   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:55:42   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:55:29   AP One 300M: Client [redacted] 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.

11.3 Toolbox

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



	Pack ID	Release Date	Details	Action
	1126	2013-08-26	✎	⬇

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 Check for Updates to download new packs or you can press Manual Upload to manually upload a firmware pack. Press Default... to define which firmware pack is default.

12 System Tab

12.1 System

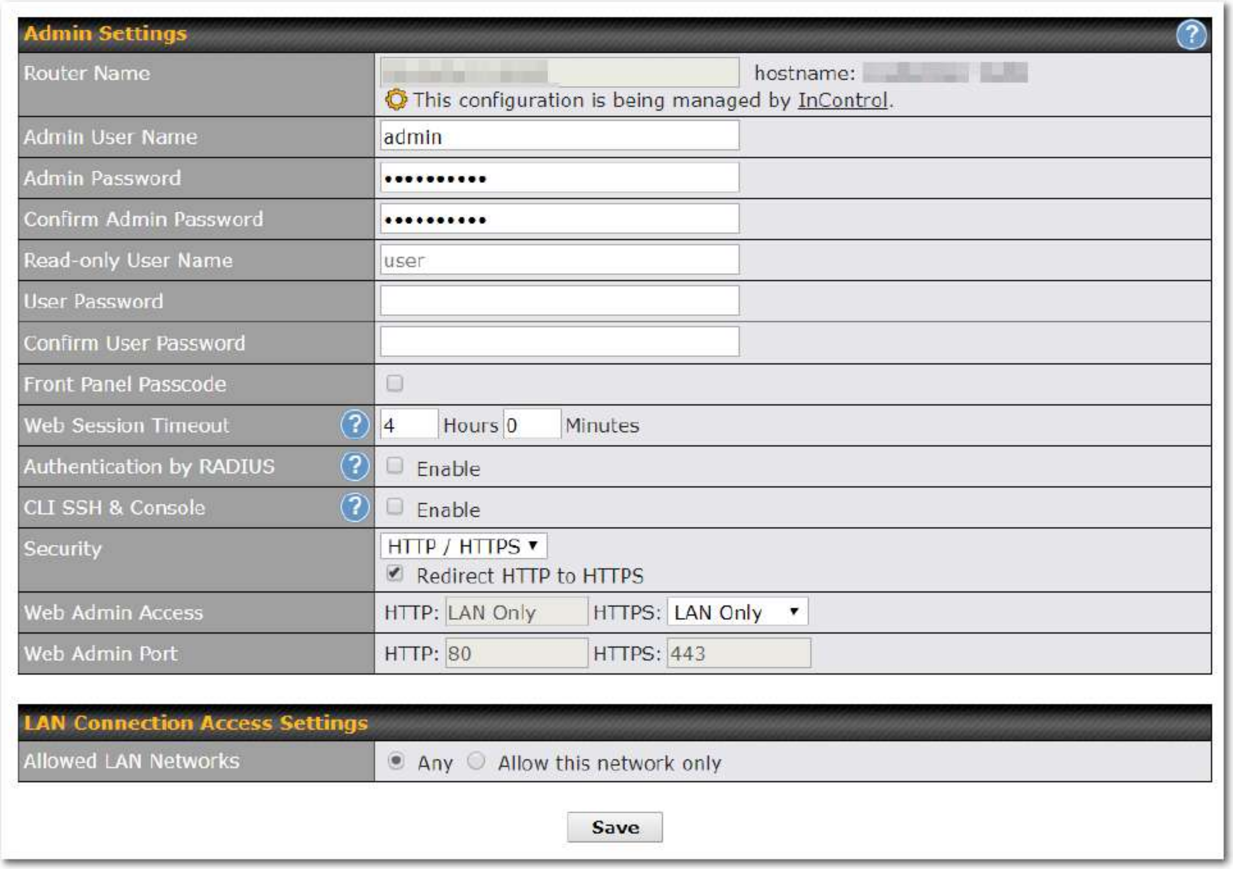
12.1.1 Admin Security

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**.



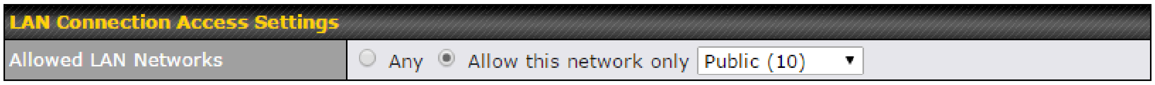
Admin Settings	
Router Name	[redacted] hostname: [redacted] This configuration is being managed by InControl.
Admin User Name	admin
Admin Password	••••••••••
Confirm Admin Password	••••••••••
Read-only User Name	user
User Password	
Confirm User Password	
Front Panel Passcode	□
Web Session Timeout	4 Hours 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 *admin* by default, but can be changed, if desired.
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	**Read-only User Name** is set as *user* by default, but can be changed, if desired.
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.

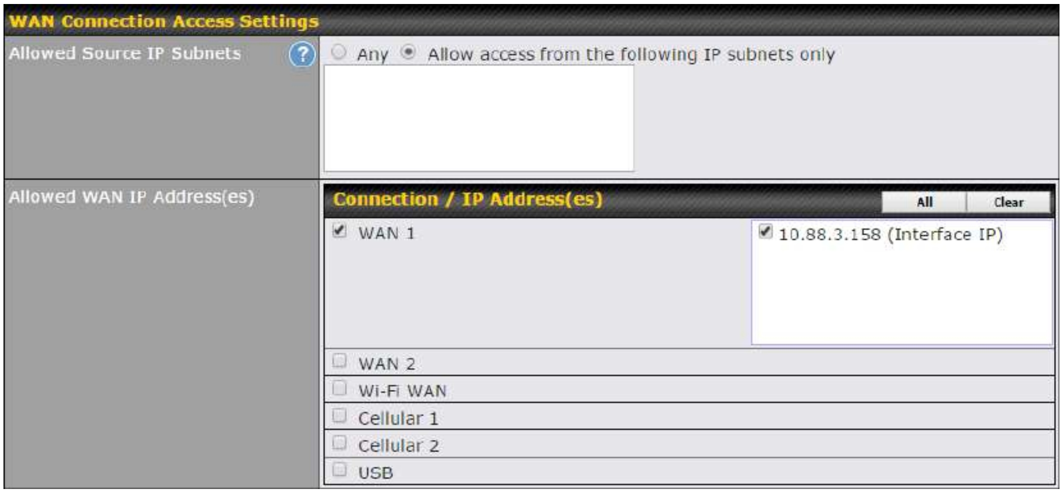
Confirm User Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to **4 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 Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Login Grace Time	This option specifies the time for CLI SSH login. The default value is 120.
CLI SSH Access Public Key	This field is for entering the Public Key for Admin Users and Read-only Users to access CLI SSH.
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.



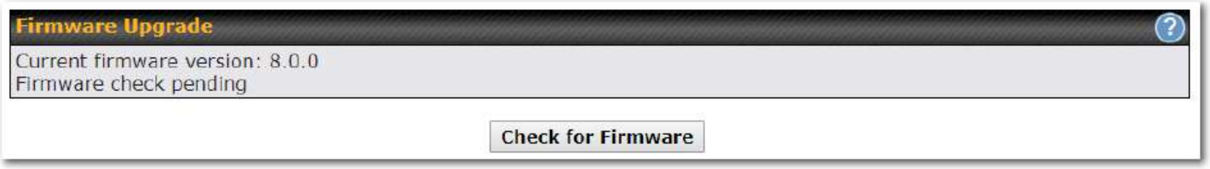
WAN Connection Access Settings	
Allowed Source IP Subnets ?	○ Any ● Allow access from the following IP subnets only
Allowed WAN IP Address(es)	Connection / IP Address(es) All Clear ☑ WAN 1 — ☑ 10.88.3.158 (Interface IP) □ WAN 2 □ Wi-Fi WAN □ Cellular 1 □ Cellular 2 □ USB

WAN Connection Access Settings	
Allowed Source IP Subnets	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 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 *w.x.y.z/m*, where *w.x.y.z* is an IP address (e.g., *192.168.0.0*), and *m* is

	the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, *192.168.0.0/24*). To define multiple subnets, separate each IP subnet one in a line. For example: ● 192.168.0.0/24 ● 10.8.0.0/16
Allowed WAN IP Address(es)	This is to choose which WAN IP address(es) the web server should listen on.

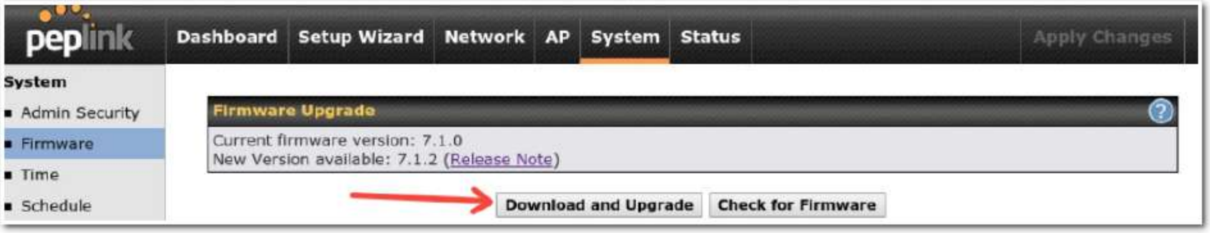
12.1.2 Firmware

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**.


Firmware Upgrade

Current firmware version: 8.0.0
Firmware check pending

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

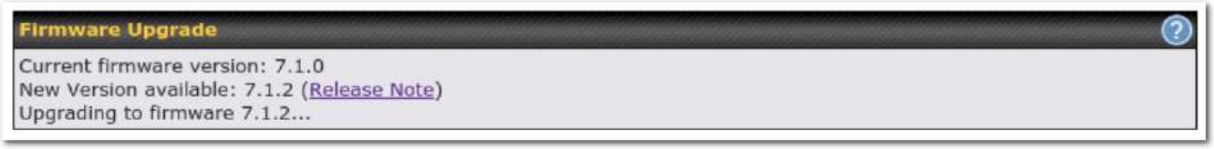


Firmware Upgrade

Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)

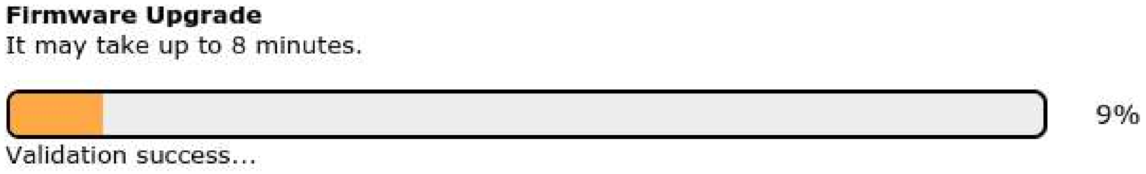
Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

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


Firmware Upgrade

Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)
Upgrading to firmware 7.1.2...

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.

9%

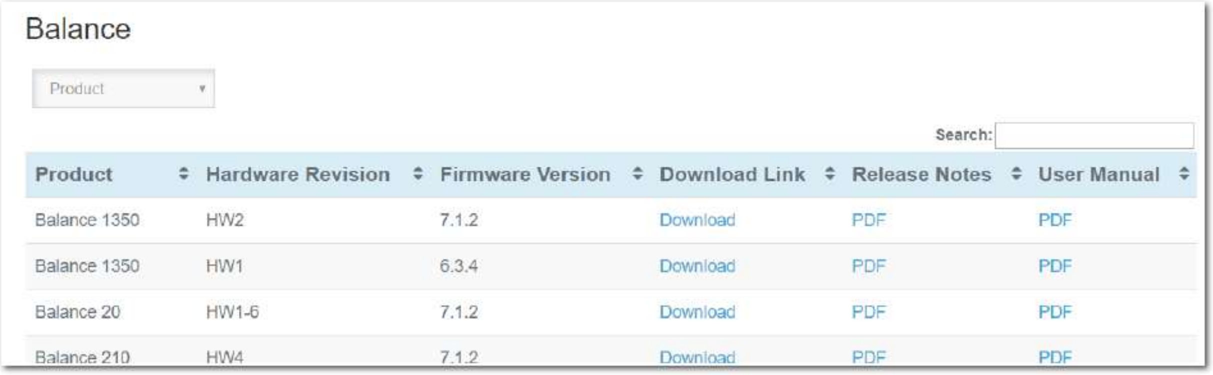
Validation success...

***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.



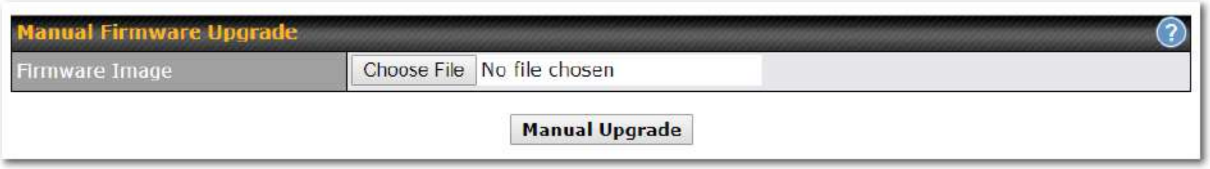
Balance

Product	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.

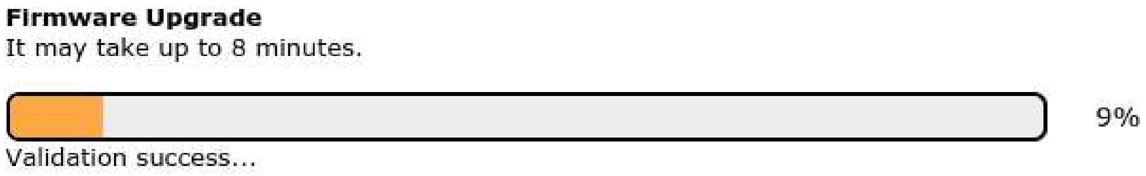
Click on the Manual Upgrade button to start the upgrade process.



Manual Firmware Upgrade

Firmware Image	Choose File No file chosen

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.

9%

Validation success...

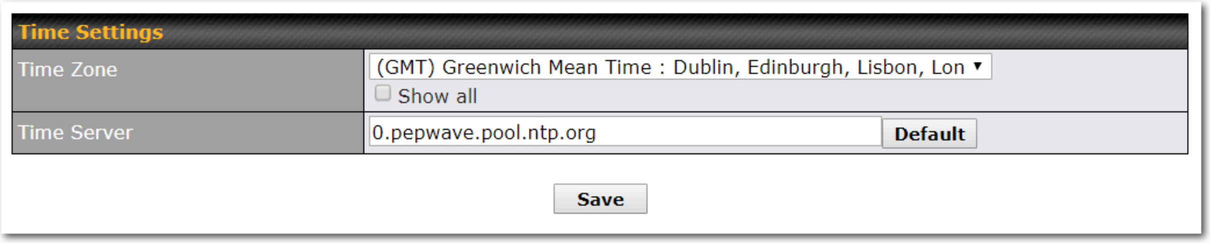
***Upgrading the firmware will cause the router to reboot.**

The InControl method

[Described in this knowledgebase article on our forum.]

12.1.3 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**.



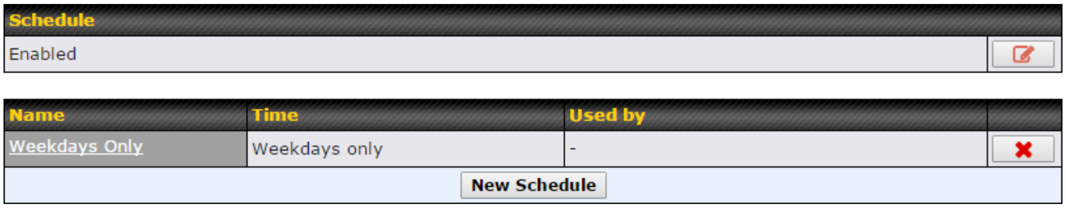
Time Settings

Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▾ □ Show all
Time Server	0.pepwave.pool.ntp.org [Default]

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.

12.1.4 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**

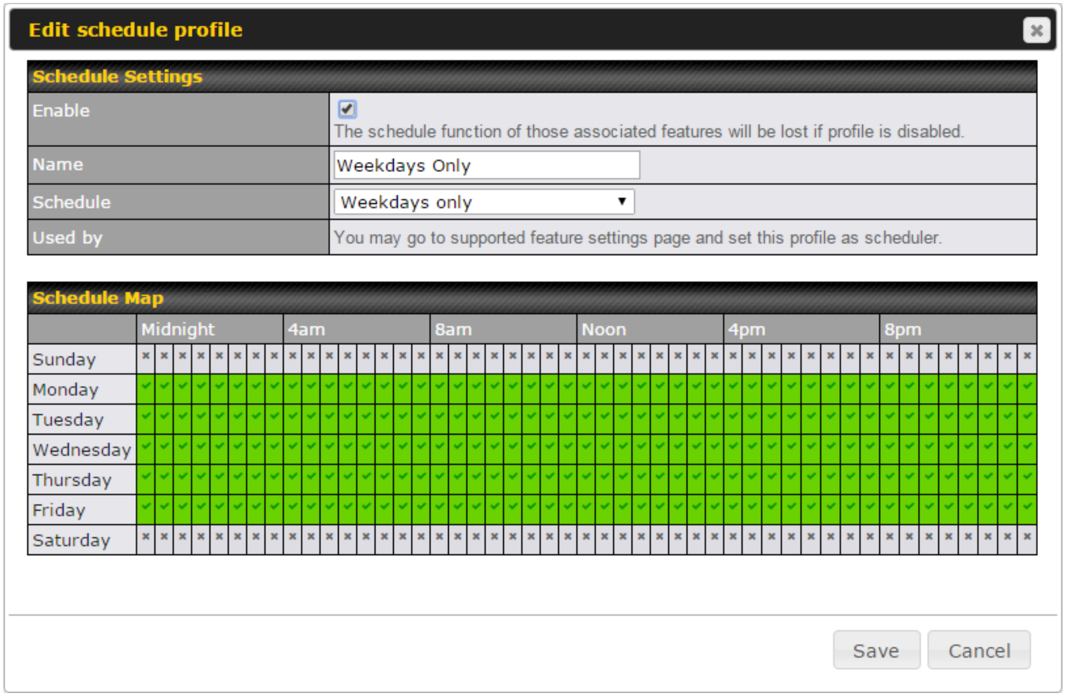


Schedule	
Enabled	

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.

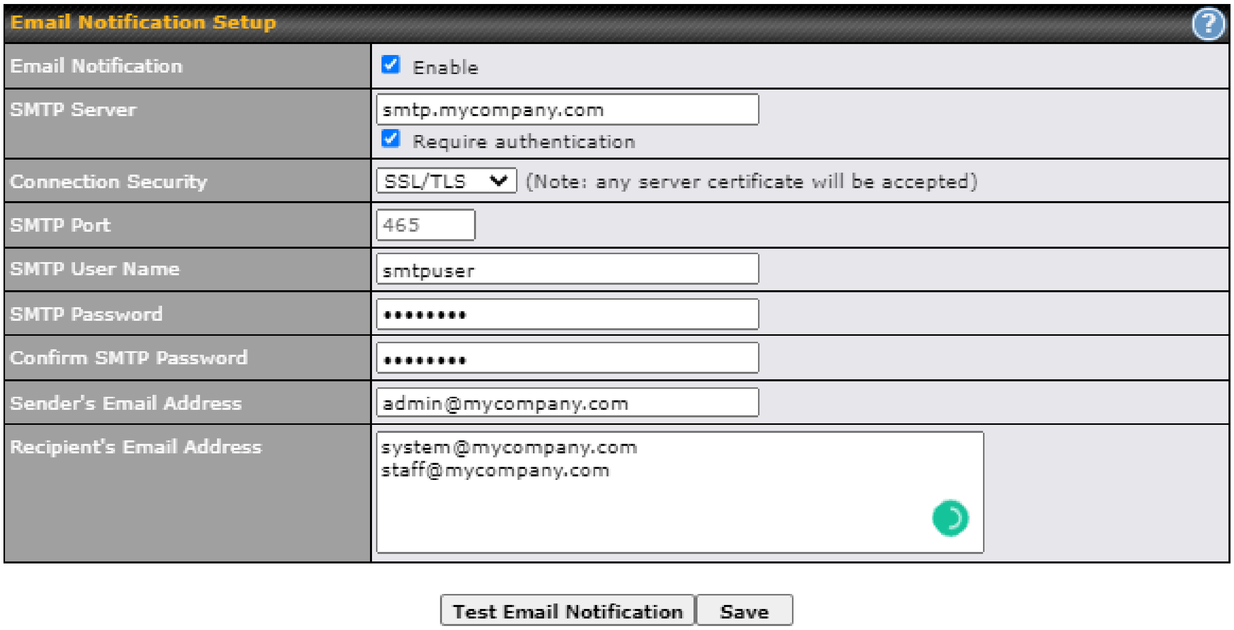
Schedule Map

	Midnight								4am								8am								Noon								4pm								8pm							
Sunday	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Monday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Thursday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Saturday	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

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.

12.1.5 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**.



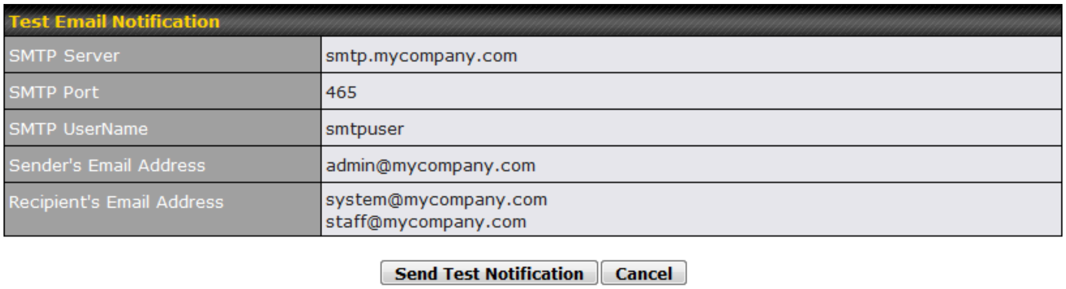
Email Notification Setup

Email Notification	☑ Enable
SMTP Server	smtp.mycompany.com ☑ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	smtpuser
SMTP Password	••••••••
Confirm SMTP Password	••••••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

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.

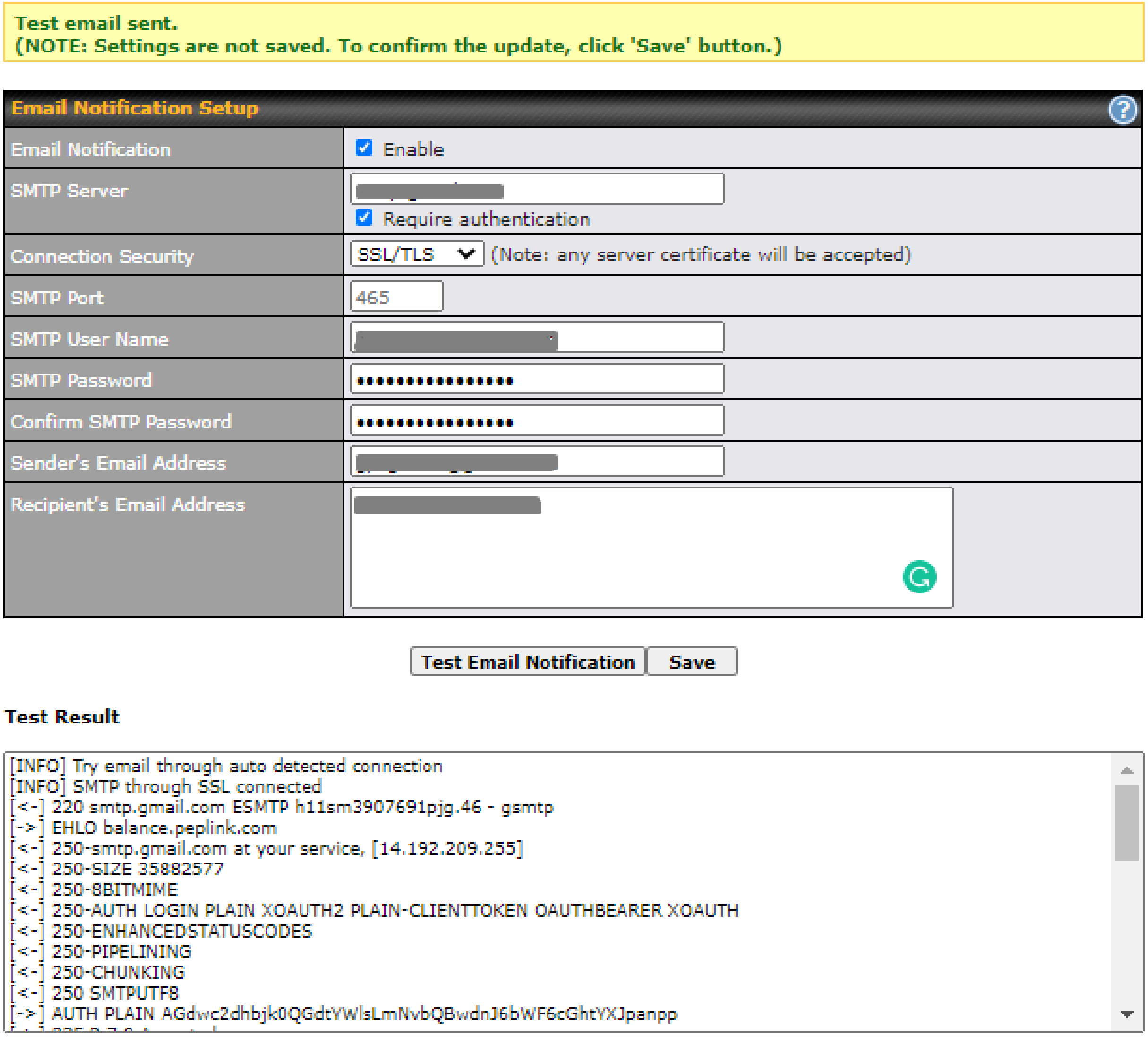
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address which the Peplink Balance will use to send its reports.
Recipient's Email Address	This setting specifies the email address(es) to which the 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

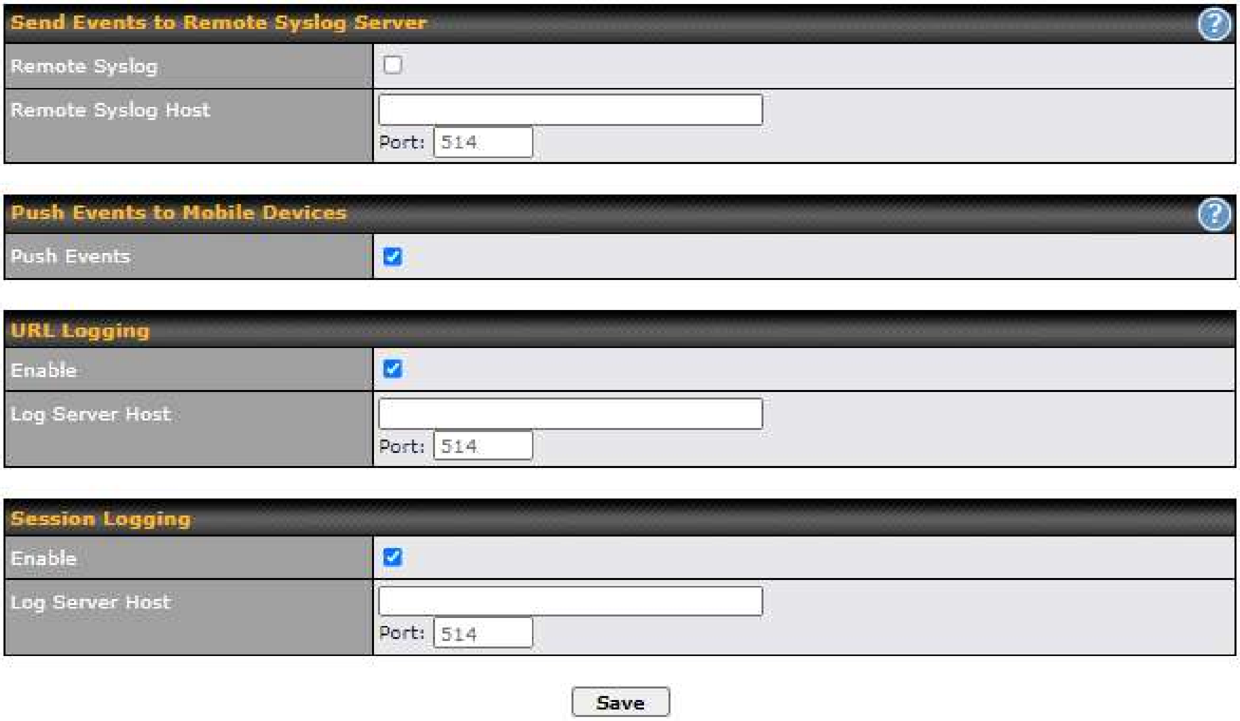
Email Notification	☑ Enable
SMTP Server	[redacted] ☑ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	[redacted]
SMTP Password	••••••••••••••••
Confirm SMTP Password	••••••••••••••••
Sender's Email Address	[redacted]
Recipient's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

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 AGdwc2dhbjk0QGdtYWlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

12.1.6 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

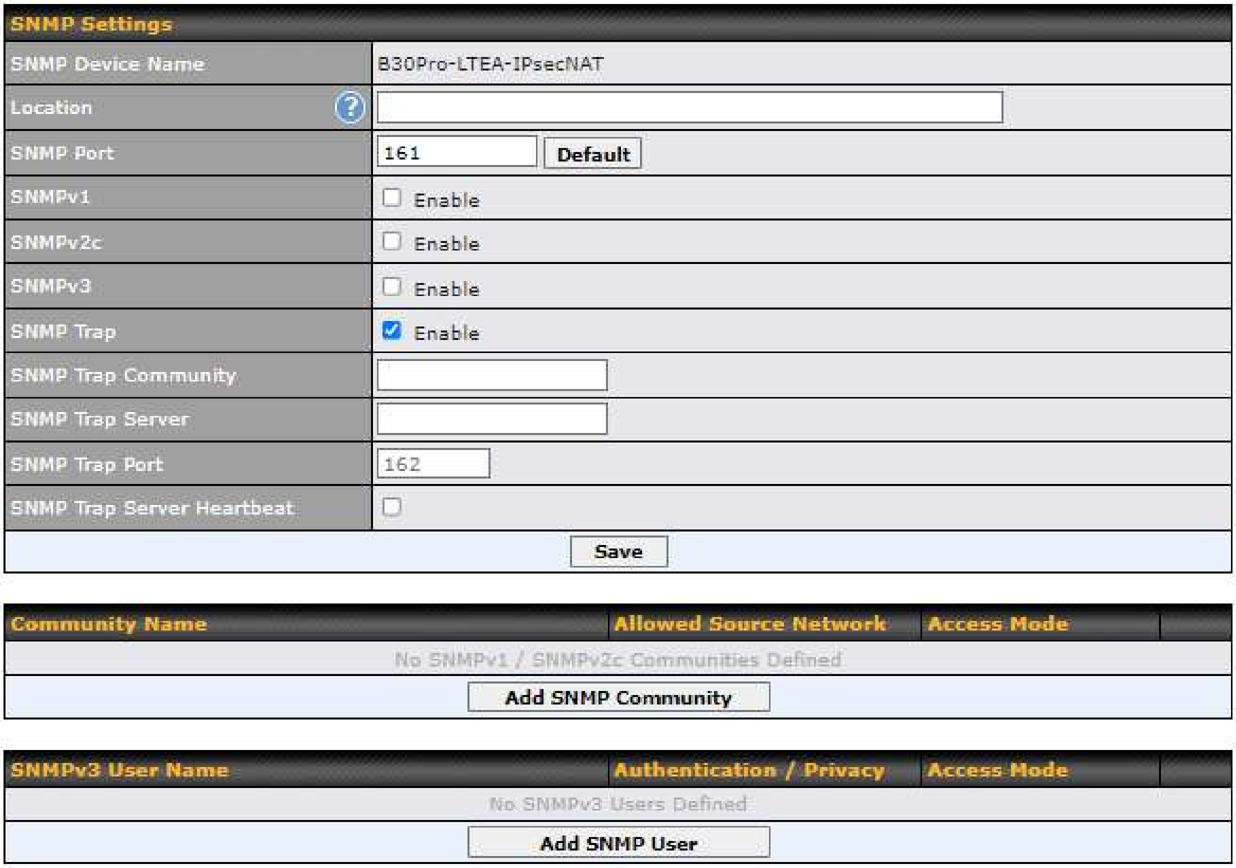
Enable ☑

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 Logging Host	This setting specifies the IP address or hostname of the Session log server.
	For more information on the Router Utility, go to: www.peplink.com/products/router-utility

12.1.7 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	B30Pro-LTEA-IPsecNAT
Location ?	
SNMP Port	161 Default
SNMPv1	☐ Enable
SNMPv2c	☐ Enable
SNMPv3	☐ Enable
SNMP Trap	☑ Enable
SNMP Trap Community	
SNMP Trap Server	
SNMP Trap Port	162
SNMP Trap Server Heartbeat	☐
Save	

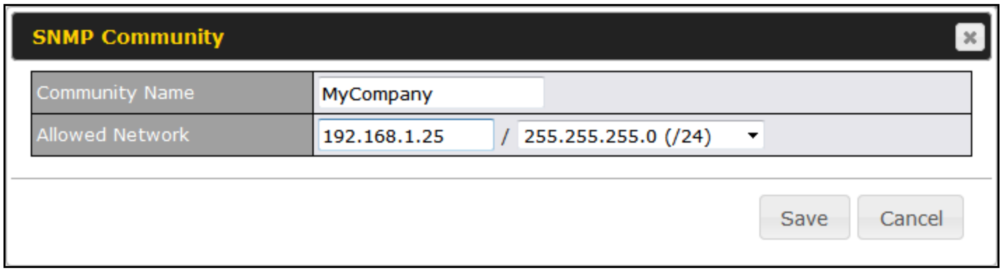
Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		
Add SNMP Community		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		
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.
SNMP Trap	This option allows you to enable SNMP Trap. If enabled, the following entry fields will

	appear.
SNMP Trap Community	This setting specifies the SNMP Trap community name.
SNMP Trap Server	Enter the IP address of the SNMP Trap server
SNMP Trap Port	This option specifies the port which the SNMP Trap server will use. The default port is **162**.
SNMP Trap Server Heartbeat	This option allows you to enable and configure the heartbeat interval for the SNMP Trap server.

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:

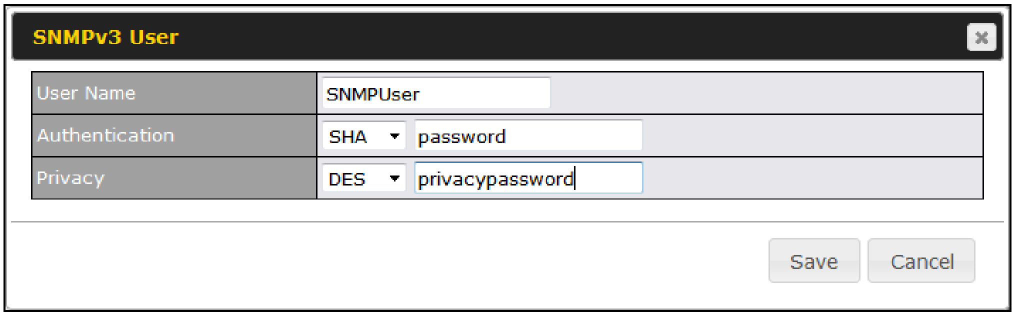


SNMP Community

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

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

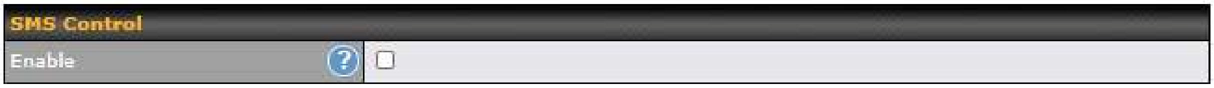
SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols: ● NONE ● MD5 ● SHA When MD5 or SHA is selected, an entry field will appear for the password.
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.

12.1.8 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*



SMS Control

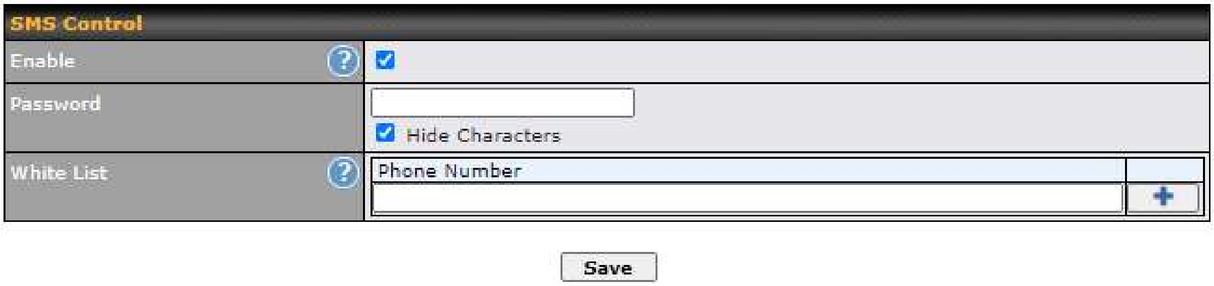
Enable ?	□

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.

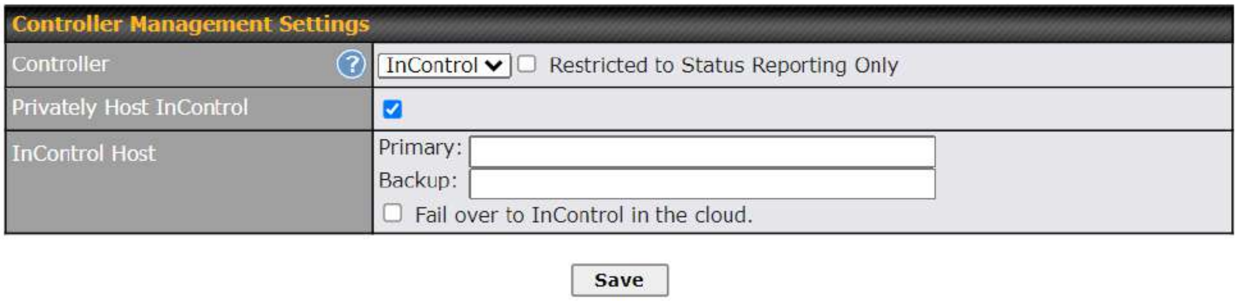


SMS Control

Enable	☑
Password	☑ Hide Characters
White List	Phone Number

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.

12.1.9 InControl



Controller Management Settings	
Controller	InControl ▾ □ Restricted to Status Reporting Only
Privately Host InControl	☑
InControl Host	Primary: Backup: □ Fail over to InControl in the cloud.

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.

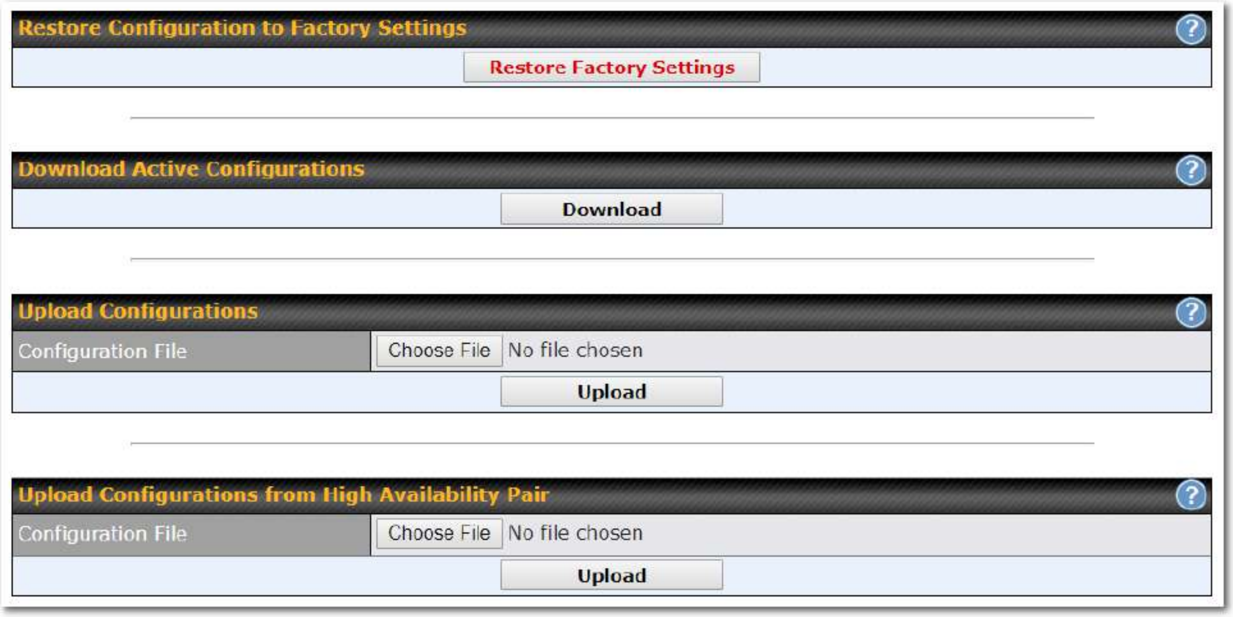
When the box **Restricted to Status Reporting Only** is ticked, the router will only report its status, but can’t be managed or configured by InControl.

Alternatively, you can also privately host InControl. Simply check the “Privately Host InControl” box and enter the IP Address of your InControl Host. If you have multiple hosts, you may enter the primary and backup IP addresses for the InControl Host and tick the “Fail over to InControl in the cloud” box. The device will connect to either the primary InControl Host or the secondary/backup ICA/IC2.

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.

12.1.10 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**.



Restore Configuration to Factory Settings

Restore Factory Settings

Download Active Configurations

Download

Upload Configurations

Configuration File: Choose File No file chosen

Upload

Upload Configurations from High Availability Pair

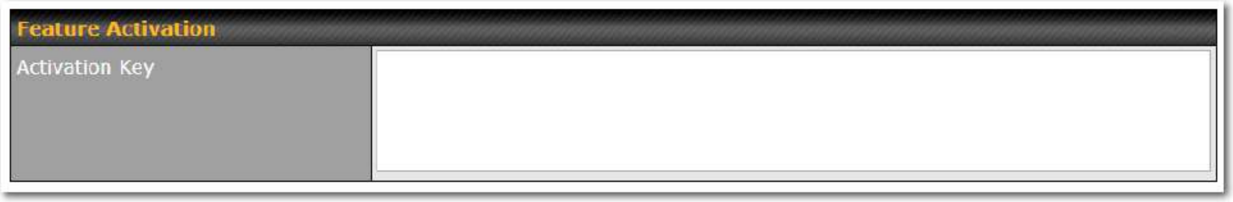
Configuration File: Choose File No file chosen

Upload

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.

12.1.11 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**.



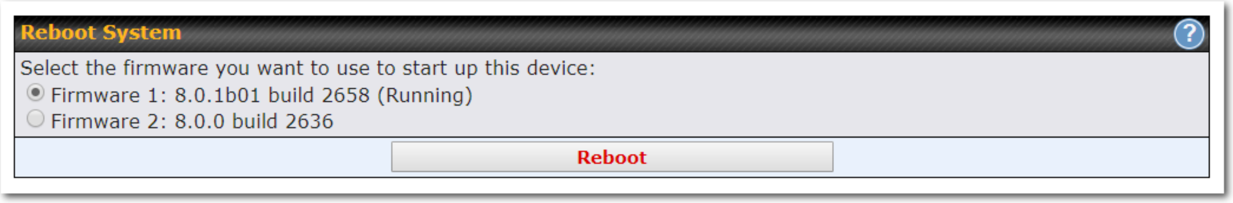
Feature Activation

Activation Key

12.1.12 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.



Reboot System

Select the firmware you want to use to start up this device:

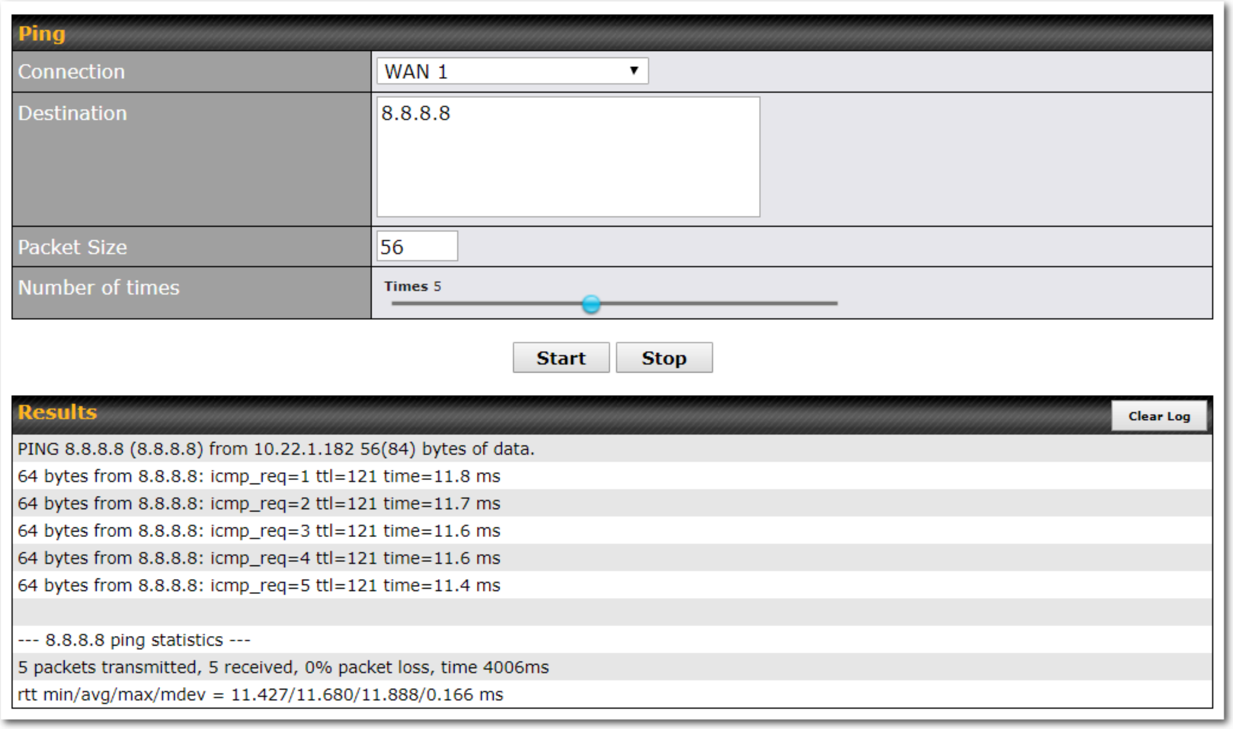
● Firmware 1: 8.0.1b01 build 2658 (Running)

○ Firmware 2: 8.0.0 build 2636

12.2 Tools

12.2.1 Ping

The ping test tool sends pings through a specific Ethernet interface or a SpeedFusion^{TM} 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

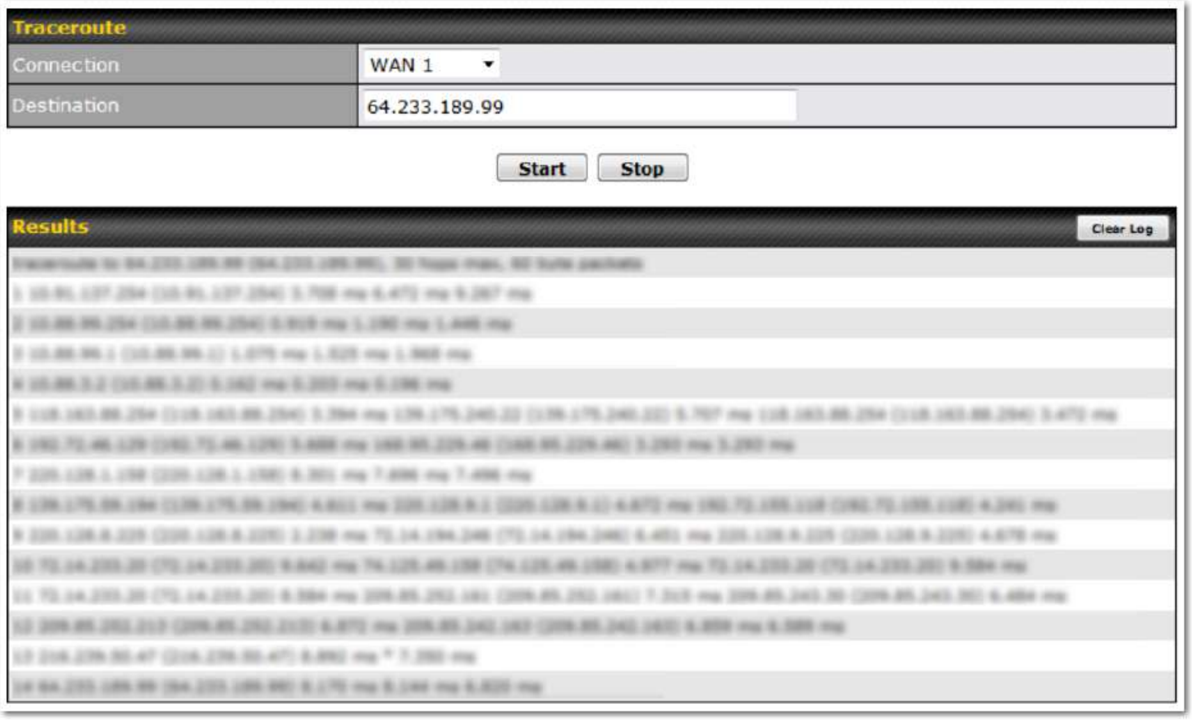
```
PING 8.8.8.8 (8.8.8.8) from 10.22.1.182 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=121 time=11.8 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=121 time=11.7 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: 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.

12.2.2 Traceroute

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



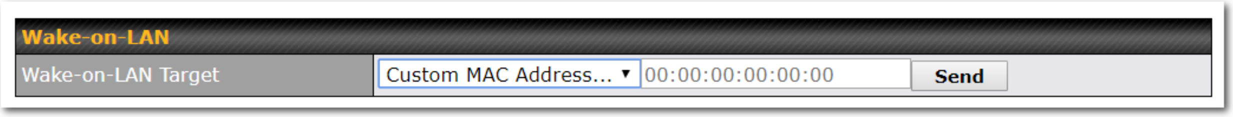
Traceroute

Connection	WAN 1 ▾
Destination	64.233.189.99

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

12.2.3 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

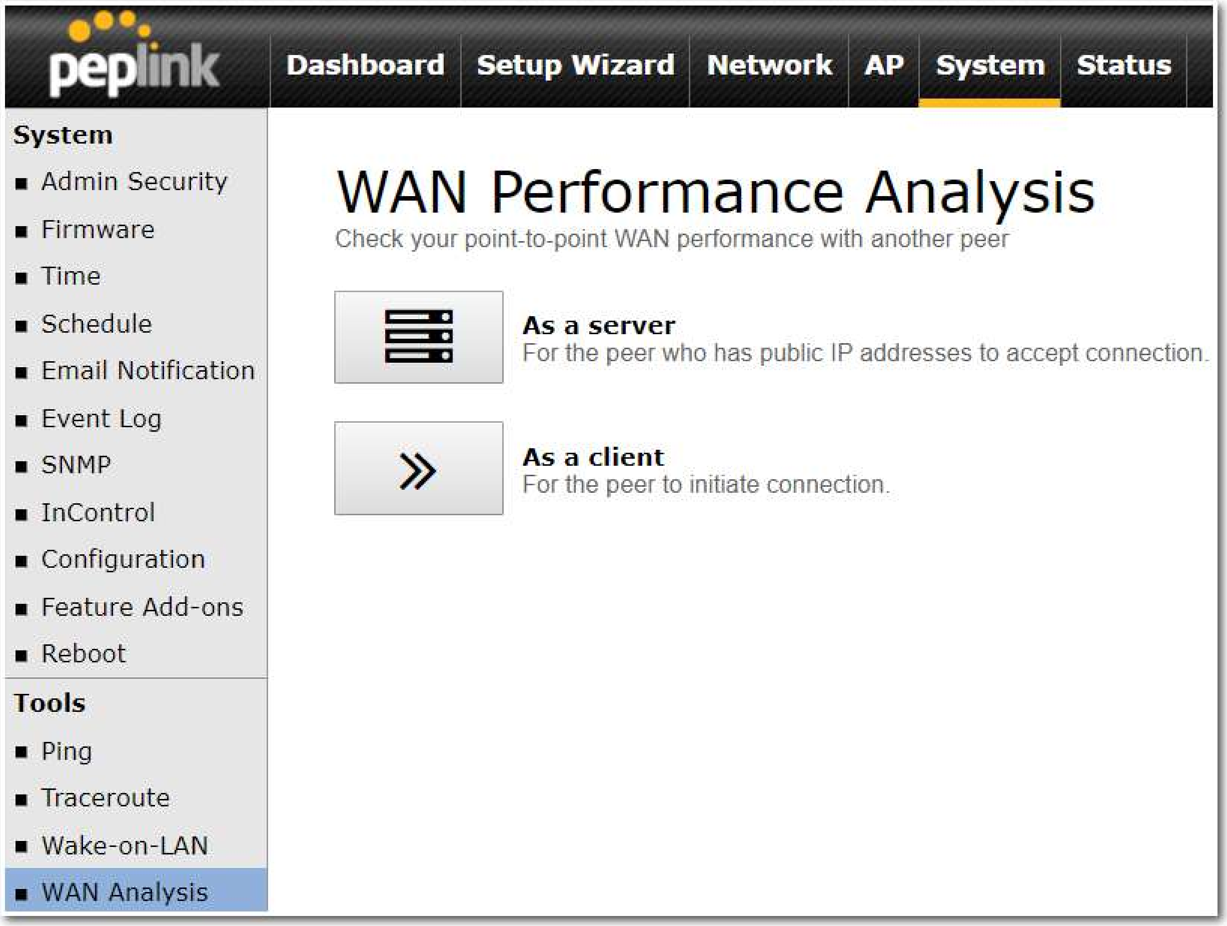
Wake-on-LAN Target	Custom MAC Address... ▾ 00:00:00:00:00:00

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

12.2.4 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.



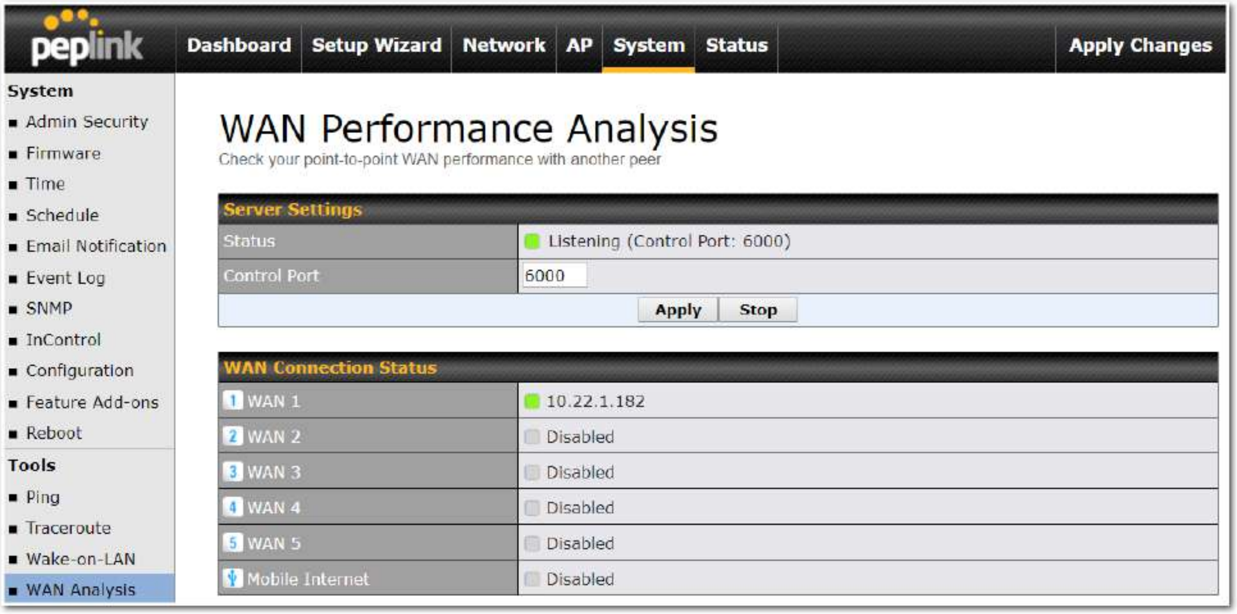
WAN Performance Analysis

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

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

As a client
For the peer to initiate connection.

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



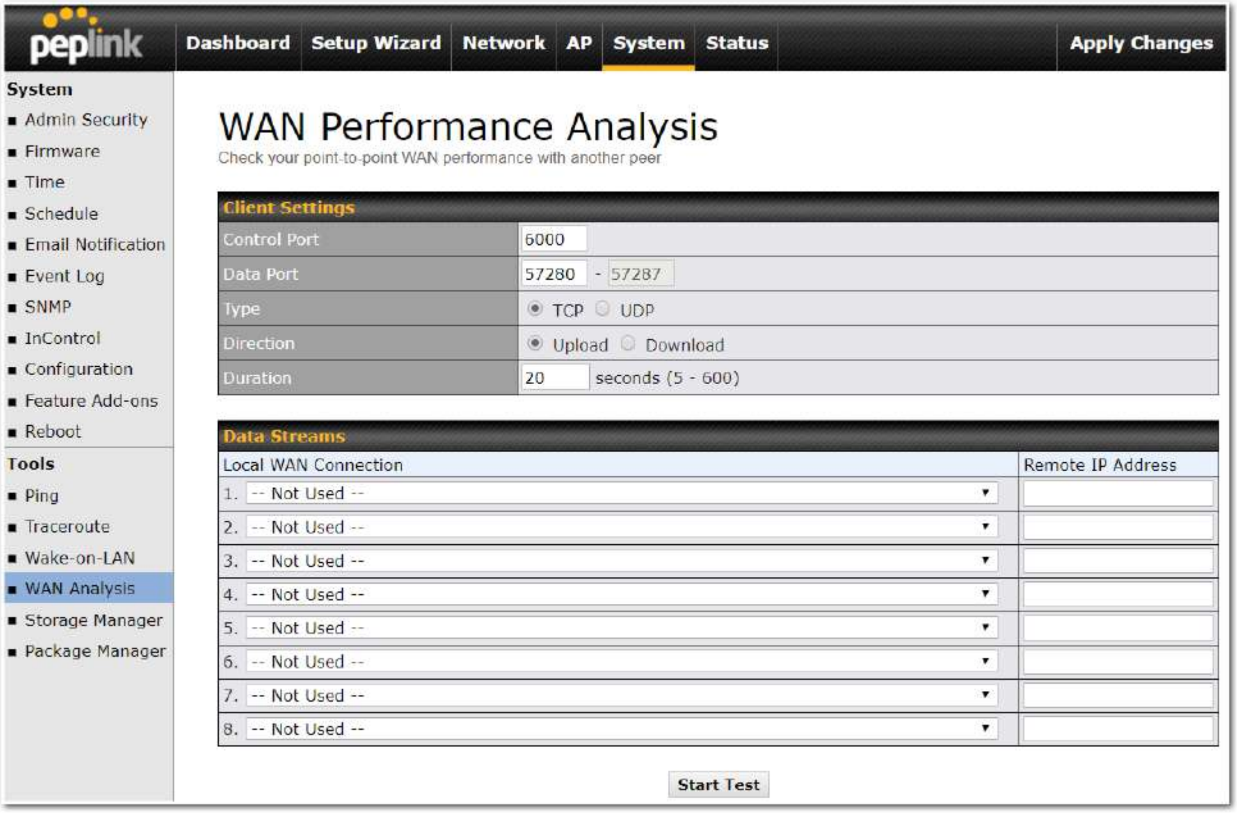
WAN Performance Analysis

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

Server Settings	
Status	🟩 Listening (Control Port: 6000)
Control Port	6000

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.



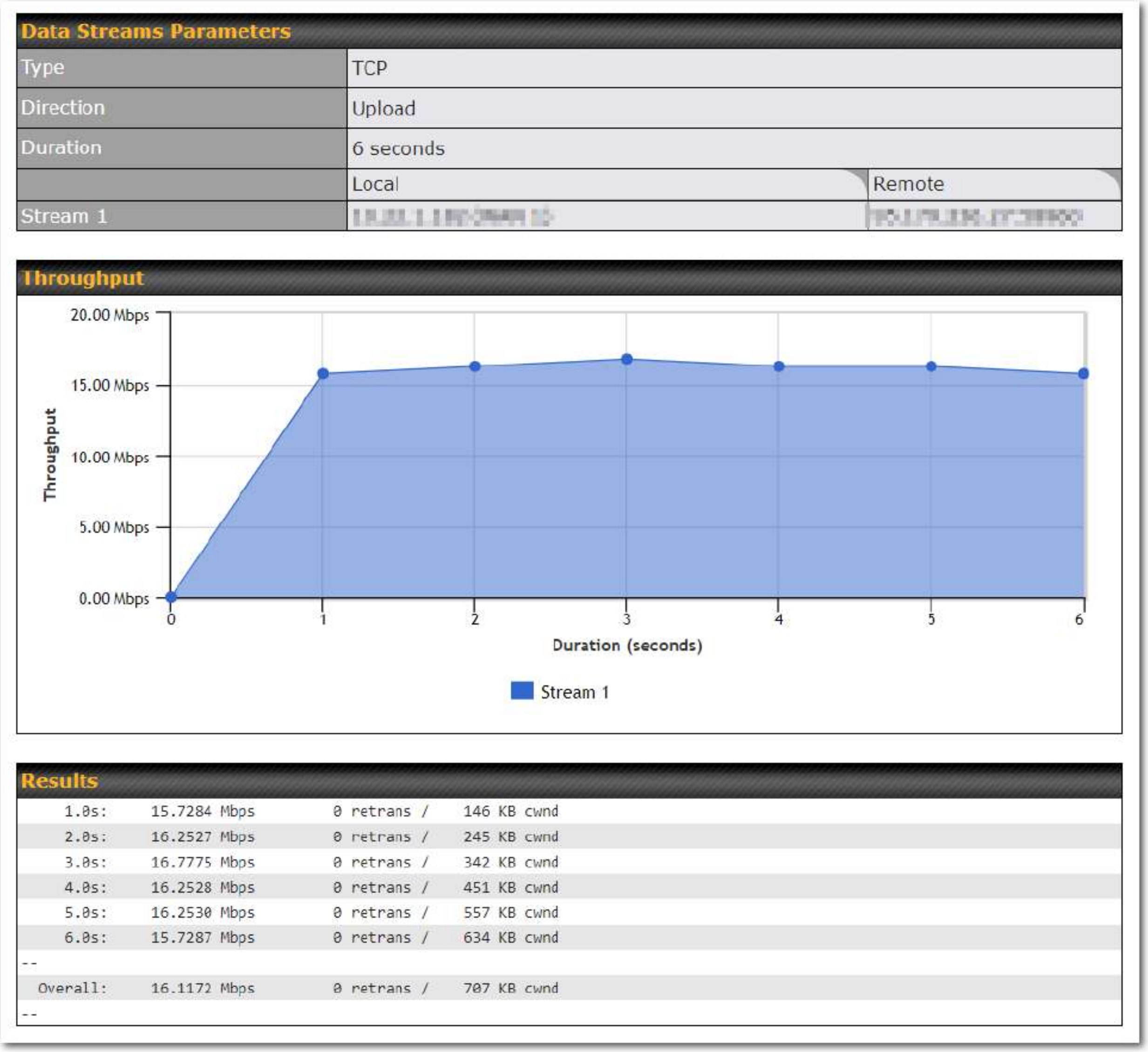
WAN Performance Analysis

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 --	

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



Data Streams Parameters

Type	TCP	
Direction	Upload	
Duration	6 seconds	
	Local	Remote
Stream 1	[redacted]	[redacted]

Throughput

Results

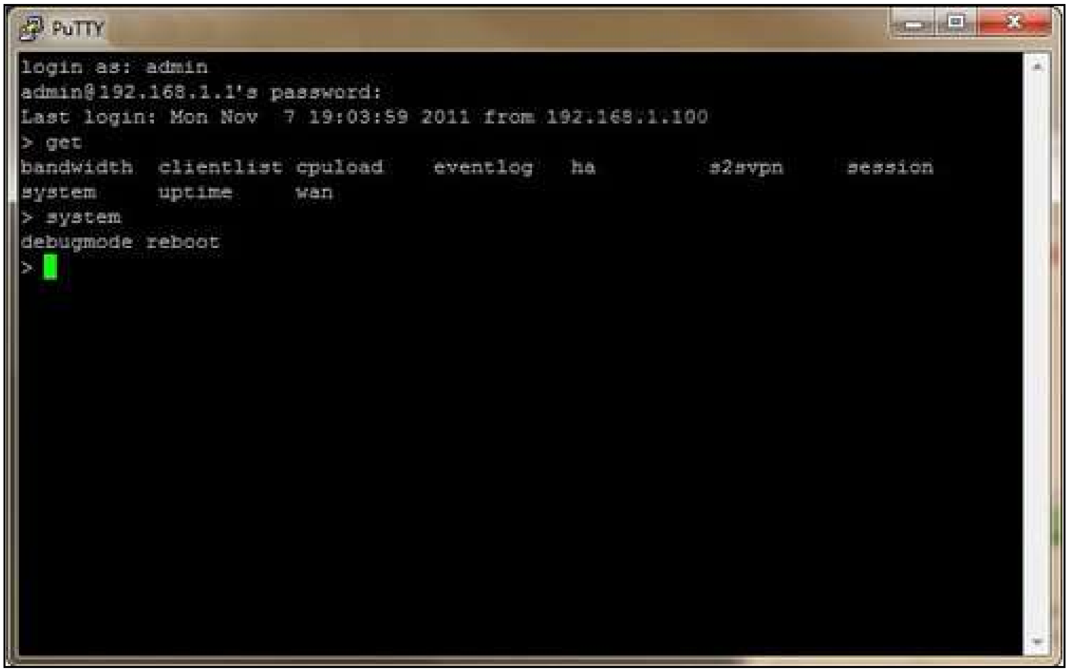
```
     1.0s:     15.7284 Mbps        0 retrans /    146 KB cwnd
     2.0s:     16.2527 Mbps        0 retrans /    245 KB cwnd
     3.0s:     16.7775 Mbps        0 retrans /    342 KB cwnd
     4.0s:     16.2528 Mbps        0 retrans /    451 KB cwnd
     5.0s:     16.2530 Mbps        0 retrans /    557 KB cwnd
     6.0s:     15.7287 Mbps        0 retrans /    634 KB cwnd
--
  Overall:     16.1172 Mbps        0 retrans /    707 KB cwnd
--
```

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.

12.3 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*.



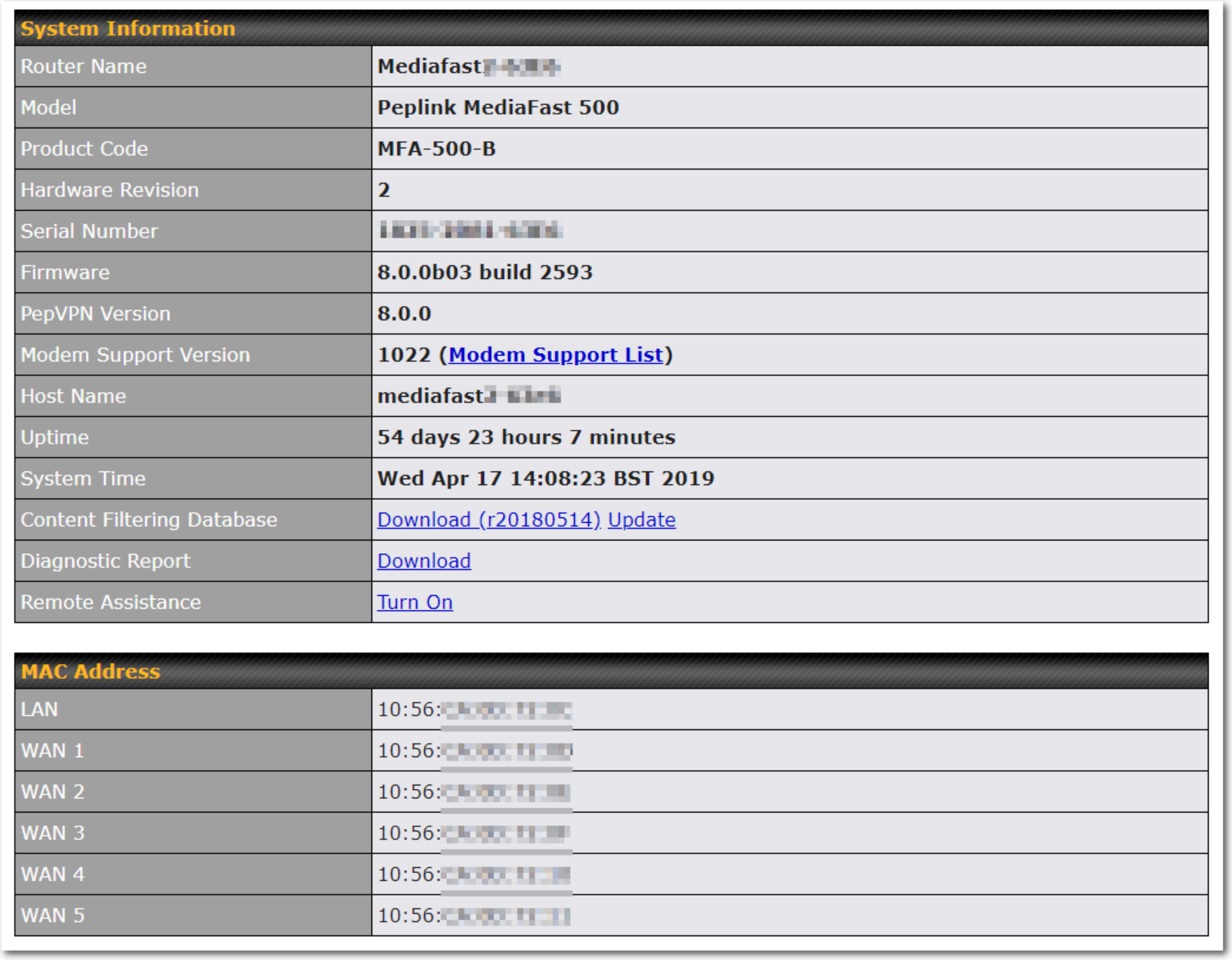
```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist cpuload    eventlog   ha         s2svpn     session
system     uptime     wan
> system
debugmode reboot
>
```

13 Status Tab

13.1 Status

13.1.1 Device

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



System Information	
Router Name	Mediafast[redacted]
Model	Peplink MediaFast 500
Product Code	MFA-500-B
Hardware Revision	2
Serial Number	[redacted]
Firmware	8.0.0b03 build 2593
PepVPN Version	8.0.0
Modem Support Version	1022 (Modem Support List)
Host Name	mediafast[redacted]
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:[redacted]
WAN 1	10:56:[redacted]
WAN 2	10:56:[redacted]
WAN 3	10:56:[redacted]
WAN 4	10:56:[redacted]
WAN 5	10:56:[redacted]

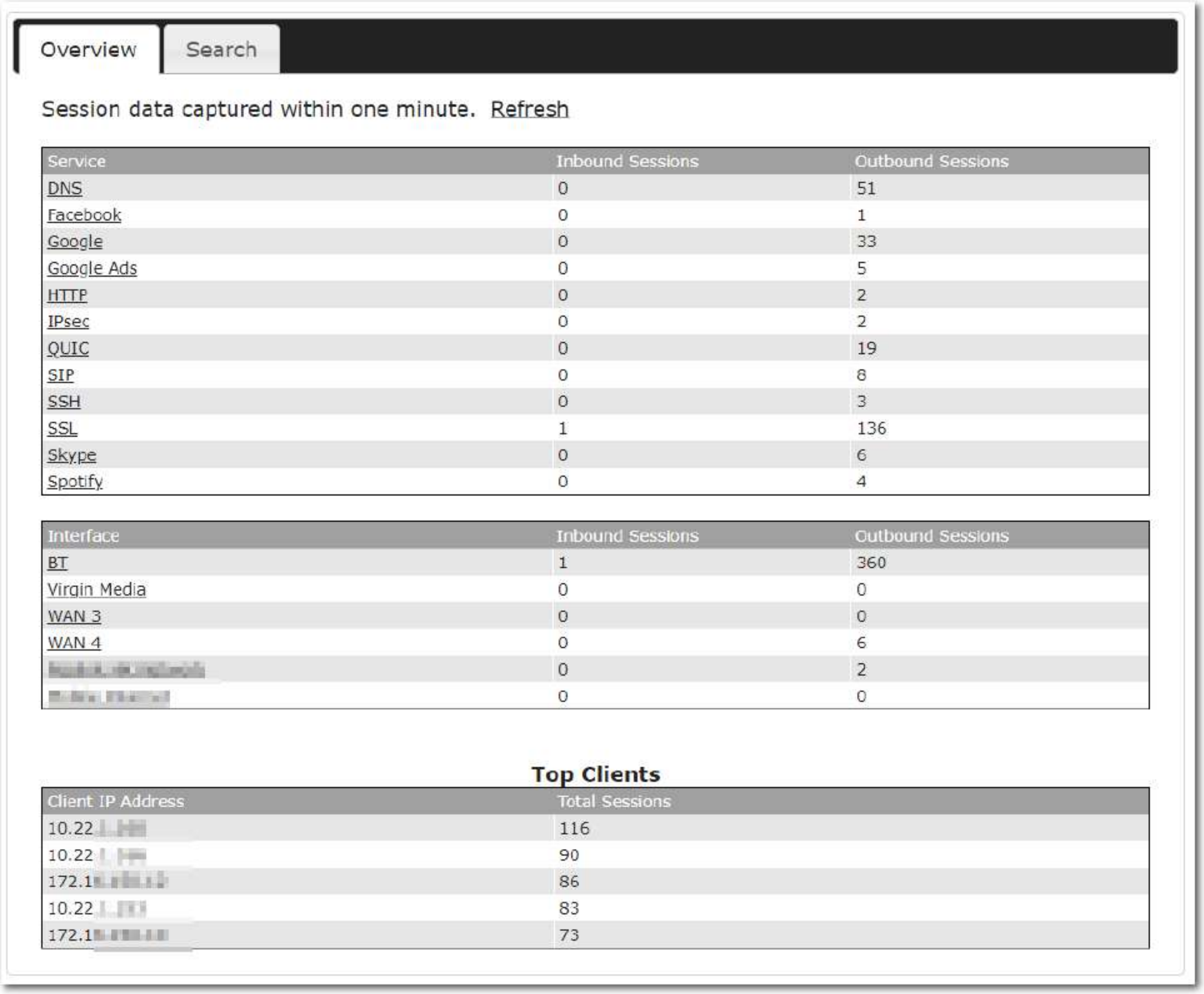
System Information	
Router Name	This is the name specified in the **Router Name** field located at **System>Admin Security**.
Model	This shows the model name and number of this device.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this 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.

13.1.2 Active Sessions

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



Session data captured within one minute. Refresh

Service	Inbound Sessions	Outbound Sessions
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

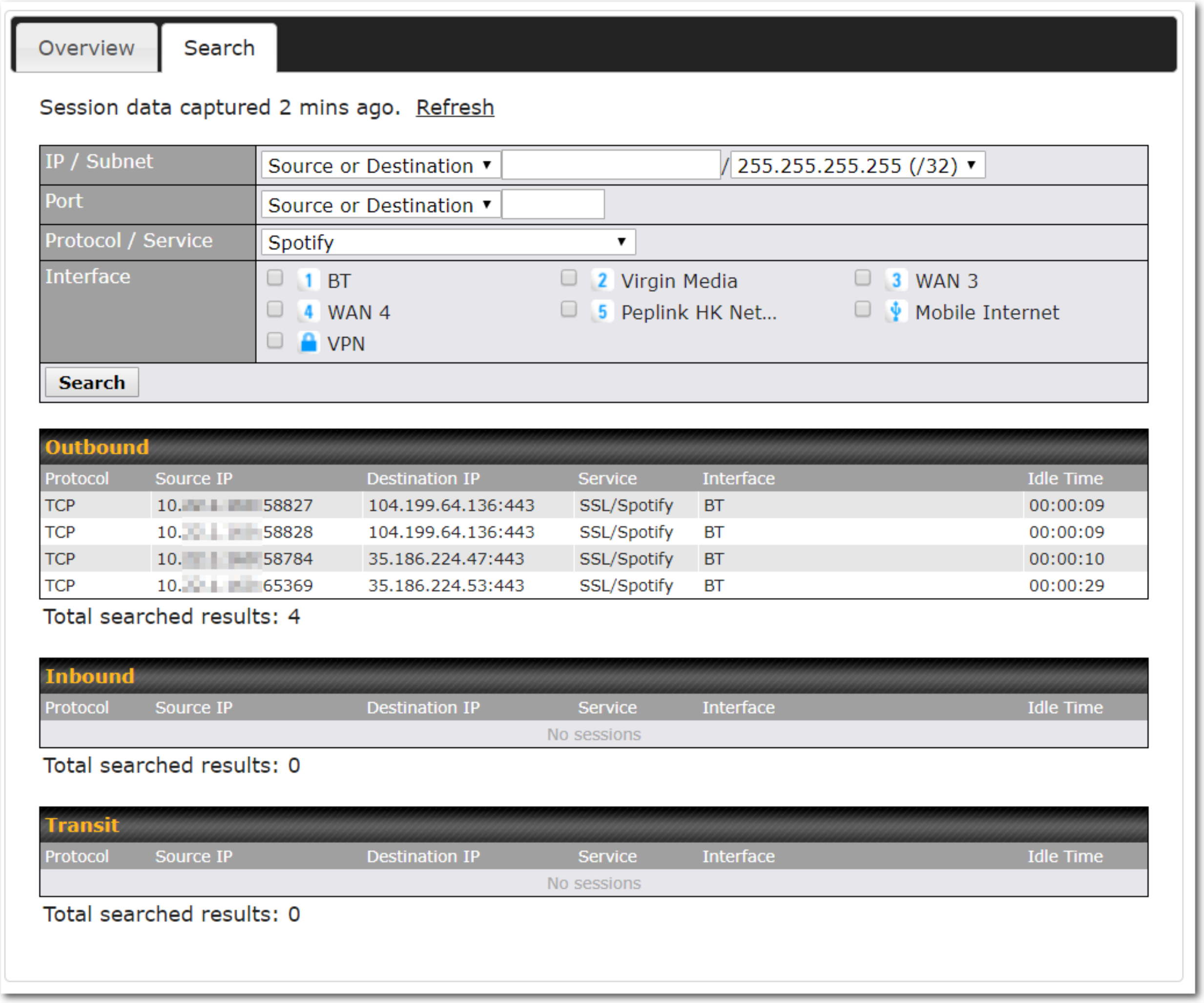
Interface	Inbound Sessions	Outbound Sessions
BT	1	360
Virgin Media	0	0
WAN 3	0	0
WAN 4	0	6
[redacted]	0	2
[redacted]	0	0

Top Clients

Client IP Address	Total Sessions
10.22[redacted]	116
10.22[redacted]	90
172.1[redacted]	86
10.22[redacted]	83
172.1[redacted]	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**.



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

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
TCP	10.[redacted]58827	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.[redacted]58828	104.199.64.136:443	SSL/Spotify	BT	00:00:09
TCP	10.[redacted]58784	35.186.224.47:443	SSL/Spotify	BT	00:00:10
TCP	10.[redacted]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			

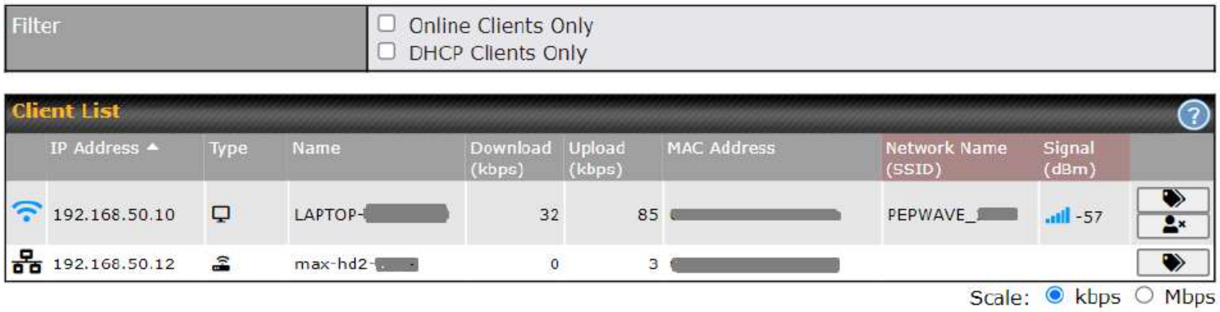
Total searched results: 0

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.

13.1.3 Client List

The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses, type, 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

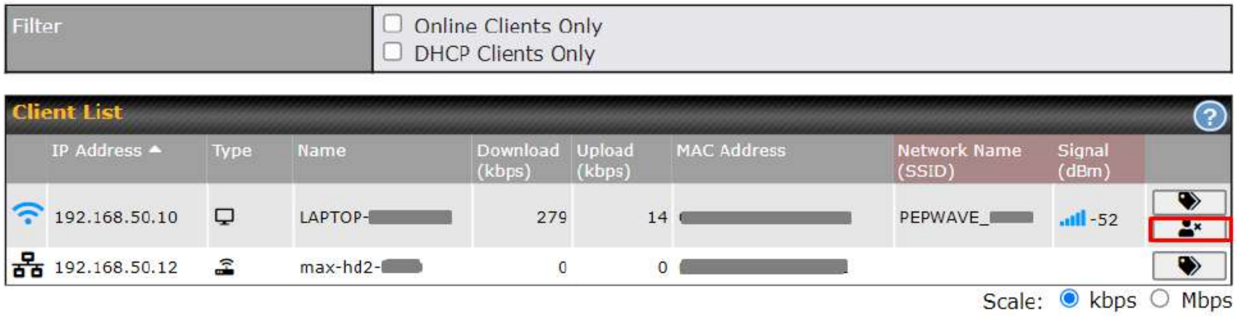
Client List

IP Address ▲	Type	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)	
192.168.50.10		LAPTOP-[redacted]	32	85	[redacted]	PEPWAVE_[redacted]	-57	🏷 👤×
192.168.50.12		max-hd2-[redacted]	0	3	[redacted]			🏷

Scale: ● kbps ○ Mbps

If the PPTP server SpeedFusion^{TM}, 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.



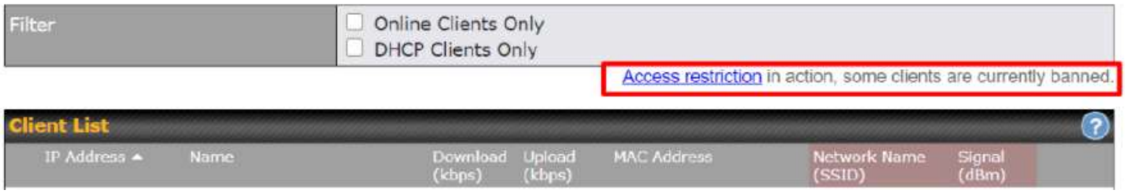
Filter	□ Online Clients Only □ DHCP Clients Only

Client List

IP Address ▲	Type	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)	
192.168.50.10		LAPTOP-[redacted]	279	14	[redacted]	PEPWAVE_[redacted]	-52	🏷 👤×
192.168.50.12		max-hd2-[redacted]	0	0	[redacted]			🏷

Scale: ● kbps ○ Mbps

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



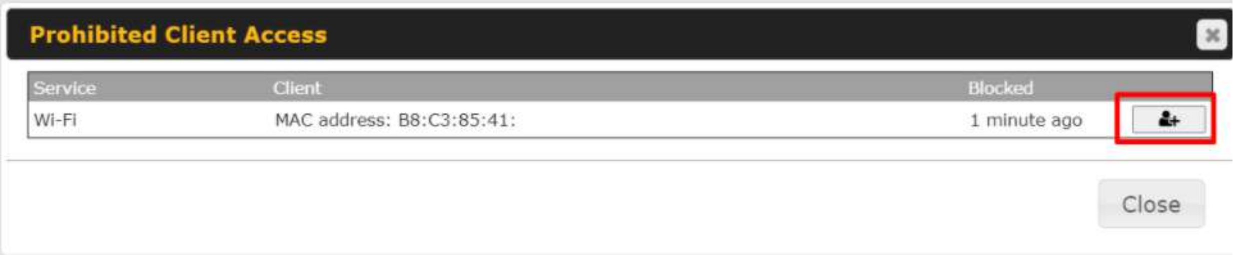
Filter	□ Online Clients Only □ DHCP Clients Only

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.

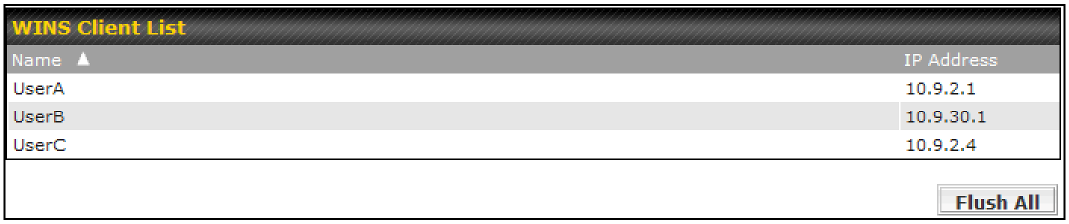


Prohibited Client Access

Service	Client	Blocked	
Wi-Fi	MAC address: B8:C3:85:41:	1 minute ago	

13.1.4 WINS Clients

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



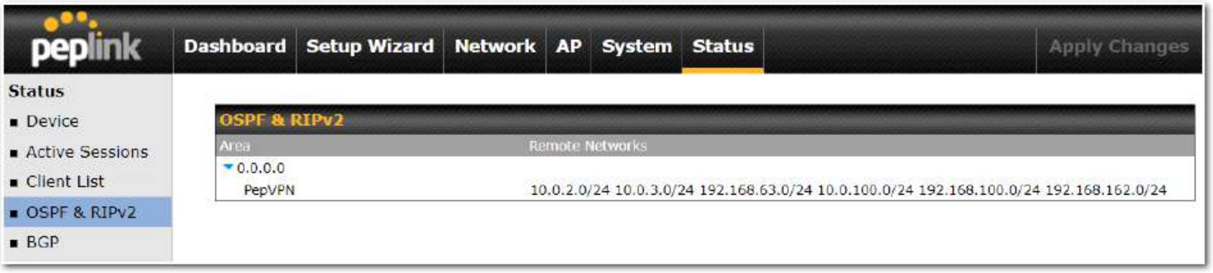
WINS Client List

Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4

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

13.1.5 OSPF & RIPv2

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

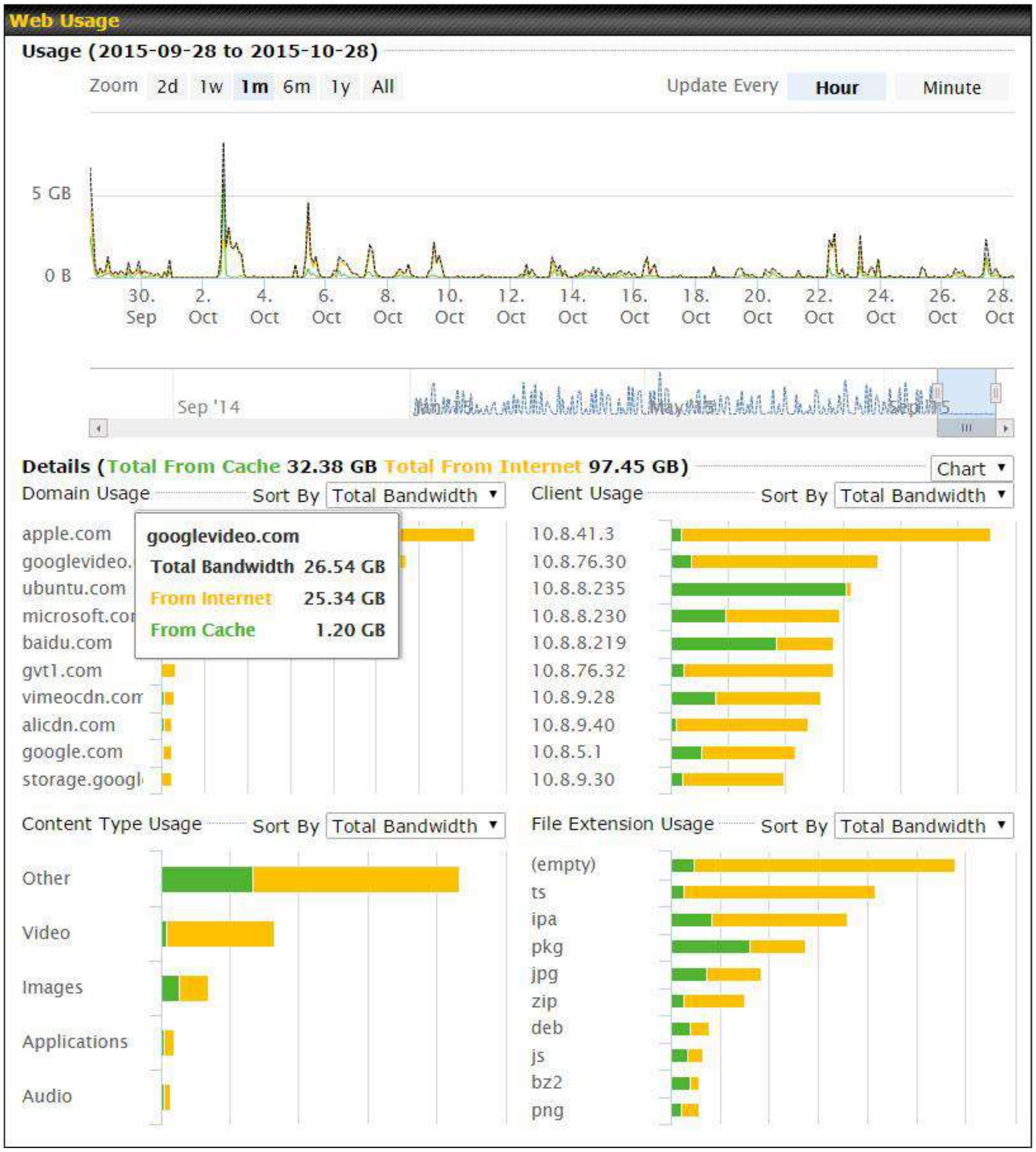


OSPF & RIPv2

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

13.1.6 MediaFast

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



Web Usage

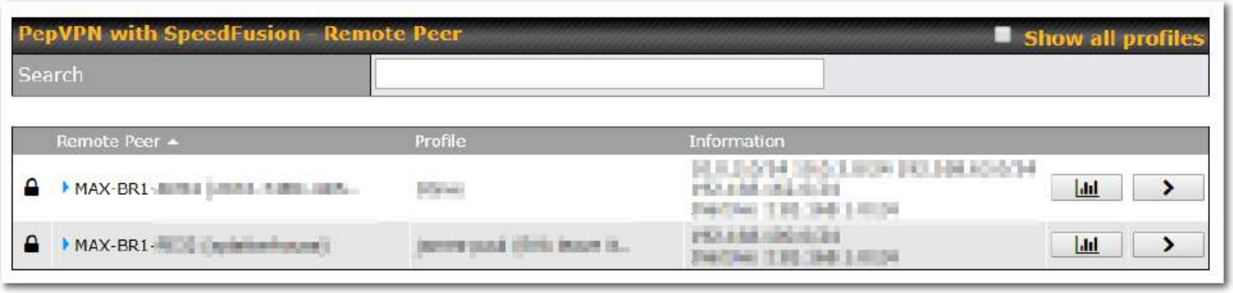
Usage (2015-09-28 to 2015-10-28)

Details (Total From Cache 32.38 GB Total From Internet 97.45 GB)

googlevideo.com
Total Bandwidth 26.54 GB
From Internet 25.34 GB
From Cache 1.20 GB

13.1.7 PepVPN / SpeedFusion Status

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



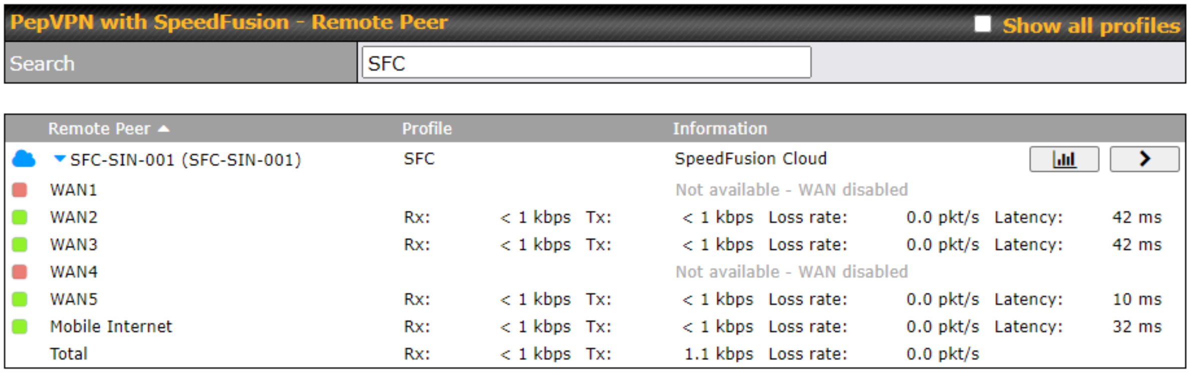
PepVPN with SpeedFusion - Remote Peer

□ Show all profiles

Search

Remote Peer ▲	Profile	Information		
🔒 ▸ MAX-BR1-[redacted]	[redacted]	[redacted]	📊	>
🔒 ▸ MAX-BR1-[redacted]	[redacted]	[redacted]	📊	>

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



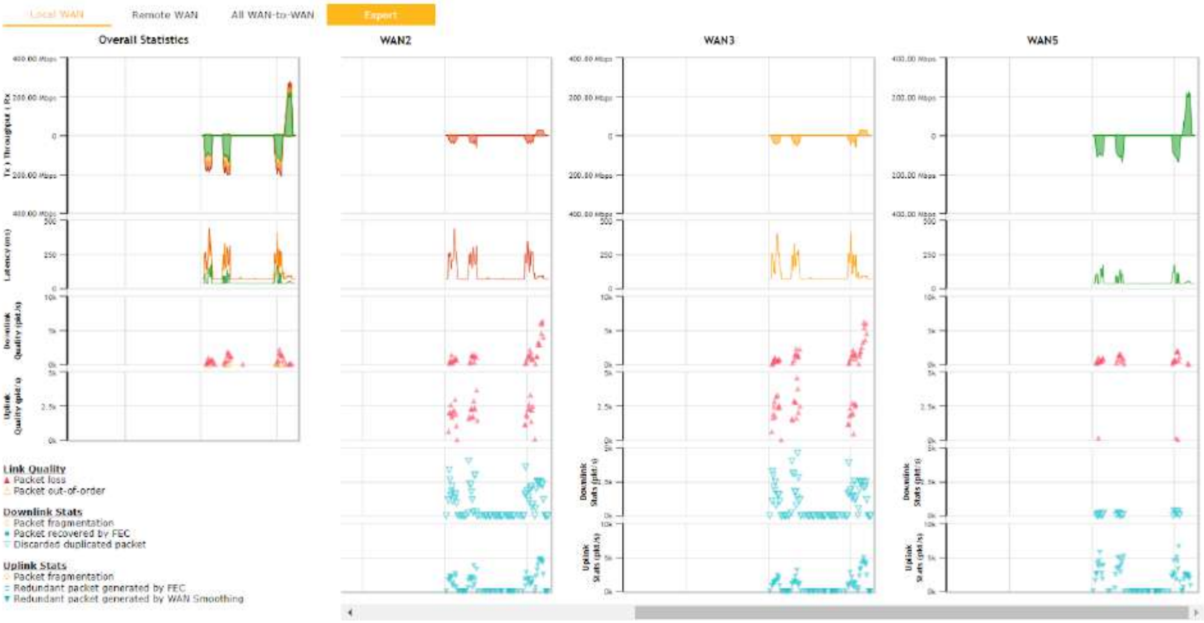
PepVPN with SpeedFusion - Remote Peer

□ Show all profiles

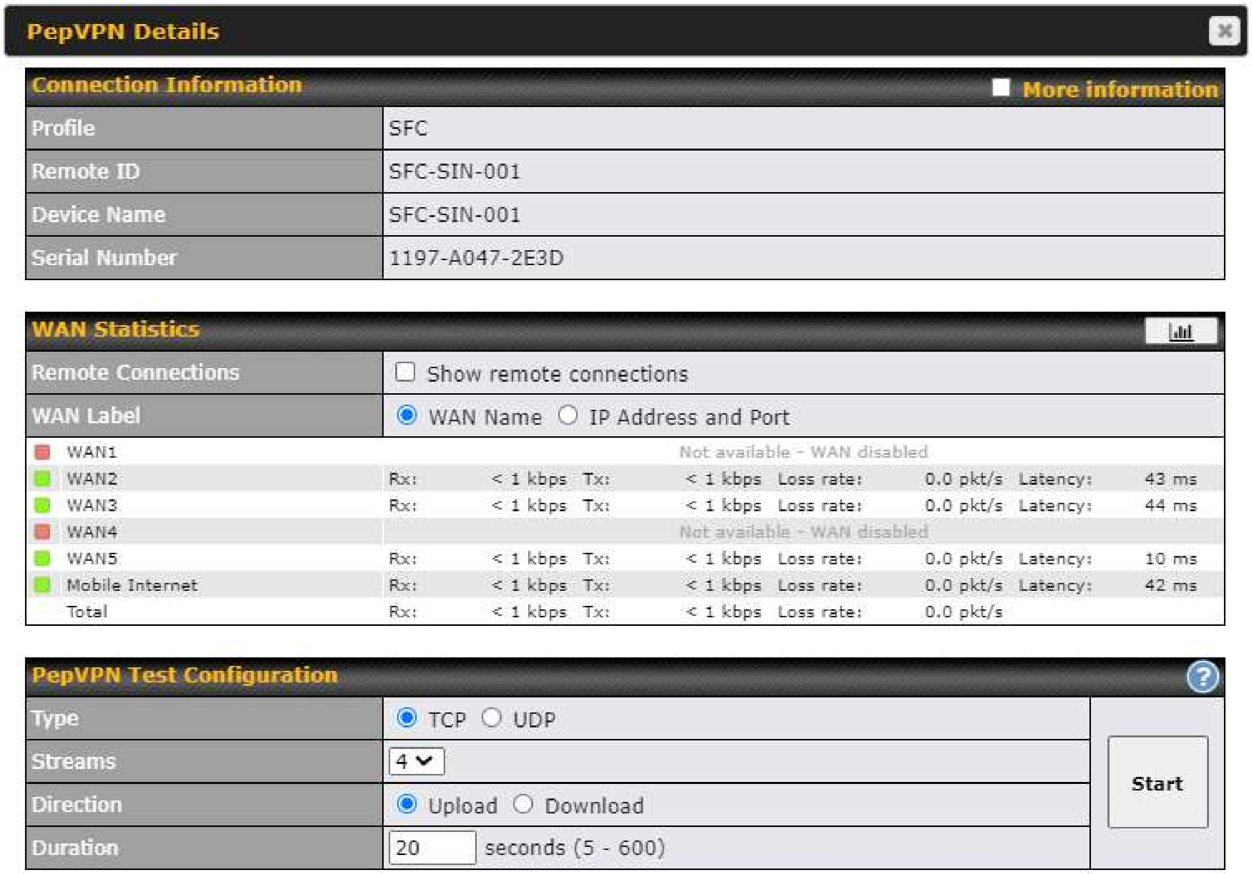
Search SFC

	Remote Peer ▲	Profile			Information				
☁	▾ SFC-SIN-001 (SFC-SIN-001)	SFC			SpeedFusion Cloud			📊	>
🟥	WAN1				Not available - WAN disabled				
🟩	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				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

Remote Connections	□ 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

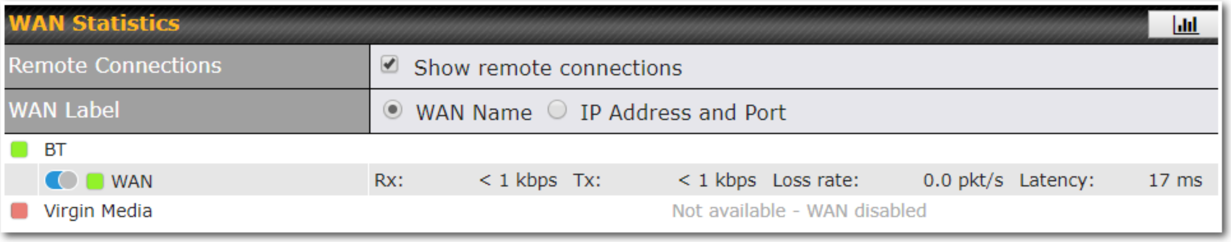
Type	● TCP ○ UDP	Start
Streams	4	
Direction	● Upload ○ Download	
Duration	20 seconds (5 - 600)	

The **connection information** shows the details of the selected PepVPN profile, consisting of the Profile name, **Router ID**, **Router Nam**e 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.

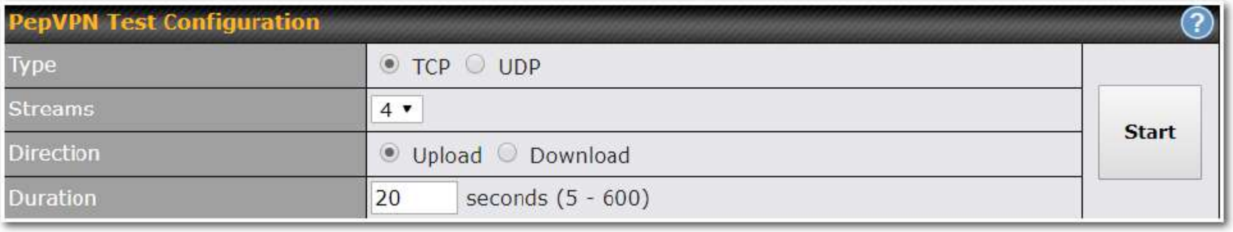


WAN Statistics

Remote Connections	☑ Show remote connections
WAN Label	● WAN Name ○ IP Address and Port

🟩 BT
🟩 WAN Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 17 ms
🟥 Virgin Media 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.



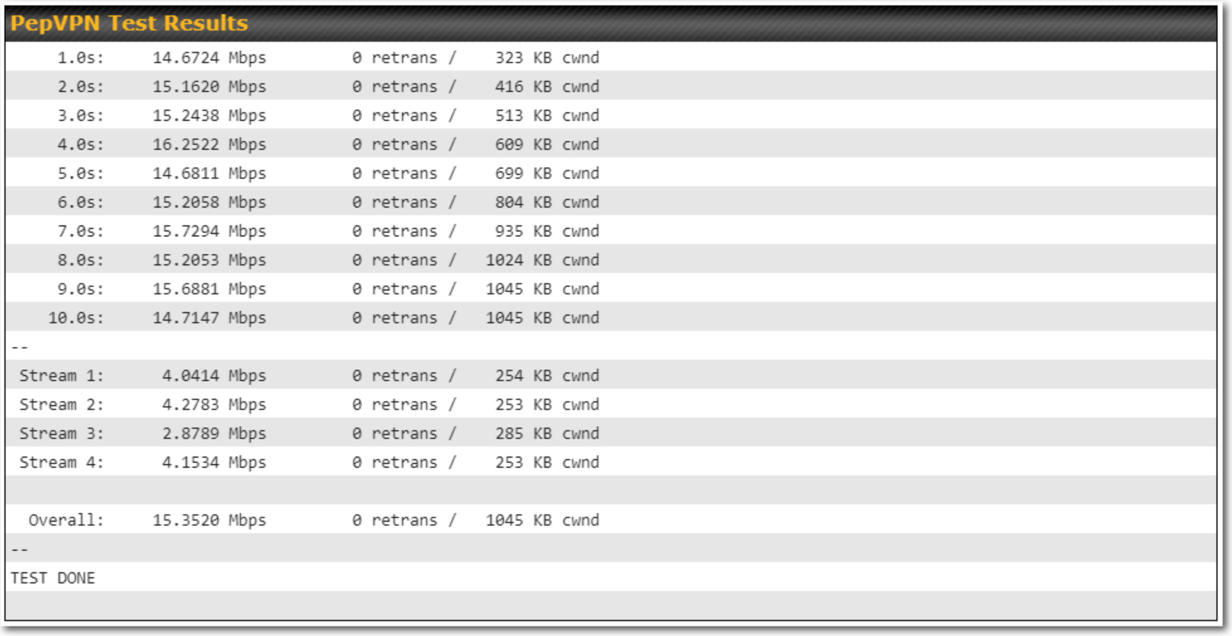
PepVPN Test Configuration

Type	● TCP ○ UDP
Streams	4 ▾
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

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

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

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



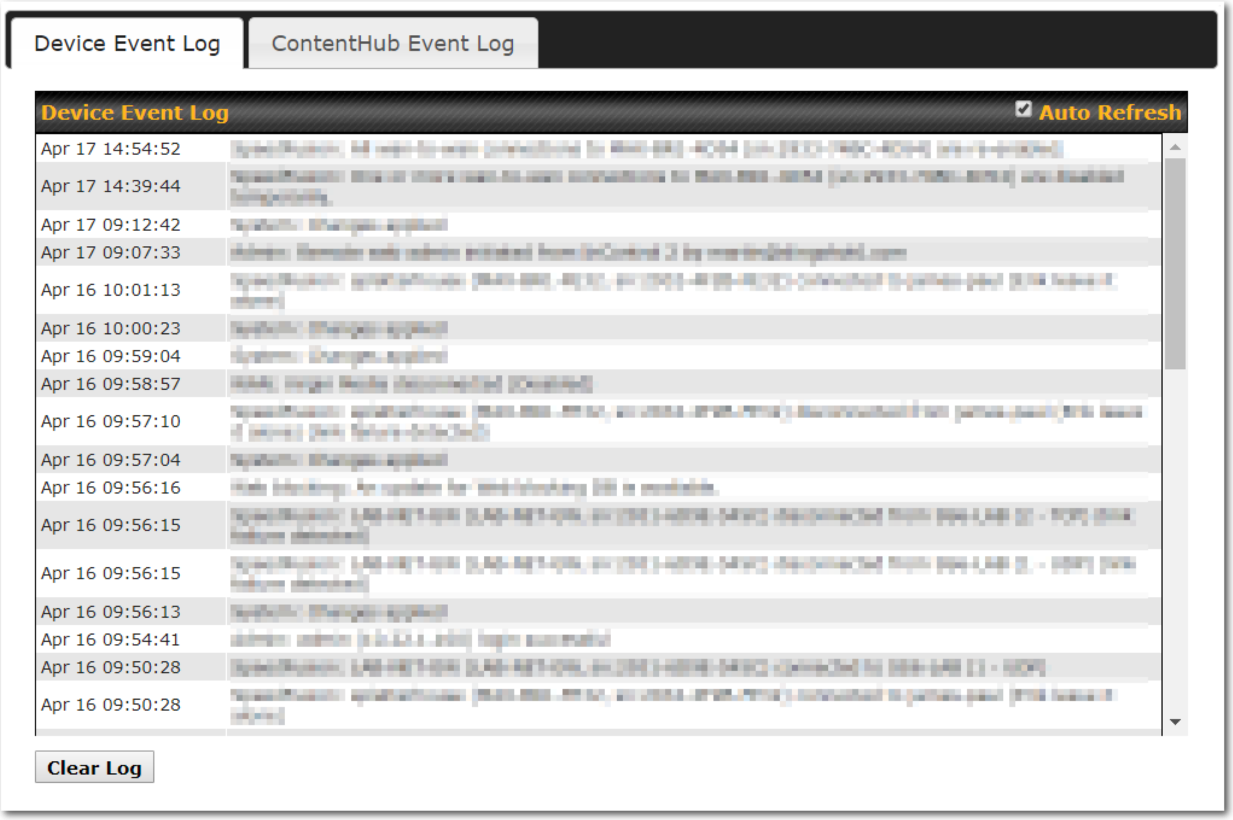
PepVPN Test Results

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

  Overall:     15.3520 Mbps        0 retrans /   1045 KB cwnd
--
TEST DONE
```

13.1.8 Event Log

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

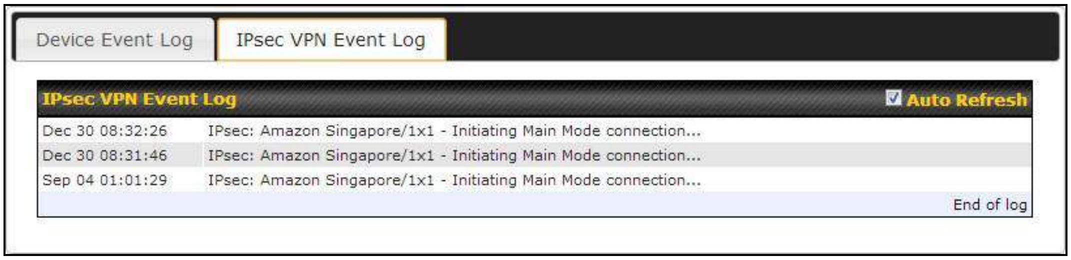
Device Event Log



```
Apr 17 14:54:52   [redacted]
Apr 17 14:39:44   [redacted]
Apr 17 09:12:42   [redacted]
Apr 17 09:07:33   [redacted]
Apr 16 10:01:13   [redacted]
Apr 16 10:00:23   [redacted]
Apr 16 09:59:04   [redacted]
Apr 16 09:58:57   [redacted]
Apr 16 09:57:10   [redacted]
Apr 16 09:57:04   [redacted]
Apr 16 09:56:16   [redacted]
Apr 16 09:56:15   [redacted]
Apr 16 09:56:15   [redacted]
Apr 16 09:56:13   [redacted]
Apr 16 09:54:41   [redacted]
Apr 16 09:50:28   [redacted]
Apr 16 09:50:28   [redacted]
```

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

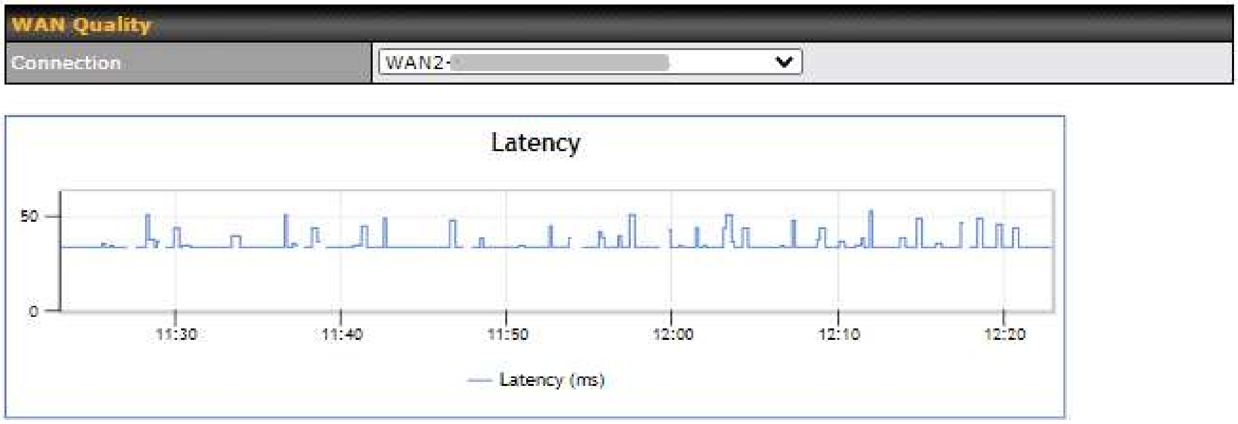


```
Dec 30 08:32:26   IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
Dec 30 08:31:46   IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
Sep 04 01:01:29   IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
                                               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

This section displays a list of events that 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**.

13.2 WAN Quality



WAN Quality	
Connection	WAN2-[redacted]

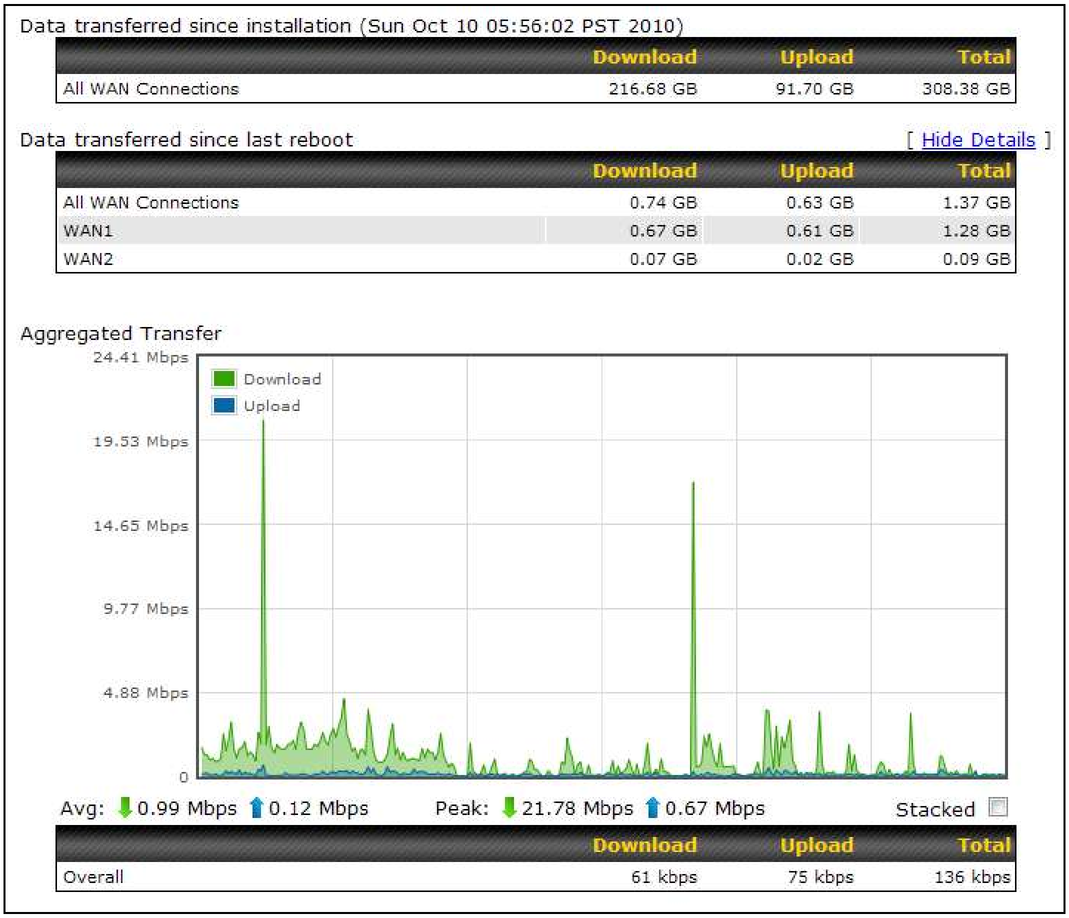
The **Status > WAN Quality** allows to show detailed information about each connected WAN connection.

13.3 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.

13.3.1 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.



Data transferred since installation (Sun Oct 10 05:56:02 PST 2010)

	Download	Upload	Total
All WAN Connections	216.68 GB	91.70 GB	308.38 GB

Data transferred since last reboot [Hide Details]

	Download	Upload	Total
All WAN Connections	0.74 GB	0.63 GB	1.37 GB
WAN1	0.67 GB	0.61 GB	1.28 GB
WAN2	0.07 GB	0.02 GB	0.09 GB

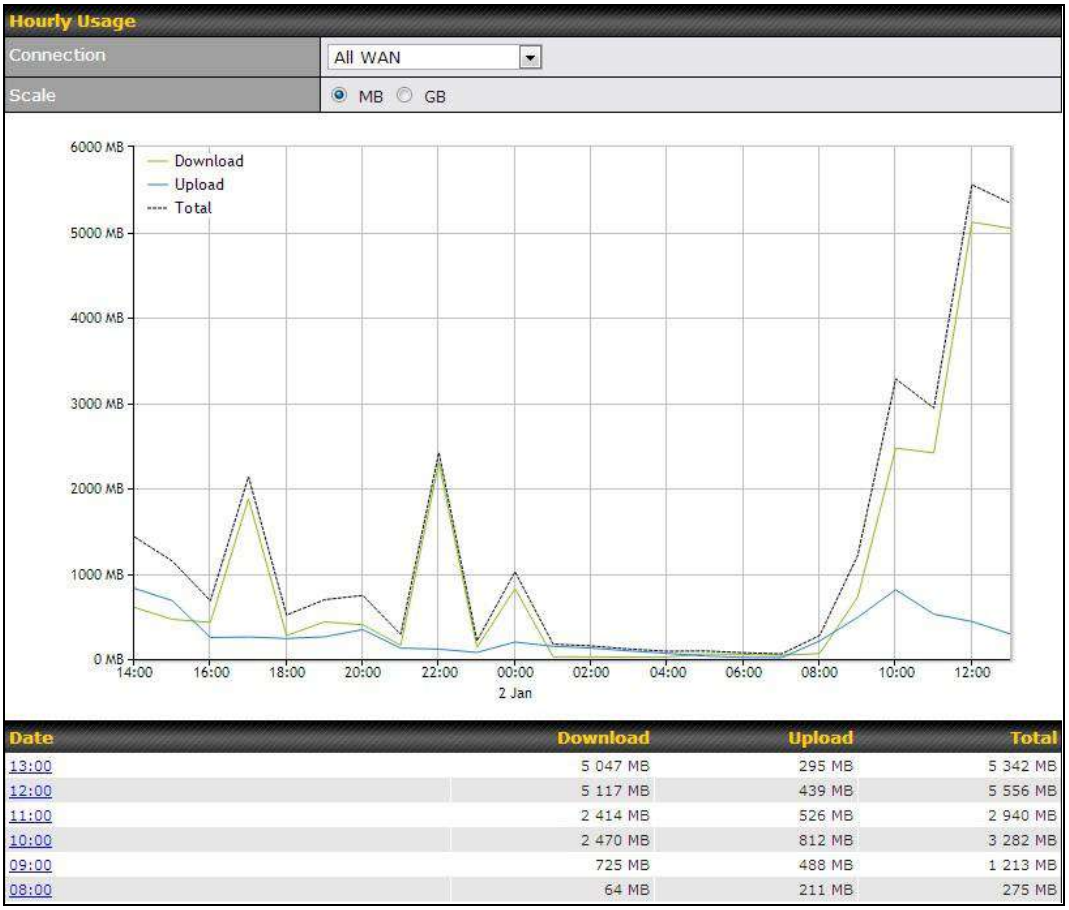
Aggregated Transfer

Avg: ⬇0.99 Mbps ⬆0.12 Mbps Peak: ⬇21.78 Mbps ⬆0.67 Mbps Stacked □

	Download	Upload	Total
Overall	61 kbps	75 kbps	136 kbps

13.3.2 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.



Hourly Usage

Connection	All WAN
Scale	● MB ○ GB

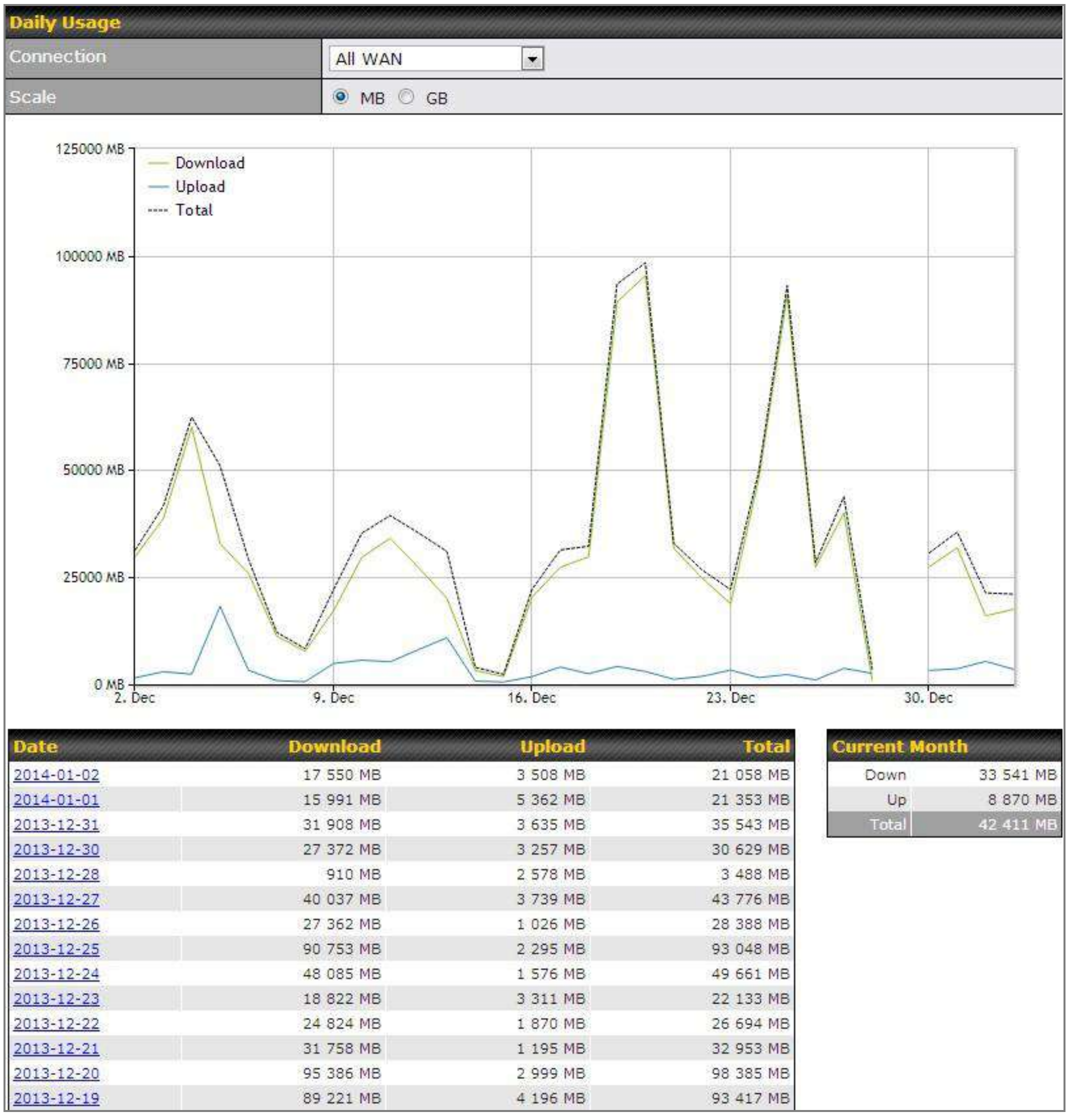
Date	Download	Upload	Total
13:00	5 047 MB	295 MB	5 342 MB
12:00	5 117 MB	439 MB	5 556 MB
11:00	2 414 MB	526 MB	2 940 MB
10:00	2 470 MB	812 MB	3 282 MB
09:00	725 MB	488 MB	1 213 MB
08:00	64 MB	211 MB	275 MB

13.3.3 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**).



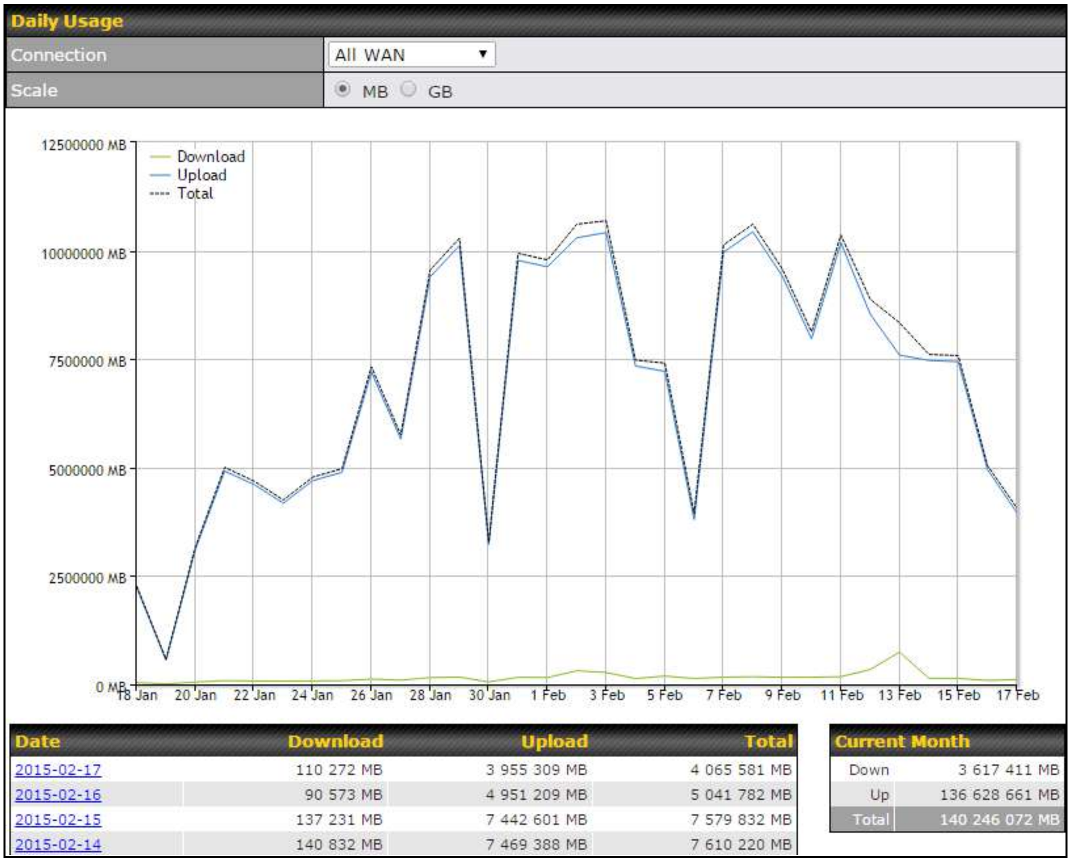
Daily Usage

Connection	All WAN
Scale	● MB ○ GB

Date	Download	Upload	Total
2014-01-02	17 550 MB	3 508 MB	21 058 MB
2014-01-01	15 991 MB	5 362 MB	21 353 MB
2013-12-31	31 908 MB	3 635 MB	35 543 MB
2013-12-30	27 372 MB	3 257 MB	30 629 MB
2013-12-28	910 MB	2 578 MB	3 488 MB
2013-12-27	40 037 MB	3 739 MB	43 776 MB
2013-12-26	27 362 MB	1 026 MB	28 388 MB
2013-12-25	90 753 MB	2 295 MB	93 048 MB
2013-12-24	48 085 MB	1 576 MB	49 661 MB
2013-12-23	18 822 MB	3 311 MB	22 133 MB
2013-12-22	24 824 MB	1 870 MB	26 694 MB
2013-12-21	31 758 MB	1 195 MB	32 953 MB
2013-12-20	95 386 MB	2 999 MB	98 385 MB
2013-12-19	89 221 MB	4 196 MB	93 417 MB

Current Month	
Down	33 541 MB
Up	8 870 MB
Total	42 411 MB

Status



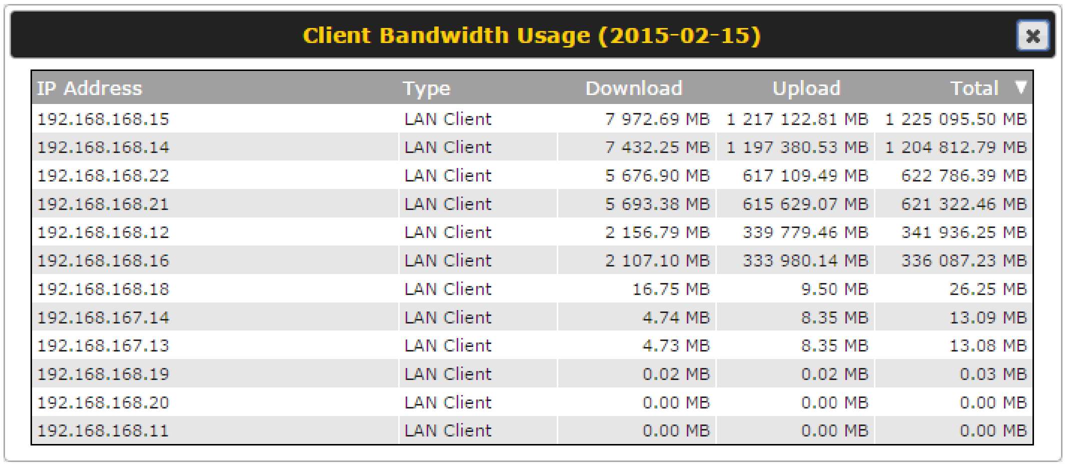
Daily Usage

Connection	All WAN ▾
Scale	● MB ○ GB

Date	Download	Upload	Total
2015-02-17	110 272 MB	3 955 309 MB	4 065 581 MB
2015-02-16	90 573 MB	4 951 209 MB	5 041 782 MB
2015-02-15	137 231 MB	7 442 601 MB	7 579 832 MB
2015-02-14	140 832 MB	7 469 388 MB	7 610 220 MB

Current Month	
Down	3 617 411 MB
Up	136 628 661 MB
Total	140 246 072 MB

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



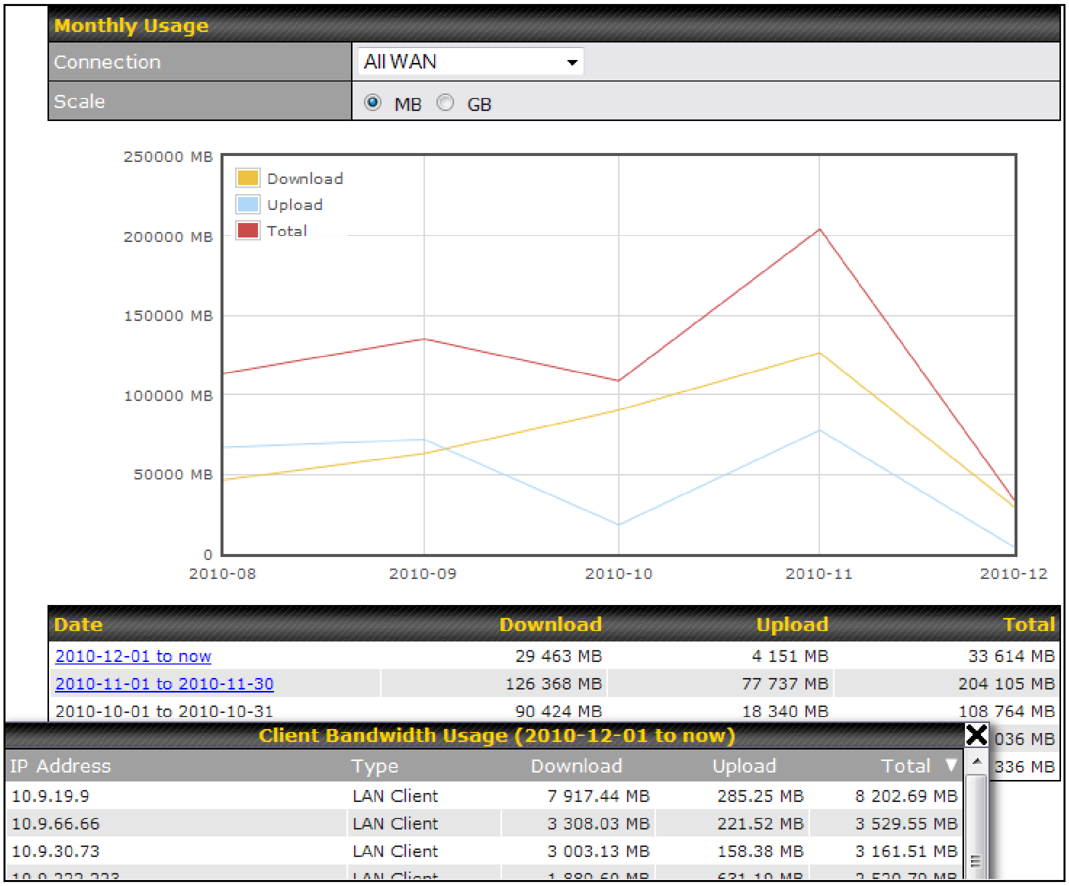
Client Bandwidth Usage (2015-02-15)

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

13.3.4 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**).



Monthly Usage

Connection	All WAN
Scale	● MB ○ GB

Date	Download	Upload	Total
2010-12-01 to now	29 463 MB	4 151 MB	33 614 MB
2010-11-01 to 2010-11-30	126 368 MB	77 737 MB	204 105 MB
2010-10-01 to 2010-10-31	90 424 MB	18 340 MB	108 764 MB
			036 MB
			336 MB

Client Bandwidth Usage (2010-12-01 to now)

IP Address	Type	Download	Upload	Total ▼
10.9.19.9	LAN Client	7 917.44 MB	285.25 MB	8 202.69 MB
10.9.66.66	LAN Client	3 308.03 MB	221.52 MB	3 529.55 MB
10.9.30.73	LAN Client	3 003.13 MB	158.38 MB	3 161.51 MB
10.9.222.223	LAN Client	1 880.60 MB	631.10 MB	2 520.70 MB

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

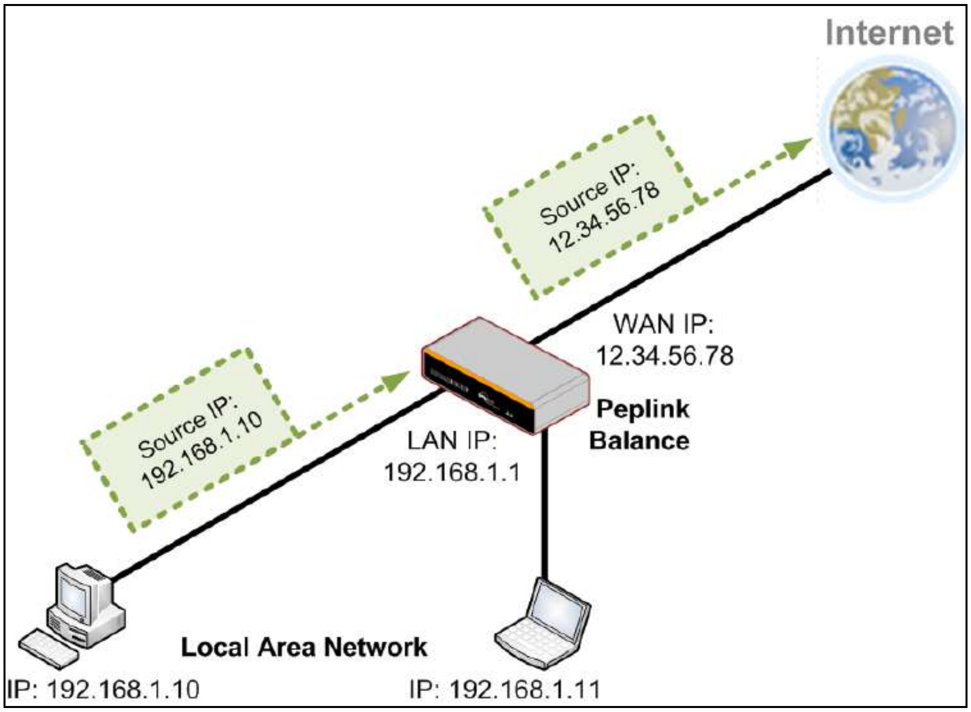
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

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.

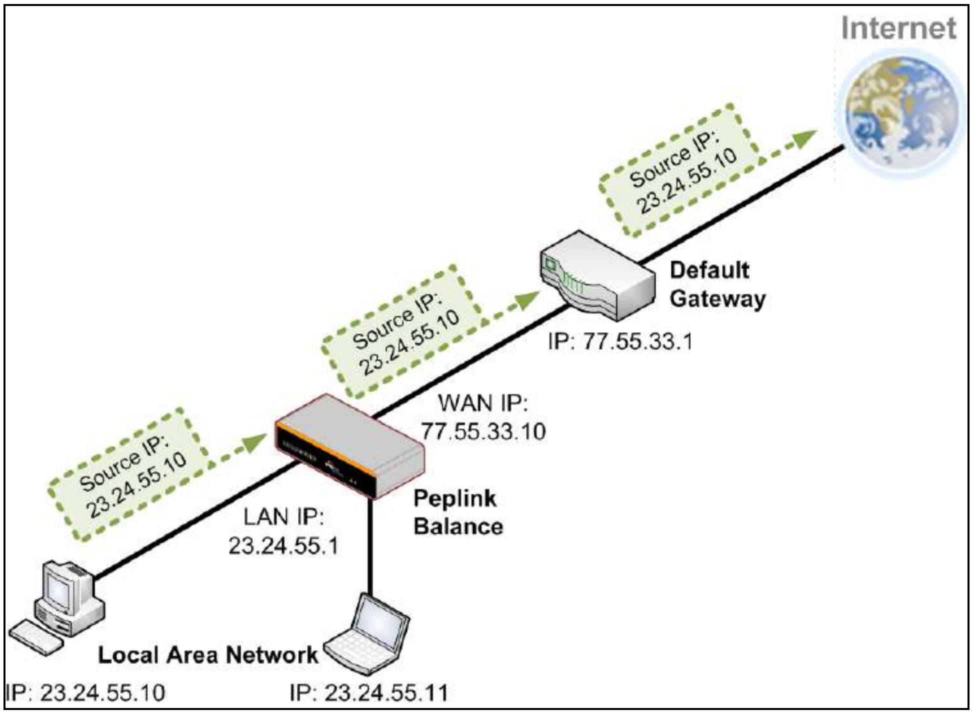
The following figure shows the packet flow in NAT mode:



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:


Internet
Source IP: 23.24.55.10
Source IP: 23.24.55.10
Source IP: 23.24.55.10
Default Gateway
IP: 77.55.33.1
WAN IP: 77.55.33.10
Peplink Balance
LAN IP: 23.24.55.1
Local Area Network
IP: 23.24.55.10
IP: 23.24.55.11

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:

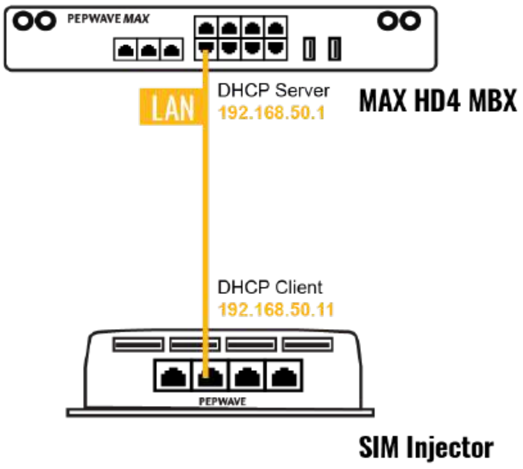
- **User**: admin
- **Password**: admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

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.

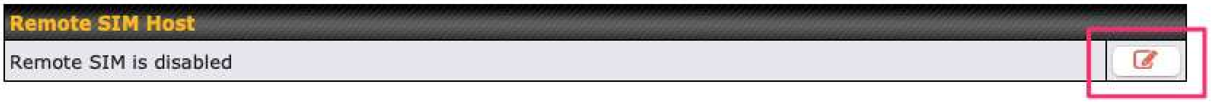
IMPORTANT: SIM cards inserted into SIM Injector must not have a PIN code.

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.

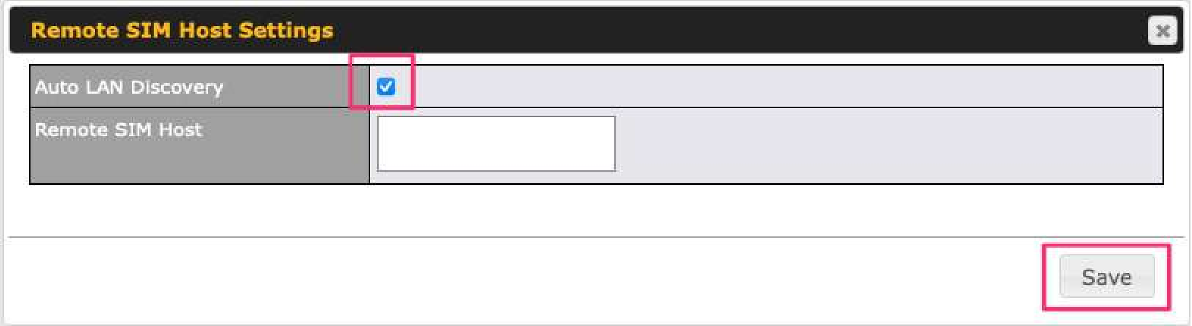
1a. If you are using a Balance cellular router, go to the **Network** tab (top navigation bar).
1b. If you are using a MAX cellular router, go to the **Advanced** tab (top navigation bar).
2. Under **Misc. settings** (left navigation bar) find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.



Remote SIM Host

Remote SIM is disabled

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



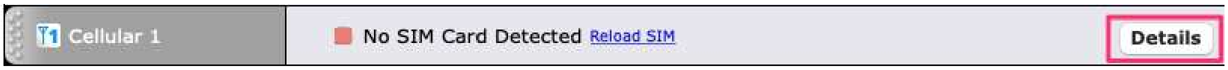
Remote SIM Host Settings

Auto LAN Discovery	☑
Remote SIM Host	

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

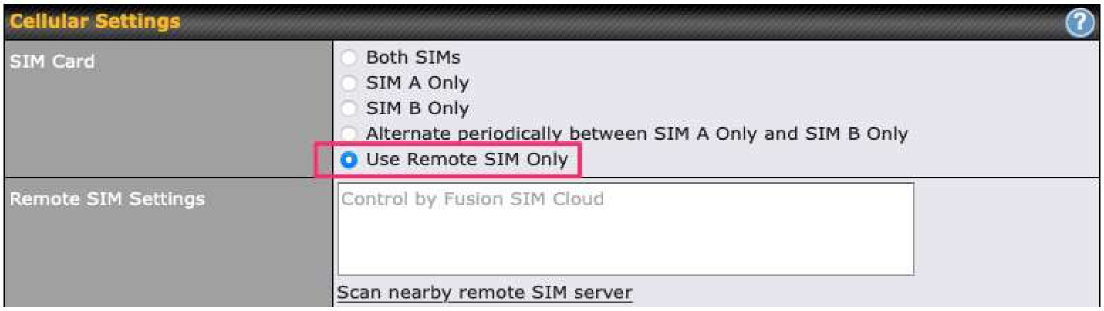
Step 2. Enable RemoteSIM for the selected Cellular interface.

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.



Cellular 1	🟥 No SIM Card Detected Reload SIM	Details

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



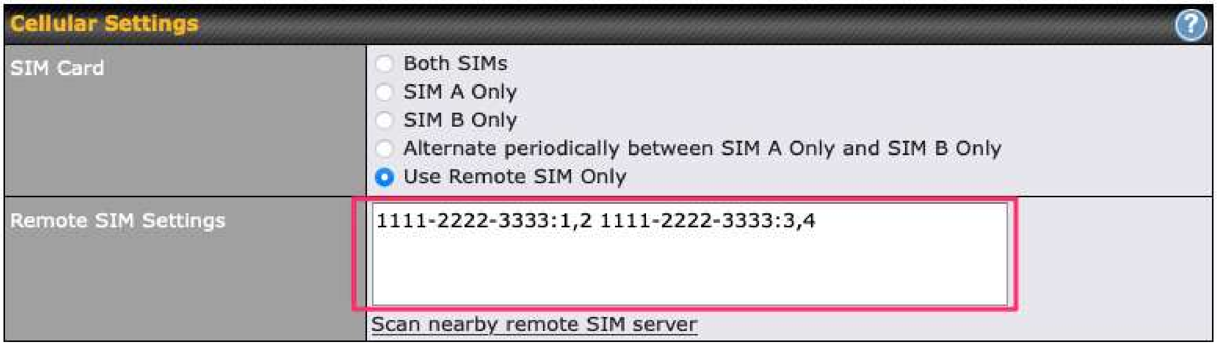
Cellular Settings

SIM Card	○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only
Remote SIM Settings	Control by Fusion SIM Cloud Scan nearby remote SIM server

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).



Cellular Settings

SIM Card
○ Both SIMs
○ SIM A Only
○ SIM B Only
○ Alternate periodically between SIM A Only and SIM B Only
● Use Remote SIM Only

Remote SIM Settings: 1111-2222-3333:1,2 1111-2222-3333:3,4

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

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

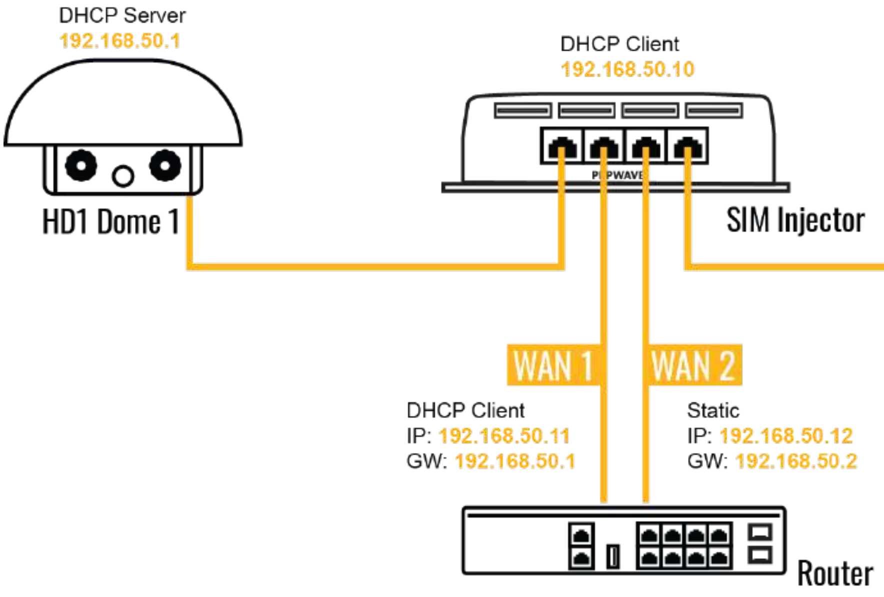
Step 3. (Optional) Custom SIM cards settings.

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.

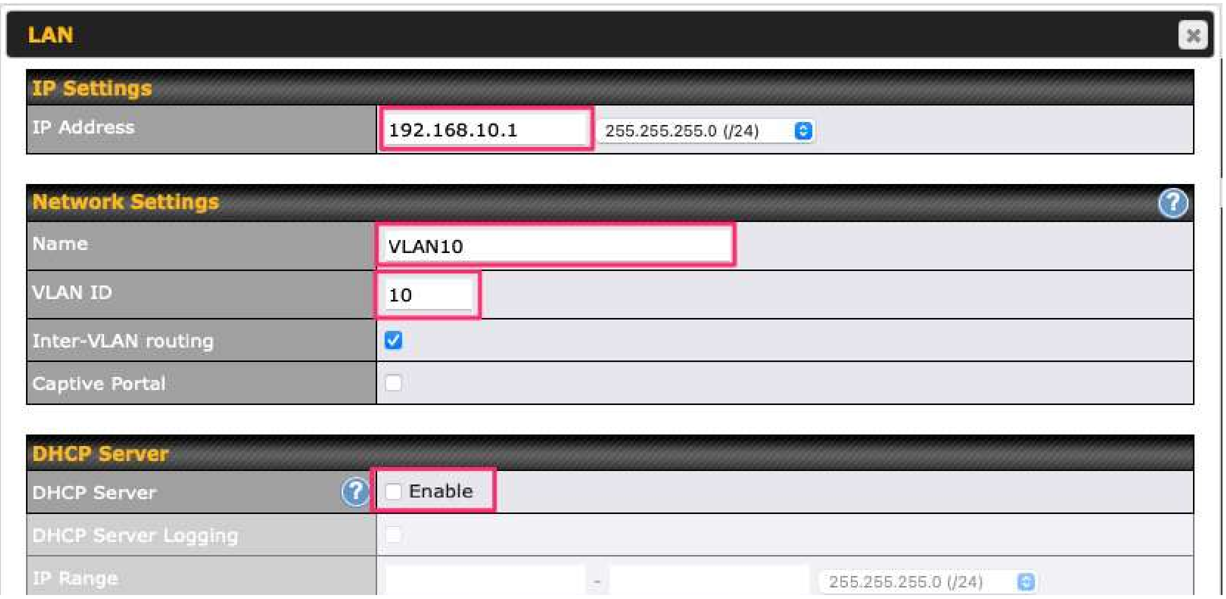
- HD Dome 1 should act as a DHCP server.
- HD Dome 2 should be configured to have a static IP address with DHCP disabled.
- Both routers should be in the same subnet (e.g. 192.168.50.1 and 192.168.50.2).

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

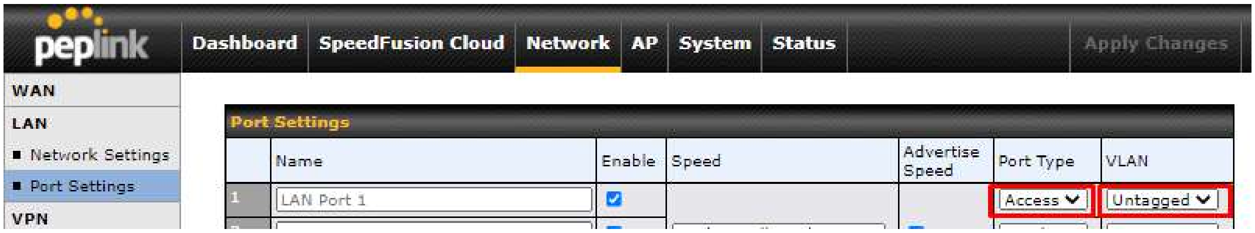
IP Settings	
IP Address	192.168.10.1 255.255.255.0 (/24)

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	☑			Access	Untagged

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

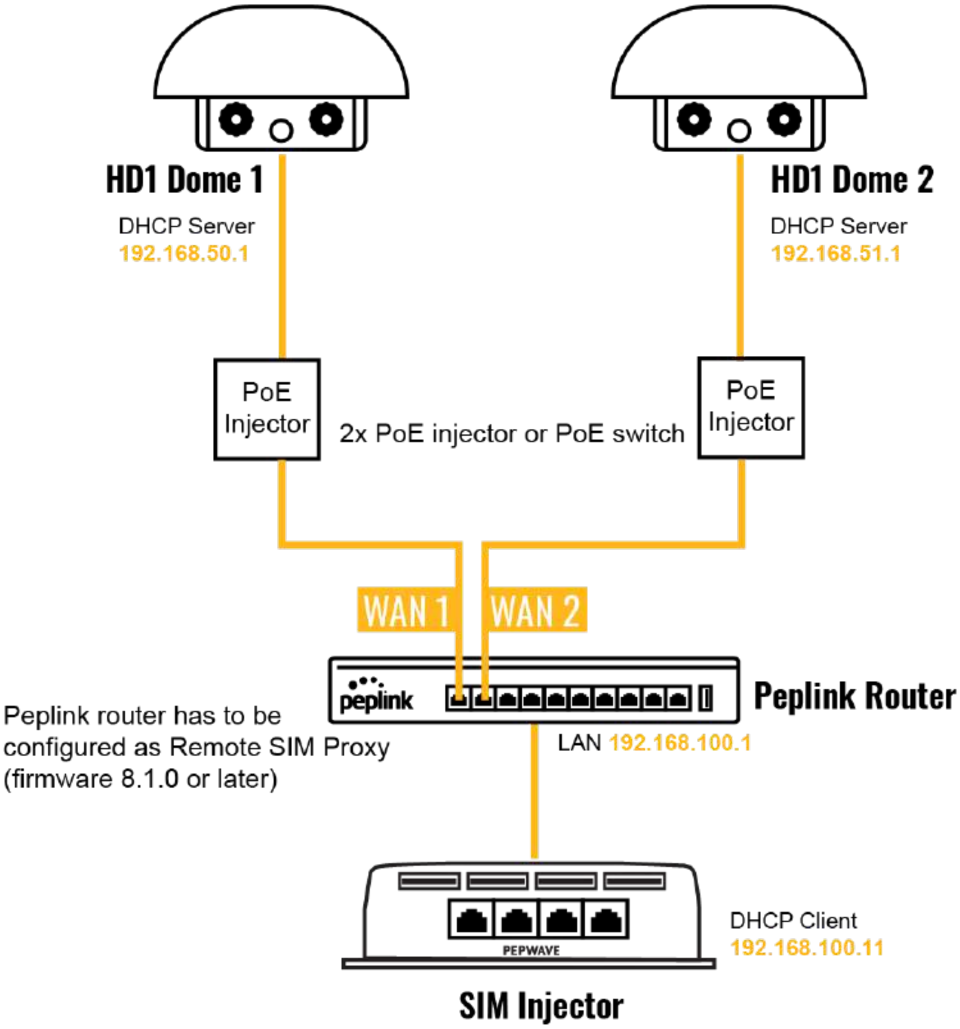
Configuration requirements for the main Router

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.

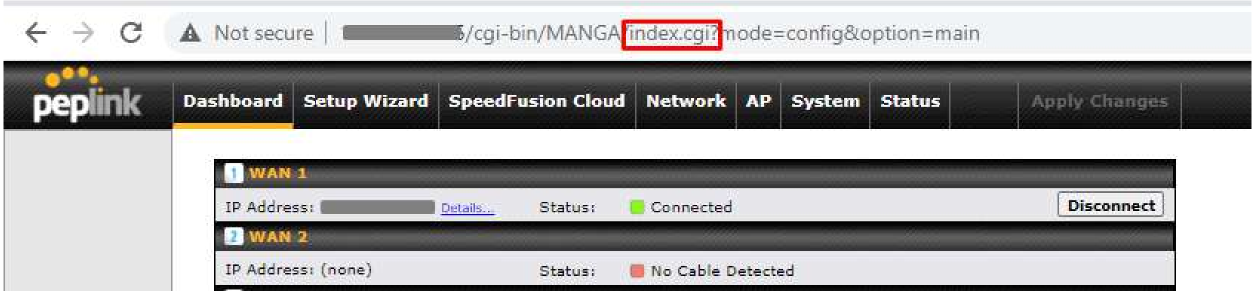
Main Router configuration

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.



Not secure | [redacted]/cgi-bin/MANGA/index.cgi?mode=config&option=main

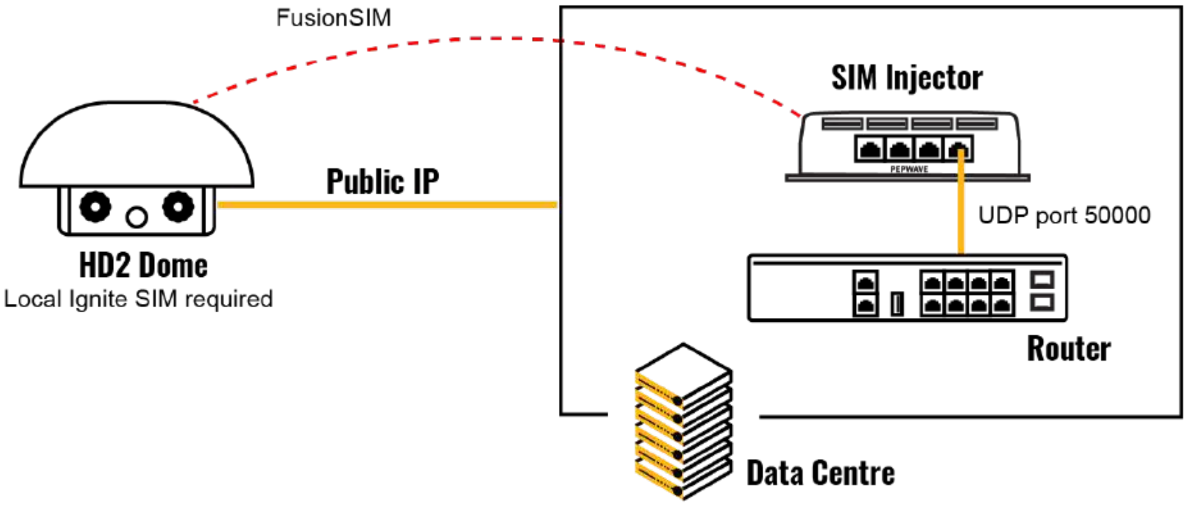
1 WAN 1
IP Address: [redacted] Details... Status: 🟩 Connected

2 WAN 2
IP Address: (none) Status: 🟥 No Cable Detected

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:

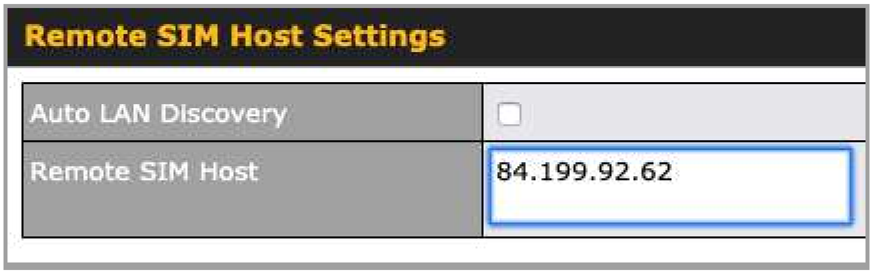
- Cellular router communicates with the SIM Injector via UDP port 50000. Therefore this port must be reachable via public IP over the Internet.
- The one way latency between the cellular router and the SIM Injector should be **up to 250 ms.** A higher latency may lead to stability issues.
- The cellular 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:

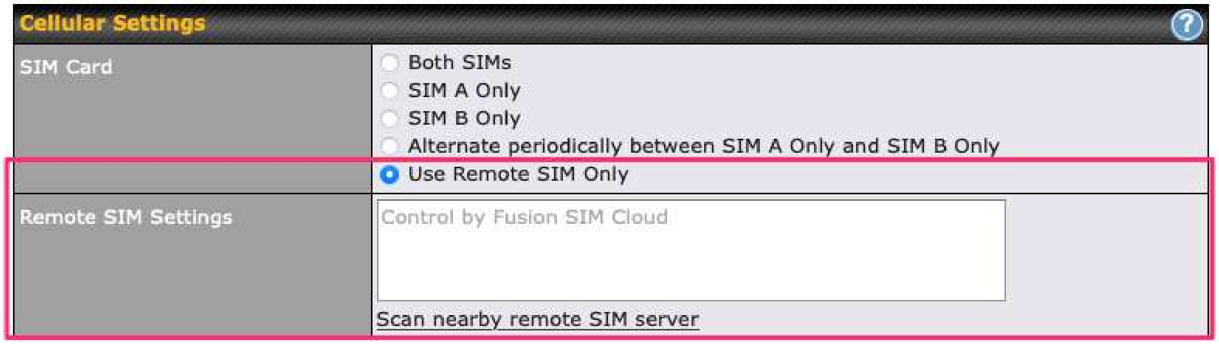
- Do NOT check **Auto LAN Discovery**.
- Adding a SIM Injector serial number to the **Remote SIM Host** field is a mistake!

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.

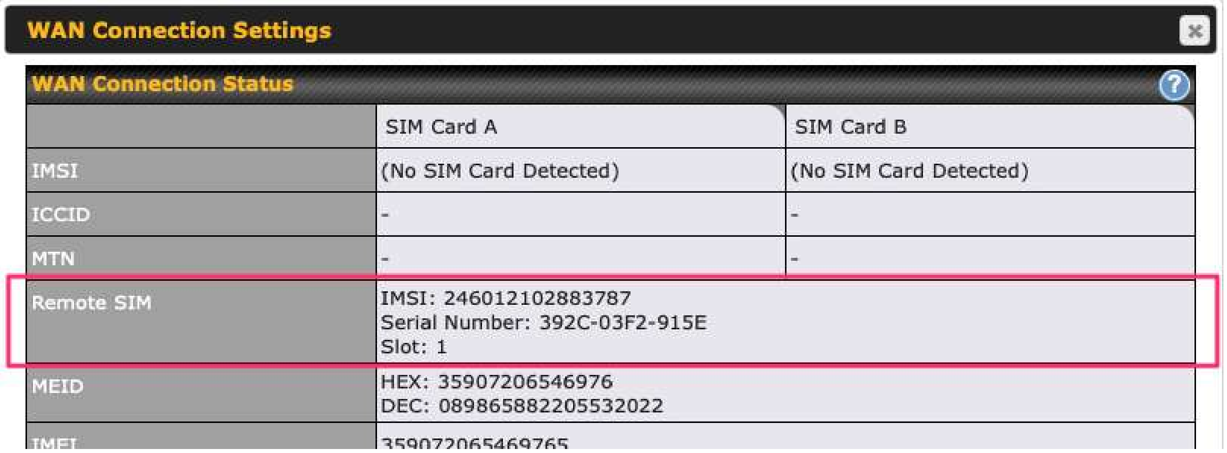


Cellular Settings

SIM Card	○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only
	● Use Remote SIM Only
Remote SIM Settings	Control by Fusion SIM Cloud Scan nearby remote SIM server

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).



WAN Connection Settings

WAN Connection Status

	SIM Card A	SIM Card B
IMSI	(No SIM Card Detected)	(No SIM Card Detected)
ICCID	-	-
MTN	-	-
Remote SIM	IMSI: 246012102883787 Serial Number: 392C-03F2-915E Slot: 1	
MEID	HEX: 35907206546976 DEC: 089865882205532022	
IMEI	359072065469765	

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.

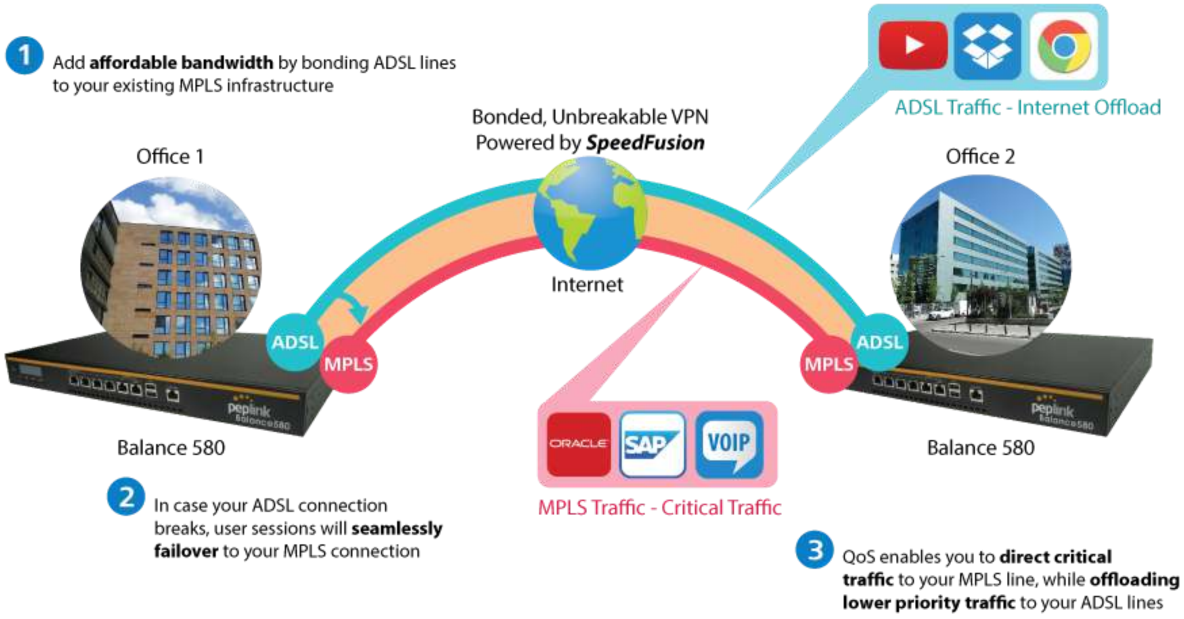
Below are typical deployments for using our Balance routers to replace expensive MPLS connections with commodity connections, such as ADSL, 3G, and 4G LTE links.

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.

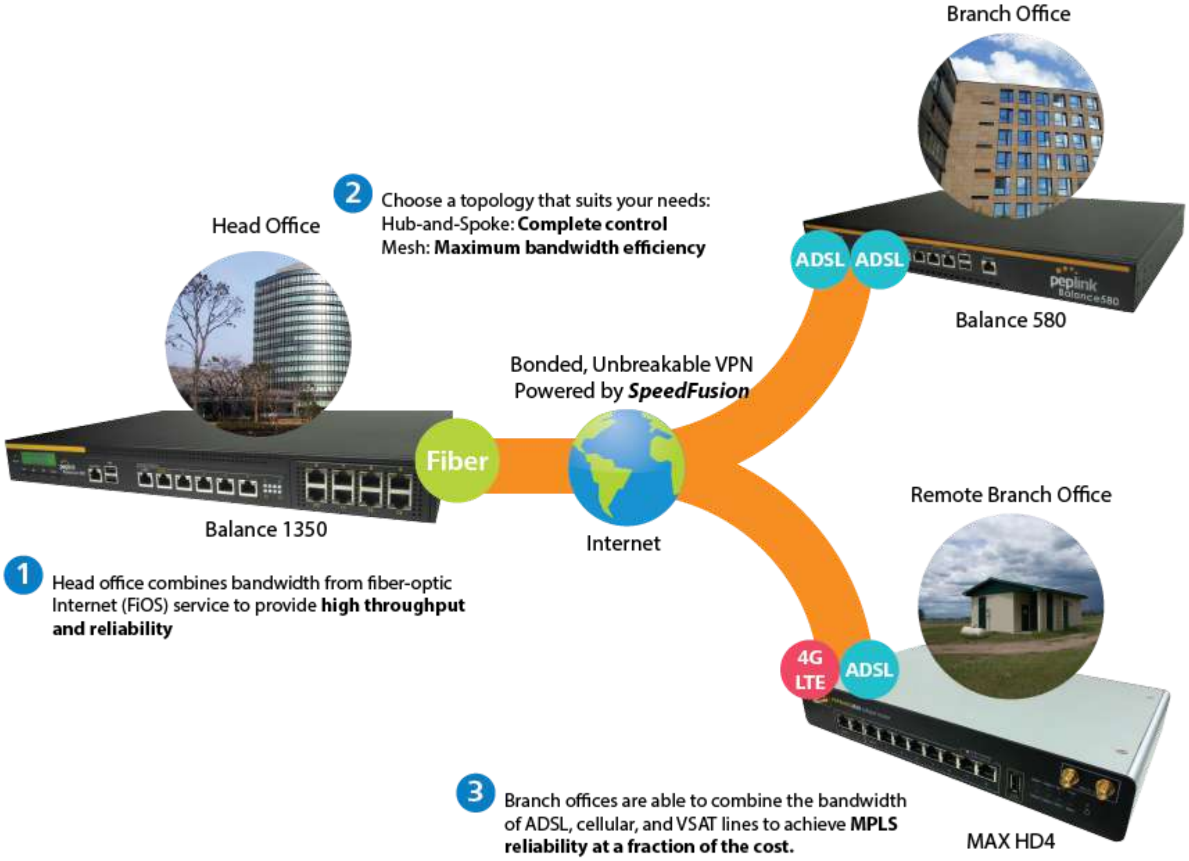
Our MediaFast series routers have been helping students at many education institutions to enjoy uninterrupted learning

Option 1: MPLS Supplement


1 Add **affordable bandwidth** by bonding ADSL lines to your existing MPLS infrastructure
Bonded, Unbreakable VPN
Powered by ***SpeedFusion***
ADSL Traffic - Internet Offload
Office 1
Office 2
Internet
ADSL
MPLS
ADSL
MPLS
Balance 580
Balance 580
ORACLE
SAP
VOIP
MPLS Traffic - Critical Traffic
2 In case your ADSL connection breaks, user sessions will **seamlessly failover** to your MPLS connection
3 QoS enables you to **direct critical traffic** to your MPLS line, while **offloading lower priority traffic** to your ADSL lines

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



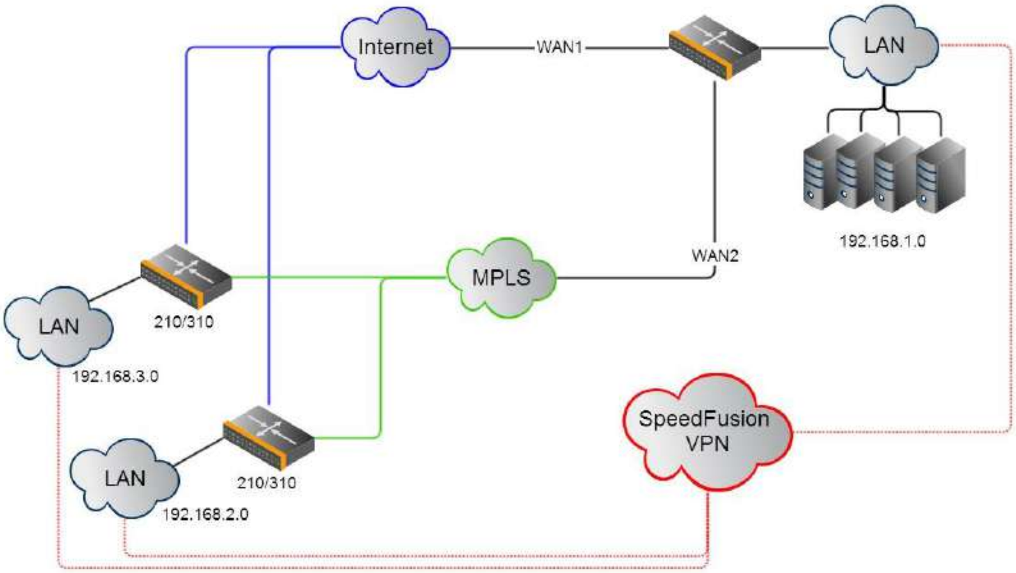
2 Choose a topology that suits your needs:
Hub-and-Spoke: **Complete control**
Mesh: **Maximum bandwidth efficiency**

1 Head office combines bandwidth from fiber-optic Internet (FiOS) service to provide **high throughput and reliability**

3 Branch offices are able to combine the bandwidth of ADSL, cellular, and VSAT lines to achieve **MPLS reliability at a fraction of the cost.**

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

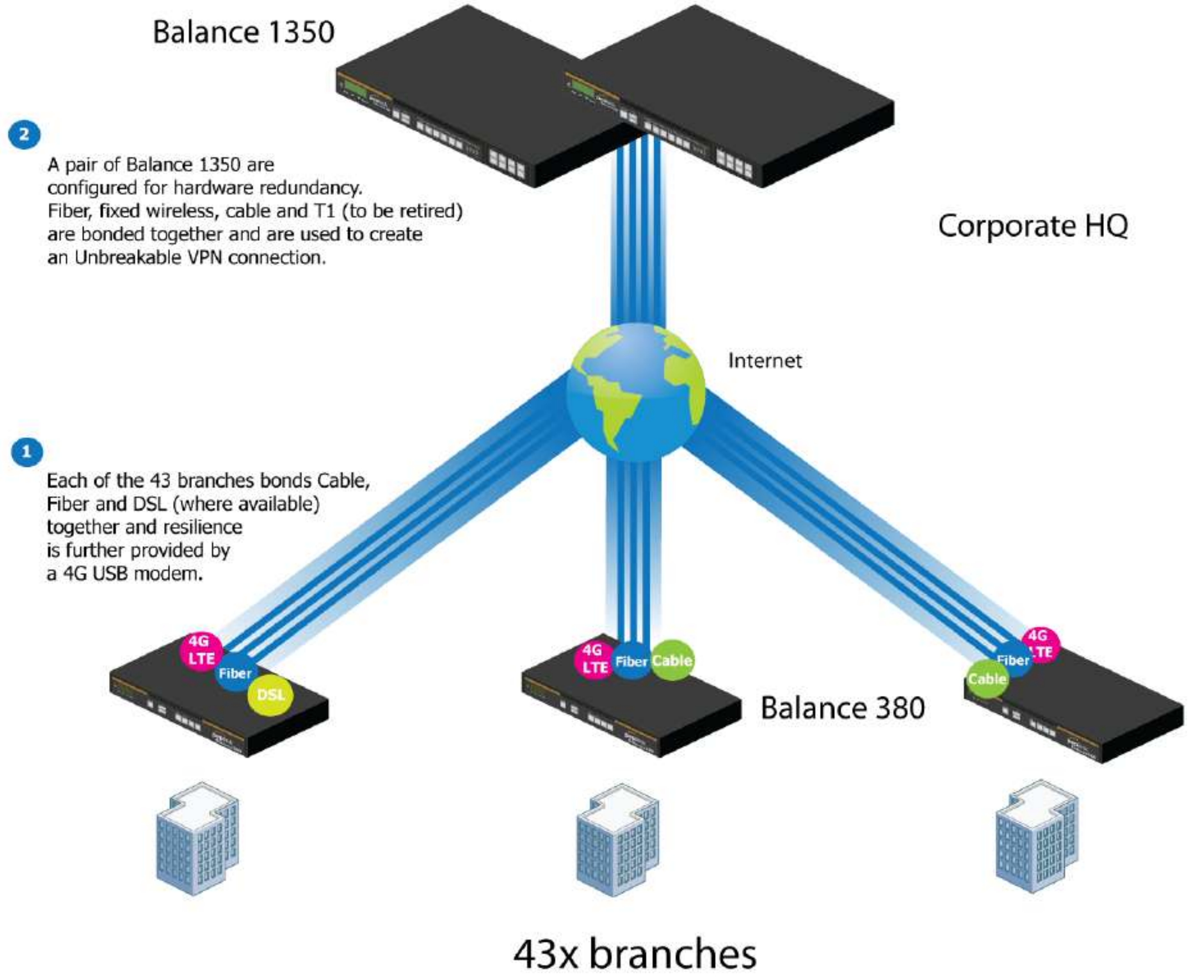
- 4x the bandwidth
- Seamless hardware failover
- Highly available network due to WAN diversity
- Highly cost-effective compared to competing solutions
- Easy resilience achieved by adding 4G USB modems

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.

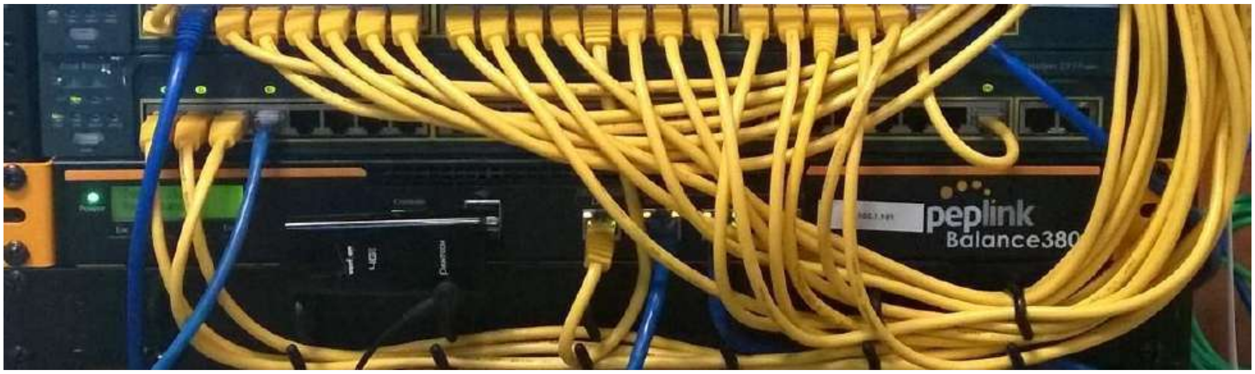
Quick Deployment and Unbreakable Connectivity

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.


Balance 1350
2
A pair of Balance 1350 are configured for hardware redundancy. Fiber, fixed wireless, cable and T1 (to be retired) are bonded together and are used to create an Unbreakable VPN connection.
Corporate HQ
Internet
1
Each of the 43 branches bonds Cable, Fiber and DSL (where available) together and resilience is further provided by a 4G USB modem.
4G LTE
Fiber
DSL
4G LTE
Fiber
Cable
Balance 380
4G LTE
Fiber
Cable
43x branches

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

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



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

PLUSS

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

Adding to Life
pluss
400 USERS
VoIP 290 EndPoints
30+ SITES

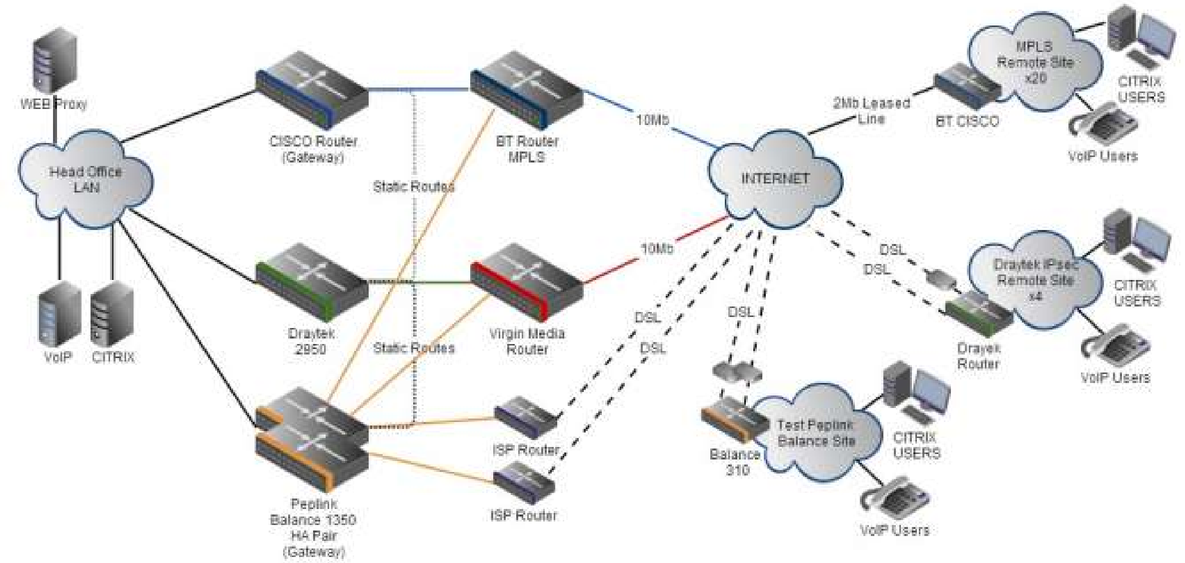
"It saves us money, is easy to manage and grows with us effortlessly."

Steve Taylor - Pluss

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

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

Steve found the solution Pluss needed in Peplink products, especially the Balance series of high-performance enterprise routers and SpeedFusion bonding technology. 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

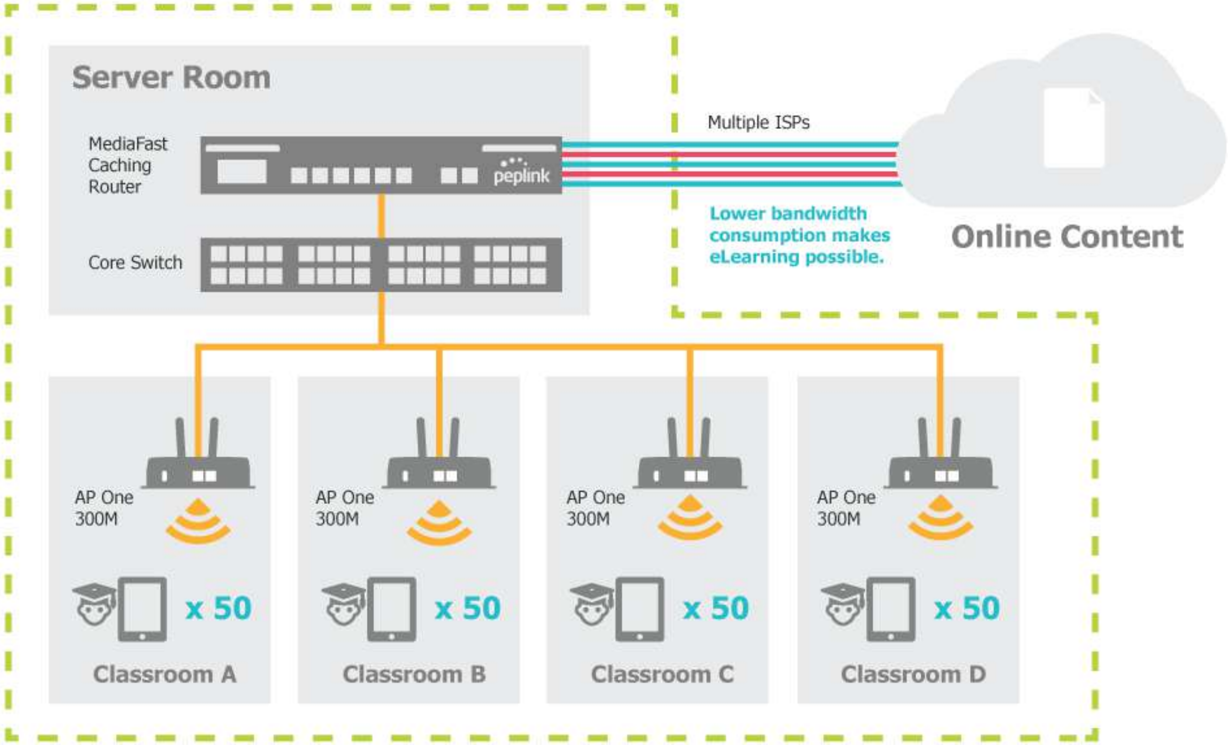
Solution

- 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



50 concurrent sessions per AP, content gets delivered ∞ times on a single download.

School Campus

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

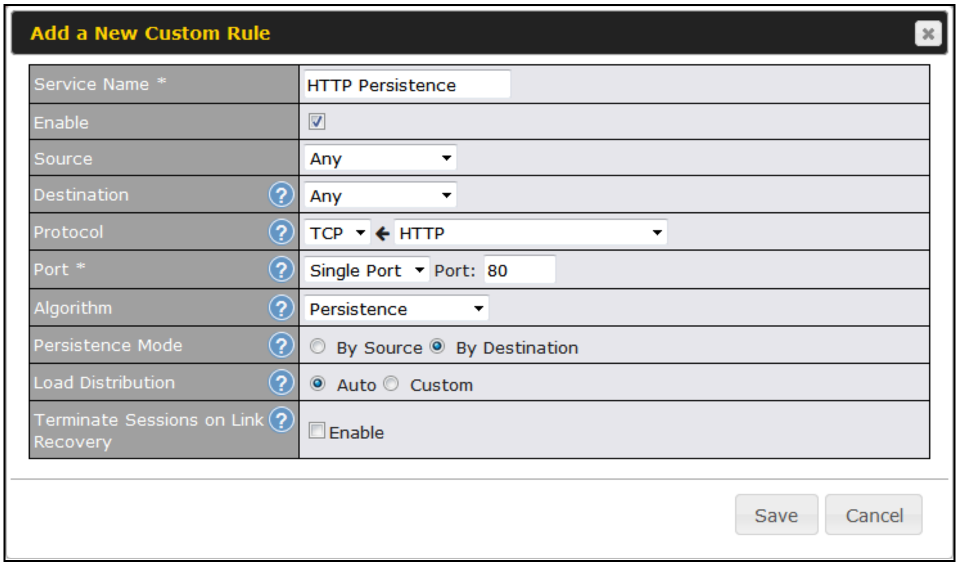
Make use of the persistence functionality of the Peplink Balance. With persistence configured and the **By Destination** option selected, the Peplink Balance will use a consistent WAN connection for source-destination pairs of IP addresses, preventing sessions from being dropped.

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

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

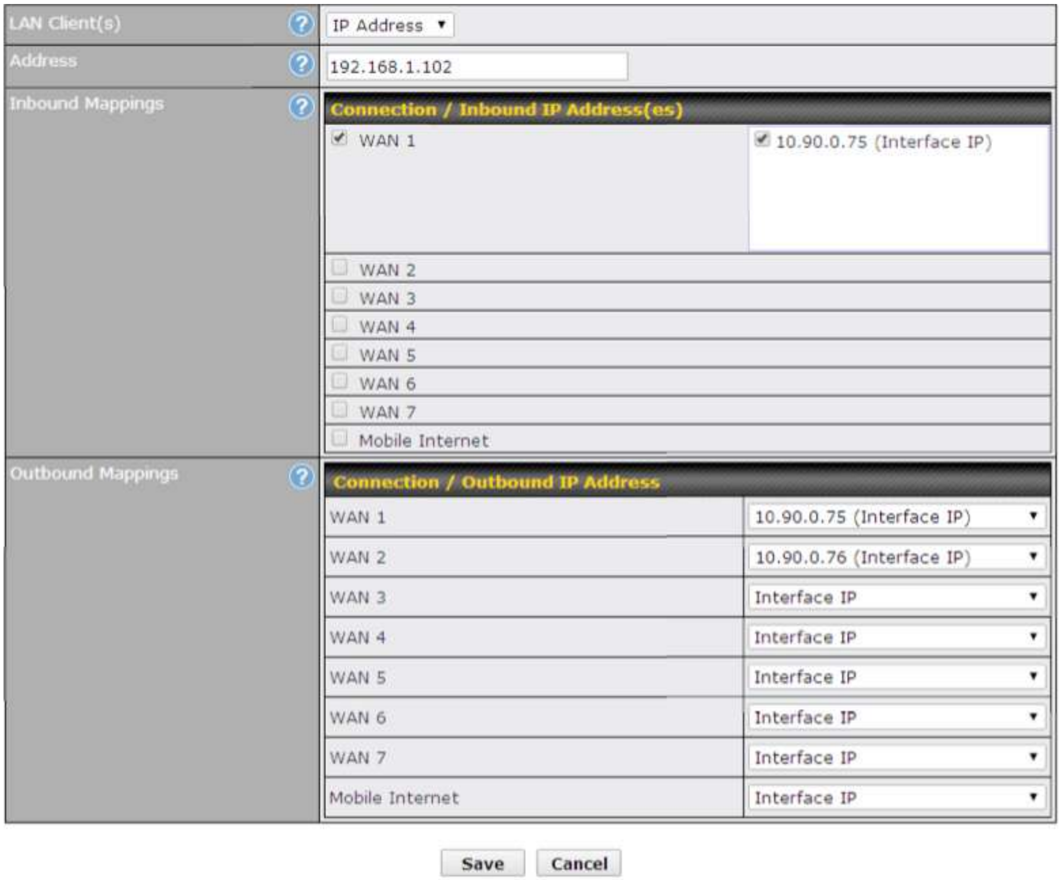
Scenario

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)	
☑ 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	
WAN 1	10.90.0.75 (Interface IP) ▾
WAN 2	10.90.0.76 (Interface IP) ▾
WAN 3	Interface IP ▾
WAN 4	Interface IP ▾
WAN 5	Interface IP ▾
WAN 6	Interface IP ▾
WAN 7	Interface IP ▾
Mobile Internet	Interface IP ▾

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

Inbound Access Restriction

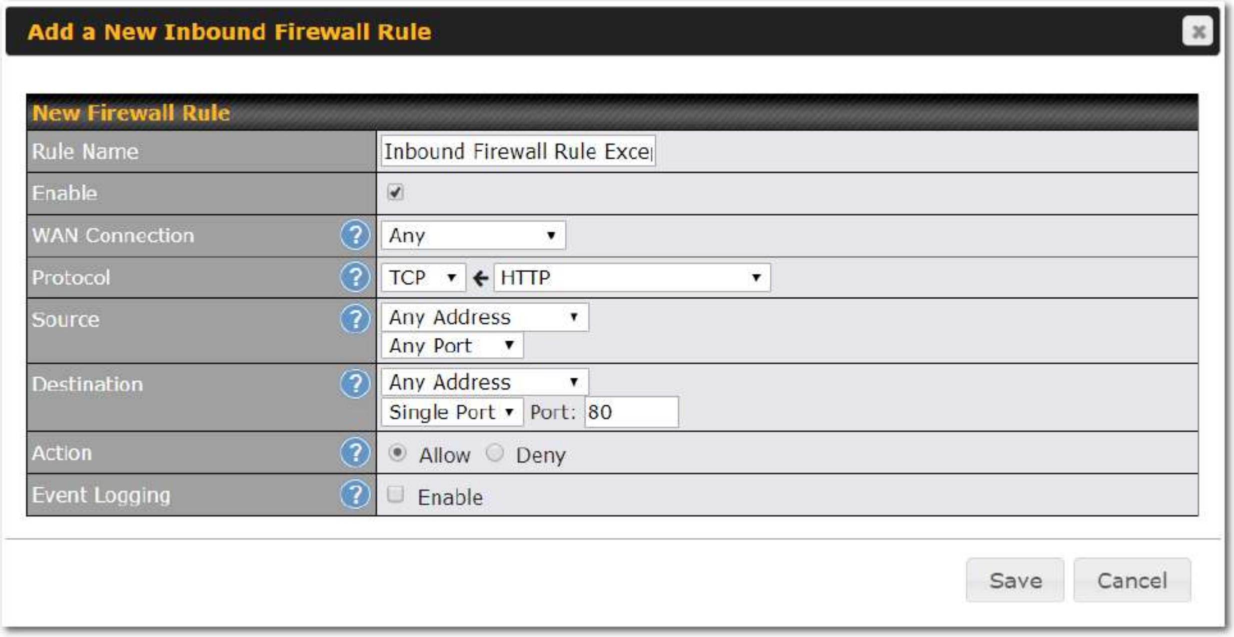
Scenario

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

Solution

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

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



Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	Inbound Firewall Rule Exce
Enable	☑
WAN Connection	Any
Protocol	TCP ← HTTP
Source	Any Address Any Port
Destination	Any Address Single Port Port: 80
Action	● Allow ○ Deny
Event Logging	□ Enable

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

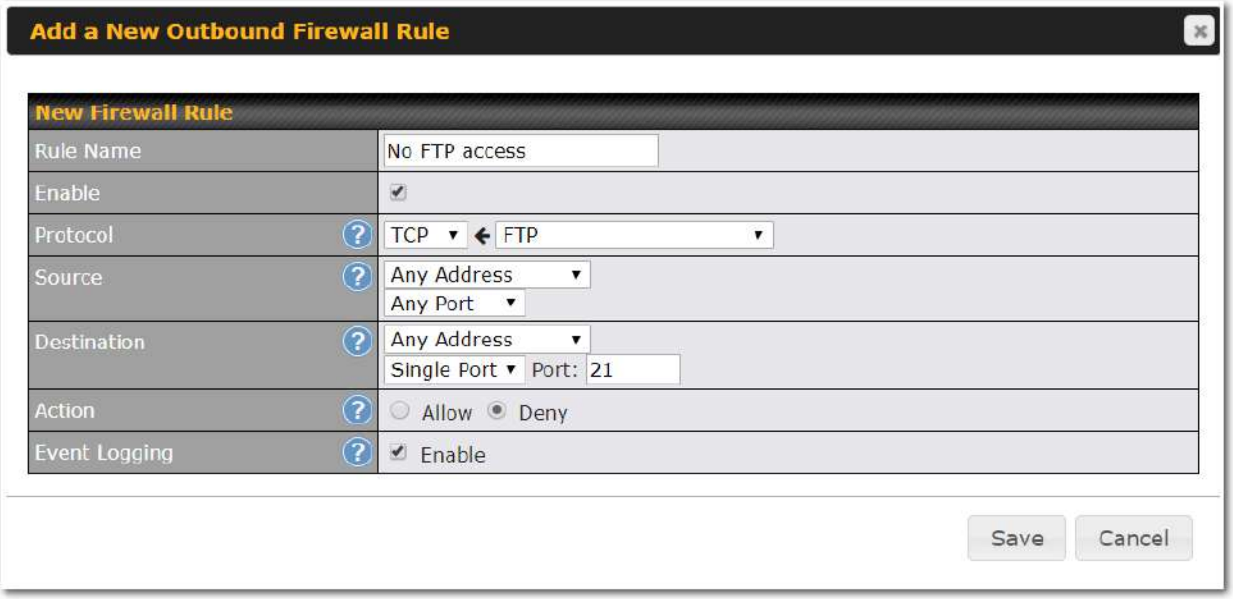
Outbound Access Restriction

Scenario

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

Solution

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



Add a New Outbound Firewall Rule

New Firewall Rule	
Rule Name	No FTP access
Enable	☑
Protocol	TCP ▾ ← FTP ▾
Source	Any Address ▾ Any Port ▾
Destination	Any Address ▾ Single Port ▾ Port: 21
Action	○ Allow ● Deny
Event Logging	☑ Enable

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

Appendix E. Overview of ports used by Peplink SD-WAN routers and other Peplink services

Default Port Number	Usage	Service	Inbound/Outbound	Default Status
UDP 5246	Data flow	InControl	Outbound	Enabled
TCP 443	HTTPS service	InControl	Outbound	Enabled
TCP 5246	Optional, used when TCP 443 is not responding	InControl	Outbound	Enabled
TCP 5246	Remote Web Admin	InControl Virtual Appliance	Outbound	Enabled
TCP 4500	VPN Data (TCP Mode)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
TCP 32015	VPN handshake	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 4500	VPN Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 32015º	VPN Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
TCP/UDP 4500+N-1^	VPN Sub-Tunnels Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 32015+N-1^	VPN Sub-Tunnels Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 4500	VPN Data	IPsec	Inbound / Outbound*	Disabled
UDP 500	VPN initiation	IPsec	Inbound / Outbound*	Disabled
UDP 500	L2TP	Remote User Access	Inbound	Disabled
UDP 1701	L2TP	Remote User Access	Inbound	Disabled
UDP 4500	L2TP	Remote User Access	Inbound	Disabled
UDP 1194	OpenVPN	Remote User Access	Inbound	Disabled
IP 47	PPTP (GRE)	Remote User Access	Inbound	Disabled
TCP 2222	Remote Assistance Direct connection	Peplink Troubleshooting Assistance	Outbound	Enabled
TCP 80	HTTP traffic	Web Admin Interface	Inbound	Enabled

		access		
TCP 443	HTTPS traffic	Web Admin Interface access (secure)	Inbound	Enabled
TCP 8822	SSH	SSH	Inbound	Disabled
UDP 161	SNMP Get	SNMP monitoring	Inbound	Disabled
UDP 162	SNMP Trap	SNMP monitoring	Outbound	Disabled
TCP, UDP 1812	Radius Authentication	Radius	Outbound	Disabled
TCP, UDP 1813	Radius Accounting	Radius	Outbound	Disabled
UDP 123	Network Time Protocol	NTP	Inbound Outbound	Disabled Enabled
TCP 60660	Real-time location data in NMEA format	GPS	Outbound	Disabled

Disclaimer:

- By default, only TCP 32015 and UDP 4500 are needed for PepVPN / SpeedFusion.
- Inbound / Outbound* - Inbound = For Server mode; Outbound = For Client mode
- UDP 32015º - If IPsec VPN or L2TP/IPsec RUA is enabled, the UDP 4500 is occupied, so PepVPN / SpeedFusion will automatically switch to UPD 32015 as VPN data port .
- UDP 32015+N-1^ / TCP/UDP 4500+N-1^ - When using Sub-Tunnels, multiple ports are in use (1 for each Sub-Tunnel profile).
- The default UDP data ports used when using (N number of Sub-Tunnel profiles) are: 4500…4500+N-1, or (when port 4500 is in use by IPsec or L2TP/IPsec) 32015…32015+N-1".

Appendix F. 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^{TM} 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 able to find the source of problem.

Problem 6

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

Solution

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

Additional troubleshooting resources:

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

Appendix G.

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

For Balance 30 Pro

Federal Communication Commission Interference Statement

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

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

Radiation Exposure Statement :

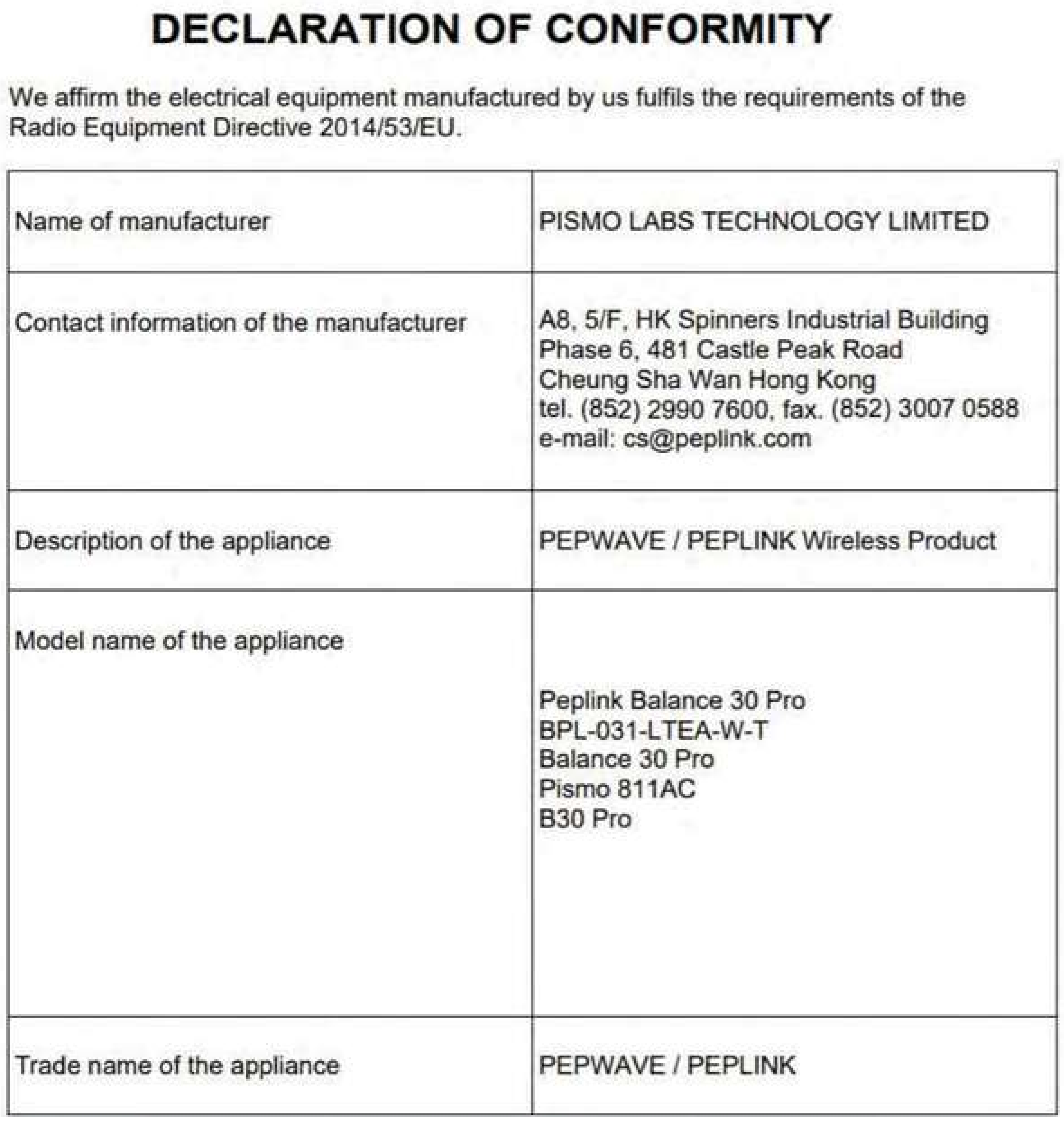
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 49 cm between the radiator and your body.

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

Battery Caution Statement

Risk of explosion if the battery is replaced by an incorrect type.

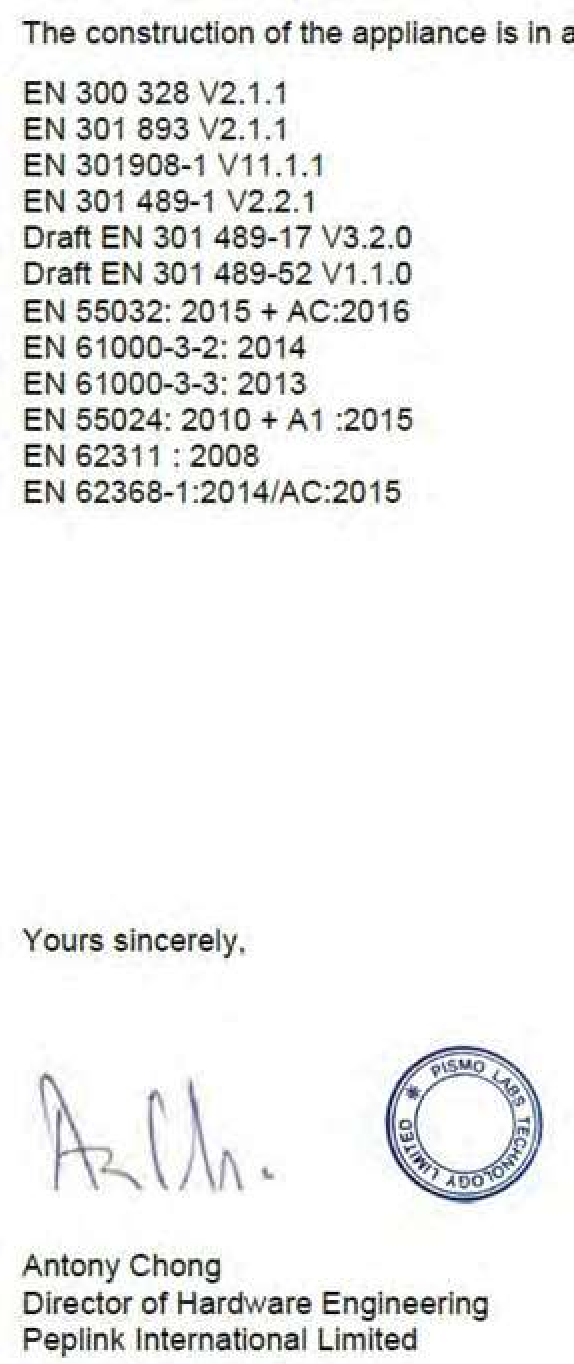
CE Statement for Pepwave Routers (Balance 30 Pro)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building Phase 6, 481 Castle Peak Road Cheung Sha Wan Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Peplink Balance 30 Pro BPL-031-LTEA-W-T Balance 30 Pro Pismo 811AC B30 Pro
Trade name of the appliance	PEPWAVE / PEPLINK



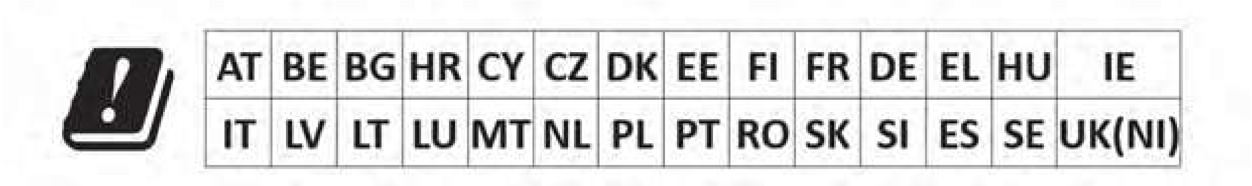
The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.1.1
EN 301 893 V2.1.1
EN 301908-1 V11.1.1
EN 301 489-1 V2.2.1
Draft EN 301 489-17 V3.2.0
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + AC:2016
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55024: 2010 + A1 :2015
EN 62311 : 2008
EN 62368-1:2014/AC:2015

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

<u>**2.4GHz (2412 - 2472 MHz) : 19.93 dBm**</u>

<u>**5GHz (5150 - 5250 MHz) : 22.88 dBm**</u>

<u>**WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)**</u>

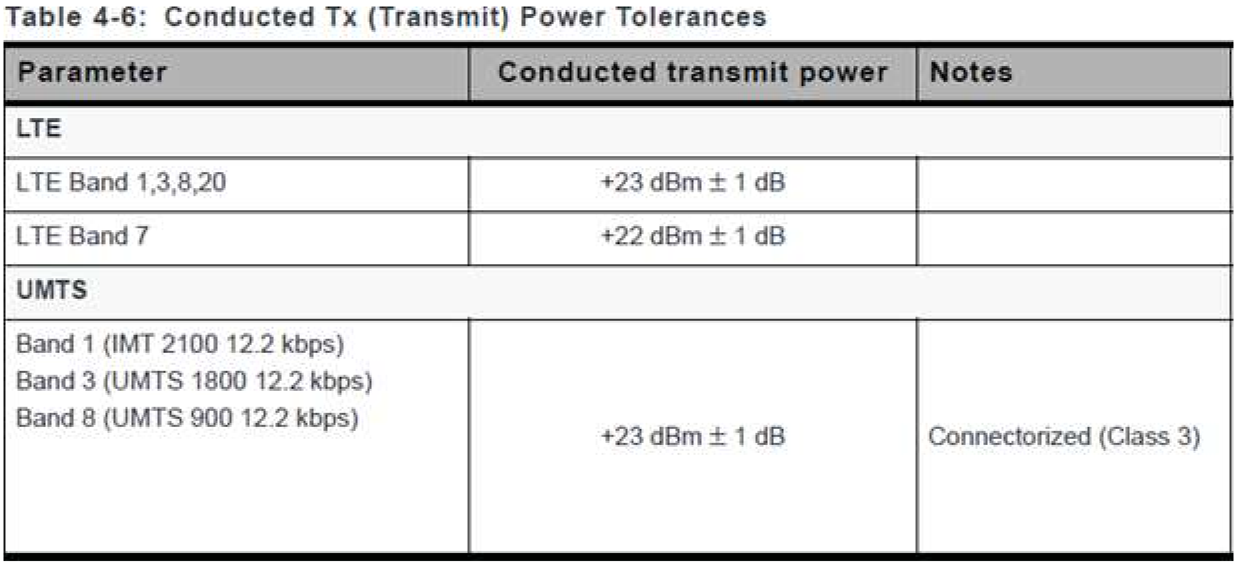


Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 3 (UMTS 1800 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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

Contact as: https://www.peplink.com/

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

For Balance one

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

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

Industry Canada Statement (Balance one)

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

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

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired opera- tion of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio ex- empts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et
(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le

brouillage est susceptible d’en

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

(ii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate and
The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est reserve uniquement pour
utilisation a l'interieur afin de reduire les risques de brouillage prejudiciable aux systemes de satellites mobiles utilisant les memes canaux

(ii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisan bande 5725-5850 MHz doit se conformer a la limitation P.I.R.E specifiee pour l'exploitation point a point et non point a point, selon le cas.
En outre, les utilisateurs devraient aussi etre avises que les utilisateurs de radars de haute puissance sont designes utilisateurs principaux (c.-a-d., qu'ils ont la priorite) pour les bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

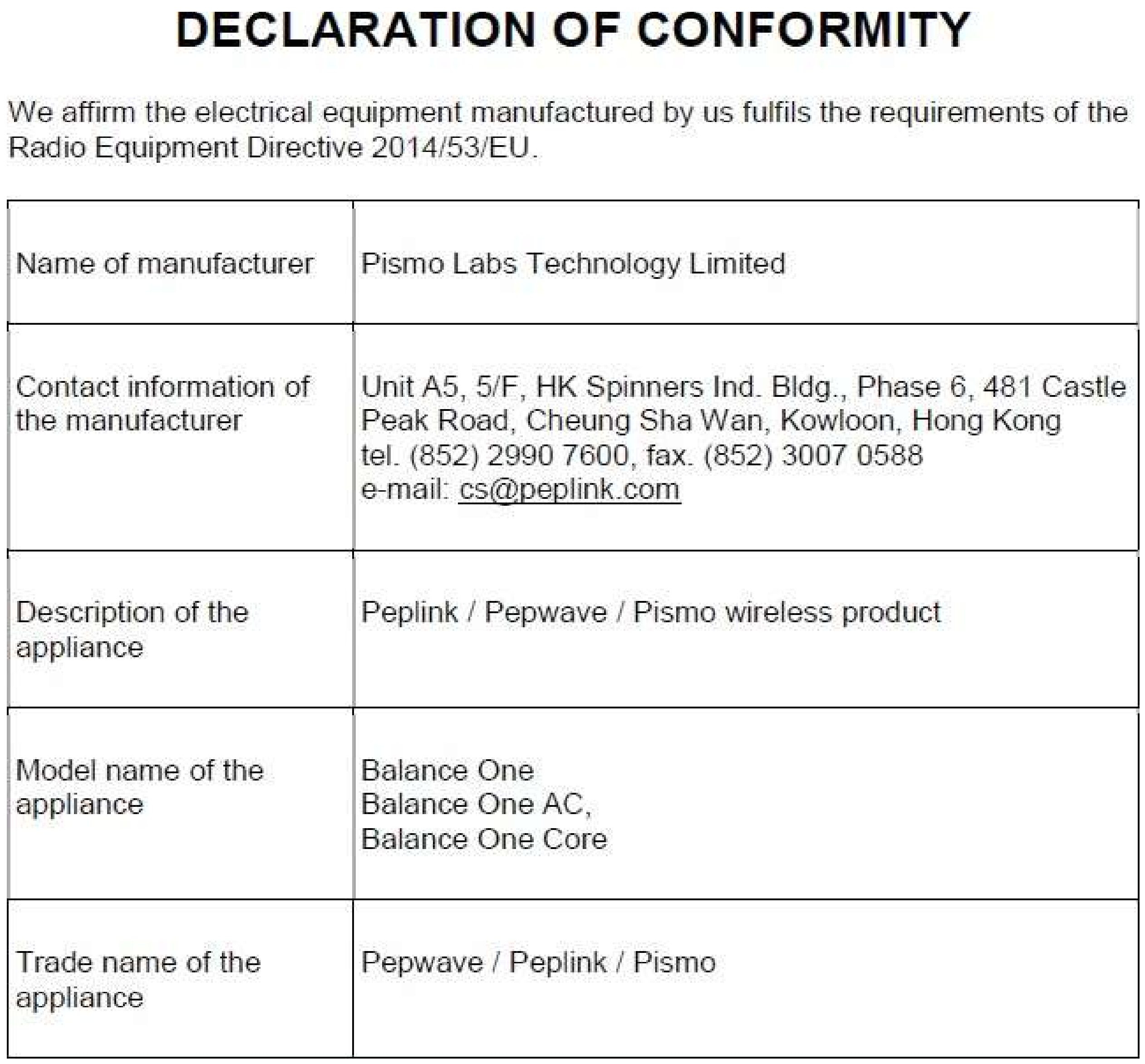
Radiation Exposure Statement

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

Cet equipement est conforme avec l'exposition aux radiations ISED definies pour un environnement non controle. Cet equipement doit etre installe et utilise a une distance minimum de 20 cm entre le radiateur et votre corps.

.

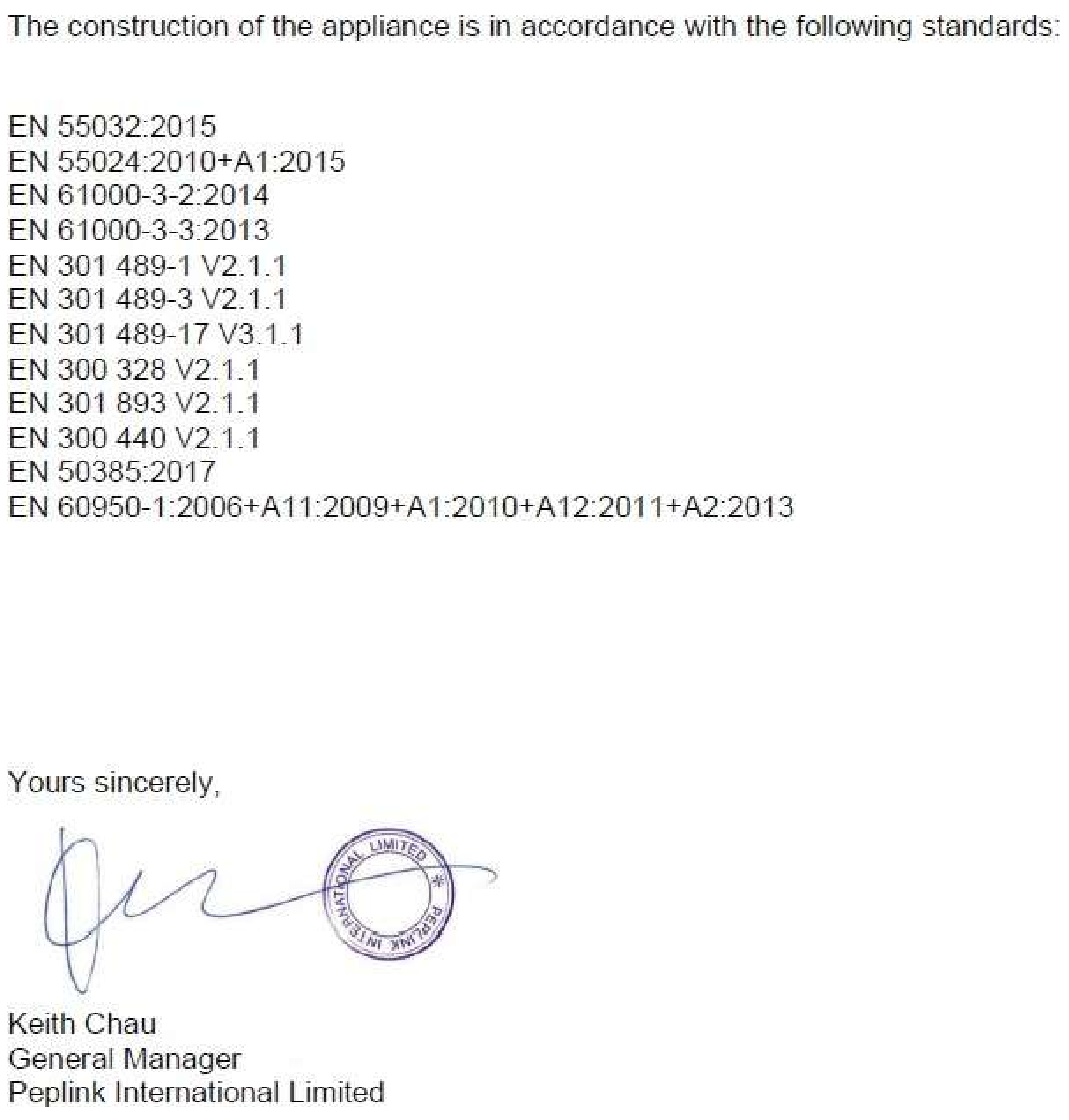
CE Statement for Pepwave Routers (Balance One)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	Pismo Labs Technology Limited
Contact information of the manufacturer	Unit A5, 5/F, HK Spinners Ind. Bldg., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	Peplink / Pepwave / Pismo wireless product
Model name of the appliance	Balance One Balance One AC, Balance One Core
Trade name of the appliance	Pepwave / Peplink / Pismo



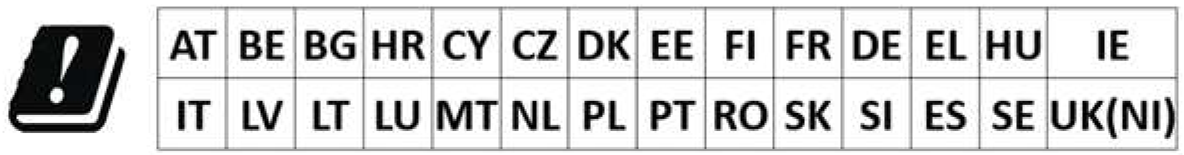
The construction of the appliance is in accordance with the following standards:

EN 55032:2015
EN 55024:2010+A1:2015
EN 61000-3-2:2014
EN 61000-3-3:2013
EN 301 489-1 V2.1.1
EN 301 489-3 V2.1.1
EN 301 489-17 V3.1.1
EN 300 328 V2.1.1
EN 301 893 V2.1.1
EN 300 440 V2.1.1
EN 50385:2017
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Yours sincerely,

PEPLINK INTERNATIONAL LIMITED

Keith Chau
General Manager
Peplink International Limited



AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

2.4GHz (2412 - 2472 MHz) : 16.59 dBm
5GHz (5150 - 5250 MHz) : 21.38 dBm

5GHz (5725 - 5850 MHz) : 13.25 dBm

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

Contact as: https://www.peplink.com/

For Balance one core, Balance 20, Balance 30 LTE, Balance 210, Balance 310X, Balance 310X 5G, Balance 310 5G, Balance 310 Fiber 5G, Balance 305, Balance 380, Balance 580, Balance 710, Balance 1350, Balance 2500, EPX, Balance SDX, MediaFast 500, MediaFast 750

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement (Balance 30 LTE, Balance 310X, Balance 310X 5G, Balance 310 5G, Balance 310 Fiber 5G)

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

Industry Canada Statement (Balance one core, Balance 20, Balance 30 LTE, Balance 310X, Balance 310X 5G, Balance 310 5G, Balance 310 Fiber 5G, Balance 305, Balance 380, Balance 580, Balance 710, Balance 1350, Balance 2500, EPX, Balance SDX, MediaFast 500, MediaFast 750)

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

Le present produit est conforme aux specifications techniques applicables d'Innovation, Sciences et Developpement economique Canada.

For Balance 30 LTE, Balance 310X, Balance 310X 5G, Balance 310 5G, Balance 310 Fiber 5G

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en

Radiation Exposure Statement (Balance 30 LTE, Balance 310X, Balance 310X 5G, Balance 310 5G, Balance 310 Fiber 5G)

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

Battery Caution Statement (Balance 30 LTE, Balance 210, Balance 310 5G, Balance 310X, Balance 310X 5G, Balance 310 Fiber 5G, Balance SDX)

Risk of explosion if the battery is replaced by an incorrect type.

Safety Statement (Balance SDX)

Class I Equipment. This equipment must be earthed. The power plug must be connected to a properly wired earth ground socket outlet. An improperly wired socket outlet could place hazardous voltages on accessible metal parts.

All Ethernet cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the appliance is located.

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

For Balance Two

Federal Communication Commission Interference Statement

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

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

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Battery Caution Statement

Risk of explosion if the battery is replaced by an incorrect type.

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

For Balance 20X

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

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

Industry Canada Statement (Balance 20X)

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

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

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired opera- tion of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio ex- empts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et
(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en

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

(ii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate and
The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est reserve uniquement pour
utilisation a l'interieur afin de reduire les risques de brouillage prejudiciable aux systemes de satellites mobiles utilisant les memes canaux

(ii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisan bande 5725-5850 MHz doit se conformer a la limitation P.I.R.E specifiee pour l'exploitation point a point et non point a point, selon le cas.
En outre, les utilisateurs devraient aussi etre avises que les utilisateurs de radars de haute puissance sont designes utilisateurs principaux (c.-a-d., qu'ils ont la priorite) pour les bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement

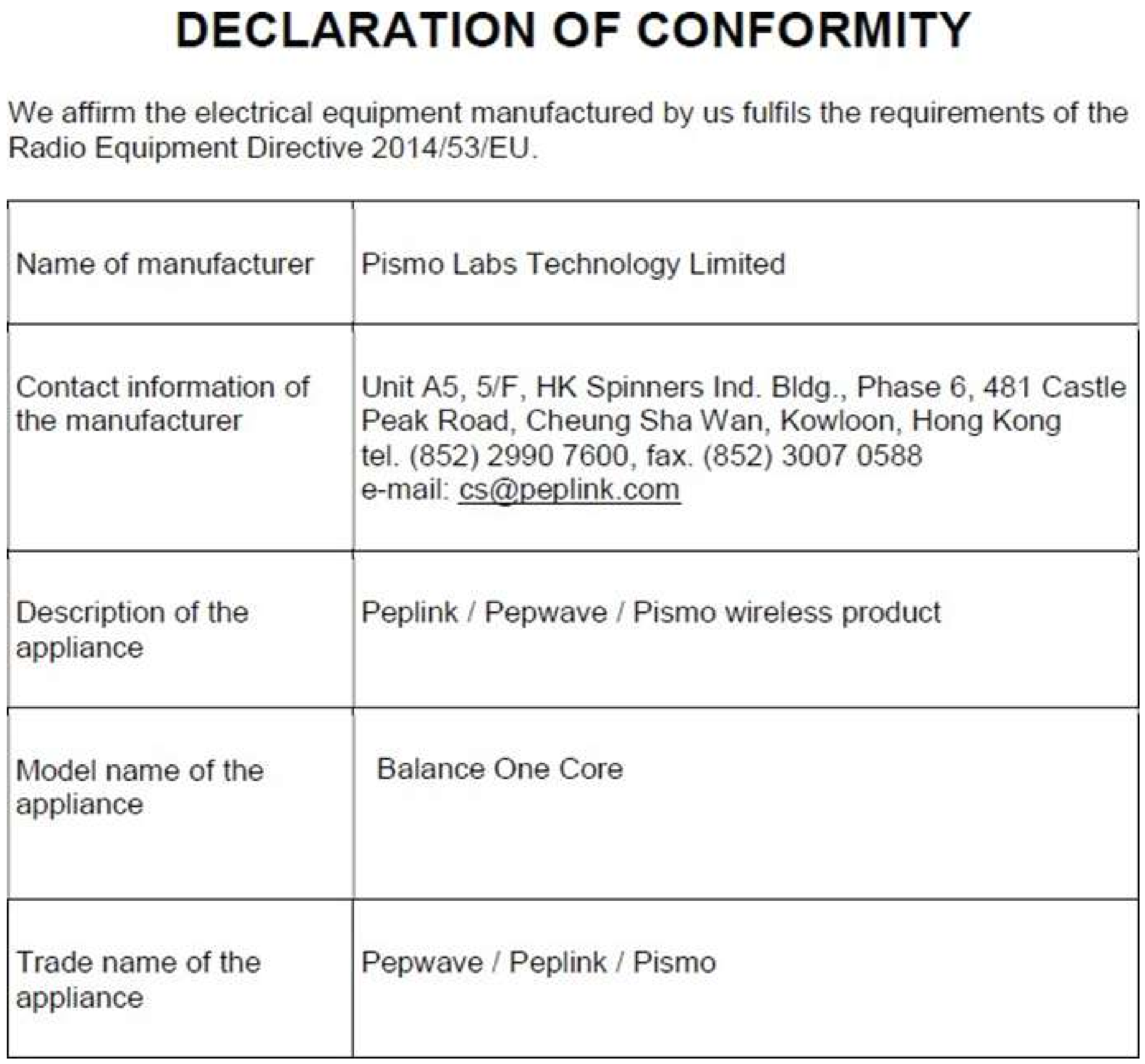
This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

Cet equipement est conforme avec l'exposition aux radiations ISED definies pour un environnement non controle. Cet equipement doit etre installe et utilise a une distance minimum de 20 cm entre le radiateur et votre corps.

Battery Caution Statement

Risk of explosion if the battery is replaced by an incorrect type.

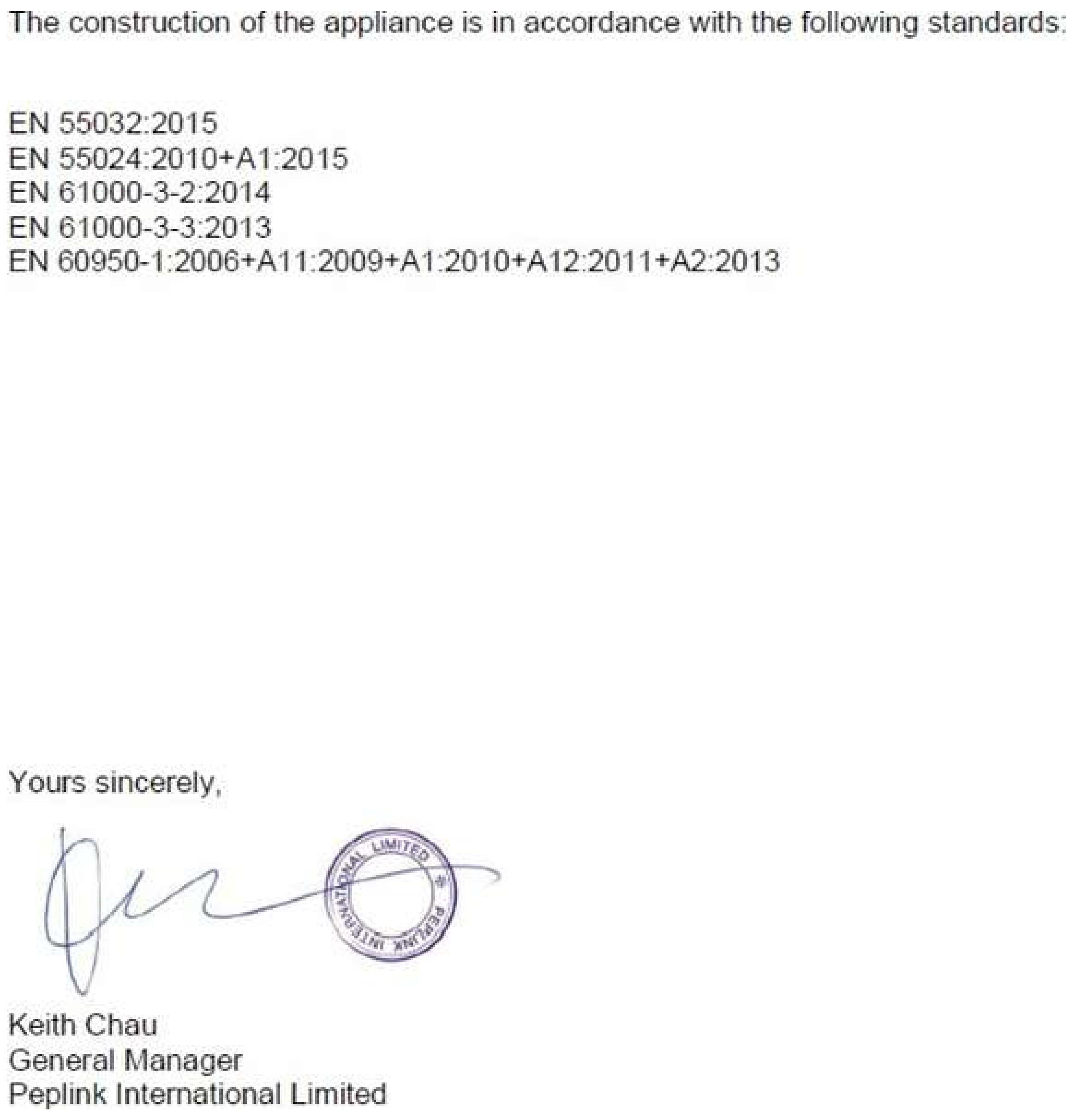
CE Statement for Pepwave Routers (Balance One Core)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	Pismo Labs Technology Limited
Contact information of the manufacturer	Unit A5, 5/F, HK Spinners Ind. Bldg., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	Peplink / Pepwave / Pismo wireless product
Model name of the appliance	Balance One Core
Trade name of the appliance	Pepwave / Peplink / Pismo



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

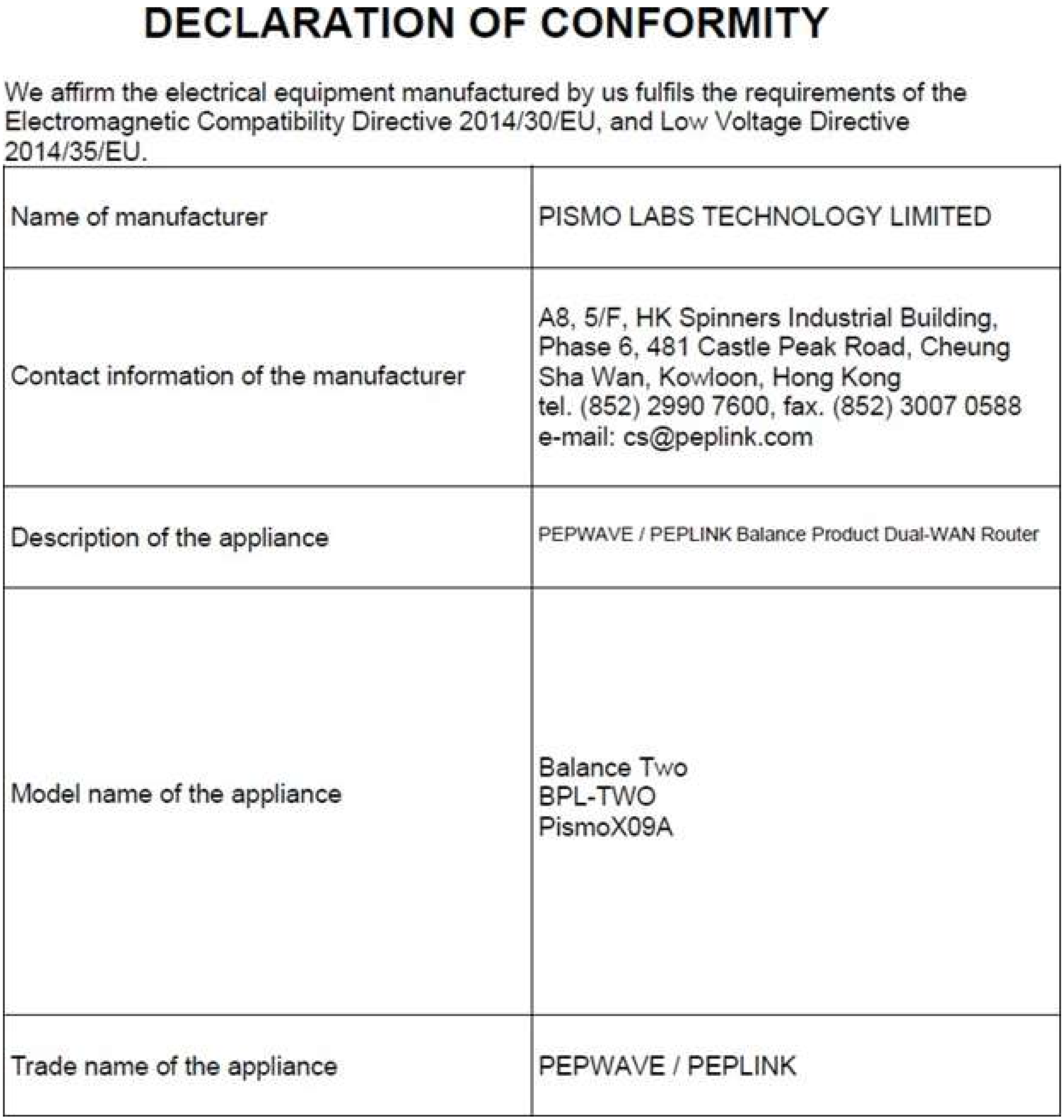
EN 55032:2015
EN 55024:2010+A1:2015
EN 61000-3-2:2014
EN 61000-3-3:2013
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Yours sincerely,

PEPLINK INTERNATIONAL LIMITED

Keith Chau
General Manager
Peplink International Limited

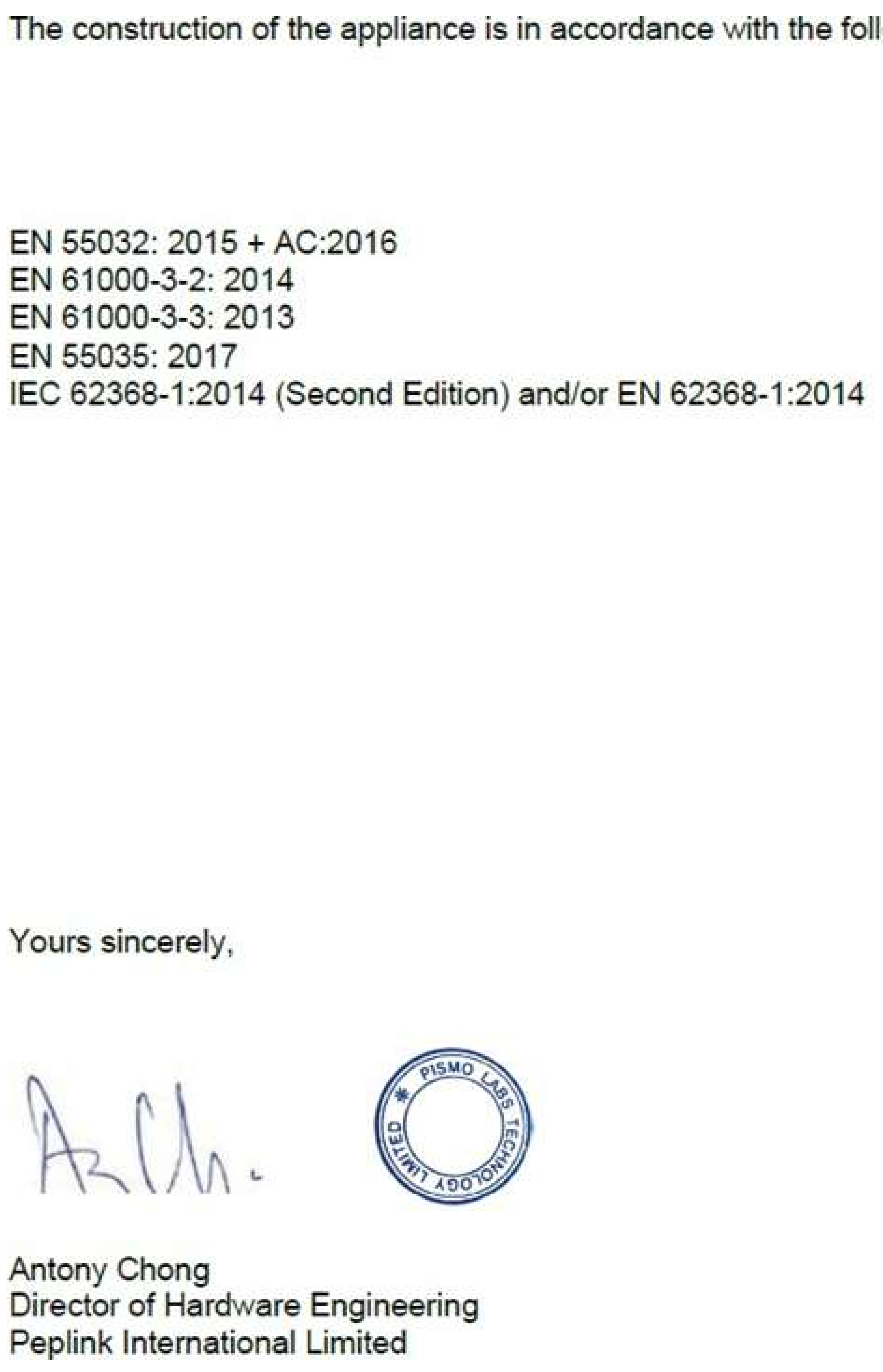
CE Statement for Pepwave Routers (Balance Two)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Electromagnetic Compatibility Directive 2014/30/EU, and Low Voltage Directive 2014/35/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building, Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Balance Product Dual-WAN Router
Model name of the appliance	Balance Two BPL-TWO PismoX09A
Trade name of the appliance	PEPWAVE / PEPLINK



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

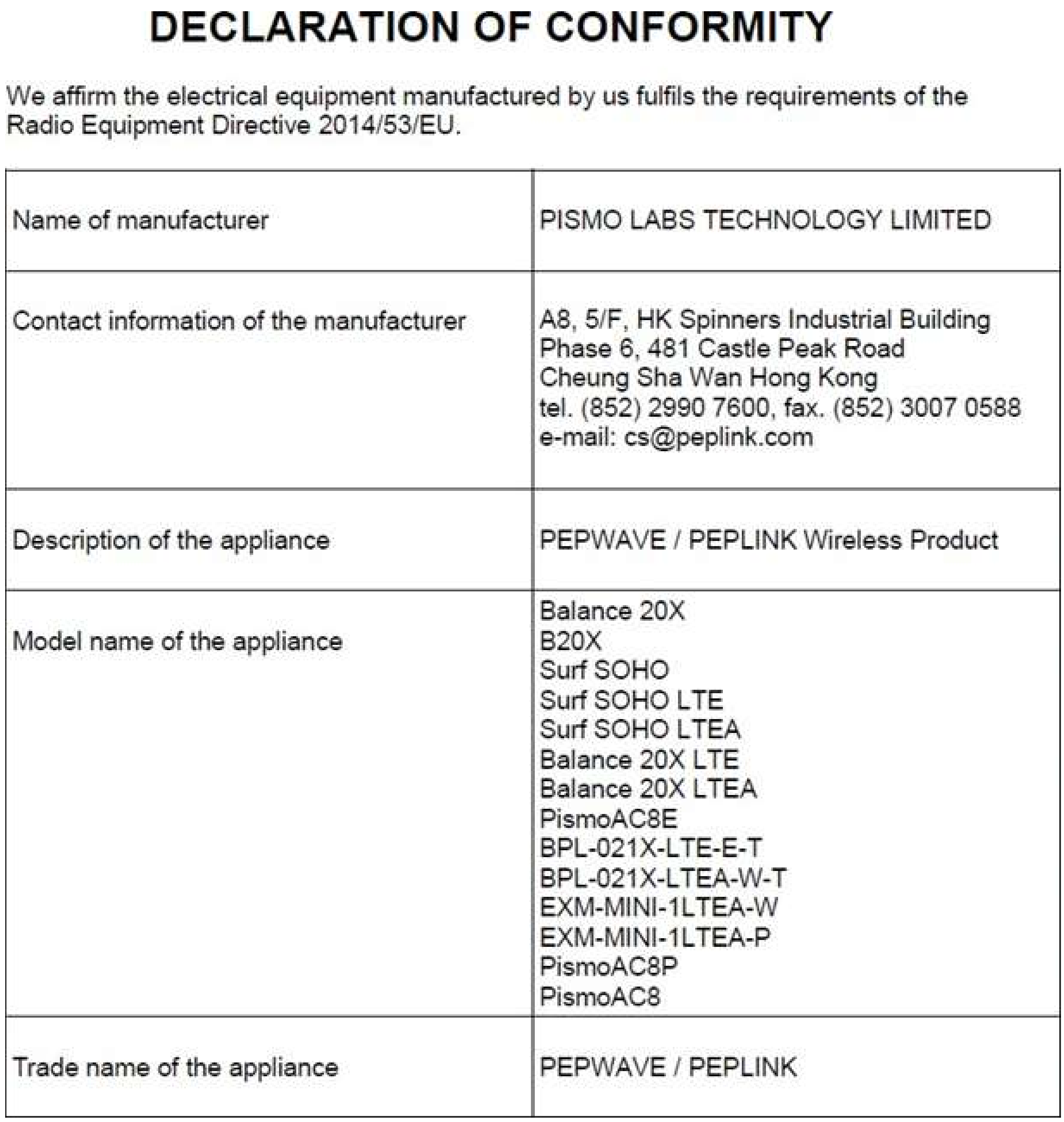
EN 55032: 2015 + AC:2016
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035: 2017
IEC 62368-1:2014 (Second Edition) and/or EN 62368-1:2014

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited

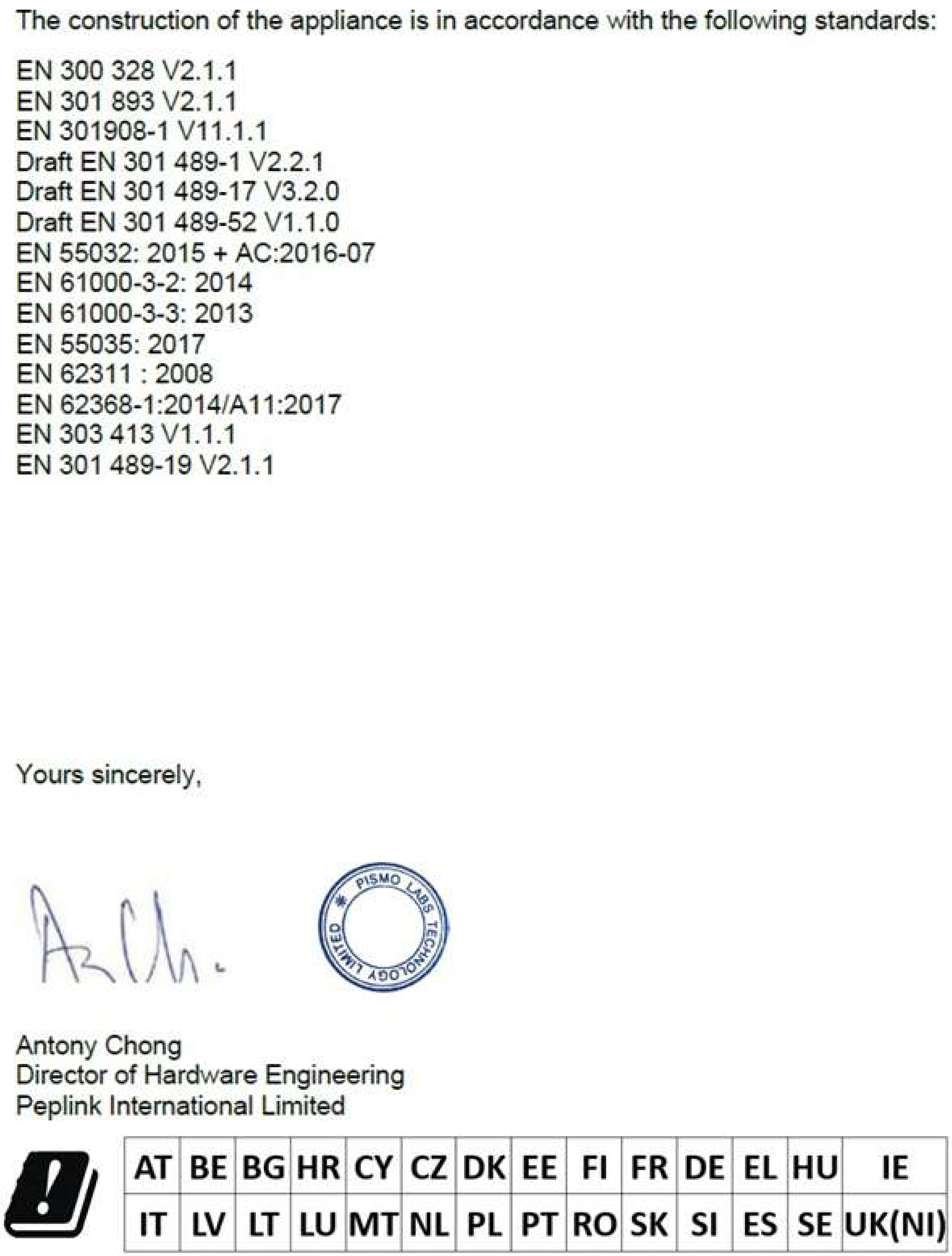
CE Statement for Pepwave Routers (Balance 20X Pro)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building Phase 6, 481 Castle Peak Road Cheung Sha Wan Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Balance 20X B20X Surf SOHO Surf SOHO LTE Surf SOHO LTEA Balance 20X LTE Balance 20X LTEA PismoAC8E BPL-021X-LTE-E-T BPL-021X-LTEA-W-T EXM-MINI-1LTEA-W EXM-MINI-1LTEA-P PismoAC8P PismoAC8
Trade name of the appliance	PEPWAVE / PEPLINK



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

EN 300 328 V2.1.1
EN 301 893 V2.1.1
EN 301908-1 V11.1.1
Draft EN 301 489-1 V2.2.1
Draft EN 301 489-17 V3.2.0
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + AC:2016-07
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035: 2017
EN 62311 : 2008
EN 62368-1:2014/A11:2017
EN 303 413 V1.1.1
EN 301 489-19 V2.1.1

Yours sincerely,

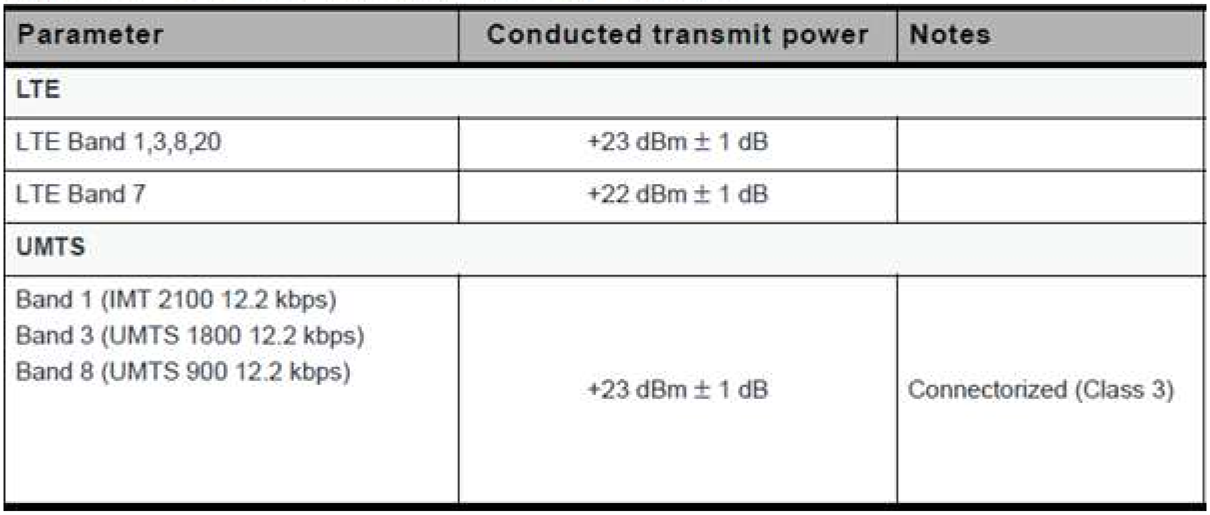
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited

AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

2.4GHz (2412 - 2472 MHz) : 19.84 dBm
5GHz (5150 - 5250 MHz) : 22.89 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

Table 4-6: Conducted Tx (Transmit) Power Tolerances

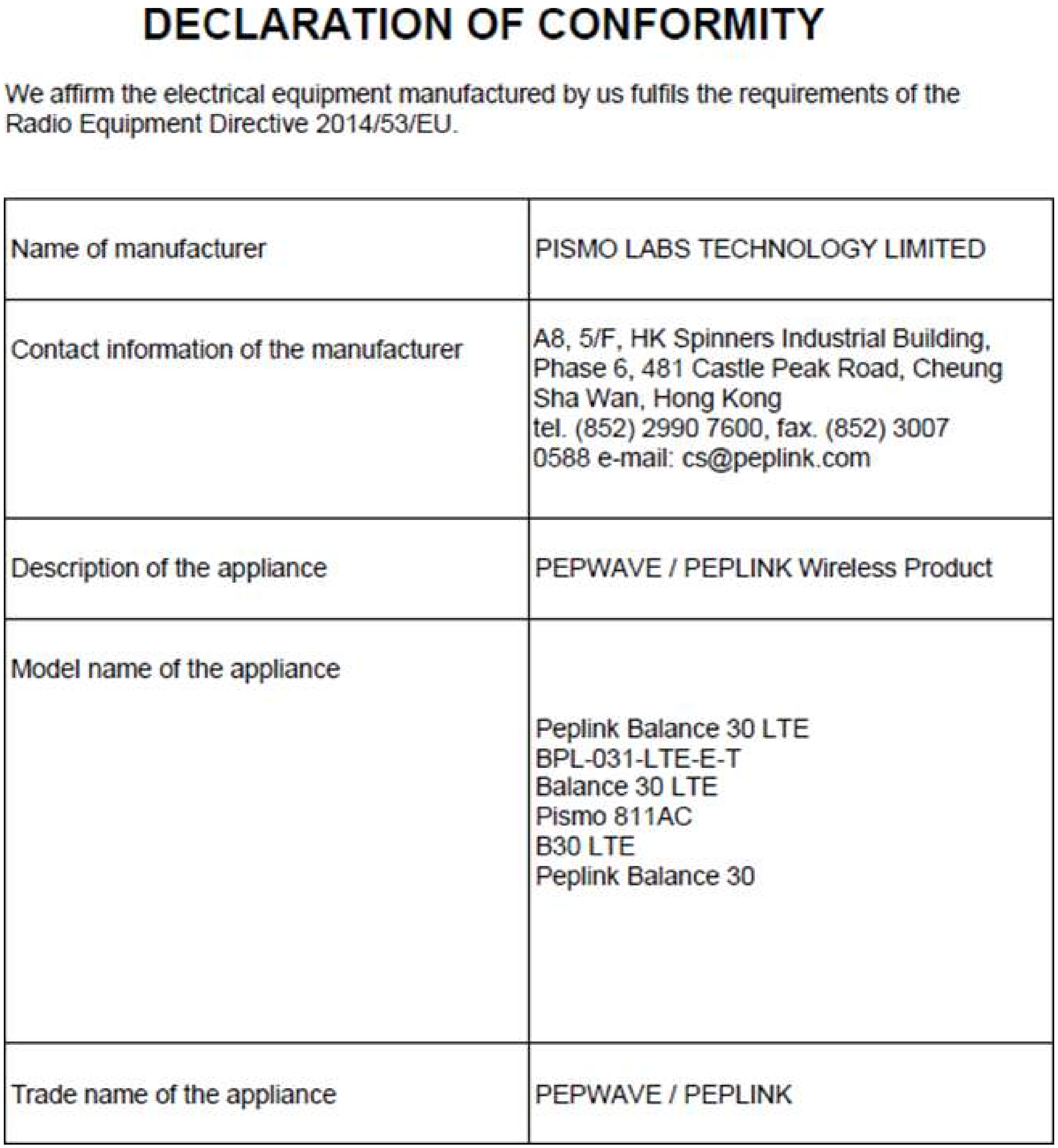


Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 3 (UMTS 1800 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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

contact as: https://www.peplink.com/

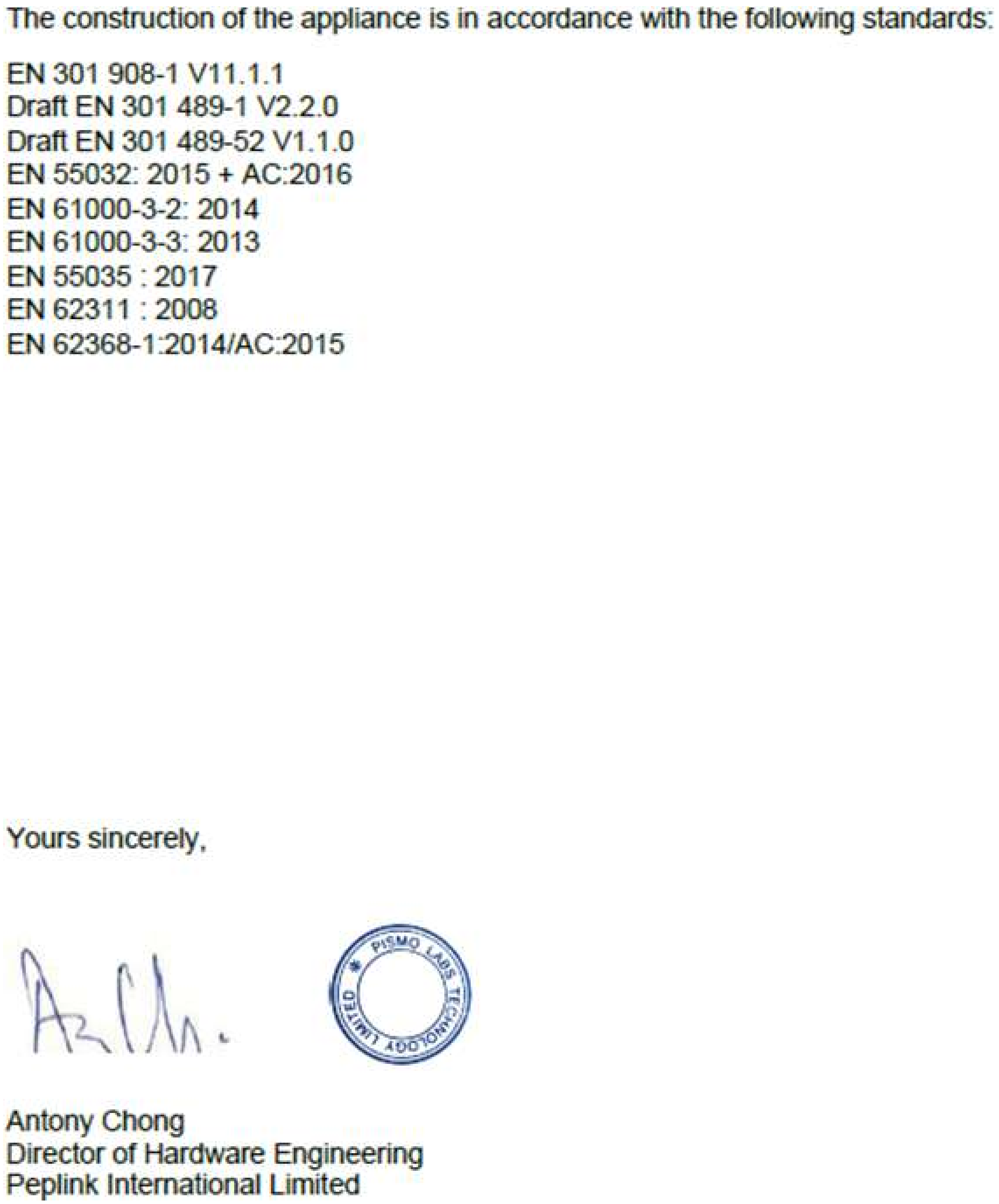
CE Statement for Pepwave Routers (Balance 30 LTE)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building, Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Peplink Balance 30 LTE BPL-031-LTE-E-T Balance 30 LTE Pismo 811AC B30 LTE Peplink Balance 30
Trade name of the appliance	PEPWAVE / PEPLINK



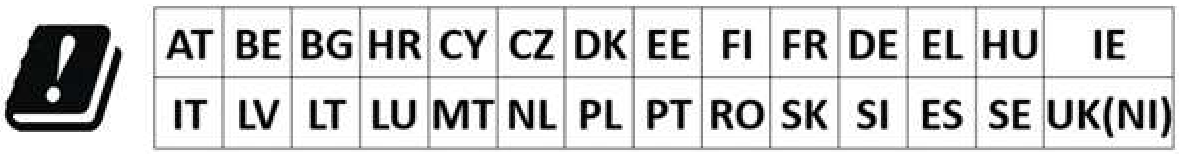
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V11.1.1
Draft EN 301 489-1 V2.2.0
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + AC:2016
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035 : 2017
EN 62311 : 2008
EN 62368-1:2014/AC:2015

Yours sincerely,

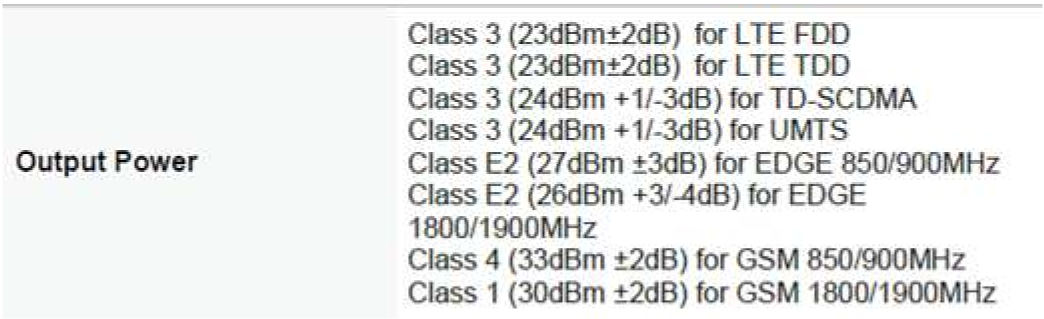
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

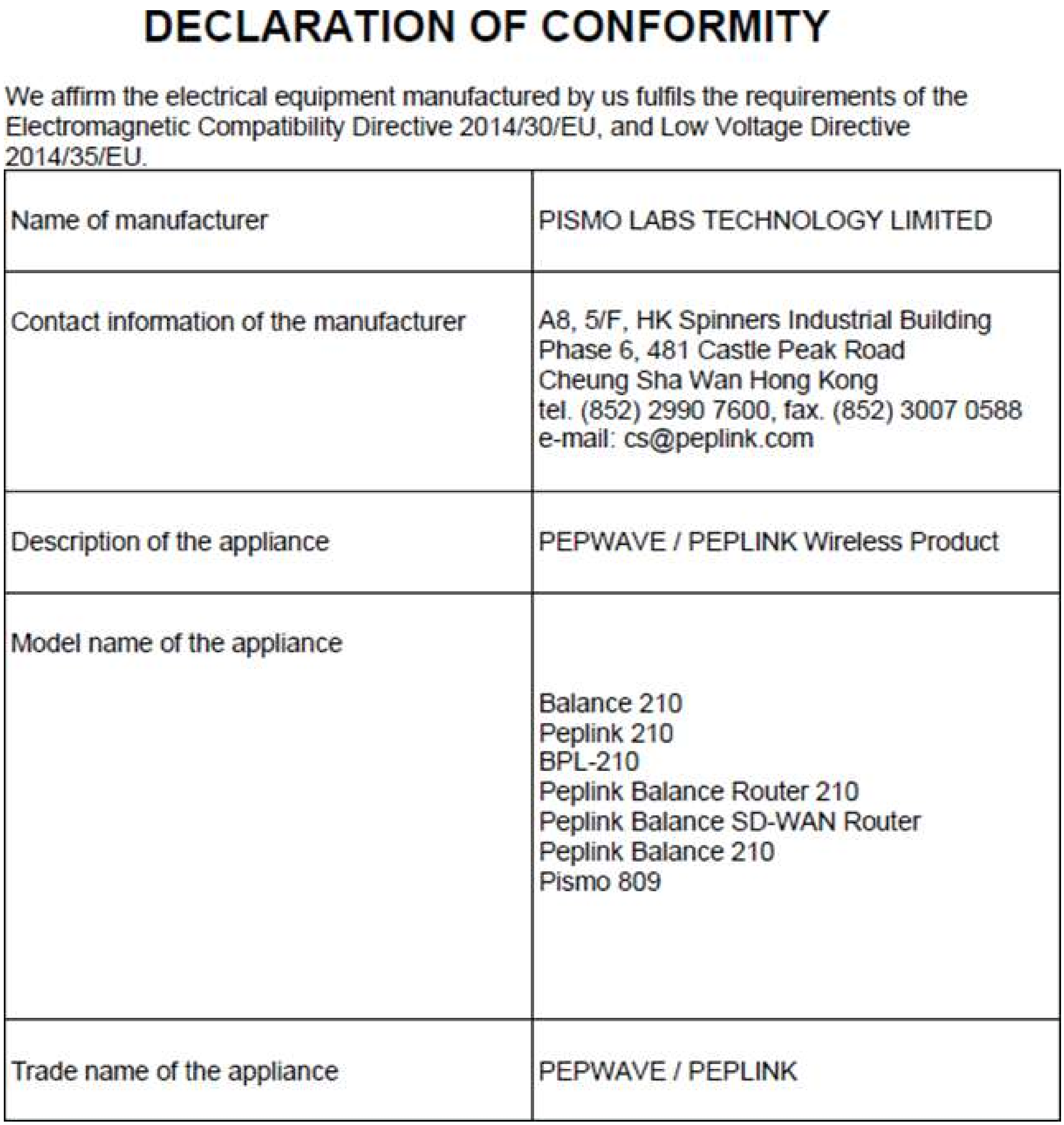


Output Power	Class 3 (23dBm±2dB) for LTE FDD Class 3 (23dBm±2dB) for LTE TDD Class 3 (24dBm +1/-3dB) for TD-SCDMA Class 3 (24dBm +1/-3dB) for UMTS Class E2 (27dBm ±3dB) for EDGE 850/900MHz Class E2 (26dBm +3/-4dB) for EDGE 1800/1900MHz Class 4 (33dBm ±2dB) for GSM 850/900MHz Class 1 (30dBm ±2dB) for GSM 1800/1900MHz

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

contact as: https://www.peplink.com/

CE Statement for Pepwave Routers (Balance 210)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Electromagnetic Compatibility Directive 2014/30/EU, and Low Voltage Directive 2014/35/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building Phase 6, 481 Castle Peak Road Cheung Sha Wan Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Balance 210 Peplink 210 BPL-210 Peplink Balance Router 210 Peplink Balance SD-WAN Router Peplink Balance 210 Pismo 809
Trade name of the appliance	PEPWAVE / PEPLINK

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

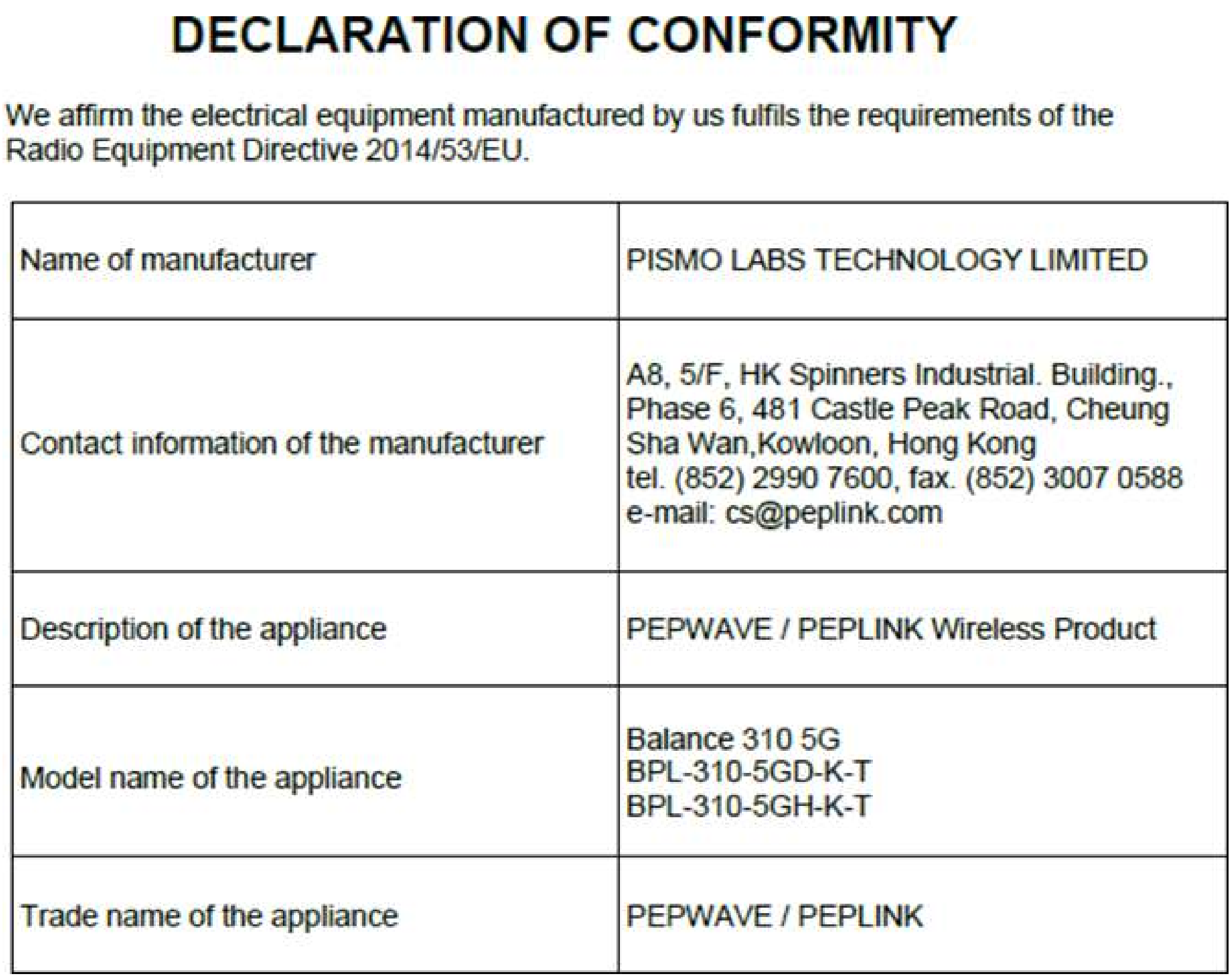
EN 55032: 2015 + AC:2016-07
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035: 2017
EN 62368-1:2014/A11:2017

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited

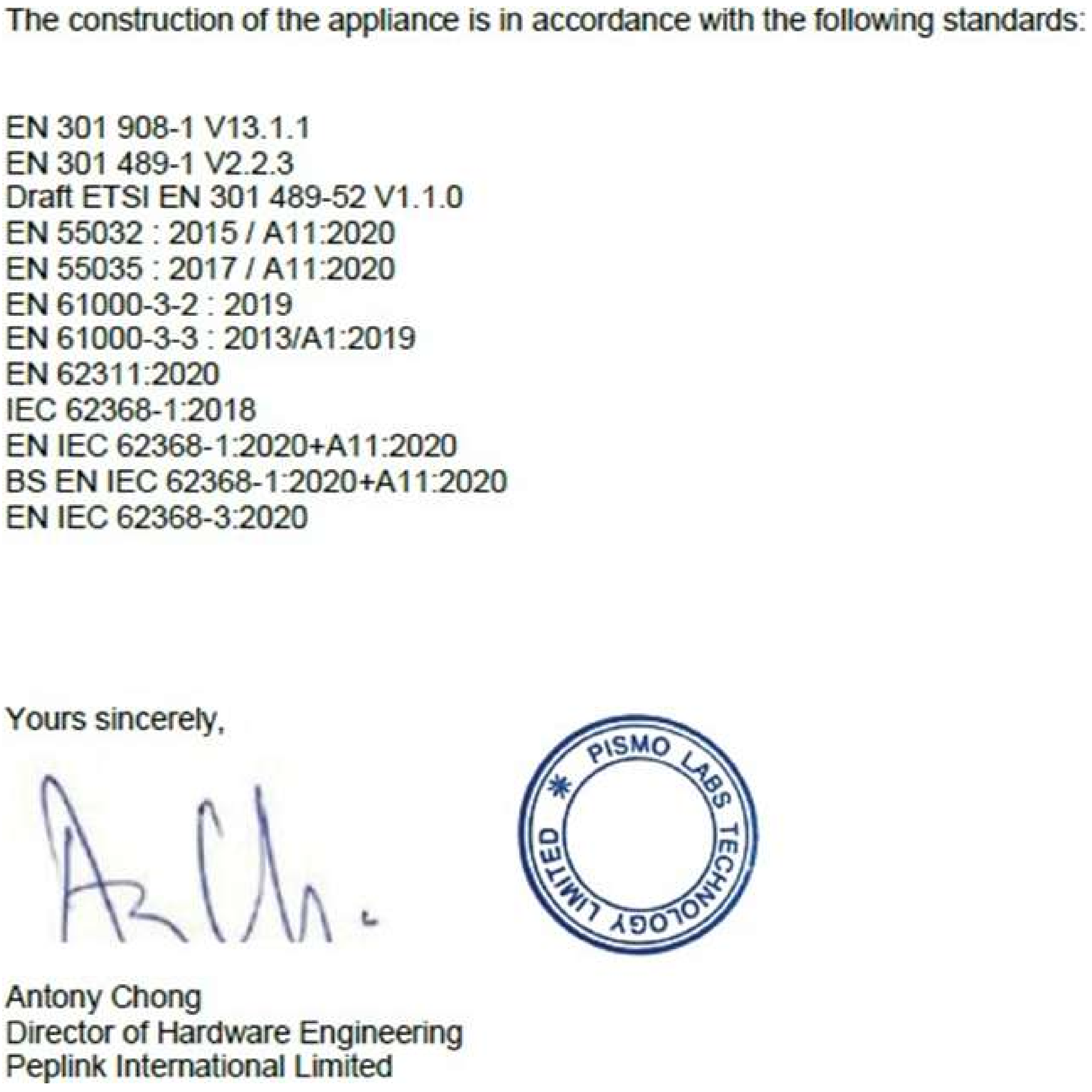
CE Statement for Pepwave Routers (Balance 310 5G)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan,Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Balance 310 5G BPL-310-5GD-K-T BPL-310-5GH-K-T
Trade name of the appliance	PEPWAVE / PEPLINK



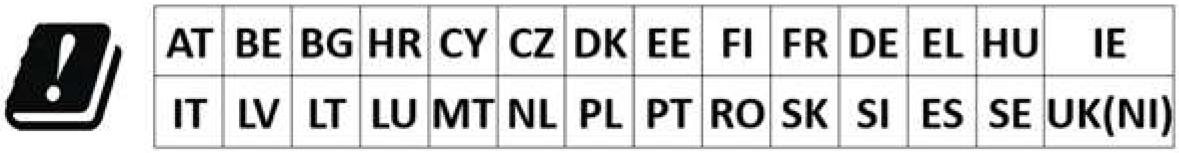
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1
EN 301 489-1 V2.2.3
Draft ETSI EN 301 489-52 V1.1.0
EN 55032 : 2015 / A11:2020
EN 55035 : 2017 / A11:2020
EN 61000-3-2 : 2019
EN 61000-3-3 : 2013/A1:2019
EN 62311:2020
IEC 62368-1:2018
EN IEC 62368-1:2020+A11:2020
BS EN IEC 62368-1:2020+A11:2020
EN IEC 62368-3:2020

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

EM7565 module:

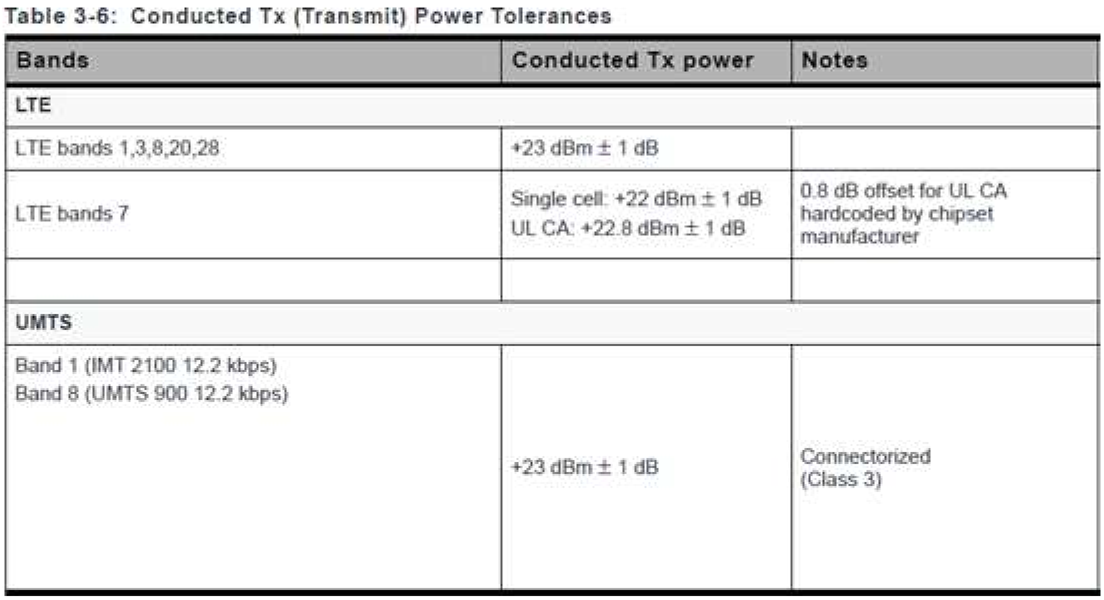


Table 3-6: Conducted Tx (Transmit) Power Tolerances

Bands	Conducted Tx power	Notes
LTE		
LTE bands 1,3,8,20,28	+23 dBm ± 1 dB	
LTE bands 7	Single cell: +22 dBm ± 1 dB UL CA: +22.8 dBm ± 1 dB	0.8 dB offset for UL CA hardcoded by chipset manufacturer
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

EM9191 module:

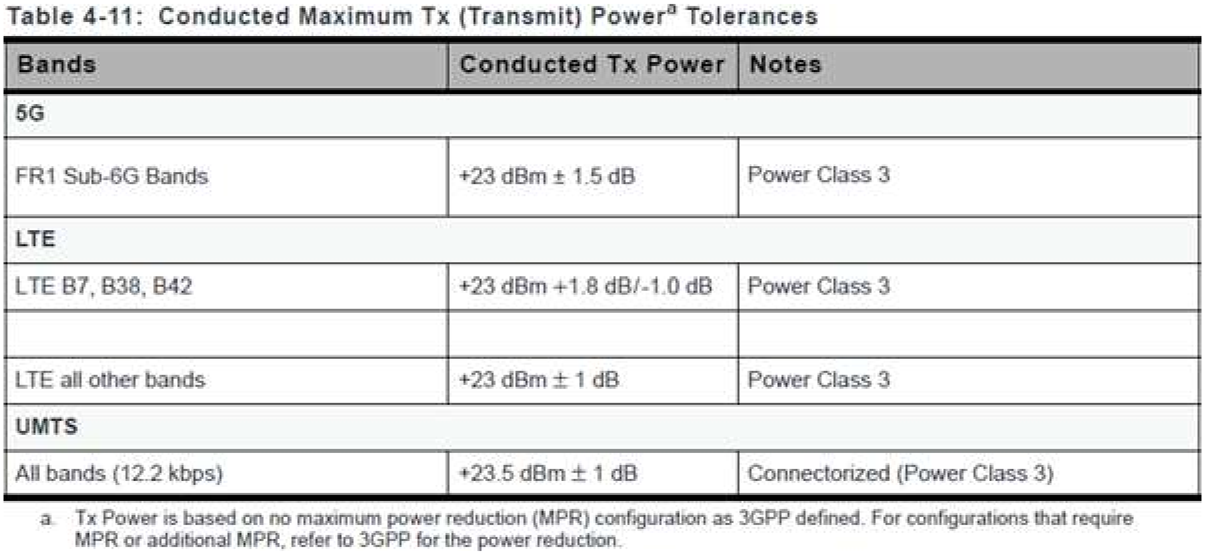
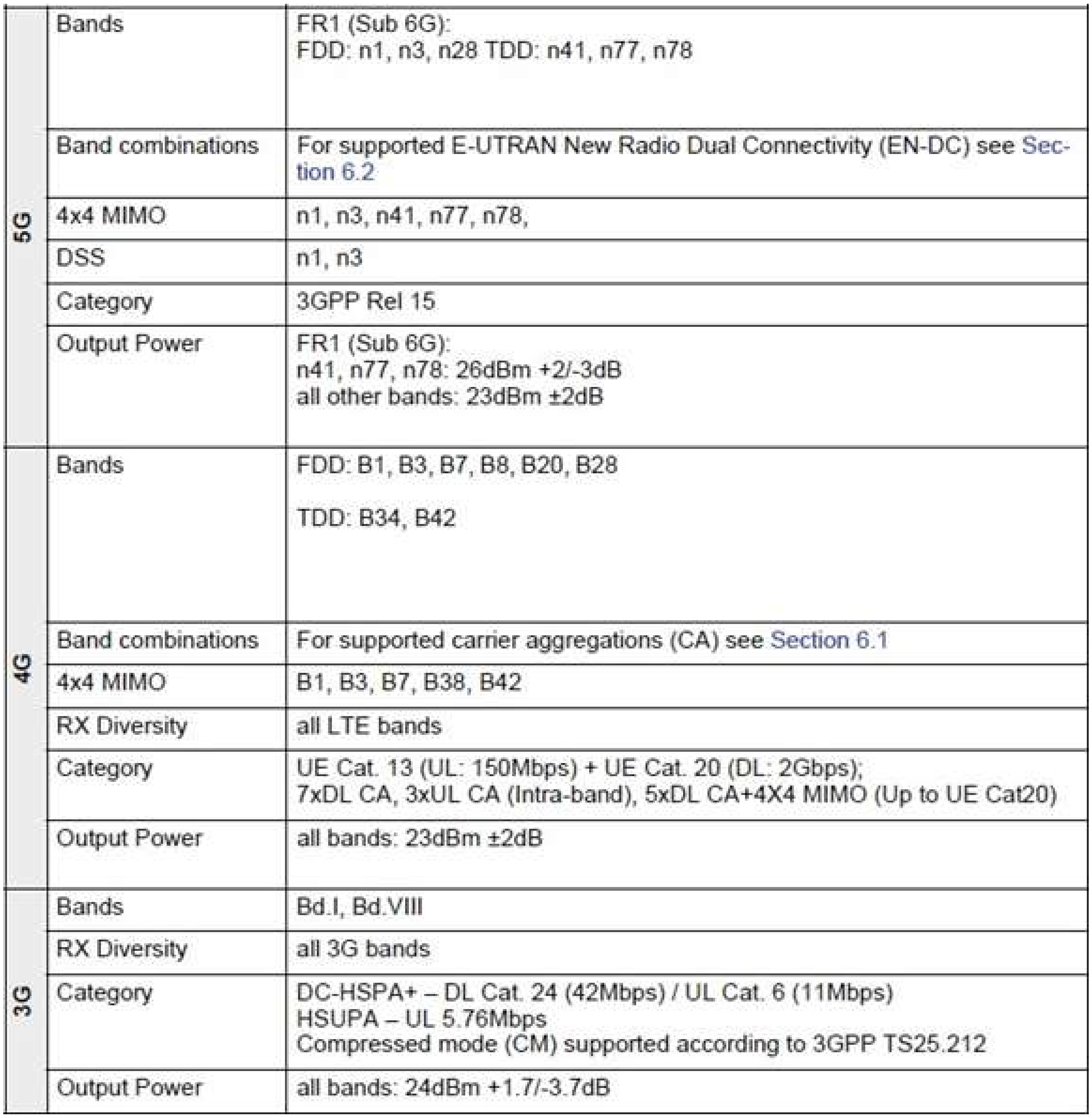


Table 4-11: Conducted Maximum Tx (Transmit) Power[a] Tolerances

Bands	Conducted Tx Power	Notes
5G		
FR1 Sub-6G Bands	+23 dBm ± 1.5 dB	Power Class 3
LTE		
LTE B7, B38, B42	+23 dBm +1.8 dB/-1.0 dB	Power Class 3
LTE all other bands	+23 dBm ± 1 dB	Power Class 3
UMTS		
All bands (12.2 kbps)	+23.5 dBm ± 1 dB	Connectorized (Power Class 3)

[a] Tx Power is based on no maximum power reduction (MPR) configuration as 3GPP defined. For configurations that require MPR or additional MPR, refer to 3GPP for the power reduction.

MV31-W module:

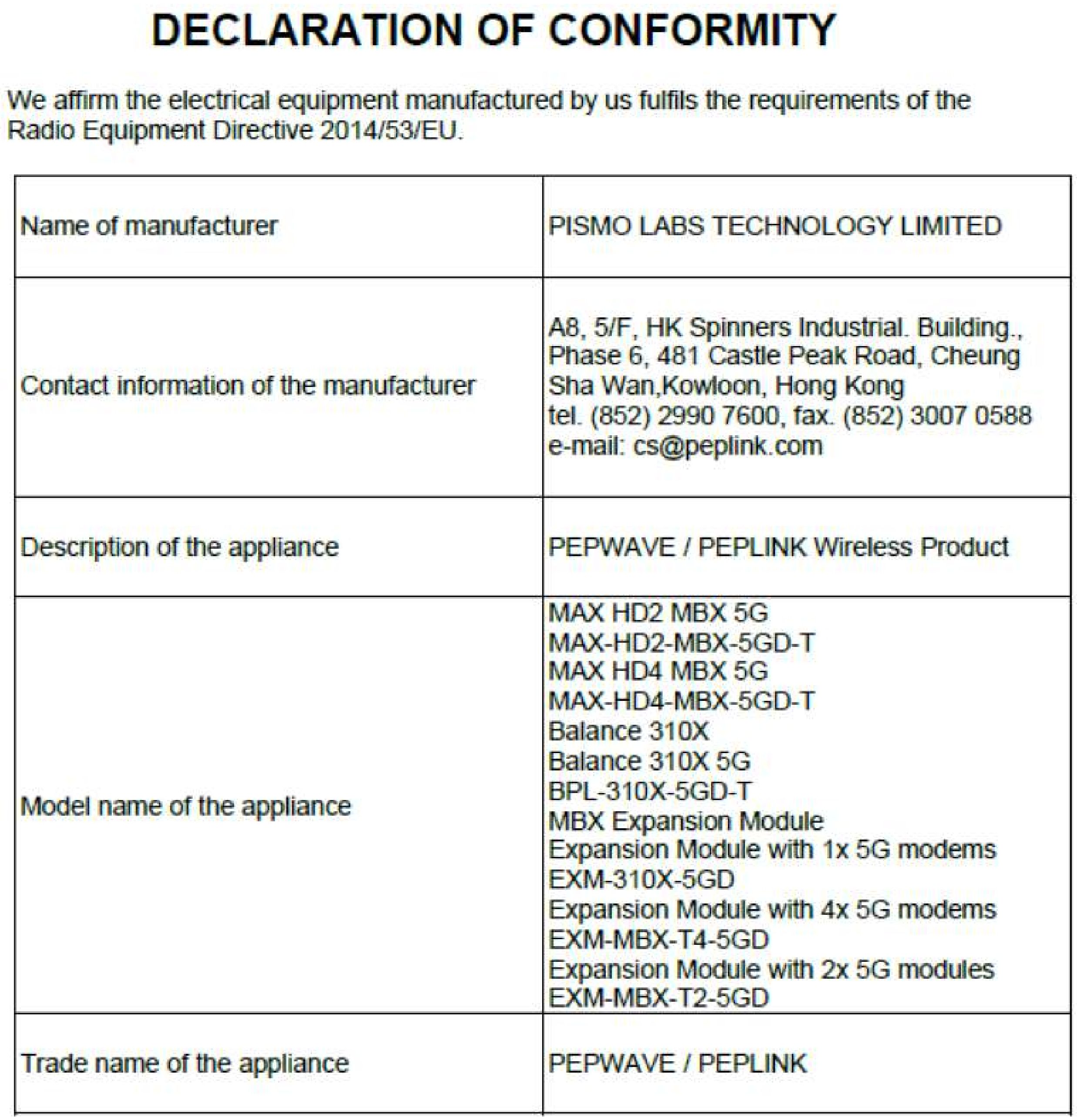


5G	Bands	FR1 (Sub 6G): FDD: n1, n3, n28 TDD: n41, n77, n78
	Band combinations	For supported E-UTRAN New Radio Dual Connectivity (EN-DC) see Section 6.2
	4x4 MIMO	n1, n3, n41, n77, n78,
	DSS	n1, n3
	Category	3GPP Rel 15
	Output Power	FR1 (Sub 6G): n41, n77, n78: 26dBm +2/-3dB all other bands: 23dBm ±2dB
4G	Bands	FDD: B1, B3, B7, B8, B20, B28 TDD: B34, B42
	Band combinations	For supported carrier aggregations (CA) see Section 6.1
	4x4 MIMO	B1, B3, B7, B38, B42
	RX Diversity	all LTE bands
	Category	UE Cat. 13 (UL: 150Mbps) + UE Cat. 20 (DL: 2Gbps); 7xDL CA, 3xUL CA (Intra-band), 5xDL CA+4X4 MIMO (Up to UE Cat20)
	Output Power	all bands: 23dBm ±2dB
3G	Bands	Bd.I, Bd.VIII
	RX Diversity	all 3G bands
	Category	DC-HSPA+ – DL Cat. 24 (42Mbps) / UL Cat. 6 (11Mbps) HSUPA – UL 5.76Mbps Compressed mode (CM) supported according to 3GPP TS25.212
	Output Power	all bands: 24dBm +1.7/-3.7dB

This equipment complies with CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 21cm between the radiator & your body.

contact as: https://www.peplink.com/

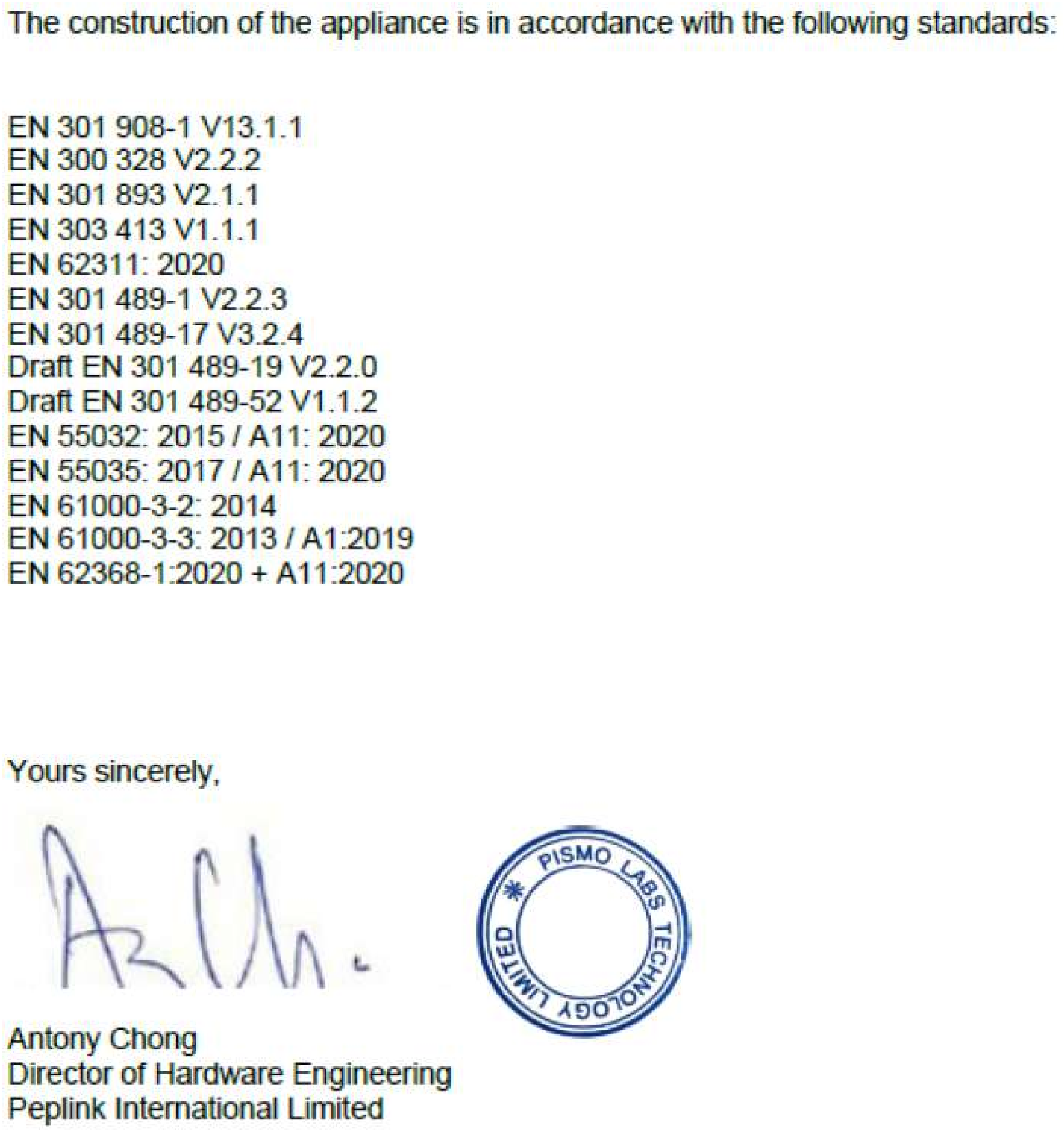
CE Statement for Pepwave Routers (Balance 310X 5G)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan,Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	MAX HD2 MBX 5G MAX-HD2-MBX-5GD-T MAX HD4 MBX 5G MAX-HD4-MBX-5GD-T Balance 310X Balance 310X 5G BPL-310X-5GD-T MBX Expansion Module Expansion Module with 1x 5G modems EXM-310X-5GD Expansion Module with 4x 5G modems EXM-MBX-T4-5GD Expansion Module with 2x 5G modules EXM-MBX-T2-5GD
Trade name of the appliance	PEPWAVE / PEPLINK



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

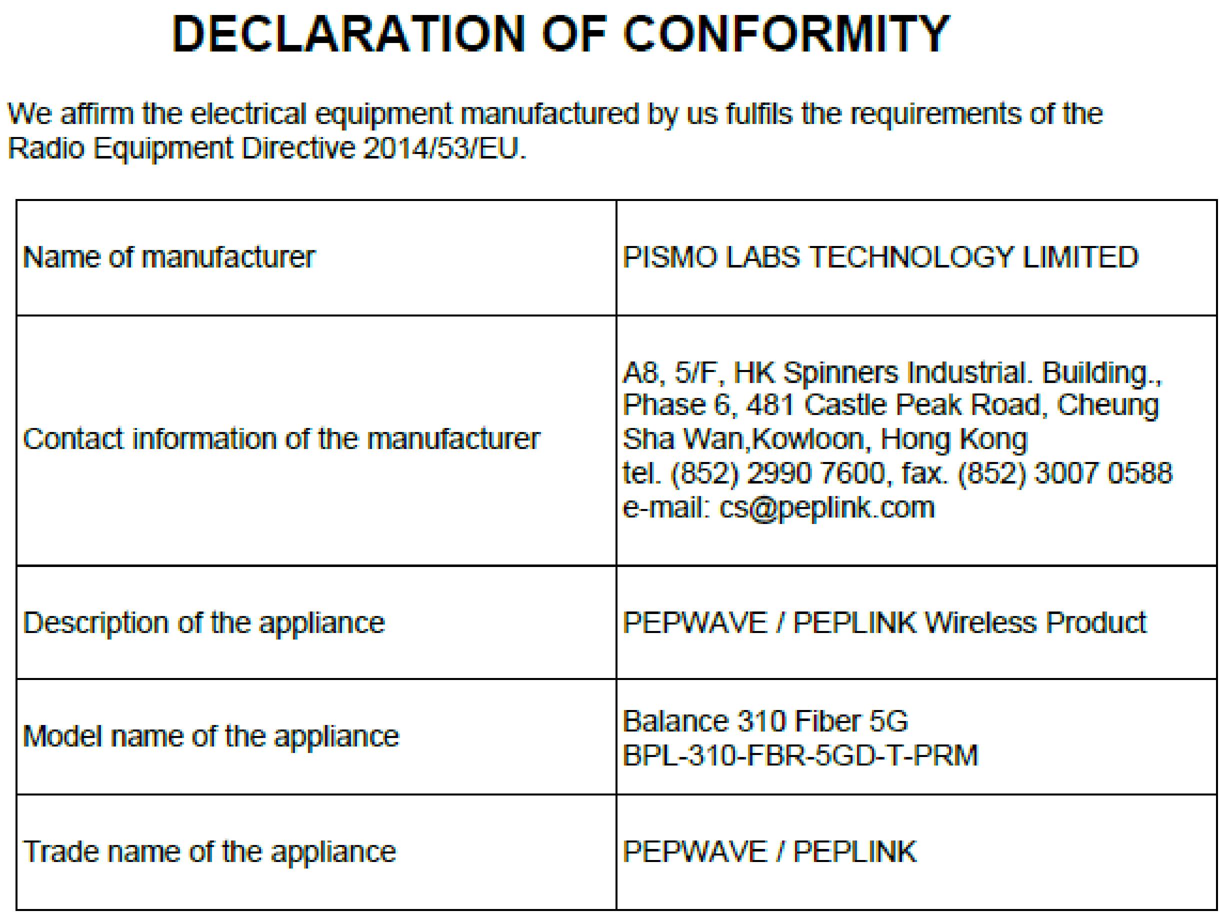
EN 301 908-1 V13.1.1
EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 303 413 V1.1.1
EN 62311: 2020
EN 301 489-1 V2.2.3
EN 301 489-17 V3.2.4
Draft EN 301 489-19 V2.2.0
Draft EN 301 489-52 V1.1.2
EN 55032: 2015 / A11: 2020
EN 55035: 2017 / A11: 2020
EN 61000-3-2: 2014
EN 61000-3-3: 2013 / A1:2019
EN 62368-1:2020 + A11:2020

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED *

Antony Chong
Director of Hardware Engineering
Peplink International Limited

CE Statement for Pepwave Routers (Balance 310 Fiber 5G)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan,Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Balance 310 Fiber 5G BPL-310-FBR-5GD-T-PRM
Trade name of the appliance	PEPWAVE / PEPLINK

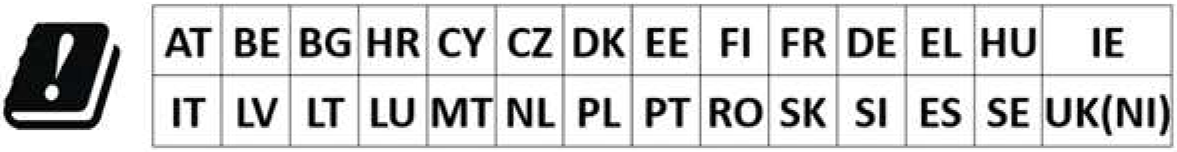
The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 301 908-1 V13.1.1
EN 62311: 2020
EN 301 489-1 V2.2.3
EN 301 489-17 V3.2.4
Draft EN 301 489-52 V1.1.2
EN 55032: 2015 / A11:2020
EN 55035: 2017 / A11:2020
EN 61000-3-2: 2014
EN 61000-3-3: 2013 / A1:2019
EN 62368-1:2020 + A11:2020

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited

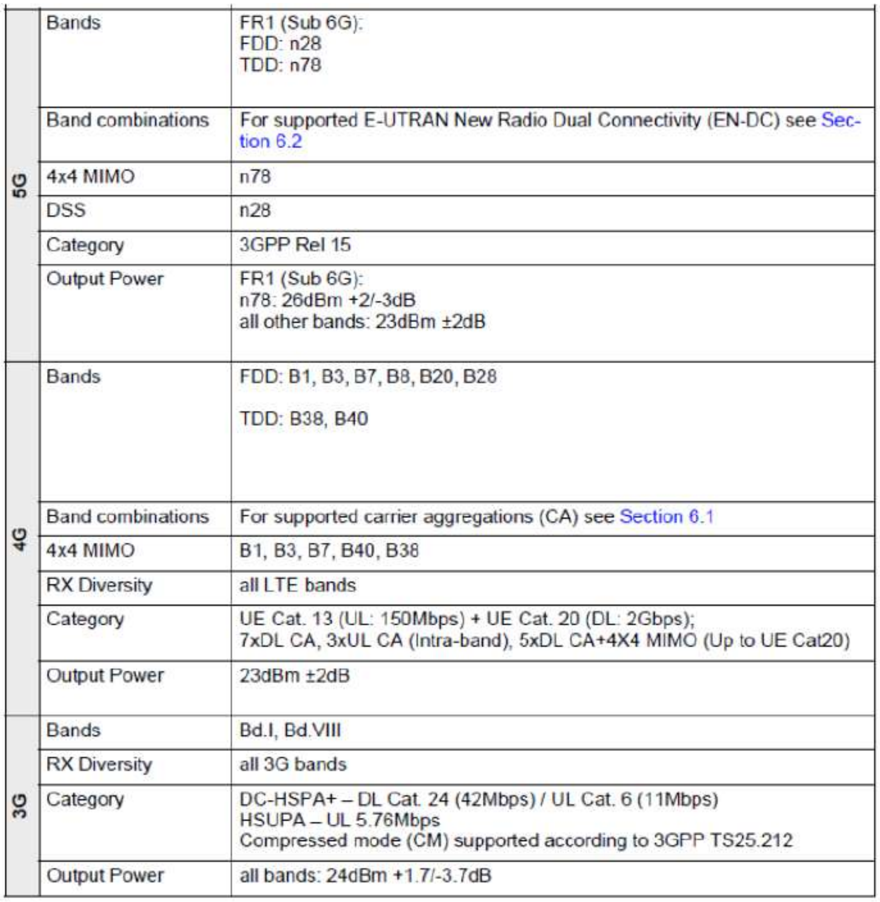


AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

2.4GHz (2412 – 2472 MHz) : 19.94 dBm

5GHz (5150 - 5250 MHz) : 22.76 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

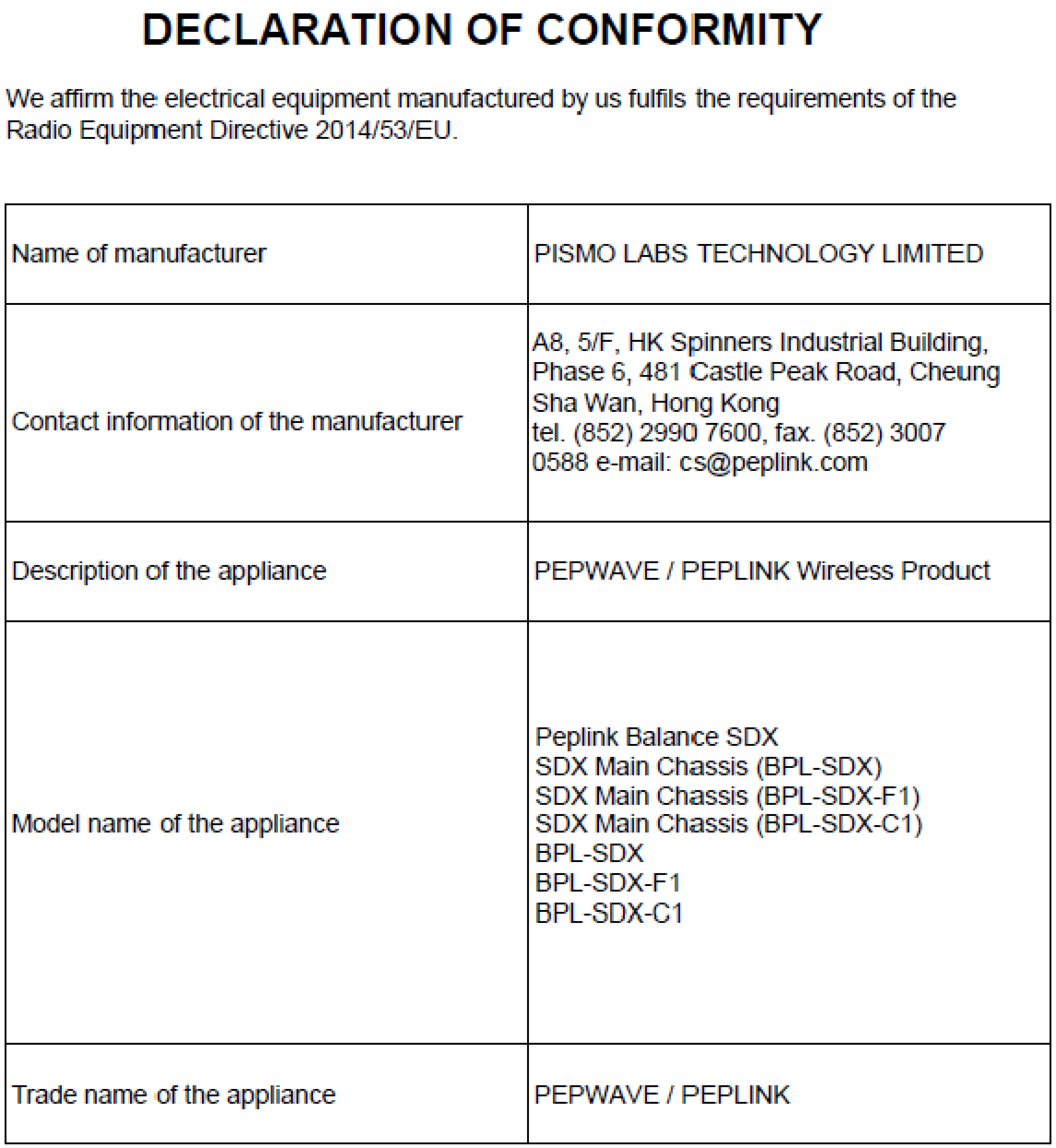


5G	Bands	FR1 (Sub 6G): FDD: n28 TDD: n78
	Band combinations	For supported E-UTRAN New Radio Dual Connectivity (EN-DC) see Section 6.2
	4x4 MIMO	n78
	DSS	n28
	Category	3GPP Rel 15
	Output Power	FR1 (Sub 6G): n78: 26dBm +2/-3dB all other bands: 23dBm ±2dB
4G	Bands	FDD: B1, B3, B7, B8, B20, B28 TDD: B38, B40
	Band combinations	For supported carrier aggregations (CA) see Section 6.1
	4x4 MIMO	B1, B3, B7, B40, B38
	RX Diversity	all LTE bands
	Category	UE Cat. 13 (UL: 150Mbps) + UE Cat. 20 (DL: 2Gbps); 7xDL CA, 3xUL CA (Intra-band), 5xDL CA+4X4 MIMO (Up to UE Cat20)
	Output Power	23dBm ±2dB
3G	Bands	Bd.I, Bd.VIII
	RX Diversity	all 3G bands
	Category	DC-HSPA+ – DL Cat. 24 (42Mbps) / UL Cat. 6 (11Mbps) HSUPA – UL 5.76Mbps Compressed mode (CM) supported according to 3GPP TS25.212
	Output Power	all bands: 24dBm +1.7/-3.7dB

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

contact as: https://www.peplink.com/

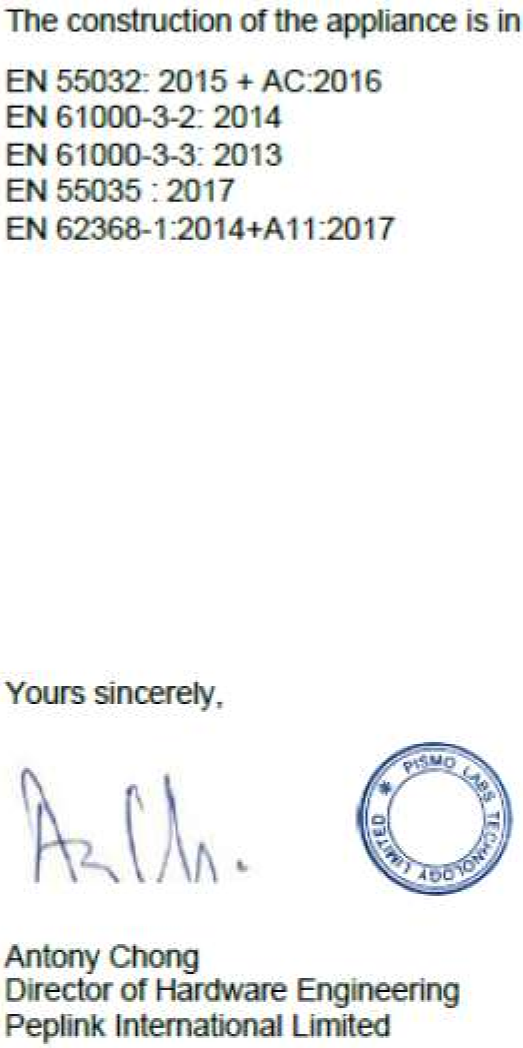
CE Statement for Pepwave Routers (Balance SDX)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building, Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Peplink Balance SDX SDX Main Chassis (BPL-SDX) SDX Main Chassis (BPL-SDX-F1) SDX Main Chassis (BPL-SDX-C1) BPL-SDX BPL-SDX-F1 BPL-SDX-C1
Trade name of the appliance	PEPWAVE / PEPLINK



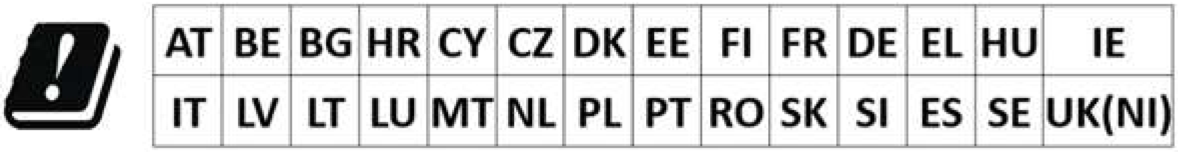
The construction of the appliance is in accordance with the following standards:

EN 55032: 2015 + AC:2016
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035 : 2017
EN 62368-1:2014+A11:2017

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

contact as: https://www.peplink.com/

FCC Requirements for Operation in the United States

Federal Communications Commission (FCC) Compliance Notice:

For Balance SDX Pro

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Industry Canada Statement (Balance SDX Pro)

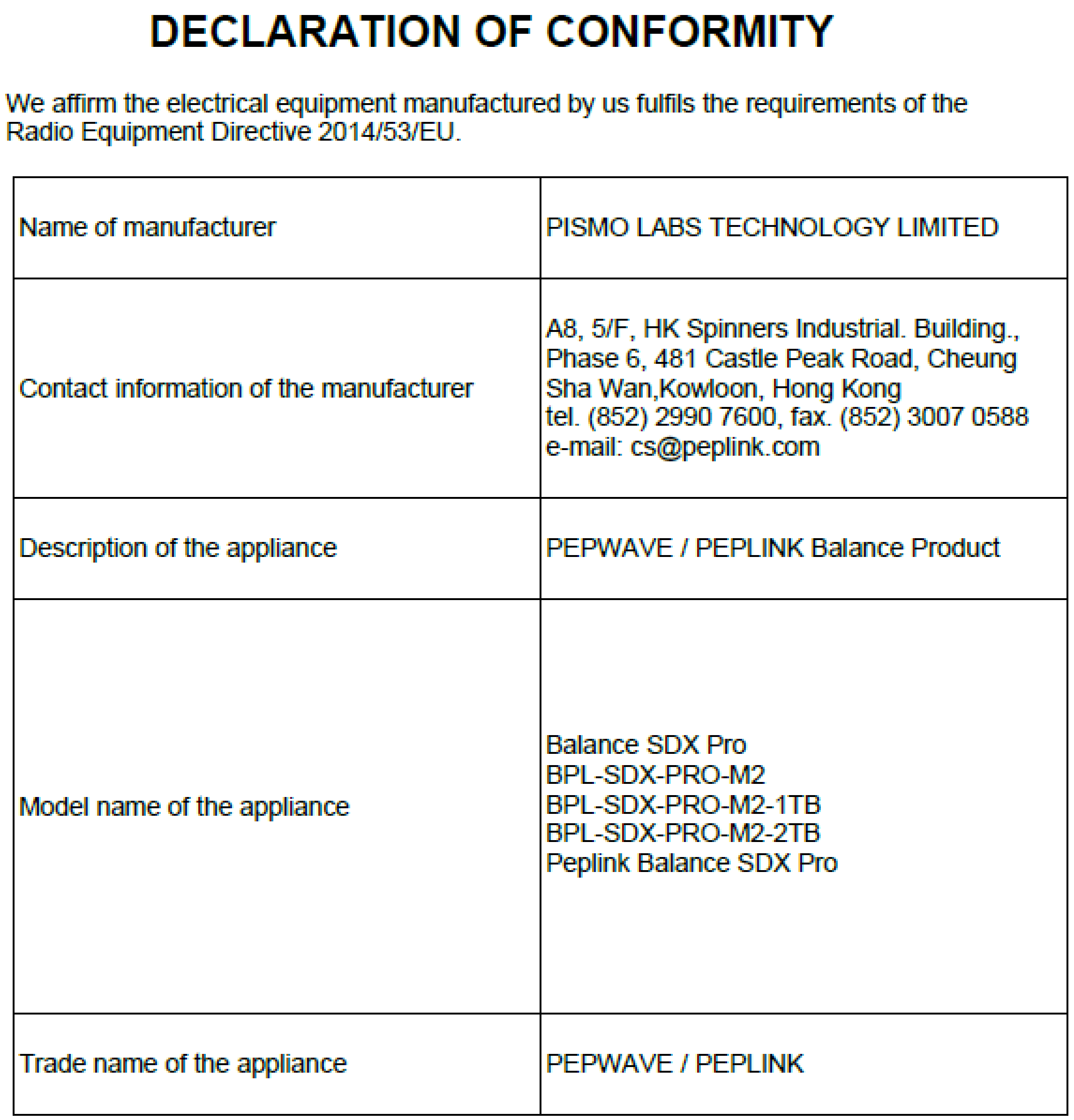
This product meets the applicable Innovation, Science and Economic Development Canada technical Specifications.

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

Battery Caution Statement (Balance SDX Pro)

Risk of explosion if the battery is replaced by an incorrect type.

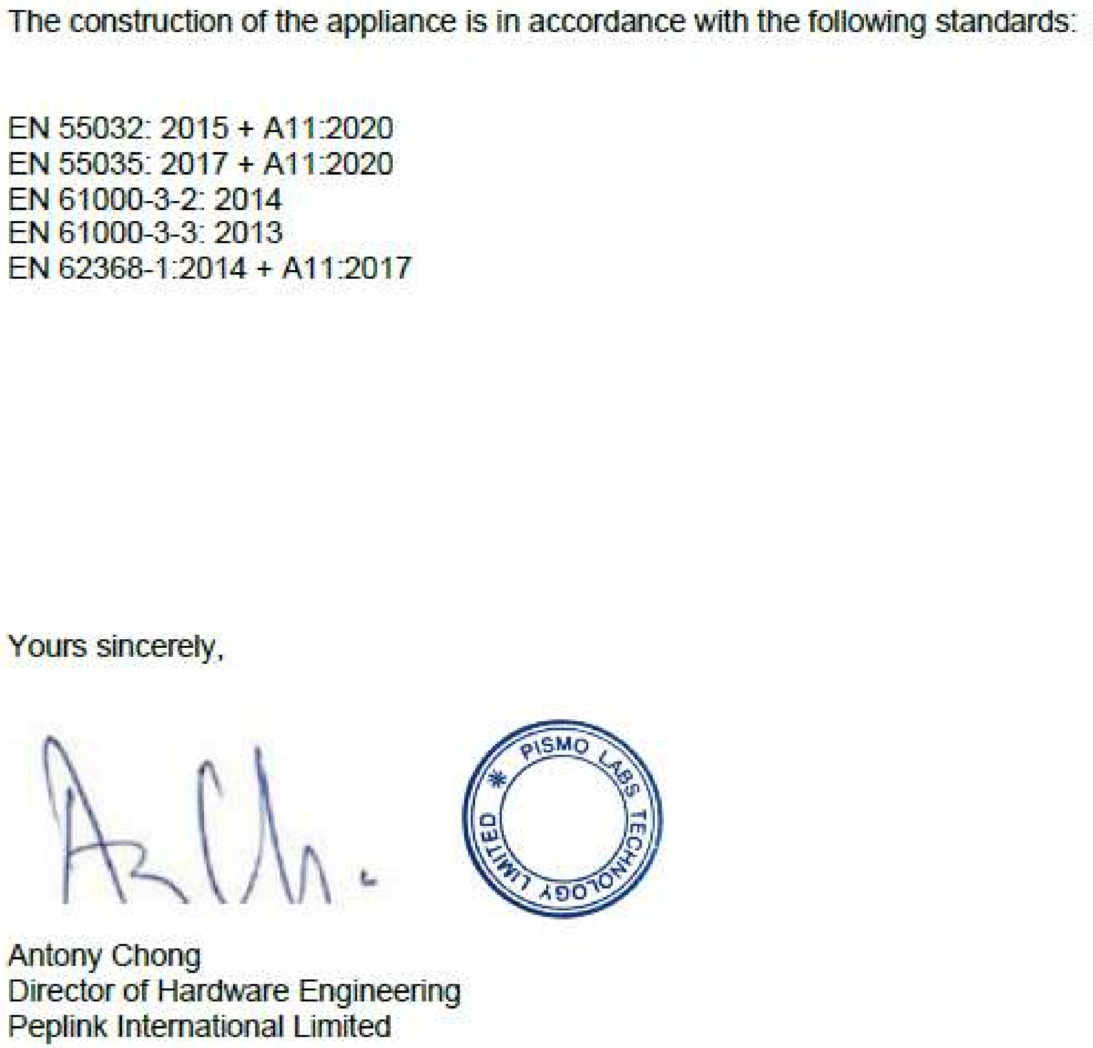
CE Statement for Pepwave Routers (Balance SDX Pro)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan,Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Balance Product
Model name of the appliance	Balance SDX Pro BPL-SDX-PRO-M2 BPL-SDX-PRO-M2-1TB BPL-SDX-PRO-M2-2TB Peplink Balance SDX Pro
Trade name of the appliance	PEPWAVE / PEPLINK



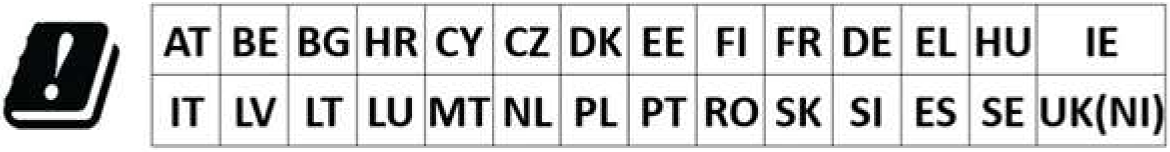
The construction of the appliance is in accordance with the following standards:

EN 55032: 2015 + A11:2020
EN 55035: 2017 + A11:2020
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 62368-1:2014 + A11:2017

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

contact as: https://www.peplink.com/

FCC Requirements for Operation in the United States

Federal Communications Commission (FCC) Compliance Notice:

For Balance 380X, Balance 580X

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it 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.

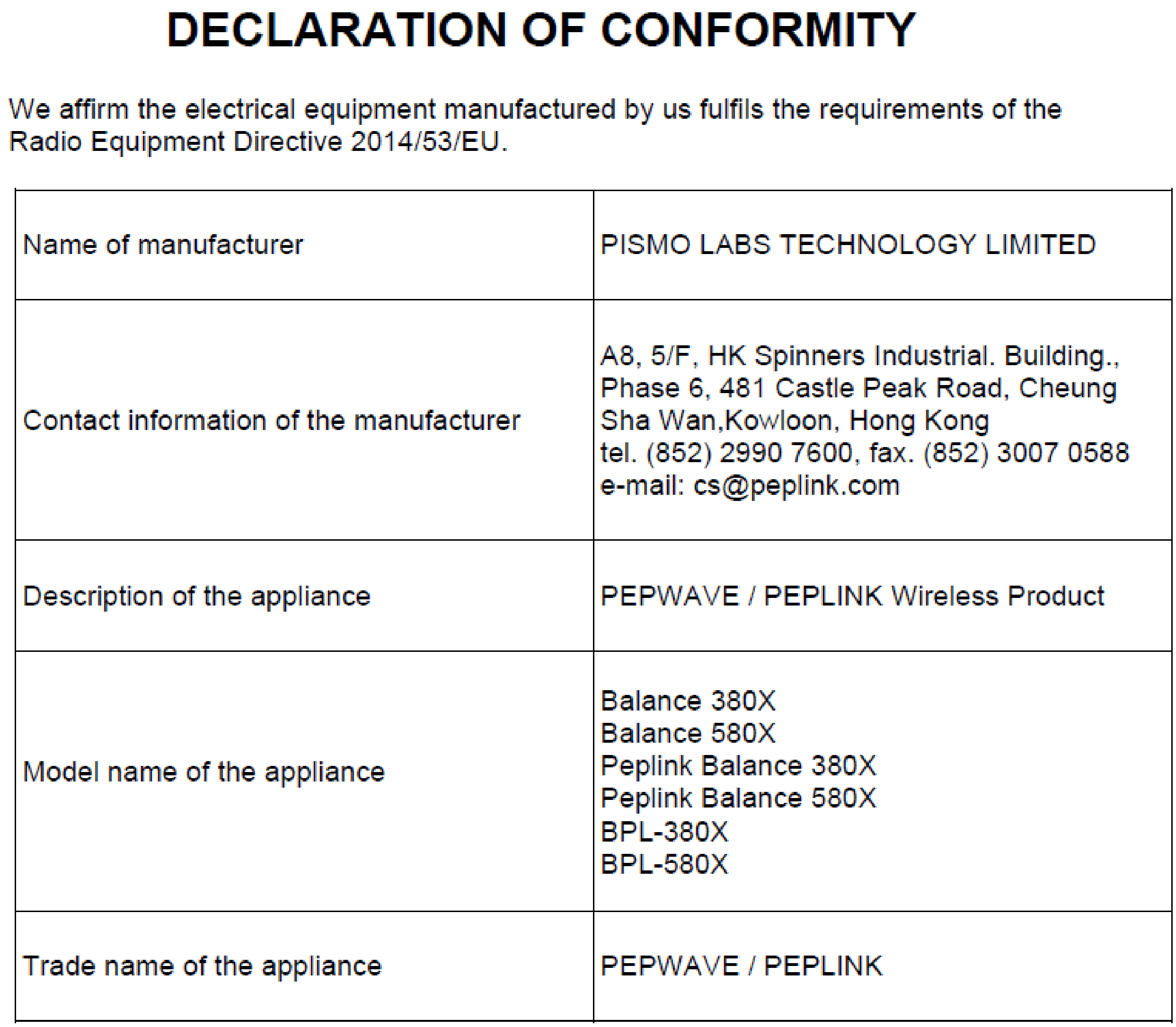
Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Industry Canada Statement (Balance 380X, Balance 580X)

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

Ce produit répond aux spécifications techniques applicables à l'innovation, Science et Développement économique Canada.

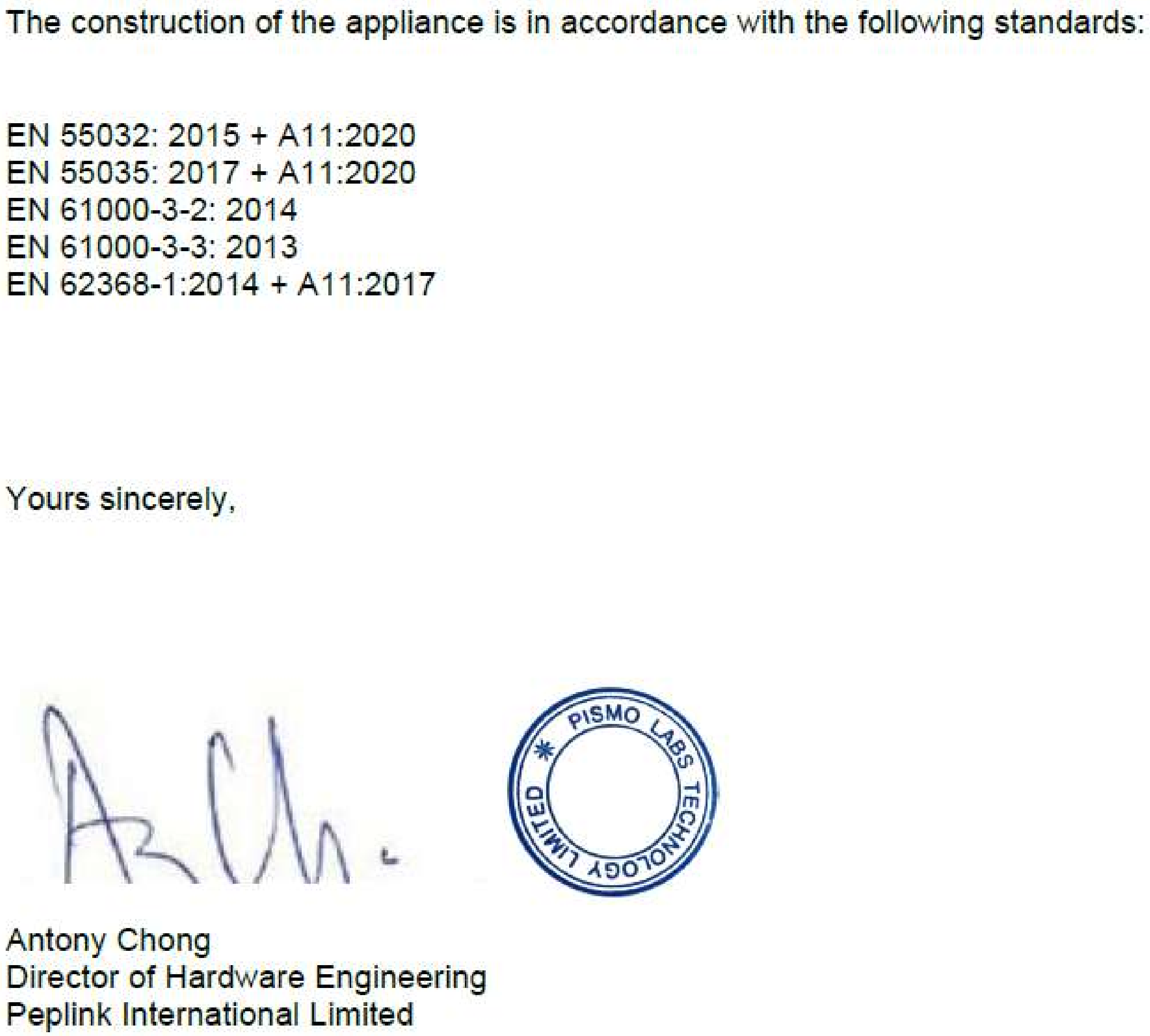
CE Statement for Pepwave Routers (Balance 380X / Balance 580X)



DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan,Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	Balance 380X Balance 580X Peplink Balance 380X Peplink Balance 580X BPL-380X BPL-580X
Trade name of the appliance	PEPWAVE / PEPLINK



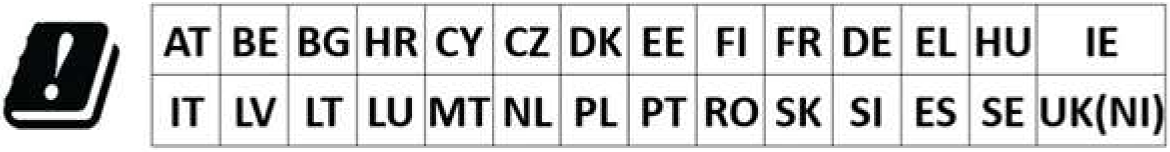
The construction of the appliance is in accordance with the following standards:

EN 55032: 2015 + A11:2020
EN 55035: 2017 + A11:2020
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 62368-1:2014 + A11:2017

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

contact as: https://www.peplink.com/

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

For Balance 20X Pro

Federal Communication Commission Interference Statement

Any changes or modifications not expressly approved by the party responsible for compliance could void your 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, it 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.

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

Radiation Exposure Statement

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

Industry Canada Statement (Balance 20X Pro)

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

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

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio ex-empts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et
(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en

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

(ii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; (detachable antenna only) ; and
The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

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

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l’intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) Le gain maximal d’antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l’exploitation point à point et non point à point, selon le cas.
En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu’ils ont la priorité) pour les bandes 5725-5850 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

(iii) Le gain maximal d’antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l’exploitation point à point et non point à point.

Radiation Exposure Statement

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

Cet appareil doit être installé et utilisé avec une distance minimale de 20cm entre l’émetteuret votre corps. Cet appareil et sa ou ses antennes ne doivent pas être co-localisés ou fonctionner en conjonction avec tout autre antenne ou transmetteur.

This radio transmitter IC: 20682-P1AX19 has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

WIFI Antenna type: Omni-directional
WIFI Antenna gain: 2.4GHz / 2.44 dBi
5150 ~ 5250 MHz / 4.10 dBi
5725 ~ 5850 MHz / 4.73 dBi

Cet émetteur radio IC : 20682-P1AX11 a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antennes répertoriés ci-dessous, avec le gain maximal autorisé indiqué. Les types d'antenne non inclus dans cette liste qui ont un gain supérieur au gain maximum indiqué pour tout type répertorié sont strictement interdits pour une utilisation avec cet appareil.

Type d'antenne WIFI : omnidirectionnelle
Gain de l'antenne Wi-Fi : 2.4 GHz / 2.44 dBi
5150 ~ 5250 MHz / 4.10 dBi
5725 ~ 5850 MHz / 4.73 dBi

Battery Caution Statement

Risk of explosion if the battery replaced by an incorrect type, place the battery into fire, a hot oven, extremely high temperature or low air pressure surrounding environment, the leakage of flammable liquid or gas, and mechanically crushing or cutting of the battery.

USB WAN Modem Port Specification

Balance Series

	20X Pro	30 LTE	30 Pro	ONE	TWO	210
Output Rating	5V DC, 2A	5V DC, 2A	5V DC, 2A	5V DC, 2A	5V DC, 1.5A	5V DC, 1A

	310X	380	380X	580	580X	710	1350	2500
Output Rating	5V DC, 0.5A	5V DC, 0.5A	5V DC, 1A	5V DC, 0.5A	5V DC, 1A	5V DC, 2.5A	5V DC, 2.5A	5V DC, 2.5A