

the host.

In the reverse lookup zone, add a pointer (PTR) resource record that maps the host IP address to the host name.

• Click the **New Reverse Lookup Zone** button and enter a reverse lookup zone name. If you are delegated the subnet *11.22.33.0/24*, the **Zone Name** should be *33.22.11.in-arpa.add*r. PTR records for *11.22.33.1*, *11.22.33.2*, ... *11.22.33.254* should be defined in this zone where the host IP numbers are *1*, *2*, ... *254*, respectively.

SOA Record		
	WARNING: You should define SOA record in your zo <u>Click here to define SOA Record</u>	ne!
NS Records		?
lost	Name Server	TTL (sec)
	WARNING: You should define NS records in your zo	ne!
	New NS Records	
NAME Records		(?
Host	Points To	TTL (sec)
	There is currently no CNAME records.	
	New CNAME Record	
PTR Records		(?
Host IP Number	Points To	TTL (sec)
	There is currently no PTR records.	1
	New PTR Record	

#### SOA Record

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

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

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

For example:

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

"ns2.mydomain.com."

**Email, Refresh, Retry, Expire, Min Time, and TTL** are entered in the same way as in the forward zone. Please refer to **Section 17.3.5** for details.

#### NS Records

NS Records			
Host Name Server	This is equivalent to 33.22.11.in-addr.arpa.	TTL (sec)	_
		3600	+

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

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

#### **CNAME** Records



Host		
Points To	This is equivalent to 33.22.11.in-addr.arpa.	
TTL (sec)	3600	

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

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



#### PTR Records

Host IP Number	This is equivalent to	
	33.22.11.in-addr.arpa.	
TTL (sec)	3600	

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

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

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

#### **DNS Record Import Wizard**

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

wizard allows you to import DNS records from an existing DNS s	server via zone transfer.
irement: Your existing DNS server is configured to allow one of ansfer DNS zone records.	the WAN's default IP addresses
ontinue. click Next.	

• Select **Next >>** to continue.

tep 1 of 3				
arger DNS Server IF Address.				
ransfer via				
WAN 1	T			
		<< Back	Next >>	Cancel
Colour Huxt >> to continue.				
NS Record Import Wizard				
ONS Record Import Wizard				
ONS Record Import Wizard Step 2 of 3 Domain Names (Zones): mycompany.com				
ONS Record Import Wizard Step 2 of 3 Domain Names (Zones): mycompany.com peplink.com				
ONS Record Import Wizard Step 2 of 3 Domain Names (Zones): mycompany.com peplink.com				
ONS Record Import Wizard Step 2 of 3 Domain Names (Zones): mycompany.com peplink.com				
ONS Record Import Wizard Step 2 of 3 Domain Names (Zones): mycompany.com peplink.com				
ONS Record Import Wizard Step 2 of 3 Domain Names (Zones): mycompany.com peplink.com				
ONS Record Import Wizard Step 2 of 3 Domain Names (Zones): mycompany.com peplink.com  (One domain name per line)		<< Back	Next >>	Cancel

#### Important Note

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

#### Peplink Balance User Manual

## peplink | PEPWAVE

Step 2 of 3	(Continue)			
WARNING: T	he <mark>foll</mark> owing doma	ain(s) already exist:		
pepli <mark>nk.</mark> com				
The existing	records of these d	omains will be over	written.	

etching zone records	
	Abor
· · · · · · · · · · · · · · · · · · ·	Abor
DNS Record Import Wizard	Abor
DNS Record Import Wizard Step 3 of 3	Abor

Domain	Result	Details
pep <mark>lin</mark> k.com	Ok	
mycompany com	Ok	8
, sompany, som	54	2
in teampany series		



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

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

#### 7.6 NAT Mappings

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

NAT mappings can be configured at Network>NAT Mappings.

LAN Clients	Inbound Mappings	Outbound Mappings	
	No NAT Mappings De	fined	
	Add NAT Rule		

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

NAT Mappings			
LAN Client(s)	?	IP Address 🔻	
Address	?	192.168.1.123	
Inbound Mappings	3	Connection / Inbound IP WAN 1 WAN 2 WAN 3 WAN 3 WAN 4 WAN 5 Mobile Internet PepVPN	Address(es)
Outbound Mappings	?	Connection / Outbound II	P Address
		WAN 1	10.22.1.182 (Interface IP) •
		WAN 2	Interface IP 🔻
		WAN 3	Interface IP 🔹
		WAN 4	192.168.254.10 (Interface IP) 🔻
		WAN 5	Interface IP
		Mobile Internet	Interface IP 🔹
			Save Cancel

#### **NAT Mapping Settings**

LAN Client(s) NAT Mapping rules can be defined for a single LAN **IP Address**, an **IP Range**, or an **IP Network**.



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

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

#### **Important Note**

Inbound firewall rules override inbound mapping settings.

#### 7.7 MediaFast

MediaFast settings can be configured by navigating to Network > MediaFast.



#### Setting Up MediaFast Content Caching

To access MediaFast content caching settings, select **Network > MediaFast**.

MediaFast	
Enable	
Domains / IP Addresses	<ul> <li>Cache all</li> <li>Whitelist</li> <li>Blacklist</li> </ul>
Source IP Subnet	<ul> <li>Image: Any O Custom</li> </ul>

	MediaFast				
Enable	Click the checkbox to enable MediaFast content caching.				
Domains / IP Addresses	Choose to <b>Cache on all domains</b> , or enter domain names and then choose either <b>Whitelist</b> (cache the specified domains only) or <b>Blacklist</b> (do not cache the specified domains).				
Source IP Subnet	This setting allows caching to be enabled on custom subnets only. If "Any" is selected, then caching will apply to all subnets.				

Secure Content Caching Enable	?	Note: Please enable MediaFast for Secure Content Caching
Domains / IP Addresses	0	Cache all Whitelist Blacklist googlevideo.com youtube.com
Source IP Subnet	?	• Any O Custom

The Secure Content Caching menu operates identically to the MediaFast menu, except it is for secure content cachting accessible through https://.



In order for Mediafast devices to cache and deliver HTTPS content, every client needs to have the necessary certificates installed\*.

\*See https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/

Cache Control					
Content Type	?	<ul> <li>Video</li> <li>Audio</li> <li>Images</li> <li>OS / Application Updates</li> </ul>			
Cache Lifetime Settings	?	File Extension	Lifetime (days)	+	

	Cache Control
Content Type	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
Cache Lifetime Settings	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.

#### **Viewing MediaFast Statistics**

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





#### **Prefetch Schedule**

Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Network > MediaFast > Prefetch Schedule**.

Name		Next Run Time	Last Run Time	Last Duration		Last Download	Actions
Course Progress	Downloading	04-11 06:00	04-09 02:03	-	3	0 B	= 🗷 🗙
National Geog	Ready	04-11 00:00	04-09 00:00	00:01	1	4.98 kB	🛓 🕜 🗙
Syllabus	Downloading	04-11 06:00	04-09 06:00	-	3	0 B	• 🖉 🗙
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01	4	115.91 kB	🛓 🕜 🗙
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01	1	62.26 kB	🛓 🕜 🗙
		Ne	w Schedule				

	Prefetch Schedule Settings
Name	This field displays the name given to the scheduled download.
Status	Check the status of your scheduled download here.
Next Run Time/Last Run Time	These fields display the date and time of the next and most recent occurrences of the scheduled download.
Last Duration	Check this field to ensure that the most recent download took as long as expected to complete. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time.
Result	This field indicates whether downloads are in progress (  ) or complete ( $\checkmark$ ).
Last Download	Check this field to ensure that the most recent download file size is within the expected range. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time. This field is also useful for quickly seeing which downloads are consuming the most storage space.
Actions	To begin a scheduled download immediately, click 📥. To cancel a scheduled download, click 💻. To edit a scheduled download, click 🕼. To delete a scheduled download, click 渊.
New Schedule	Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:

	MediaFast Schedul	e				
	Name (optional)					
	Active	2				
	URL	URL				
		•				
	Depth	2 V levels Default				
	Time Period	From 00 • : 00 • to 01 • : 00 •				
	Repeat	Everyday				
	Bandwidth Limit	0 Gbps • (0: Unlimited)				
	Simply provide the reque	Save & Apply Now Cancel ested information to create your schedule.				
Clear Web Cache	Click to clear all cached	content. Note that this action cannot be undone.				
<b>Clear Statistics</b>	Click to clear all prefetch	n and status page statistics.				

#### 7.8 ContentHub

Integrated into MediaFast-enabled routers, ContentHub allows you to deliver webpages and applications using the local storage on your router.

Users will be able to access news, articles, videos, and access your web app, without the need for internet access.

ContentHub Storage needs to be configured before content can be uploaded to the ContentHub. Follow the link on the information panel to configure storage.

ContentHub storage has not been configured. Click here to review storage configuration

To access ContentHub, navigate to Network > ContentHub and check the Enable box.:



nable		ی (۲)					
				Save			
Schedule							
Vahcitac	Source		Next Update	Last Updated	Elapsed Time	Status Actions	
websites	_		No	Schedule			

On an external server configure content (a website or application) that will be synced to the ContentHub; for example a html5 website.

To configure a website or application as content follow these steps.

#### Configure a website to be published from the contenthub

This option allows you to sync a website to the Peplink router, this website will then be published with the specified domain from the router itself and makes the content available to the client via the HTTP/HTTPS protocol.

Only FTP sync is supported for this type of Contenthub content.

The content should be uploaded to an FTP server before.

Click New Website, and the following configuration options will appear:

Active	
Туре	Website      Application
Protocol	HTTP V
Domain/Path	http://
Source	ftp     ://       Username:
Period	Everyday • From 00 •: 00 • to 01 •: 00 •
Bandwidth Limit	0 Gbps ▼ (0: Unlimited)

The Active checkbox toggles the activation of the content. For type, select Website.

Туре	HTTP,HTTPS or both
Domain/Pat h	The contenhub uses this as the domain name for client access (such as http://mytest.com).
Source	Enter the server details that the content will be downloaded from. Enter your credentials under <b>Username</b> and <b>Password</b> .
Period	This field determines how often the Router will search for updates to the source content.
Method	Only applicable for application: Choose between sync or file upload
Bandwidth Limit	Used to limit the bandwidth for each client to access the web server.



Click "Save & Apply Now" to activate the changes. Below is a screenshot after configuration:

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions			
http://mytest.	.com						+	ß	×
/(root)	ftp://10.8.76.254/web	-				*	C	C	×
		Net	w Website						

"

The content will be synced based on the **Period** that is configured before.

If you want to trigger the sync manually, you can click "

When the sync is completed, you'll see a summary as shown in the screenshot below:

Thttp://mytest.com /(root) ftp://10.8.76.254/web 05-23 03:41 00:00:11 ♥ ▲		
/(root) ftp://10.8.76.254/web 05-23 03:41 00:00:11 📀 🛃	+ 🕜	
	6 6	
New Website Status details	Close	

To access the content, open a browser in MFA's client and enter the domain configured before (such as <a href="http://mytest.com">http://mytest.com</a>).

#### Configure an application to be published from the contenthub

Mediafast Routers allow you to configure and publish ant application from the router itself by using the supported framework

- Python (version 2.7.12)
- Ruby (version 2.3.3)
- Node.js (version 6.9.2)

First install the desired framework in "Package Manager" as below:

#### Peplink Balance User Manual

## peplink | PEPWAVE

peplink	Dashboard	Setup Wizard	Network	AP System	Status	Apply Changes
System						
<ul> <li>Admin Security</li> </ul>	(Last Upd	ate: Tue May 23 0	4:02:36 UTC 2	2017)		
Firmware	Package	List				Update All
Time	Node.js	9.2 (17178)				
<ul> <li>Schedule</li> </ul>	Size: 8.99 Date: Fri Fi	MB eb 24 07:45:28 UTC 2	2017			
Email Notification	Python					
Event Log	Version: 2. Size: 20.29	.7.12 (17178) 9 MB				<b>±</b>
SNMP	Date: Fri F	eb 24 07:45:28 UTC 2	2017			
<ul> <li>InControl</li> </ul>	Version: 2.	.3.3 (17178)				
<ul> <li>Configuration</li> </ul>	Size: 31.44 Date: Fri F	4 MB eb 24 07:45:30 UTC 2	2017			
Feature Add-ons						
Reboot						
Tools						
Ping						
Traceroute						
Wake-on-LAN						
Storage Manager						
Package Manager						
Logout						

After installing the framework, you can select the type to "Application" and configure the website:

Active	
Туре	O Website 💽 Application
Protocol	HTTP \$
Domain (	http://
Method (	🕜 💿 Sync 🔿 File Upload
Source	ftp     ://       Username:
Period	Everyday \$ From 00 \$: 00 \$ to 01 \$: 00 \$
Bandwidth Limit	0 Gbps 🗘 (0: Unlimited)

The setting is same as Website type and you can refer to the description in the above section

For the Application type, you need to pack your application as below:

- 1. Implement two bash script files, start.sh and stop.sh in root folder, to start and stop your application. the Mediafast router will only execute start.sh and stop.sh when the corresponding website is enabled and disabled respectively.
- 2. Compress your application files and the bash script to .tar.gz format.
- 3. Upload this tar file to the router.

#### **MDM Settings**

In addition to performing content caching, MediaFast-enabled routers can also serve as an MDM, administrating to client devices. To access MDM Settings, navigate to **Network > MDM Settings**:

MDM Settings				
Enable				
Account Settings	O Follow Web Admin Account  Custom			
Username				
Password				
Confirm Password				

	MDM Settings
Enable	Click this checkbox to enable MDM on your router.
Account Settings	Click <b>Follow Web Admin Account</b> to allow client devices to use the built-in administrator account when performing MDM. Set <b>Custom</b> to specify a username and password your router will use to log into your client devices.

Please refer to the knowledgebase for information about enrolling client devices to MDM: <u>https://forum.peplink.com/t/how-to-enroll-a-device-to-the-mdm-server/8454</u>

#### Docker

MediaFast enabled routers can host Docker containers when running firmware 7.1 or later. Docker is an open platform for developing, shipping, and running applications. From firmware version 7.1.0 upwards it is possible to install and run Docker Containers on your Peplink Mediafast 500 or 750 router.

Due to the nature of Docker and its unlimited variables; this feature is supported by Peplink up to the point of creating a running Docker Container. Information about Docker can be found on the Docker Documentation site: https://docs.docker.com/ 2

This will allow you to run for example a file sharing platform (Owncloud), a web server (Wordpress, Joomla), a learning platform (Moodle) or a visualisation tool for viewing large scale data (Kibana). The Peplink router will search through the Docker Hub repository when creating a new Docker Container. https://hub.docker.com/explore/ 7

For detailed configuration instructions please refer to our knowledge base: <u>https://forum.peplink.com/t/how-to-run-a-docker-application-on-a-peplink-mediafast-router/16021</u>

#### 7.9 Captive Portal

Captive Portal	Access Mode	Info
	No Captive Portal	
	New Portal	

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

General Settings	
Name	demoportal
Enable	
Hostname	captive-portal.peplink.com     Default
Access Mode	Open Access     User Authentication     External Server
Portal Access Settings	
Access Quota	30     mins (0: Unlimited)       0     MB (0: Unlimited)
Quota Reset Time	<ul> <li>● Daily at 00 ▼ :00</li> <li>○ 1440 minutes after quota reached</li> </ul>
Inactive Timeout	0 minutes (0: No Timeout)
Allowed Networks	Domain Name / IP Address / Network
Allowed Clients	MAC / IP Address
Splash Page	Built-in      External, URL:      http://
Popup Handling	<ul> <li>Bypass Popup (Redirection only takes place on normal browser)</li> <li>Automatically show splash page on Safari for Apple (iOS / macOS) devices</li> </ul>
Logout Hastoomo	(Not configured)

	Captive Portal Settings
Enable	Check <b>Enable</b> and then, optionally, select the LANs/VLANs that will use the captive portal.
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click <b>Default</b> .
Access Mode	Click <b>Open Access</b> to allow clients to freely access your router. Click <b>User</b> <b>Authentication</b> to force your clients to authenticate before accessing your router. Select <b>External Server</b> to use the Captive Portal with a HotSpot system. As described in the following knowledgebase article: <u>https://forum.peplink.com/t/using-hotspotsystem-wi-fi-on-pepwave-max-routers/</u>



	This authenticates your d	lients through a RADIUS serv	ver After selecting this	
	option, you will see the fo	llowing fields:		
	Authentication	ADTUS Server Y		
	Auth Server	Port 1812	Default	
	Auth Server Secret	Hide Characters		
RADIUS Server	CoA-DM			
RADIOS Server	Accounting Server	Port 1813	Default	
	Accounting Server Secret	Hide Characters		
	Accounting Interim Interval 🛛 🕐	seconds		
	Fill in the necessary inform enable authentication.	mation to complete your conr	nection to the server and	
	This authenticates your cl	lients through a LDAP server	. Upon selecting this option,	
	you will see the following	TIEIOS:		
	Authentication	AP Server		
		Bort 390	Default	
I DAP Sonvor		Use DN/Password to bind to LDAP Server	Delauit	
LDAF Server	Base DN			
	Base Filter			
	Fill in the necessary infor	mation to complete your conr	nection to the server and	
	enable authentication.			
Access Quota	Set a time and data cap to	o each user's Internet usage.		
Quota Reset	<b>Set</b> This menu determines how your usage quota resets. Setting it to <b>Daily</b>			
Time	establish a timer for each	user that begins after the qu	ota has been reached.	
Inactive	Clients will get disconnec	ted when the inactive the cor	ifigured time is reached.	
Timeout	Default 0: no timeout			
Allowed	To whitelist a network, en	ter the domain name / IP add	Iress here and click	
Notworks	To delete an existing netv	vork from the list of allowed n	etworks, click the	
INCLWUINS	button next to the listing.			
	To whitelist a client, enter	the MAC address / IP addre	ss here and click	
Allowed Clients	to writtenst a client, enter the MAC address / IP address here and click			
	delete an existing client from the list of allowed clients, click the			
	to the hourig.			

Peplink Balance User Manual



'n.

Splash Page	Here, you can choose between using the Balance's built-in captive portal and redirecting clients to a URL you define.
Popup Handling	Configurable options for popup handling: - Bypass Popup (Redirection only takes place on normal browser) - Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostnan	A hostname that can be used to logout captive portal when being accessed on browser.
Customize splash page	Click on the provided link in the Captive portal profile to customize the splash page. A new browser tab is opened with a WYSIWYG editor of the splash page o edit the content, click on the corresponding element after switching Edit Mode to ON.

	Captive Portal
•	
pe	PITIK PEPWAVE
Use default	Logo Image
Choose Fi	le No file chosen
NOTE: Size max 51	2KB. Supported images types: JPEG, PNG and GIF.
	EMPTY STRING
I have read	and agree to the terms and conditions
You must ac can proceed	ccept the terms and conditions before you I
	Agree
Powered by Peplink.	
Portal Configuration	
Show Quota Status	2
Custom Landing Page	0
Page: Login	Edit mode ON 🕜 🕐
Success Quota reached	Jair



#### 7.10 QoS

#### 7.10.1 User Groups

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

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

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

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

Add / Edit User	Group		
Client			
Grouped by	?	IP Address 🔻	
Group	?	Manager 🔻	

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

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

#### 7.10.2 Bandwidth Control

This section is to define how much minimum bandwidth will be reserved to each user group when a WAN connection is **in full load**. When this feature is enabled, a slider with two indicators will be shown. You can move the indicators to adjust each group's weighting. The lower part of the table shows the corresponding reserved download and uploads bandwidth value of each connection. By default, **50%** of bandwidth has been reserved for Manager, **30%** for Staff, and **20%** for Guest.

Group Bandwidth Reservation				
Enable				
		•	Ð	
_	Manager	Staff	Guest	
Bandwidth %	50%	30%	20%	
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M	

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

Individual Bandwidth Lim	it					
Enable						
User Bandwidth Limit	Manager	Downl r: Unlimi	oad ted	Upload Unlimi	d ited	
	Staff:	0	Mbps •	0	Mbps •	(0: unlimited)
	Guest:	0	Mbps •	0	Mbps 🔻	(0: unlimited)

#### 7.10.3 Application

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



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

Application	Priority						
	Manager	Staff	Guest				
All Supported Streaming Applications	<u>↑ High</u>	- Normal	<u>↑ High</u>	*			
All Email Protocols	† High ▼	↑ High 🔹	† High ▼	×			
MySQL	↑ High 🔻	- Normal 🔹	↓Low •	×			
SIP	↑ High 🔻	Low T	↓ Low ▼	*			
		Add					



#### **Prioritization for Custom Application**

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

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

Add / Edit Applica	tion	
Туре	📀 💿 Supported Applications 🔘 Custom Appli	ications
Category	Miscellaneous	
Application	All Supported Miscellaneous Protocols	
	HTTP NTP SNMP STUN	OK Cancel

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



#### **DSL/Cable Optimization**

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

DSL/Cable Optimization	
Enable	۲

#### 7.11 Firewall

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

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

Outbound (LAN to WAN)

Inbound (WAN to LAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

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

#### 7.11.1 Access Rules

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

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

Click Add Rule to display the following screen:

#### Peplink Balance User Manual

New Firewall Rule			
Rule Name			
Enable		Always on	
Protocol	?	Any 🔻 🗲 :: Protocol Selection Tool :: 🔻	
Source IP & Port	?	Any Address 🔻	
Destination IP & Port	?	Any Address 🔻	
Action	?	Allow O Deny	
Event Logging	?	Enable	

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

Inbound Firewall R	tules (WDrag and dro	p rows t	o change rule order)		
Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy
<u>Default</u>	Any	Any	Any	Any	Allow
			Add Rule		

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

New Firewall Rule	
Rule Name	
Enable	Always on
WAN Connection	Any
Protocol	Any • • :: Protocol Selection Tool :: •
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	Illow Deny
Event Logging	() Enable

#### Inbound / Outbound Firewall Settings

**Rule Name** This setting specifies a name for the firewall rule.



Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule. Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	<ul> <li>This setting specifies the protocol to be matched.</li> <li>Via a drop-down menu, the following protocols can be specified: <ul> <li>TCP</li> <li>UDP</li> <li>ICMP</li> <li>IP</li> </ul> </li> <li>Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)</li> <li>After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remains manually modifiable.</li> </ul>
Source IP & Port	This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the <b>Source IP &amp; Port</b> setting, as indicated with the following screenshots:
Destination IP & Port	This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the <b>Destination IP &amp; Port</b> setting, as indicated with the following screenshots:
Action	This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:

https://www.peplink.com

Copyright @ 2019 Peplink



	<ul> <li>Source IP &amp; port</li> <li>Destination IP &amp; port</li> <li>With the value of Allow for the Action setting, the matching traffic passes through the router (to be routed to the destination). If the value of the Action setting is set to Deny, the matching traffic does not pass through the router (and is discarded).</li> </ul>
Event Logging	<ul> <li>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page Status&gt;Event Log. A sample message is as follows:</li> <li>Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1</li> <li>DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80</li> <li>CONN: The connection where the log entry refers to</li> <li>SRC: Source IP address</li> <li>DST: Destination IP address</li> <li>LEN: Packet length</li> <li>PROTO: Protocol</li> <li>SPT: Source port</li> <li>DPT: Destination port</li> </ul>

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

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

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

Rule	Protocol	Source IP Port	Destination IP Port	Policy
No web ac	GESS TCP	Any Any	Any 80	Deny 🗙
No FTP a	<u>access</u> the	Any Any	Any 21	Deny
<u>Default</u>	Any	Any	Any	Allow

To remove a rule, click the **to** button.

Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default** rule will be applied. The **Default** rule is **Allow** for both outbound and inbound access.

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

#### Intrusion Detection and DoS Prevention

Intrusion Detection and Do	S Prevention		36
Intrusion Detection and DoS Prevention			
		Save	Cancel

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

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

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

#### 7.11.2 Content Blocking

Application Block Please Select Appl	ing ication		۲	(2)
Web Blocking Preset Category				?
High Moderate Low Custom	<ul> <li>Adware</li> <li>Dating</li> <li>P2P/File sharing</li> <li>Malware</li> <li>Social Networking</li> <li>Violence</li> </ul>	<ul> <li>Aggressive</li> <li>Drugs</li> <li>Gambling</li> <li>Pornography</li> <li>Contraband</li> <li>Weapons</li> </ul>	<ul> <li>Audio-Video</li> <li>File Hosting</li> <li>Games</li> <li>Proxy/Anonymizer</li> <li>Update Sites</li> </ul>	
Content Filtering D Update	atabase Auto 🛛 🔋 📋			
Customized Domai	ns			?
Exempted Domains	from Web Blocking			+ (2) +
Exempted User G	roups			?
Staff	Exempt			
Guest	🗆 Exempt			
Exempted Subne Network	ts		Subnet Mask 255.255.255.0 (/24)	? •
URL Logging Enable				
Log Server Host	l.	≜ P	Port: 514	

#### **Application Blocking**

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



#### Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for those on the Exempted User Groups or Exempted Subnets defined below.

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

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

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

#### **Customized Domains**

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

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

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

#### **Exempted User Groups**

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

#### **Exempted Subnets**

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

#### **URL Logging**

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

#### 7.12 OSPF & RIPv2

The Peplink Balance supports OSPF and RIPv2 dynamic routing protocols. Click the Network tab from the

https://www.peplink.com

Copyright @ 2019 Peplink

#### Peplink Balance User Manual



top bar, and then click the **Routing Protocols > OSPF & RIPv2** item on the sidebar to reach the following menu:

Router ID	LAN IP Address		C
Area	Interfaces		
0.0.0.0	Untagged LAN (192.16	8.112.1/24), WAN 4 (192.168.254.10/24)	×
		\dd	
RIPv2			
No RIPv2 Defined.			C
OCDE & DIDUS Doute Ad			
USPF & RIPVZ ROULE AU	vertisement		
PepVPN Route Isolation	C Enable		
PepVPN Route Isolation Network Advertising	C Enable     C		+
PepVPN Route Isolation Network Advertising	C Enable     C Enable     All LAN/VLAN networks w	▼ Il be advertised when no network advertising is chosen.	+
PepVPN Route Isolation Network Advertising Static Route Advertising	Constant	Il be advertised when no network advertising is chosen.	+
PepVPN Route Isolation Network Advertising Static Route Advertising		II be advertised when no network advertising is chosen. Subnet Mask	+
PepVPN Route Isolation Network Advertising Static Route Advertising	Create Contended     Cont	Il be advertised when no network advertising is chosen.     Subnet Mask     255.255.255.0 (/24) ▼	+

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

Area ID	0.0.0.0
Link Type	Isolate Broadcast O Point-to-Point
Authentication	None 🔻
Interfaces	<ul> <li>Untagged LAN (192.168.112.1/24)</li> <li>Management VLAN (10.0.2.1/24)</li> <li>jamestest (10.22.37.1/24)</li> <li>WAN 1</li> <li>WAN 2</li> <li>WAN 3</li> <li>WAN 4 (192.168.254.10/24)</li> <li>WAN 5</li> </ul>

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

To access RIPv2 settings, click

Authentication	None 🔻	
Interfaces	<ul> <li>Untagged LAN (192.168.112.1/24)</li> <li>Management VLAN (10.0.2.1/24)</li> <li>jamestest (10.22.37.1/24)</li> <li>WAN 1</li> <li>WAN 2</li> <li>WAN 3</li> <li>WAN 4 (192.168.254.10/24)</li> <li>WAN 5</li> </ul>	

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

)		
All LAN/VLAN networks will be advertised when no network advertising is chosen.		
🖉 Enable		
) 🔻	+	
)	g is chosen.	

	OSPF & RIPv2 Route Advertisement
PepVPN Route Isolation	Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption
Network Advertising	Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.
Static Route Advertising	Enable this option to advertise LAN static routes over OSPF & RIPv2. Static routes that match the Excluded Networks table will not be advertised.
#### 7.13 BGP

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

BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	×
		Add	¥7.

Click "x" to delete a BGP profile Click "Add" to add a new BGP profile

BGP Profile						
Profile Name						
Enable						
Interface	WAN 1	•				
Router ID	LAN IP Add     Custom:	LAN IP Address     Custom:				
Autonomous System						
Neighbor	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
			disable			+
Hold Time	240					

	BGP
Name	This field is for specifying a name to represent this profile.
Enable	When this box is checked, this BGP profile will be enabled. Otherwise, it will be disabled.
Interface	The interface where BGP neighbor is located
Autonomous System	The Autonomous System Number (ASN) of this profile
Neighbor	BGP Neighbor's details
IP address	Neighbor's IP address
Autonomous System	Neighbor's ASN
Multihop/TTL	Time-to-live (TTL) of BGP packet. Leave it blank if BGP neighbor is directly connected, otherwise you must specify a TTL value. Accurately, this option should be used if the configured neighbor IP



	address does not match the selected Interface's network subnets. TTL value must be between 2 to 255.
Password	Optional password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this neighbor. The value must be a comma separated ASN. For example "64530,64531" will prepend "64530, 64531" to received routes.
Hold Time	Time in seconds to wait for a keepalive message from the neighbor before considering the BGP connection is staled. This value must be either 0 (infinite hold time) or between 3 and 65535 inclusively.

Route Advertisement				
Network Advertising	?	• +		+
Static Route Advertising	?	Enable		
		Excluded Networks	Subnet Mask	
			255.255.255.0 (/24) 🔻	+
Advertise OSPF Route	?			

Network Advertising	Networks to be advertised to BGP neighbor.
Static Route Advertising	Enable this option to advertise LAN static routes. Static routes that match the Excluded Networks table will not be advertised.
Advertise OSPF Route	When this box is checked, all learnt OSPF routes will be advertised.

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

	This option selects the route import filter mode. <b>None</b> : all BGP routes will be accepted.
Filter Mode	Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.
	<b>Reject</b> : Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.



Restricted Networks	This specifies the network in the "route import" entry <b>Exact Match:</b> When this box is checked, only routes with the same Networks and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnet will be filtered.		
Route Ex Export to	port other BGP Profile 🕐 🗔		
Export to	OSPF 🕐 🗆		
Export to other BGP Profile	• When this box is checked, routes learnt from this BGP profile will export to other BGP profiles.		
Export to OSPF	When this box is checked, routes learnt from this BGP profile will export to the OSPF routing protocol.		

### 7.14 Remote User Access

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

#### 7.14.1 L2TP with IPsec

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

L2TP with IPsec Remote User Access Settings		
Pre-shared Key	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.	
Listen On	This setting is for specifying the WAN IP addresses that allow remote user access.	
Disable Weak Ciphers	Click the 2 button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.	

Continue to configure the authentication method.



#### 7.14.2 OpenVPN

Remote User Access Settings		
Enable	8	
VPN Type	○ L2TP with IPsec ○ PPTP ● OpenVPN You can obtain the OpenVPN client profile from the <u>status page</u> .	

Select OpenVPN and continue to configure the authentication method.

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

OpenVPN Client Profile 🛛	Route all traffic   Split tunnel

You have a choice between 2 different OpenVPN Client profiles.

#### 8 "route all traffic" profile

Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel

#### 9 "split tunnel" profile

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

#### 9.1.1 PPTP

Remote User Access Settings	
Enable	8
VPN Type	○ L2TP with IPsec ● PPTP ○ OpenVPN

No additional configuration required.

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

Continue to configure authentication method.

#### 9.1.2 Authentication Methods

Connect to Network	?	Untagged LAN V		
Authentication		Local User Accounts *		
User Accounts	•	Username	Password	
		Authentication Method		
<b>Connect to</b> Select the VLAN network for remote users to enable remote user access on.				



#### Network

Authentication Determine the method of authenticating remote users

#### User accounts:

This setting allows you to define the Remote User Accounts.

Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

#### Note:

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

The password must be between 8 and 12 characters long.

#### LDAP Server:

Connect to Network	⑦ 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 V
Auth Server	Port 1812 _J 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 V
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.

#### 9.2 Misc. Settings

#### 9.2.1 High Availability

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

In an HA configuration, two same-model Peplink Balance units provide redundancy and failover in a master-slave arrangement. In the event that the master unit is down, the slave unit becomes active. High availability will be disabled automatically where there is a drop-in connection configured on a LAN bypass port.

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



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

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

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

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

peplink PEPWAVE



#### Interface for Master Router

#### Interface for Slave Router

High Availability		
Enable	?	
Group Number	0	5 💌
Preferred Role	?	Master O Slave
Resume Master Role Upon Recovery	0	
Virtual IP	0	
LAN Administration IP	?	192.168.1.1
Subnet Mask	?	255.255.255.0

Enable	3		
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 <b>Group Number</b> 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 <b>Master</b> mode is selected in <b>Preferred Role</b> . If this option is enabled, once the device has recovered from an outage, it will take over and resume its <b>Master</b> role from the slave unit.
Configuration Sync.	This option is displayed when <b>Slave</b> mode is selected in <b>Preferred Role</b> . If this option is enabled and the <b>Master Serial Number</b> entered matches with the actual master unit's, the master unit will automatically transfer the configuration to this unit. Please make sure the <b>LAN IP Address</b> and the <b>Subnet Mask</b> fields are set correctly in the LAN settings page. You can refer to the <b>Event Log</b> for the configuration synchronization status.
Master Serial Number	If <b>Configuration Sync.</b> 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 <b>Virtual IP</b> . The <b>Virtual IP</b> and the <b>LAN Administration IP</b> 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.



https://www.peplink.com

Copyright @ 2019 Peplink



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

#### 9.2.2 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 Certificates

#### 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

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

#### 9.2.3 Service Forwarding

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

#### Peplink Balance User Manual



SMTP Forwarding Setu	P. (?)
SMTP Forwarding	🖾 Enable
Web Proxy Forwarding	Setup (2)
Web Proxy Forwarding	🗆 Enable
<b>DNS Forwarding Setup</b>	
Forward Outgoing DNS Requests to Local DNS Pr	oxy Enable
Custom Service Forwar	ding Setup
Custom Service Forwardi	ng 🗍 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 <b>Enable</b> .
Web Proxy Forwarding	When this option is enabled, all outgoing connections destined for the proxy server specified in <b>Web Proxy Interception Settings</b> will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting <b>Enable</b> .
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 <b>Section 16.1</b> ).

#### Web Proxy Forwarding

Web Proxy Forwarding Set	up			2
Web Proxy Forwarding	🗷 Enable	🗷 Enable		
Web Proxy Interception S	ettings			
Proxy Server	IP Address 123.123.11.2 (Current settings in user	22 Port s' browser)	8080	
Connection	Ei Fa	nable prwarding?	Proxy Server IP A	ddress : Port
WAN 1	E	1		:
WAN 2	2	1	22.2.2.2	: 8765
WAN 3	2	9	33.3.3.2	: 8080
WAN 4		I.		

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**

<b>Custom Service Forwarding S</b>	etup		
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.

#### 9.2.4 Service Passthrough

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

Service Passthrough Support	
SIP 🥐	<ul> <li>Standard Mode</li> <li>Compatibility Mode</li> <li>Define custom signal ports</li> <li>1.</li> <li>2.</li> <li>3.</li> </ul>
H.323	🗹 Enable
FTP (?	Enable     Define custom control ports     1, 2, 3,
TFTP	Enable
IPsec NAT-T	<ul> <li>Enable</li> <li>Define custom ports         <ol> <li>2.3.</li> <li>Route IPsec Site-to-Site VPN             via WAN 1</li> </ol> </li> </ul>

(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: <b>Standard Mode</b> and <b>Compatibility Mode</b> .
	If your SIP server's signal port number is non-standard, you can check the box <b>Define</b> custom signal ports and input the port numbers to the text boxes.

Peplink Balance User Manual



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.
	<b>Define custom control ports</b> 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 <b>Enable</b> if you want to enable TFTP passthrough support.
	This field is for enabling the support of IPsec NAT-T passthrough. UDP ports 500, 4500, and 10000 are monitored by default
IPsec NAT-T	You may add more custom data ports that your IPsec system uses by checking <b>Define</b> <b>custom ports</b> . If the VPN contains IPsec site-to-site VPN traffic, check <b>Route IPsec</b> <b>Site-to-Site VPN</b> and choose the WAN connection to route the traffic to.

#### 9.2.5 Grouped Networks

Grouped Networks		
Name	Networks	
	Add Group	

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

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

Grouped Networks			
Name	Accounting	<u>A</u>	
Networks	Network	Subnet Mask	
	192.168.50.192	255.255.255.224 (/27) 🔹 🗶	
		255.255.255 (/32) 🔹 🕂	

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

peplink	Dashboard	Setup Wizard	Network	АР	System	Status
WAN						
LAN	Outboun	d Policy				
Network Settings	Custom					
Port Settings						
VPN	Add a l	New Custom Ru	le			
SpeedFusion						
IPsec VPN	Service	Name				
Outbound Policy	Enable		I Alw	ays or	1 <b>T</b>	
Inbound Access	Source		Groupe	ed Net	wor 🔻 🛛 Acc	ounting 🔻

#### 9.2.6 SIM Toolkit

The SIM Toolkit ,accessible via **Networks > Misc Settings > SIM Toolkit**, 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	294282983983984
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	<b>*</b>	
SIM Card	1		
IMSI	856195002108538		
USSD Code	*138#	Submit	
USSD Status	Request is sent succ	essfully	
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	234307308582988	
Tool	SMS V	

SMS		Refresh
Jun 21, 2017 18:00	Per Transfergens, ynne met generaam tijn veiktering - ynn men strangerijke ooken ynn fest ingin at streer an dit	×
May 06, 2017 12:23	346041 where is 'the one will is wedging dealers. So to pass 9962 accounts on pass dealers on a webby phase whole here we pass the count of the count of the second of t	×
Mar 15, 2017 10:03	From literative previous mandatures in the domentar time stop and the week. If your period is attained, you use period in previous director, you are period by the Cit.	×
Mar 06, 2017 14:50	(Adopt) (France 1: Now over edd) is made in view. On its pass Php2 measurement providentings or or a realistic picture adult have improvement in strength strength strength of the strengt of the strength of the strength	×
Dec 28, 2016 09:53	From Horns its, an input you've approximation to mention half-prove offer that the contrast you, this offer applied to your first it take, that mention meaning charge net report to induction on some next bit. These	×
Dec 06, 2016 13:09	Maker effective 2. New new solid it model 2-robust 00-bit pour Phy? accessive or pour displaye at on a making phone-class interview, a result of the standard phone acceleration of the interview.	×
Nov 08, 2016 11:29	From Theory is placed maintenance in the Burginian fluid MC amonths used. If pure sension is allocated, you can get optimize the territory of the territory of the sension of the territory of ter	×
Sep 07, 2016 17:05	From literations and the temperature process makes or streaming backgrounds they up to a back with or to meet your remaining to be a back of the process of the second se	×

### 10 AP Tab

### 10.1 AP

#### 10.1.1 AP Controller

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



AP Controller		
AP Management	?	8
Support Remote AP	?	
Sync. Method	?	As soon as possible •
Permitted AP	0	O Any O 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, <b>CAPWAP Access Controller addresses</b> (field 138), will be added to the DHCP server. A local DNS record, <b>AP Controller</b> , will be added to the local DNS proxy.
Support Remote AP	<ul> <li>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.</li> <li>The DHCP server and/or local DNS server of the remote AP's network should be configured in the <b>DNS Proxy Settings menu</b> under <b>Network&gt;LAN</b>. The procedure is as follows:</li> <li>1. Define an extended DHCP option, <b>CAPWAP Access Controller addresses</b> (field 138), in the DHCP server, where the values are the AP controller's public IP addresses; and/or</li> <li>2. Create a local DNS record for the AP controller with a value corresponding to the AP controller's public IP address.</li> </ul>
Sync. Method	<ul> <li>Select the required option to synchronize the managed AP's. Options are:</li> <li>As soon as possible (default)</li> <li>Progressively (synchronize AP's in groups)</li> </ul>



	• One at a time (synchronize one AP at a time)
Permitted AP	Access points to manage can be specified here. If <b>Any</b> is selected, the AP controller will manage any AP that reports to it. If <b>Approved List</b> is selected, only APs with serial numbers listed in the provided text box will be managed.

#### 10.1.2 Wireless SSID

SSID		Security Policy
	No SSID Defined	
	Add	

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

The below settings ishows a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).



SSID	
SSID Settings	2
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 V
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 <b>0</b> , 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. <b>Broadcast SSID</b> is enabled by default.
Data Rate <sup>A</sup>	Select <b>Auto</b> to allow the Pepwave router to set the data rate automatically, or select <b>Fixed</b> and choose a rate from the displayed drop-down menu.
Multicast Filter <sup>A</sup>	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate <sup>A</sup>	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected <b>Protocol</b> and <b>Channel Bonding</b> settings will affect the rate options and values available here.

https://www.peplink.com

# peplink | PEPWAVE



IGMP Snooping <sup>A</sup>	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 <sup>A</sup>	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 <sup>A</sup>	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

<sup>A</sup> - 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	<ul> <li>Interview of the second second</li></ul>	
	Security Settings	
Security Policy	<ul> <li>This setting configures the wireless authentication and encryption methods Available options are :</li> <li>Open (No Encryption)</li> <li>WPA2 -Personal (AES:CCMP)</li> </ul>	

- 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.

Access Control S	ettings		
Restricted Mode	Deny all except listed 🔻		
MAC Address List	•		
		Access Control	
Restricted Mode	The settings allow administrator to control access using MAC address filtering. Available options are <b>None</b> , <b>Deny all except listed</b> , and <b>Accept all except listed</b>		ess using MAC address filtering. listed, and Accept all except listed
MAC Address	Connection accepted ba	coming from the MAC addresses i sed on the option selected in the p	n this list will be either denied or previous field.

List	If more than one MA	C address needs to	be entered, y	/ou can use a c	arriage return
	to separate them.				

RADIUS Server Settings	Primary Server		Secondary Serve	r
Host				
Secret				
	Hide Characters		Hide Character	s
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	In field, enter the UDP authentication port(s) used by your RADIUS server(s) or click

https://www.peplink.com

Copyright @ 2019 Peplink



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

#### 10.1.3 AP > Profiles

AP Settings	2
AP Profile Name	
SSID	<ul> <li>2.4 GHz 5 GHz</li> <li>PEPLINK_63E6</li> </ul>
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	<ul> <li>This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow.</li> <li>If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).</li> <li>If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).</li> <li>NOTE: Users are required to choose an option suitable to local laws and regulations.</li> </ul>	
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	802.1	11ng			802.11n/ac			
Channel Width	Auto	, <b>T</b>			Auto	T		
Channel	Auto Chan	nels: 1 2 3 4 5 6 7 8	Edit 9 10 11	]	Auto Chann 165	• els: 36 40 44 48 14	Edit 49 153 157	161
Auto Channel Update	Daily at 03 ▼ :00 ✓ Wait until no active client associated		Daily a	at 03 ▼ :00 ait until no active cl	ient associ	iated		
Output Power	Fixed: Max 🔹 🗖 Boost		Fixed	: Max 🔻 🗖 🛙	Boost			
Client Signal Strength Threshold	0	-95 dBm (0: Unl	imited)		0	-95 dBm (0: Unl	imited)	
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 <b>802.11ng</b> and <b>802.11na</b> . By default, <b>802.11ng</b> is selected.
Channel Width	Available options are <b>20 MHz</b> , <b>40 MHz</b> , and <b>Auto (20/40 MHz)</b> . Default is <b>Auto (20/40 MHz)</b> , 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 – <b>Max</b> , <b>High</b> , <b>Mid</b> , and <b>Low</b> . The actual output power will be bound by the regulatory limits of the selected country.
Client Signal Strength Threshold	This setting determines the maximum strength at which the Wi-Fi AP can broadcast
Maximum number of clients	This setting determines the maximum number of clients that can connect to this Wi-Fi frequency.

Advanced Wi-Fi AP settings can be displayed by clicking the an 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 *
отім 🕐	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 📀	O Auto O 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 <sup>A</sup>	This option is for setting the transmit bit rate for sending a beacon. By default, <b>1Mbps</b> is selected.
Beacon Interval <sup>A</sup>	This option is for setting the time interval between each beacon. By default, <b>100ms</b> is selected.
DTIM <sup>A</sup>	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 <b>1 ms</b> .
RTS Threshold <sup>A</sup>	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 <sup>A</sup>	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 <sup>A</sup>	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to $9 \ \mu s$ .

#### Peplink Balance User Manual



ACK Timeout <sup>A</sup>	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to $48 \ \mu s$ .
Frame Aggregation <sup>A</sup>	This option allows you to enable frame aggregation to increase transmission throughput.
- Advanced feature	e, please click the 🔯 button on the top right-hand corner to activate.

 Web Administration Settings

 Enable

 Web Access Protocol

 Web Access Protocol

 Management Port

 443

 HTTP to HTTPS Redirection

 Admin Username

 admin

 Admin Password

 Image: 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.			

#### **10.2 AP Controller Status**

#### 10.2.1 Info

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

#### Peplink Balance User Manual



	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 <b>2.4 Ghz</b> and <b>5 Ghz</b> . Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.
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 <b>Zoom</b> to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

#### 10.2.2 Access Points (Usage)

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

Search Filter								
AP Name / Serial Num	ber / 🛛 🗚	1						
SSID	E	Include Offline APs						
Search Result								
Managed ADs								
Hanayea Ars							Expand	Collapse
							Expand	Collapse
Name	IP Address	MAC	Location	Firmware	Pack ID	Con	Expand	Collapse
<ul> <li>Name</li> <li>Default (8/9 online)</li> </ul>	IP Address	MAC	Location	Firmware	Pack ID	Con	Expand	Collapse

			Usa	age				
AP Name/Serial Number	This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.							
<b>Online Status</b>	This button to	This button toggles whether your search will include offline devices.						
	This table sho clients, upload expand and co collapse all gro	ws the de traffic, an ollapse inf oups by u	tailed ir nd dowr formatic sing the	nformation nload traffi on on each e Expand	on each A c. Click the device gr	AP, includi e blue arro oup. You buttons.	ng chann ows at the could also	el, number of ∋ left of the table to o expand and
Managed Wireless Devices	Click the in it	1P Address 10.9.2.7 10.9.2.123 10.9.2.102 10.9.2.101 10.9.2.66 10.9.2.76 10.8.9.84 10.8.9.73 10.8.9.18 10.10.11.23 10.10.11.71	Type 802.11ng 802.11ng 802.11ng 802.11ng 802.11ng 802.11ng 802.11ng 802.11ng 802.11ng 802.11ng	Signal Excellent (37) Excellent (42) Good (23) Excellent (29) Excellent (29) Excellent (29) Excellent (29) Excellent (25) Good (23) Excellent (35) Poor (12)	r each clie Balance Balance Balance Balance Balance Balance Balance Wireless Wireless Wireless Wireless Marketing Marketing	Upload 66.26 MB 6.65 MB 1.86 MB 3.42 MB 640.29 KB 2.24 KB 9.86 MB 9.36 MB 118.05 MB 74.78 MB 84.84 KB	Download 36.26 MB 2.26 MB 606.63 KB 474.52 KB 43.57 KB 3.67 KB 9.76 MB 11.14 MB 7.92 MB 4.58 MB 119.32 KB	6

#### Peplink Balance User Manual

Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:E0
Product Name	Pepwave AP Pro Duo
Name	
.ocation	
Firmware Version	3.5.2
Firmware Pack	Default (None) 🔻
AP Client Limit	Follow AP Profile O 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 V 5 GHz: Follow AP Profile V

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.





Peplink Balance User Manual

### peplink | PEPWAVE

Events	
an 2 11:53:39 Client 00:26:BB:08:AC:FD associated with Wireless_11a	
an 2 11:39:31 Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
an 2 11:16:55 Client A8:BB:CF:E1:0F:1E disassociated from Balance_11a	
an 2 11:11:54 Client A8:BB:CF:E1:0F:1E associated with Balance_11a	
an 2 11:10:45 Client 60:67:20:24:B6:4C associated with Marketing_11a	
an 2 11:00:36 Client 00:21:6A:35:59:A4 associated with Balance_11a	
an 2 11:00:20 Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
an 2 10:59:09 Client 00:21:6A:35:59:A4 disassociated from Balance_11a	
an 2 10:42:28 Client F4:B7:E2:16:35:E9 associated with Balance_11a	
an 2 10:29:12 Client 84:7A:88:78:1E:4B associated with Balance_11a	
an 2 10:24:27 Client 90:89:31:0D:11:EC disassociated from Marketing_11a	
an 2 10:24:27 Client 90:B9:31:0D:11:EC roamed to Marketing_11a at 2830-BFC8-D23	0
an 2 10:13:22 Client E8:8D:28:A8:43:93 associated with Balance_11a	
an 2 10:13:22 Client E8:8D:28:A8:43:93 roamed to Balance_11a from 2830-BF7F-6940	0
an 2 10:07:52 Client CC:3A:61:89:07:F3 associated with Wireless_11a	
an 2 10:04:35 Client 60:67:20:24:B6:4C associated with Marketing_11a	
an 2 10:03:38 Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
an 2 09:58:27 Client 00:26:BB:08:AC:FD disassociated from Wireless_11a	
an 2 09:52:46 Client 00:26:BB:08:AC:FD associated with Wireless_11a	
an 2 09:20:26 Client 8C:3A:E3:3F:17:62 associated with Balance_11a	

#### 10.2.3 Wireless SSID

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



https://www.peplink.com

Copyright @ 2019 Peplink



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

#### **10.2.4 Wireless Client**

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

Search Filter				
Client MAC / SSID / AP Serial Number				
Maximum Result (1-256)	50			
Search Result				
		Search		
Ton 10 Clients of last hour (1)	dated at 03.0	0)		
Client MAC Address		Upload	Download	
C0:EE:FB:20:13:36		53.5 KB	101.4 KB	습교

Here, you will be able to see your network's heaviest users as well as search for specific users. Click the  $\frac{1}{2}$  icon to bookmark specific users, and click the  $\frac{1}{2}$  icon for additional details about each user:

#### Peplink Balance User Manual

Information							
Status		Associated					
Access Point		1111-2222-3333					
SSID		Peplink WLAN 853B					
IP Address		192.168.1.34					
Duration		00:27:31					
Usage (Upload / Dow	nload)	141.28 MB/4	.35 MB				
RSSI		-48					
Rate (Upload / Downl	load)	150M / 48M					
Туре		802.11na					
20.0 kbps -							
10.0 kbps							
10.0 kbps	08:00	12:00	16:00	20:00	11-23		
10.0 kbps 0.0 kbps 04:00 SSID	08:00 AP	12:00	16:00	20:00 <b>To</b>	11-23 Upload	Download	
10.0 kbps	08:00 AP 192C-:	12:00 1835-642F	16:00 From Nov 23 03:43:04	20:00 <b>To</b>	11-23 Upload 141.28 MB	Download 4.35 MB	
10.0 kbps	08:00 AP 192C- 192C-	12:00 1835-642F 1835-642F	16:00 From Nov 23 03:43:04 Nov 23 02:58:36	20:00 <b>To</b> Nov 23 03:47:52	11-23 Upload 141.28 MB 173.7 KB	Download 4.35 MB 94.2 KB	

#### 10.2.5 Nearby Device

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

BSSID	SSID	Channel	Encountion	Last Seen	Mark as
00:1A:DD:EC:25:22	Wireless	11	WPA2	10 hours ago	0 0
00:1A:DD:EC:25:23	Accounting	11	WPA2	10 hours ago	0 0
00:1A:DD:EC:25:24	Marketing	11	WPA2	11 hours ago	0 0
00:03:7F:00:00:00	MYB1PUSH	1	WPA & WPA2	11 minutes ago	0 0
00:03:7F:00:00:01	MYB1	1	WPA2	15 minutes ago	0 0
00:1A:DD:B9:60:88	PEPWAVE_CB7E	1	WPA & WPA2	5 minutes ago	0 0
00:1A:DD:BB:09:C1	Micro_S1_1	6	WPA & WPA2	1 hour ago	0 🙁
00:1A:DD:BB:52:A8	MAX HD2 Gobi	11	WPA & WPA2	2 minutes ago	0 8
00:1A:DD:BF:75:81	PEPLINK_05B5	4	WPA & WPA2	1 minute ago	0 0
00:1A:DD:BF:75:82	LK_05B5	4	WPA2	1 minute ago	0 8
00:1A:DD:BF:75:83	LK_05B5_VLAN22	4	WPA2	1 minute ago	0 8
00:1A:DD:C1:ED:E4	dev_captive_portal_test	1	WPA & WPA2	3 minutes ago	08
00:1A:DD:C2:E4:C5	PEPWAVE_7052	11	WPA & WPA2	2 hours ago	0 8
00:1A:DD:C3:F1:64	dev_captive_portal_test	6	WPA & WPA2	6 minutes ago	0 8
00:1A:DD:C4:DC:24	ssid_test	8	WPA & WPA2	2 minutes ago	08
00:1A:DD:C4:DC:25	SSID New	8	WPA & WPA2	2 minutes ago	0 8
00:1A:DD:C5:46:04	Guest SSID	9	WPA2	2 minutes ago	0 3
00:1A:DD:C5:47:04	PEPWAVE_67B8	1	WPA & WPA2	5 minutes ago	0 8
00:1A:DD:C5:4E:24	G BR1 Portal	2	WPA2	2 minutes ago	08
00:1A:DD:C6:9A:48	ssid test	8	WPA & WPA2	2 hours ago	0 0

#### **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.

#### 10.2.6 Event Log

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

Filter						
Search key	Client MAC Ad	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name				
Time	From	hh:mm to	bh:mm			
Alerts only	0					
		Search				

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client \$4:58:48:20:48:01 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client #4:E#: AB: 20: #0:05 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:64:48:20:46:05 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client Condition and associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 68:67:20:24:08:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client \$4:54:48:20:48:05 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client Con 21 184 135 199 44 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 10 00: 20 00: 40 19 associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 10:00:20:30:40:77 disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:54:48:20:48:05 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 10 Prove Proceeding associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client #4:##.Add 10:##:Df associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client \$4:54:48:30:48:05 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client #4:E4:48:20:48:05 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client #4 #4 AB 10:40:09 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client S4: S4: Add 20: Ad	
Jan 2 10:56:19	AP One 300M: Client 00:26:66:05:64:44 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client %C194 #5110-39:40 associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client #4: #4: #4: #0: #8: DS 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.

#### 10.3 Toolbox

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

1126 2013-08-26	
Firmware Packs	

This is the first menu that will appear. Here, you can manage the firmware of your AP. Clicking on will 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.

### 11 System Tab

#### 11.1 System

#### 11.1.1 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	0
Router Name	bostname: <b>Second Second</b> hostname: <b>Second Second</b> hostname: <b>Second</b>
Admin User Name	admin
Admin Password	
Confirm Admin Password	•••••
Read-only User Name	user
User Password	
Confirm User Password	
Front Panel Passcode	0
Web Session Timeout	2 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 V
Web Admin Port	HTTP: 80 HTTPS: 443
LAN Connection Access Settin	ds
Allowed LAN Networks	Any      Allow this network only

#### Save

	Admin Settings
Router Name	This field allows you to define a name for this Pepwave router. By default, <b>Router Name</b> is set as <b>MAX_XXXX</b> , where <i>XXXX</i> 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 <i>user</i> by default, but can be changed, if desired.
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm User Password	This field allows you to verify and confirm the new user password.



Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to <b>4 hours</b> .
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 $\mbox{MS-CHAP}$ $\mbox{v2}$ and $\mbox{PAP}.$
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 <b>Section 30.5</b> .
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: <ul> <li>HTTP</li> <li>HTTPS</li> <li>HTTP/HTTPS</li> </ul> <li>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.</li>
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
Web Admin Access	<ul><li>This option is for specifying the network interfaces through which the web admin interface can be accessed:</li><li>LAN only</li></ul>


	<ul> <li>LAN</li> <li>If LAN/WAN</li> <li>displayed.</li> </ul>	N/WAN I is chosen, the <b>WAN C</b>	onnection Acco	ess Settings form will b	е
LAN Connection Act	cess Settings	O Any <ul> <li>Allow this network</li> </ul>	conly Public (10)	T	
Allowed LAN Networks	This field allo	LAN Connection Acco	ess Settings cific networks or \	VLANs to access the Web	UI.
WAN Connection Allowed Source IP	Access Settings Subnets	S	he following IP subne	ts only	
Allowed WAN IP A	ddress(es)	Connection / IP Address(es	)	Ali Clear 10.88.3.158 (Interface IP)	
		WAN 2 Wi-Fi WAN Cellular 1 Cellular 2			
		WAN Connection Acc	ess Settings		
Allowed Source IP Subnets	This field al An add Allow access The allowed subnet mus <i>192.168.0.0</i> 32 inclusive To define m 192 0 102	<ul> <li>Ilows you to restrict web</li> <li>y - Allow web admin acd dress restriction.</li> <li>v access from the folio s only from the defined l area will</li> <li>d IP subnet addresses s</li> <li>st be in form of w.x.y.z/n</li> <li>0), and m is the subnet r</li> <li>ely (For example, 192.16</li> <li>nultiple subnets, separat</li> <li>2.168.0.0/24</li> <li>8.0.0/16</li> </ul>	admin access of cesses to be from P subnets. Whe be displayed be should be entered a, where <i>w.x.y.z</i> mask in CIDR fo 58.0.0/24). te each IP subne	only from defined IP sub m anywhere, without IP ts only - Restrict web a en this is chosen, a text eneath: ed into this text area. Ea r is an IP address (e.g., ormat, which is between et one in a line. For exa	nets. dmin input ch IP 0 and mple:
Allowed WAN IP Address(es)	This is to cl	hoose which WAN IP ac	ldress(es) the w	eb server should listen	on.



# 11.1.2 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	0
Current firmware version: 8.0.0 Firmware check pending	
	Check for Firmware

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

peplink	Dashboard	Setup Wizard	Network	AP	System	Status	Apply Changes
System		,					
Admin Security	Firmwar	e Upgrade					0
Firmware	Current fi	rmware version: 7	.1.0	to l			
<ul> <li>Time</li> </ul>	New vers	ion available: 7.1.2	( <u>Kelease No</u>	<u>(e</u> )			
<ul> <li>Schedule</li> </ul>			> Dov	vnloa	d and Upgra	de Check for Firmwar	e

Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process. The router will download and then apply the firmware. The time that this process takes will depend on your internet connection's speed.



The firmware will now be applied to the router<sup>\*</sup>. 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.

Validation success...

9%

### \*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 <u>here</u> Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the Balance line.

Balance					
Product					
				Search	:
Product	Hardware Revision	+ Firmware Version	a	Release Notes	s 🗢 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 Upgra	ade .	
Firmware Image	Choose File	No file chosen
		Manual Upgrade

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<sup>\*</sup>. 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%

1

Validation success...

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

# The InControl method

Described in this knowledgebase article on our forum.

### 11.1.3 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, Edinbur	rgh, Lisbon, Lon ▼
Time Server	0.pepwave.pool.ntp.org	Default
	Save	
	Time Settings	
Time Zone	This specifies the time zone (along with the correspon in which Peplink Balance operates. The <b>Time Zone</b> va event log of the Peplink Balance and e-mail notification zone options.	ding Daylight Savings Time scheme) alue affects the time stamps in the ns. Check <b>Show all</b> to show all time
Time Server	This setting specifies the NTP network time server to b	be utilized by the Peplink Balance.

### 11.1.4 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** 

# peplink | PEPWAVE

Schedule Enabled			7
Name	Time	lised by	
Weekdays Only	Weekdays only	-	×
		New Schedule	4. <u>.</u> .

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

Schedule S	et	tan	ıg				-	2	1	2	1	-	8	00		0		00	-	-		-	8	00		90	899	1	0		-	80		888			-					8	000		80		-	
Enable	nable							The schedule function of those associated features will be lost if profile is disabled.																																								
Name							V	Weekdays Only																																								
Schedule											Weekdays only												Π																									
Used by											Y	OL	i n	na	y g	go	to	รเ	Jpl	poi	te	d f	ea	tur	e :	set	ting	gs	pa	ige	ar	d	se	t tł	his	pi	ofi	le	as	S	he	əd	ule	er.:				
													_		1000										_		_	110						_				_				_						
Schedule N	laj		-	10			88		10	66	8	68	8	8	88	66		-	66	-		6	60	(ii)		-	10	-	0	60	10			-	8		-	68	-		-	8	-		8	-	-	60
	м	idr	nig	ht					1a	m	i.				-		8	ап	n						N	ioc	n						40	m							8	pr	m					
																	-								1							- 200									2000	, XIII						
Sunday	×	×	×	×	× :	K 3	¢ 2	é i	• >	¢ 1	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	2	¢ >	1	×	×	×	×
Sunday Monday	×	×	×	×	× :	× 1	e 3	- 1	<	e 1	×	×	×	×	* *	×	×	×	XX	×	×	×	×	×	×	×	×	* *	×	×	*	×	×	×	××	* *	×	×	×	×	×	>	e >		×	×	×	×
Sunday Monday Tuesday	×××	x S S	××	×	× :	K 1					×	×	× •	XXX	××	×	×××	XXX	××	× > >	×	×	×	×××	×	X X X	× × ×	× × ×	×	x X X	* *	×	× •	×	×××	* *	×	* * *	×	×××	×	>	e >		×	×	×	×
Sunday Monday Tuesday Wednesday	XXXX	X X X X	× × × ×	×	×						×	× • • •	×	XXXXX	XXXX	XXXX	××××	XXXXX	XXXX	× •	×	×	×	X X X X	×	X S S S	* * *	X X X	×××××	× × × ×	* * *	×	× • •	× × ×	XXXX	* * *	X	* * * *	×	××××	×××××	>			X	×	× • •	×
Sunday Monday Tuesday Wednesday Thursday	XXXXX	X X X X X	XXXXX	×	×						×××××	× 、 、 、 、 、	×	XXXXX	XXXXX	XXXXX	XXXXX	X X X X X	XXXXX	X Y Y Y	×	×	× × × ×	XXXXX	×	X S S S S	* * *	X X X X	× × × × ×	X X X X X	× × × ×	× • • •	× × × ×	× × ×	X X X X	* * * *	×	* * * *	XXXXX	XXXXX	XXXXX	3			X	× × × × ×	XYYYY	× • • •
Sunday Monday Tuesday Wednesday Thursday Friday	K K K K X	x 5 5 5 5 1	××××××	× × × × ×	×						XXXXXX	× × × × ×	× × × × ×	XXXXXXX	XXXXXX	XXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	XXXXXXX	XXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	×	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	× × × × ×	× > > > >	× > > > > >	X S S S S S	× × × × ×	K K K K K	XXXXXXXX	X X X X X	x	× ×	× × × × × ×	× × × ×	t t t t x x	* * * * *	× × × ×	X X X X X	× × × × ×	× × × × ×	× × × × ×				×	x	× × × × ×	× > > > > > > > > > > > > > > > > > > >

# peplink | PEPWAVE

	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.

# **11.1.5 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	0
Email Notification	☑ Enable
SMTP Server	smtp.mycompany.com           Image: State of the state of
SSL Encryption	(Note: any server certificate will be accepted)
SMTP Port	465 Default
SMTP User Name	smtpuser
SMTP Password	
Confirm SMTP Password	•••••
Sender's Email Address	łdmin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Test Email Notification Save

	Email Notification Settings
Email Notification	This setting specifies whether or not to enable email notification. If <b>Enable</b> is checked, the Peplink Balance will send email messages to system administrators when the WAN status changes or when new firmware is available. If <b>Enable</b> 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 <b>Require authentication</b> .
SSL Encryption	Check the box to enable SMTPS. When the box is checked, <b>SMTP Port</b> will be changed to <b>465</b> automatically.

https://www.peplink.com



SMTP Port	This field is for specifying the SMTP port number. By default, this is set to <b>25</b> ; when <b>SSL Encryption</b> is checked, the default port number will be set to <b>465</b> . You may customize the port number by editing this field. Click <b>Default</b> to restore the number to its default setting.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if <b>Require authentication</b> is checked in the <b>SMTP Server</b> 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 finsihed setting up email notifications, you can click the **Test Email Notification** button to test the settings before saving. After **Test Email Notification** is clicked, you will see this screen to confirm the settings:

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

Send Test Notification Cancel

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

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

### **Test Result**

[INFO] Try email through connection #3	-	~
[<-] 220 ESMTP	ľ	
[->] EHLO balance		≡
<pre>[&lt;-] 250-smtp Hello balance [210.210.210.210]</pre>	l	
250-SIZE 100000000		
250-8BITMIME		
250-PIPELINING		
250-AUTH PLAIN LOGIN		
250-STARTTLS	ſ	
		*



# 11.1.6 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		
Push Events to Mobile De	vices	0
Push Events		

Save

	Remote Syslog Settings
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
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.
peplink PEPWAVE	For more information on the Router Utility, go to: www.peplink.com/products/router-utility

# 11.1.7 SNMP

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

SNMP Settings				
SNMP Device Name	Balance_0D8	4		
SNMP Port	161	Default		
SNMPv1	🖾 Enable			
SNMPv2c	🔲 Enable			
SNMPv3	🔲 Enable			
		Save		
Community Name		Allowed Source Network	Access Mode	
MyCompany		192.168.1.20/24	Read Only	
		Add SNMP Community	1	
CNUID+O User Name		Authentiation / Driver	Access Made	
SNMPV5 USER Name		SHA / DES	Read Only	
	[		Incau only	

https://www.peplink.com

Copyright @ 2019 Peplink

# peplink | PEPWAVE

	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 <b>161</b> .
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.

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

Contraction of the	nity Name	MyCompany	
Allowed	Allowed Network	192.168.1.25 / 255.255.255.0 (/24) 🔹	
		Save Car	ncel
		SNMP Community Settings	

https://www.peplink.com



### 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:

	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	<ul> <li>This setting specifies via a drop-down menu one of the following valid authentication protocols:</li> <li>NONE</li> <li>MD5</li> <li>SHA</li> <li>When MD5 or SHA is selected, an entry field will appear for the password.</li> </ul>	
Privacy Protocol	<ul> <li>This setting specifies via a drop-down menu one of the following valid privacy protocols:</li> <li>NONE</li> <li>DES</li> <li>When DES is selected, an entry field will appear for the password.</li> </ul>	

### 11.1.8 InControl

InControl Management	
InControl Management 📀	🗹 Allow InControl Management
Privately Host InControl	<b>2</b>
InControl Host	

Save

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

When this check box is checked, the device's status information will be sent to the Peplink InControl

https://www.peplink.com