

OSPF settings
✕

Area ID	0.0.0.0
Link Type	☒ Broadcast ☐ Point-to-Point
Authentication	None ▾
Interfaces	? ☐ Untagged LAN ☐ V167 (192.168.167.1/24) ☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ WAN 5 ☒ PepVPN

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

To access RIPv2 settings, click on .

RIPv2 settings
✕

Authentication	None ▾
Interfaces	☐ Untagged LAN ☐ V167 (192.168.167.1/24) ☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ WAN 5

RIPv2 Settings	
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are MD5 and Text . Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver RIPv2 packets.

OSPF & RIPv2 Route Advertisement

SpeedFusion VPN Route Isolation	☐ Enable						
Network Advertising	--- All LAN/VLAN networks will be advertised when no network advertising is chosen.						
Static Route Advertising	☒ Enable <table> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> <th></th> </tr> <tr> <td></td> <td>255.255.255.0 (/24)</td> <td>+</td> </tr> </table>	Excluded Networks	Subnet Mask			255.255.255.0 (/24)	+
Excluded Networks	Subnet Mask						
	255.255.255.0 (/24)	+					

Save

OSPF & RIPv2 Route Advertisement	
SpeedFusion VPN Route Isolation	Isolate SpeedFusion VPN peers from each other. Received SpeedFusion VPN routes will not be forwarded to other SpeedFusion VPN peers to reduce bandwidth consumption..
Network Advertising	Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.
Static Route Advertising	Enabling OSPF & RIPv2 Route Advertising allows it to advertise LAN static routes over OSPF & RIPv2. Static routes on the Excluded Networks table will not be advertised.

21.2 BGP

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

BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	
Add			

Click the **"X"** to delete a BGP profile.
Click **"Add"** to create a new BGP profile.

BGP Profile						
Profile Name						
Enable	☒					
Interface	Untagged LAN (192.: ▼)					
Router ID	☒ LAN IP Address ☐ Custom:					
Autonomous System						
Neighbor		IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending
				disable		
Hold Time		240				
Next Hop Self		☐				
IBGP Local Preference		100				
BFD		☐ Enable				

BGP Profile	
Name	This field specifies the name that represents this profile.
Enable	When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.
Interface	The interface in which the BGP neighbor is located.
Router ID	This field specifies the unique IP as the identifier of the local device running BGP.
Autonomous System	The Autonomous System Number (ASN) assigned to this profile.
Neighbor	BGP Neighbors and their details.
IP address	The IP address of the Neighbor.
Autonomous System	The Neighbor's ASN.
Multihop/TTL	This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255.
Password	(Optional) Assign a password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received

	routes.
Hold Time	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
Next Hop Self	Enable this option to advertise your own source address as the next hop when propagating routes.
iBGP Local Preference	This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100
BFD	Enable this option to add Bidirectional Forwarding Detection for path failure. All directly connected Neighbors that use the same physical interface share the same BFD settings. All multihop Neighbors share the same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.

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

Network Advertising	Select the Networks that will be advertised to the BGP Neighbor.
Static Route Advertising	Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised.
Custom Route Advertising	Additional routes to be advertised to the BGP Neighbor.
Advertise OSPF Route	When this box is checked, every learnt OSPF route will be advertised.
Set Community	Assign a prefix to a Community.

Community:
Two numbers in new-format.
e.g. 65000:21344
Well-known communities:
no-export 65535:65281
no-advertise 65535:65282
no-export-subconfed 65535:65283
no-peer 65535:65284

Route Prefix:
Comma separated networks.
e.g. 172.168.1.0/24,192.168.1.0/28

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

Filter Mode

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

None: All BGP routes will be accepted.

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

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

Restricted Networks / Blocked Networks

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

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

Otherwise, routes within the Networks and Subnets will be filtered.

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

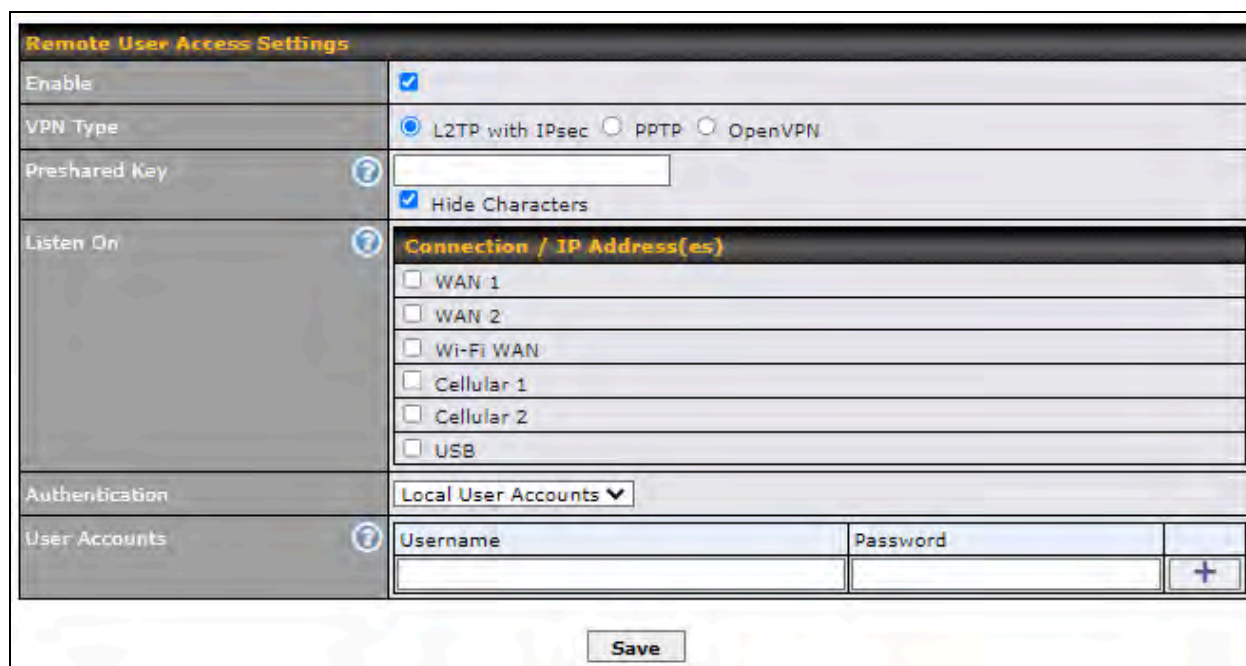
Filter Mode

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

	None: All BGP routes will be accepted. Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. Reject: Routes in "Blocked Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks / Blocked Networks	This field specifies the network(s) in the "route export" entry. Exact Match: When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.
Export to other BGP Profile	When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.
Export to OSPF	When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.

22 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 **Advanced > Remote User Access** and choose the required VPN type.



Remote User Access Settings								
Enable	☒							
VPN Type	☒ L2TP with IPsec ☐ PPTP ☐ OpenVPN							
Preshared Key	☒ Hide Characters							
Listen On	Connection / IP Address(es) ☐ WAN 1 ☐ WAN 2 ☐ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB							
Authentication	Local User Accounts ▼							
User Accounts	<table border="1"> <thead> <tr> <th>Username</th> <th>Password</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td>+</td> </tr> </tbody> </table>		Username	Password				+
Username	Password							
		+						
Save								

Remote User Access Settings

Enable

When this box is checked, this Remote User Access profile will be enabled.
If it is left unchecked, it will be disabled.

VPN Type

This field allows you to select the VPN type for the remote user access connection. The available options are:

L2TP with IPsec

PPTP

OpenVPN

Preshared Key

?

Hide Characters

If L2TP with IPsec is selected, it may need to enter the pre-shared key for the remote user access.

PPTP

VPN Type	☐ L2TP with IPsec ☒ PPTP ☐ OpenVPN
----------	---

If PPTP selected, there is 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

- OpenVPN

VPN Type	☐ L2TP with IPsec ☐ PPTP ☒ OpenVPN You can obtain the OpenVPN client profile from the status page.
Connection Security Refresh	60 minute(s)

If the OpenVPN is selected, 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:

- **"Route all traffic" profile**
Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel
- **"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.

Pre-shared Key

If **L2TP with IPsec** is selected in the VPN Type, enter the pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.

Disabled Weak Ciphers

You may click the button to show in the Pre-shared key and enable this option. When checked, weak ciphers such as 3DES will be disabled. Please note: Legacy and Android devices may not able to connect.

Connection Security Refresh

If **OpenVPN** is selected in the VPN Type, this settings is for specifying the interval for refreshing the connection.

Listen On

This setting is for specifying the WAN IP addresses that allow remote user access.

Port

If **OpenVPN** is selected in the VPN Type, the **Port** setting specifies the port(s) that correspond to the service.

Authentication

Determine the method of authenticating remote users:

- **Local User Accounts**

Authentication	Local User Accounts ▼										
User Accounts	Add	<table border="1"> <thead> <tr> <th>Username</th> <th>Password</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> X </td> </tr> <tr> <td> </td> <td> </td> <td> X </td> </tr> </tbody> </table>	Username	Password				X			X
Username	Password										
		X									
		X									

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**

Authentication	LDAP Server ▼
Authentication Protocol	MS-CHAP v2 ▼
LDAP Server	Port 389
	☐ 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 Protocol	MS-CHAP v2 ▼
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles
Authentication Host	
Authentication Port	1812
Authentication Secret	
	☒ Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles
Accounting Host	
Accounting Port	1813
Accounting Secret	
	☒ Hide Characters
Source Network Address	Untagged LAN ▼

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

• **Active Directory**

Authentication	Active Directory ▼
Server IP Address	
Server Hostname	
Domain	
Custom Workgroup	(Optional)
Admin Username	
Admin Password	
	☒ Hide Characters

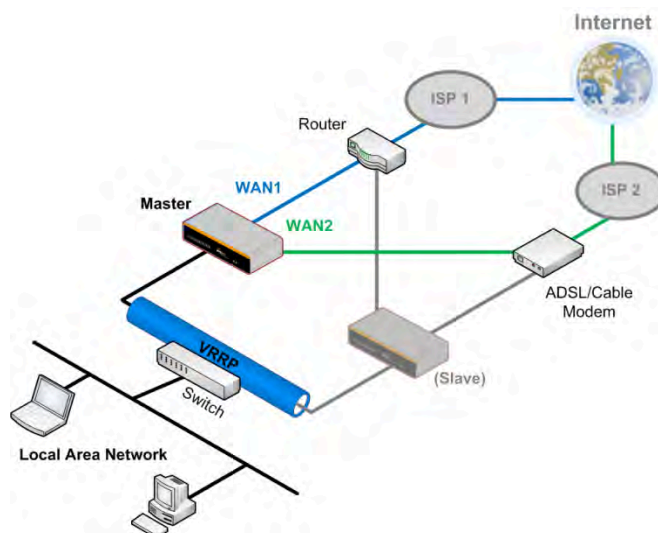
Enter the matching Active Directory details to allow for Active Directory server authentication.

23 Miscellaneous Settings

The miscellaneous settings include configuration for High Availability, Certificate Manager, service forwarding, service passthrough, GPS forwarding, GPIO, Groupe Networks (depending the feature is supported on the model of Peplink router that is being used).

23.1 High Availability

Many Peplink routers support high availability (HA) configurations via an open standard virtual router redundancy protocol (VRRP, RFC 3768). In an HA configuration, two Peplink routers 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.



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

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

- In an HA configuration, the two Peplink routers communicate with each other using VRRP over the LAN.
- The two Peplink routers 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 router is received in 3 seconds (or longer) since the last heartbeat signal, the slave Peplink router becomes active.
- The slave Peplink router initiates the WAN connections and binds to a previously

configured LAN IP address.

- At a subsequent point when the master Peplink router recovers, it will once again become active.

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

Interface for Master Router

High Availability	
Enable	☒
Group Number	
Preferred Role	☒ Master ☐ Slave
Resume Master Role Upon Recovery	☒
Virtual IP Address	
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

Interface for Slave Router

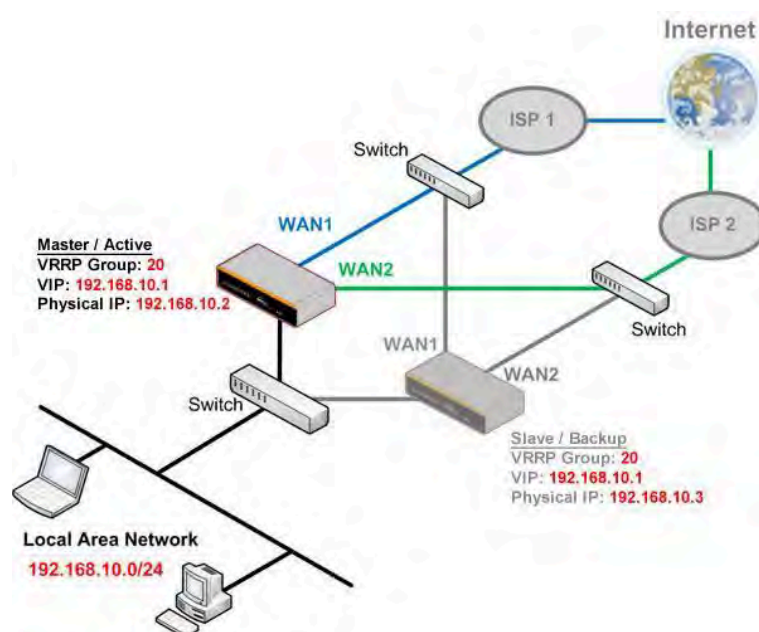
High Availability	
Enable	☒
Group Number	
Preferred Role	☐ Master ☒ Slave
Configuration Sync.	☐ Master Serial Number:
Establish Connections in Slave Role	☐
Virtual IP Address	
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

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

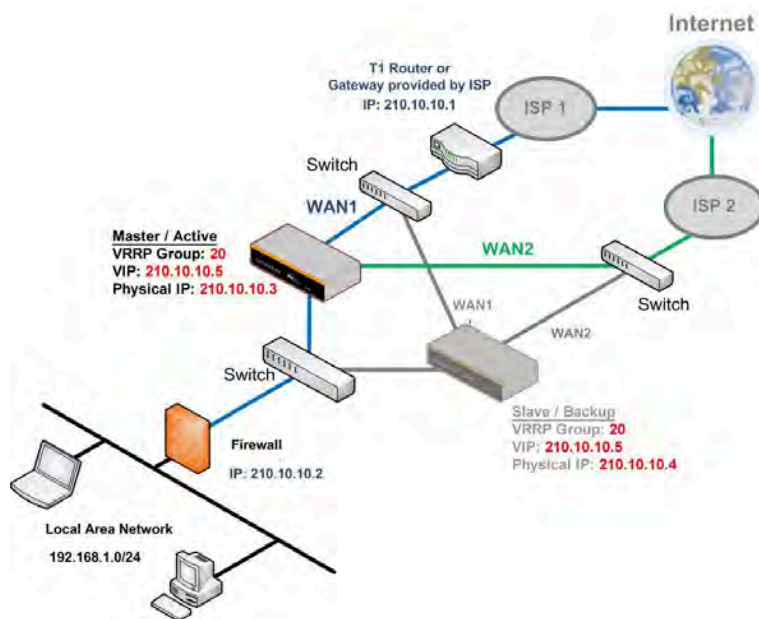
Administration IP must be under the same network.	
LAN Administration IP	This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN.
Subnet Mask	This setting specifies the subnet mask of the LAN.

Important Note

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



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



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

23.2 RADIUS Server

RADIUS Server settings are located at **Advanced > Misc. Settings > RADIUS Server**.

Authentication Server	Host	Port
No server profiles defined		
New Profile		

Accounting Server	Host	Port
No server profiles defined		
New Profile		

To configure the Authentication Server and Accounting Server, click **New Profile** to display the following screen:

Authentication Server

Name	
Host	
Port	1812
Secret	☒ Hide Characters

Save

Cancel

Authentication Server	
Name	This field is for specifying a name to represent this profile.
Host	Specifies the IP address or hostname of the RADIUS server host.
Port	This setting specifies the UDP destination port for authentication requests. By default, the port number is 1812.
Secret	This field is for entering the secret key for communicating to the RADIUS server.

Accounting Server

Name	
Host	
Port	1813
Secret	☒ Hide Characters

Save

Cancel

Accounting Server	
Name	This field is for specifying a name to represent this profile.
Host	Specifies the IP address or hostname of the RADIUS server host.
Port	This setting specifies the UDP destination port for accounting requests. By default, the port number is 1813.
Secret	This field is for entering the secret key for communicating to the RADIUS server.

23.3 Certificate Manager

Certificate		
SpeedFusion/IPsec VPN	No Certificate	
Web Admin SSL	Default Certificate is in use	
Captive Portal SSL	Default Certificate is in use	
OpenVPN CA 	Default Certificate is in use	

Wi-Fi WAN Client Certificate
No Certificates defined
Add Certificate

Wi-Fi WAN CA Certificate
No Certificates defined
Add Certificate

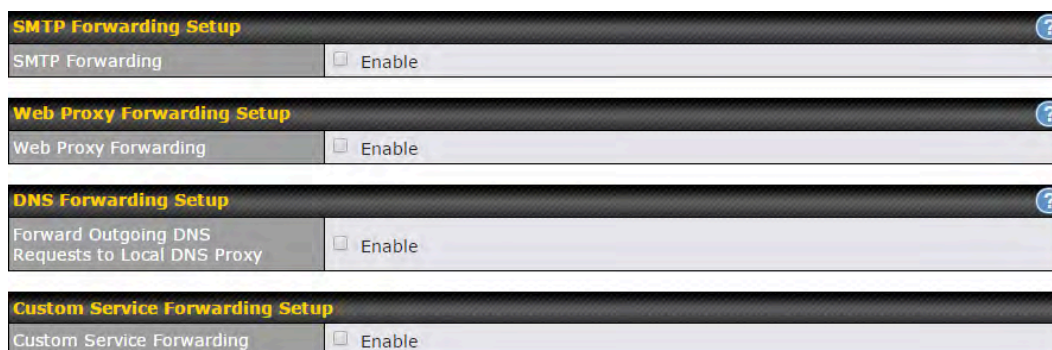
This section allows for certificates to be assigned to the local VPN, Web Admin SSL, Captive Portal SSL, OpenVPN CA, Wi-Fi WAN Client certificate and Wi-Fi WAN CA Certificate.

The following knowledge base article describes how to create self-signed certificates and import it to a Peplink Product.

<https://forum.peplink.com/t/how-to-create-a-self-signed-certificate-and-import-it-to-a-peplink-product/>

23.4 Service Forwarding

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



SMTP Forwarding Setup ?

SMTP Forwarding ☐ Enable

Web Proxy Forwarding Setup ?

Web Proxy Forwarding ☐ Enable

DNS Forwarding Setup ?

Forward Outgoing DNS Requests to Local DNS Proxy ☐ Enable

Custom Service Forwarding Setup

Custom Service Forwarding ☐ Enable

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

23.4.1 SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP's SMTP server. All outgoing SMTP connections are blocked except those connecting to the ISP's. Peplink routers support intercepting and redirecting 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	☐		
Wi-Fi WAN	☐		
Cellular 1	☐		
Cellular 2	☐		
USB	☐		

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

Note

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see **Section 14.2**).

23.4.2 Web Proxy Forwarding

Web Proxy Forwarding Setup

Web Proxy Forwarding
☒ Enable

Web Proxy Interception Settings

Proxy Server

IP Address
Port

(Current settings in users' browser)

Connection	Enable Forwarding?	Proxy Server IP Address : Port
WAN 1	☐	:
WAN 2	☐	:
Wi-Fi WAN	☐	:
Cellular 1	☐	:
Cellular 2	☐	:
USB	☐	:

When this feature is enabled, the Peplink router will intercept all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings**, choose a WAN connection with reference to the outbound policy, and then forward them 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, web proxy connections for the WAN will be simply forwarded to the connection's original destination.

23.4.3 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.

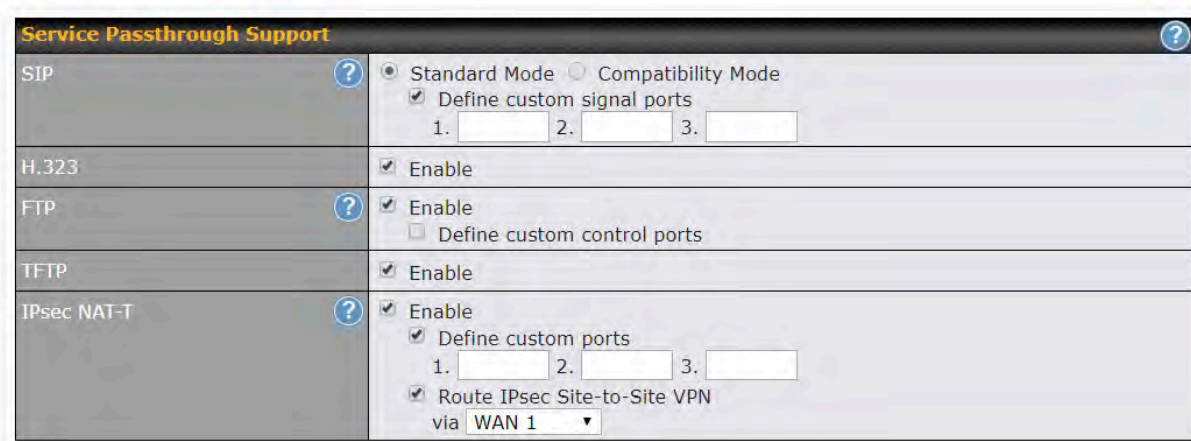
23.4.4 Custom Service Forwarding

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

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

23.5 Service Passthrough

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



The screenshot shows the 'Service Passthrough Support' configuration page. It contains a table with settings for SIP, H.323, FTP, TFTP, and IPsec NAT-T. SIP is configured in Standard Mode with custom signal ports defined. H.323, FTP, and TFTP are all enabled. IPsec NAT-T is also enabled with custom ports and site-to-site VPN routing set to WAN 1.

Service Passthrough Support	
SIP	☒ Standard Mode ☐ Compatibility Mode ☒ Define custom signal ports 1. 2. 3.
H.323	☒ Enable
FTP	☒ Enable ☐ Define custom control ports
TFTP	☒ Enable
IPsec NAT-T	☒ Enable ☒ Define custom ports 1. 2. 3. ☒ Route IPsec Site-to-Site VPN via WAN 1

Some Internet services need to be specially handled in a multi-WAN environment. Peplink routers can handle these services such that Internet applications do not notice being 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 router can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in NAT mode. Such passthrough support is always enabled, and there are two modes for selection: Standard Mode and Compatibility Mode . If your SIP server's signal port number is non-standard, you can check the box Define custom signal ports and input the port numbers to the text boxes.
H.323	With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Peplink router.
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 router monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, you can check Define custom control ports and enter the port numbers in the text boxes.
TFTP	The Peplink router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select Enable if you want to enable TFTP passthrough support.

IPsec NAT-T

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

23.6 UART

Selected Peplink MAX routers feature a RS-232 serial interface on the built-in terminal block. The RS-232 serial interface can be used to connect to a serial device and make it accessible over an TCP/IP network.

The serial interface can be enabled and parameters can be set on the web admin page under **Advanced > UART**. Make sure they match the serial device you are connecting to.

Serial to Network	
Enable	☒
Allowed Source IP Subnets	☒ Any ☐ Allows access from the following IP subnets only
Web Console	☐

Serial Parameters	
Baud Rate	9600 ▼
Data Bits	8 ▼
Stop Bits	1 ▼
Parity	None ▼
Flow Control	None ▼
Interface	RS232 ▼

Operating Settings	
Operation Mode	TCP Server Mode ▼
Local TCP Port	4001
Max Connection	1
TCP Alive Check Time	7 min(s)
Inactivity Time	0 ms

Data Packing	
Packing Length	0 byte(s)
Delimiter	☐
Delimiter process	Do Nothing ▼
Force Transmit	0 ms

There are 4 pins i.e. TX, RX, RTS, CTS on the terminal block for serial connection and they correspond to the pins in a DB-9 connector as follows:

DB-9 Peplink MAX Terminal Block

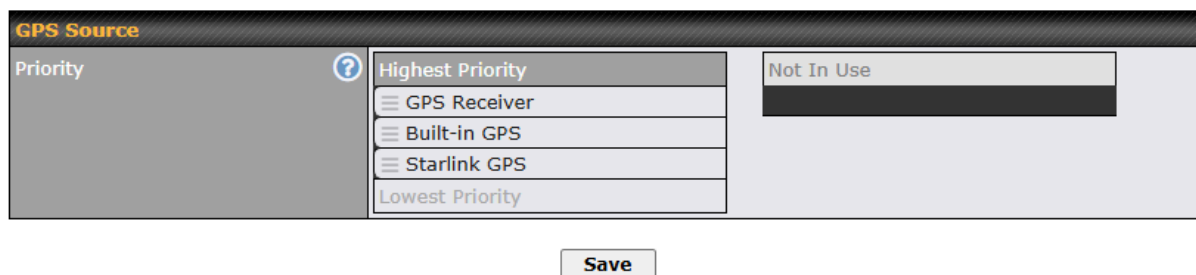
Pin 1	–
Pin 2	Rx (rated +25V)
Pin 3	Tx (rated +12V)
Pin 4	–
Pin 5	–
Pin 6	–
Pin 7	RTS
Pin 8	CTS
Pin 9	–

The RS232 serial interface is not an isolated RS232. External galvanic isolation may be added if required.

Be sure to check whether your serial cable is a null modem cable, commonly known as crossover cable, or a straight through cable. If in doubt, swap Rx and Tx, and RTS and CTS, at the other end and give it another go.

Once connected, your serial device should be accessible on your Peplink MAX router LAN IP address at the specified TCP port.

23.7 GPS



Priority	?	
		Highest Priority
		GPS Receiver
		Built-in GPS
		Starlink GPS
		Lowest Priority

Not In Use

Save

This settings is to specific the priority of the GPS source to be used for receiving GPS data. The device will always use the highest priority GPS source to receive GPS data. A lower priority GPS source will only be used when all higher priority GPS source data is invalid or unavailable. GPS source type will be shows on the Dashboard map.



23.8 GPS Forwarding

Using the GPS forwarding feature, some Peplink routers can automatically send GPS reports to a specified server. To set up GPS forwarding, navigate to **Advanced > Misc. Settings > GPS Forwarding**.

GPS Forwarding						
Enable	☒					
Destination ?	IP Address / Host Name	Port	Protocol	Format	Report Interval	
			UDP	NMEA	☒ Default 1 s	☒ Stationary
			UDP	TAIP	☒ Default 1 s	☒ Stationary
NMEA Sentence Type	☐ GPRMC ☐ GPGGA ☐ GPVTG ☐ GPGSA ☐ GPGSV					
NMEA Vehicle ID ?	☐					
TAIP Sentence Type	☐ PV - Position / Velocity Solution ☐ CP - Compact Position Solution ☐ LN - Long Navigation Solution					
TAIP ID (optional)						

Save

GPS Forwarding

Enable

Check this box to turn on GPS forwarding.

Server Enter the name/IP address of the server that will receive GPS data. Also specify a port number, protocol (**UDP** or **TCP**), Format (**NMEA** or **TAIP**) and a report interval. Click  to save these settings.

NMEA Sentence Type If you've chosen to send GPS reports in NMEA format, select one or more sentence types for sending the data (**GPRMC**, **GPGGA**, **GPVTG**, **GPGSA**, and **GPGSV**).

Vehicle ID The vehicle ID will be appended in the last field of the NMEA sentence. Note that the NMEA sentence will become customized and non-standard.

TAIP Sentence Type/TAIP ID (optional) If you've chosen to send GPS reports in TAIP format, select one or more sentence types for sending the data (**PV—Position / Velocity Solution** and **CP—Compact Velocity Solution**). You can also optionally include an ID number in the **TAIP ID** field.

23.9 GPS Receiver

GPS Receiver for Raw NMEA 0183 Network Stream 			
Enable	☒		
Protocol	☒ TCP ☐ UDP		
Port			
Access Control	Sender IP Address / Network	Subnet Mask	
		255.255.255.0 (/24) 	

Save

GPS Receiver for Raw NMEA 0183 Network Stream

Enable Check this box to turn on GPS forwarding.

Protocol Select protocol **TCP** or **UDP**

Port Specific port number.

Access Control Enter the IP address / Network of the sender. Click  to save these settings.

23.10 Ignition Sensing

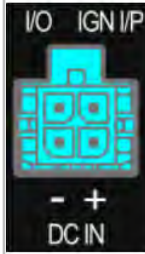
Ignition Sensing detects the ignition signal status of a vehicle it is installed in.

This feature allows the router to start up or shut down when the engine of that vehicle is started or turned off.

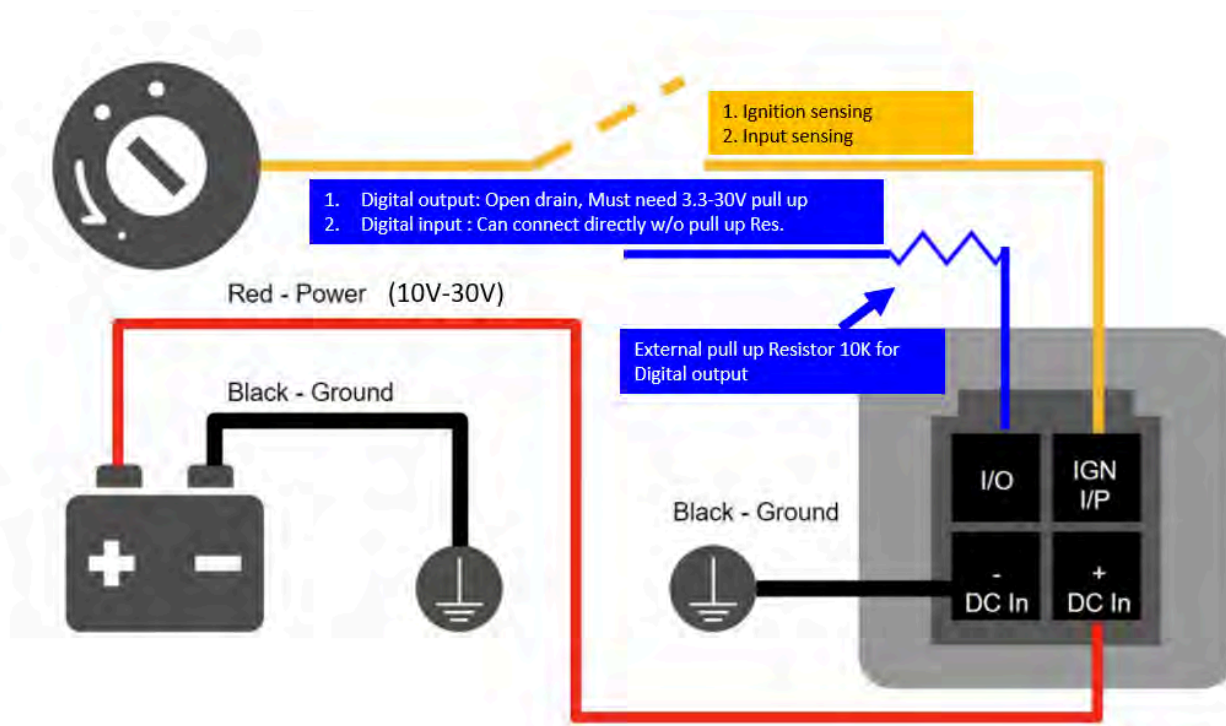
The time delay setting between ignition off and power down of the router is a configurable setting, which allows the router to stay on for a period of time after the engine of a vehicle is turned off.

Note: Ignition Sensing is supported on MAX Orbit 2 and MAX Orbit 4 only. MAX Orbit 8 does not support Ignition Sensing.

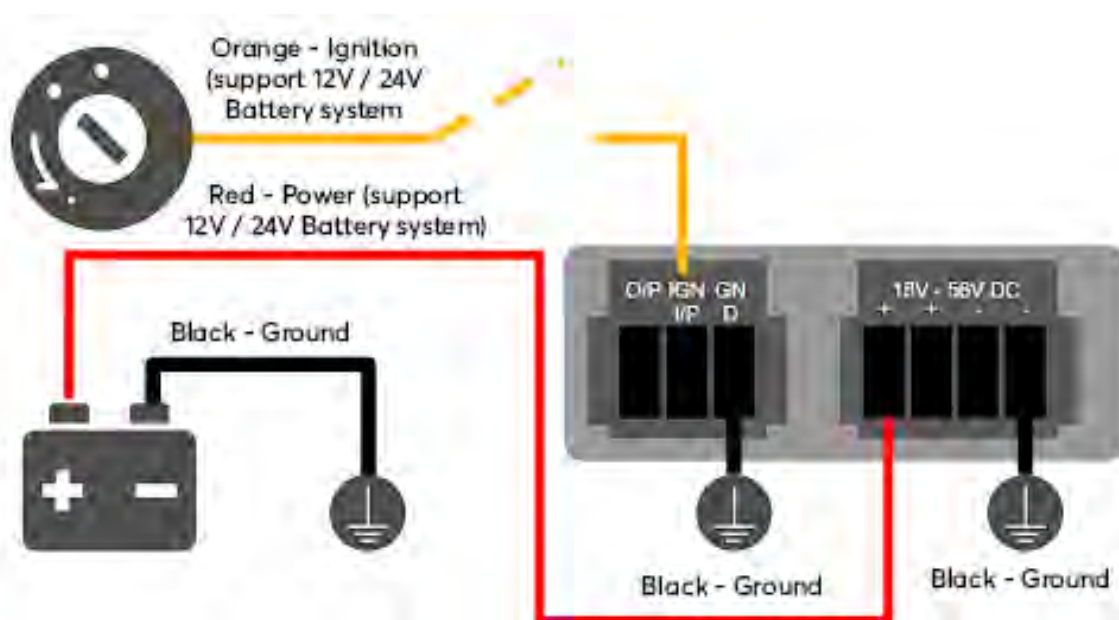
Ignition Sensing installation

Function		Colour Wire
	I/O optional *	Brown
	IGN I/P connected to positive feed on the ignition **	Orange
	DC IN - connected to permanent negative feed (ground)	Black
	DC IN + connected to permanent positive feed (power)	Red
* Currently not functional; will be used for additional features in future firmware. ** Connecting IGN I/P is optional and is needed only if the Ignition Sensing feature is configured.		

Connectivity diagram for devices with 4-pin connector



Connectivity diagram for devices with terminal block connection



GPIO Menu

Note: This feature is applicable for certain models that come with a GPIO interface.

Ignition Sensing options can be found in **Advanced > Misc. Settings > GPIO**.

The configurable option for Ignition Input is **Delay**; the time in seconds that the router stays powered on after the ignition is turned off.

a.) Ignition sensing: 9-30V active high for IGN purpose

b.) Input Sensing: I/O input

IGN I/P	
Name	IGN I/P
Enable	☒
Type	Digital Input ▾
Mode	Input Sensing ▾
State Name	High: High Low: Low
Delay	seconds

The O/P (connected to the I/O pin on a 4 pin connector) can be configured as a digital input, a digital output, or an analog input.

Digital Input – the connection supports input sensing; it reads the external input and determines if the settings should be 'High' (on) or 'Low' (off).

State Name - This field is to custom names shows on event log when digital input is high or low.

a.) Digital output:

Open drain for IO output. It is required to add an external pull up resistor of 10K for 3.3-30V pull up voltage.

(DO NOT exceed 250mA)

3.3-30V active high, 0.05-0.5V active low(mapping to 3.3-30V pull up voltage)

b.) Digital input: I/O input

O/P	
Enable	☒
Type	Digital Output ▾
Mode	WAN Status ▾

Note: The Digital Output state (on/off) upon rebooting the device may vary depending on the model, eg. MAX BR1 MK2 = Persistent; MAX Transit Mini with ContentHub = Reset to default, etc.

Analog Input - to be confirmed. In most cases, it should read the external input and determine the voltage level.

23.11 NTP Server

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

Compatible with: MAX Orbit 2, MAX Orbit 4, MAX Orbit 8

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

NTP Server	
Enable	☐

[Save](#)

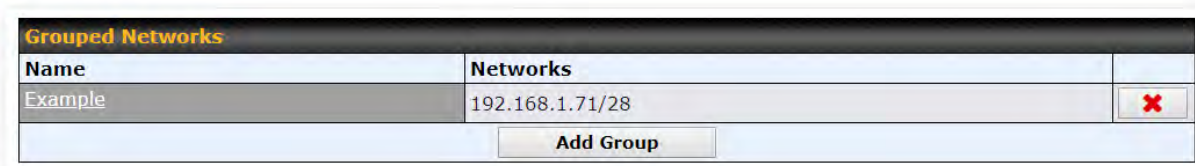
Time Settings can be found at **System > Time > Time Settings**

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

[Save](#)

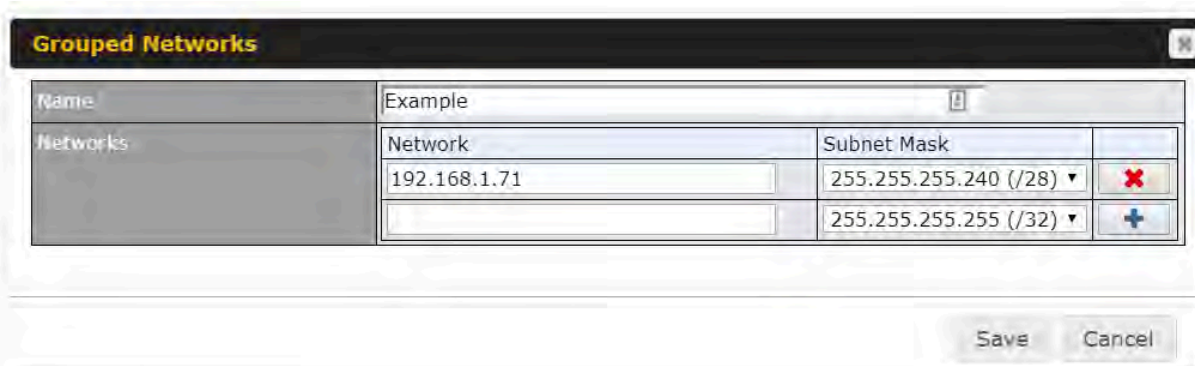
23.12 Grouped Networks

Advanced > Misc. Settings > Grouped Networks allows to configure destination networks in grouped format.



Grouped Networks		
Name	Networks	
Example	192.168.1.71/28	
Add Group		

Select Add group to create a new group with single IPAddresses or subnets from different VLANs.



Grouped Networks			
Name	Example 		
Networks	Network	Subnet Mask	
	192.168.1.71	255.255.255.240 (/28) ▼	
		255.255.255.255 (/32) ▼	
Save Cancel			

The created network groups can be used in outbound policies, firewall rules.

23.13 UDP Relay

You may define the UDP relay by clicking the **Advanced > Misc Settings > UDP Relay**. You can click  to enable the UDP relay to relay UDP Broadcast or Multicast traffic for LAN/VLAN/SpeedFusion VPN.



Click “*New UDP Relay Rule*” to define the relay rule.

Name	Port / Multicast Address	Source Network	Destination Network
No UDP relay rules defined			
New UDP Relay Rule			

UDP Relay

Name

Port

Multicast ☒ Address:

Source Network LAN: Untagged LAN

Destination Network Any

UDP Relay	
Name	This field is for specifying a name to represent this profile.
Port	This feid is to enter the specific port number for the UDP relay
Multicast	If Multicast is not selected, it will broadcast relay rule. If Multicast is selected, you may need to enter a valid multicast address.
Secure Network	Select the specific connection as a source network to where the device is to relay UDP Broadcast packets.
Destination Network	You may select the specific connection from the drop-down list or may custom combination network as a destination network that receives the UDP packet relays.

24 AP

24.1 AP Controller

The AP controller acts as a centralized controller of Peplink Access Points. With this feature, users can customize and manage up to 1500 Access Points from a single Peplink router interface.

To configure, navigate to the **AP** tab, and the following screen appears.

AP Controller	
AP Management	☒ Integrated AP ☒ External AP
Sync. Method	As soon as possible ▼
Permitted AP	☒ Any ☐ Approved List

AP Controller	
AP Management	The AP controller for managing Peplink APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, CAPWAP Access Controller addresses (field 138), will be added to the DHCP server. A local DNS record, AP Controller , will be added to the local DNS proxy.
Sync Method	- As soon as possible - Progressively - One at a time
Permitted AP	Access points to manage can be specified here. If Any is selected, the AP controller will manage any AP that reports to it. If Approved List is selected, only APs with serial numbers listed in the provided text box will be managed.

24.2 Wireless SSID

SSID	Security Policy
No SSID Defined	
Add	

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

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



SSID

SSID Settings

SSID	
Schedule	Always on ▾
VLAN	Untagged LAN ▾
Broadcast SSID	☒
Data Rate	☒ Auto ☐ Fixed ☐ Minimum
Multicast Filter	☐
Multicast Rate	MCS24/MCS16/MCS8/MCS0/6M ▾
IGMP Snooping	☐
Layer 2 Isolation	☐
Maximum number of clients	2.4 GHz: Unlimited 5 GHz: Unlimited
Band Steering	Disable ▾

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Schedule	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 Peplink AP One unit to the Ethernet segment via the LAN port). The default value of this setting is 0 , which means VLAN tagging is disabled (instead of tagged with zero).
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate ^A	Select Auto to allow the Peplink router to set the data rate automatically, or select Fixed and choose a rate from the displayed drop-down menu.
Multicast Filter^A	This setting enables the filtering of multicast network traffic to the wireless SSID.

Multicast Rate^A	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected Protocol and Channel Bonding settings will affect the rate options and values available here.
IGMP Snooping^A	To allow the Peplink router to listen to internet group management protocol (IGMP) network traffic, select this option.
Layer 2 Isolation^A	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to the upper communication layer(s). By default, the setting is disabled.
Maximum Number of Clients^A	Indicate the maximum number of clients that should be able to connect to each frequency.
Band Steering^A	To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency. Choose between: Force - Clients capable of 5 GHz operation are only offered with 5 GHz frequency. Prefer - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered. Disable - Default

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

Security Settings	
Security Policy	Open (No Encryption) ▼

Security Settings

Security Policy This setting configures the wireless authentication and encryption methods. Available options are:

- **Open (No Encryption)**
- **Enhanced Open (OWE)**
- **WPA3 – Personal (AES:CCMP)**
- **WPA3 – Enterprise (AES:CCMP)**
- **WPA2/WPA3 – Personal (AES:CCMP)**
- **WPA2 – Personal (AES:CCMP)**
- **WPA2 – Enterprise (AES:CCMP)**
- **WPA/WPA2 – Personal (TKIP/AES: CCMP)**
- **WPA/WPA2 – Enterprise (TKIP/AES: CCMP)**

To allow any Wi-Fi client to access your AP without authentication, select **Open (No Encryption)**. Details of each available authentication method follow.

Security Settings	
Security Policy	Enhanced Open (OWE) ▼
Transition Mode	☒

Enhanced Open (OWE)

Transition Mode With the option enabled, legacy clients will be able to connect in Open mode. With the option disabled, legacy clients will not be able to connect. OWE-supported clients will always connect in OWE mode.

Security Settings	
Security Policy	WPA3 - Personal ▼
Encryption	AES:CCMP
Shared Key	 ☒ Hide Characters
Fast Transition	☐

WPA3 – Personal

Shared Key Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Characters** to toggle visibility.

Fast Transition Fast Transition

[802.11r] When this option is ticked, the transition process for a mobile client

is improved as it moves between access points.

Security Settings	
Security Policy	WPA3 - Enterprise ▼
Encryption	AES:CCMP
802.1X Version	☒ v1 ☐ v2
Fast Transition	☐

WPA3 – Enterprise

802.1X Version

Choose **v1** or **v2** of the 802.1x EAPOL. When **v1** is selected, both **v1** and **v2** clients can associate with the access point. When **v2** is selected, only **v2** clients can associate with the access point. Most modern wireless clients support **v2**. For stations that do not support **v2**, select **v1**. The default is **v2**.

Fast Transition

Fast Transition

[802.11r] When this option is ticked, the transition process of a mobile client is improved as it moves between access points.

Security Settings	
Security Policy	WPA2/WPA3 - Personal ▼
Encryption	AES:CCMP
Shared Key	☒ Hide Characters
Management Frame Protection	Default (Optional) ▼
Fast Transition	☐

WPA2/WPA3 – Personal

Shared Key Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Characters** to toggle visibility.

Management Frame Protection This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication, and QoS Action.

Fast Transition Fast Transition [802.11r] When this option is ticked, the transition process of a mobile client is improved as it moves between access points.

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Private Pre-Shared Key	☐
Shared Key	☒ Hide Characters
Management Frame Protection	Default (Disabled) ▼
Fast Transition	☐

Security Settings					
Security Policy	WPA2 - Personal ▼				
Encryption	AES:CCMP				
Private Pre-Shared Key ?	☒				
	Name	Shared Key	MAC	VLAN ID	
	UserA	 ☒ Hide Characters	: : : : :	Untagge	✖
	UserB	 ☒ Hide Characters	AA:AA:AA:AA:AA	Untagge	✖
		 ☒ Hide Characters	: : : : :	Untagge	+
Management Frame Protection	Default (Disabled) ▼				

WPA2 – Personal

Private Shared Key

Enable the Private Pre-Shared Key (PPSK) option to set unique pre-shared keys for individual users or groups on the same SSID. Please provide the following information for each user or group:

Name (Optional)

Name for the profile

Shared Key

The passphrase key is used for data encryption and authentication. You can click “Hide/Show Characters” to toggle the visibility of the shared key.

**MAC
(Optional)**

By default, all MAC addresses are allowed. If a specific MAC address is entered, only that device can access this WiFi SSID using the provided shared key.

**VLAN ID
(Optional)**

The VLAN is assigned to the user upon logging into the WiFi. If not specified, the user will be assigned to the default untagged LAN.

*Each “Shared Key + MAC” combination must be unique in a different profile.

Shared Key

Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Characters** to toggle visibility.

**Management Frame
Protection**

This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication, and QoS Action.

**Fast
Transition**

Fast Transition

[802.11r] When this option is ticked, the transition process of a mobile client

is improved as it moves between access points.

Security Settings	
Security Policy	WPA2 - Enterprise ▼
Encryption	AES:CCMP
802.1X Version	☒ v1 ☐ v2
Management Frame Protection	Default (Disabled) ▼
Fast Transition	☐

WPA2 – Enterprise

802.1X Version Choose **v1** or **v2** of the 802.1x EAPOL. When **v1** is selected, both **v1** and **v2** clients can associate with the access point. When **v2** is selected, only **v2** clients can associate with the access point. Most modern wireless clients support **v2**. For stations that do not support **v2**, select **v1**. The default is **v2**.

Management Frame Protection This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication, and QoS Action.

Fast Transition Fast Transition

[802.11r] When this option is ticked, the transition process of a mobile client is improved as it moves between access points.

Security Settings	
Security Policy	WPA/WPA2 - Personal ▼
Encryption	TKIP/AES:CCMP
Private Pre-Shared Key ?	☐
Shared Key ?	 ☒ Hide Characters
Management Frame Protection	Default (Disabled) ▼

Security Settings					
Security Policy		WPA/WPA2 - Personal ▼			
Encryption		TKIP/AES:CCMP			
Private Pre-Shared Key ?	☒				
	Name	Shared Key	MAC	VLAN ID	
	UserA	 ☒ Hide Characters	AA:AA:AA:AA:AA	Untagge	✖
	UserB	 ☒ Hide Characters	BB:BB:BB:BB:BB	20	✖
	UserC	 ☒ Hide Characters	CC:CC:CC:CC:CC	Untagge	+
Management Frame Protection		Default (Disabled) ▼			

WPA/WPA2 – Personal

Private Shared Key

Enable the Private Pre-Shared Key (PPSK) option to set unique pre-shared keys for individual users or groups on the same SSID. Please provide the following information for each user or group:

Name (Optional)

Name for the profile

Shared Key

The pass-phrase key is used for data encryption and authentication. You can click “Hide/Show Characters” to toggle the visibility of the shared key.

MAC (Optional)

By default, all MAC addresses are allowed. If a specific MAC address is entered, only that device can access this WiFi SSID using the provided shared key.

VLAN ID (Optional)

The VLAN is assigned to the user upon logging into the WiFi. If not specified, the user will be assigned to the default untagged LAN.

*Each “Shared Key + MAC” combination must be unique in a different

profile.

Shared Key Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Characters** to toggle visibility.

Management Frame Protection This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action.

Security Settings	
Security Policy	WPA/WPA2 - Enterprise ▼
Encryption	TKIP/AES:CCMP
802.1X Version	☒ v1 ☐ v2
Management Frame Protection	Default (Disabled) ▼

WPA/WPA2 – Enterprise

802.1X Version Choose **v1** or **v2** of the 802.1x EAPOL. When **v1** is selected, both v1 and v2 clients can associate with the access point. When **v2** is selected, only v2 clients can associate with the access point. Most modern wireless clients support v2. For stations that do not support v2, select **v1**. The default is **v2**.

Management Frame This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation,

Protection Deauthentication and QoS Action.

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

Access Control	
Restricted Mode	The settings allow the administrator to control access using MAC address filtering. Available options are None , Deny all except listed , Accept all except listed and Radius MAC Authentication .
MAC Address List	Connection coming from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field. If more than one MAC address needs to be entered, you can use a carriage return to separate them.

RADIUS Settings		
	Primary	Secondary
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles	
Authentication Host		
Authentication Port	1812	1812
Authentication Secret	 ☒ Hide Characters	 ☒ Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles	
Accounting Host		
Accounting Port	1813	1813
Accounting Secret	 ☒ Hide Characters	 ☒ Hide Characters
NAS-Identifier	Device Name	

RADIUS Settings	
Authentication Host	This field is for specifying the IP address of the primary RADIUS server for Authentication and, if applicable, the secondary RADIUS server.

Authentication Port	In the field, the UDP authentication port(s) used by your RADIUS server(s) or click the Default is 1812 .
Authentication Secret	This settings is enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
Accounting Host	This field is for specifying the IP address of the primary RADIUS server for Accounting and, if applicable, the secondary RADIUS server.
Accounting Port	In the field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the Default is 1813 .
Accounting Secret	This settings is enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
NAS-Identifier	Choose between Device Name , LAN MAC address , Device Serial Number and Custom Value

Guest Protect

Block All Private IP	☐		
Custom Subnet	Network	Subnet Mask	
		255.255.255.0 (/24) ▼	+
Block Exception	Network	Subnet Mask	
		255.255.255.0 (/24) ▼	+

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

Firewall Settings

Firewall Mode	Disable ▼ Disable Flexible - Allow all except... Lockdown - Block all except...
---------------	---

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

24.3 Wireless Mesh

The screenshot shows a 'Wireless Mesh' configuration window. At the top, there's a header with 'Wireless Mesh' on the left and 'Frequency Band' on the right. Below the header, a message states 'No Wireless Mesh Defined'. At the bottom center, there is an 'Add' button.

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

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

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

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

24.4 Settings

To configure the AP settings, navigating to **AP > Settings** :

AP Settings	
SSID	2.4 GHz 5 GHz ☒ ☒ PEPWAVE_A712
Operating Country	United States
	2.4 GHz 5 GHz
Protocol	802.11n 802.11n/ac
	Integrated AP supports 802.11n/ac only
Channel Width	Auto
Channel	Auto Edit Channels: 1 6 11
Auto Channel Update	Daily at ☐ 00:00 ☐ 01:00 ☐ 02:00 ☒ 03:00 ☐ 04:00 ☐ 05:00 ☐ 06:00 ☐ 07:00 ☐ 08:00 ☐ 09:00 ☐ 10:00 ☐ 11:00 ☐ 12:00 ☐ 13:00 ☐ 14:00 ☐ 15:00 ☐ 16:00 ☐ 17:00 ☐ 18:00 ☐ 19:00 ☐ 20:00 ☐ 21:00 ☐ 22:00 ☐ 23:00 ☒ Wait until no active client associated
Output Power	Max Boost
Client Signal Strength Threshold	Disabled
Maximum number of clients	Unlimited
Discover Nearby Networks	☒ Note: Feature will be automatically turned on with Auto Channel / Dynamic Output Power
Beacon Rate	1 Mbps
Beacon Interval	100 ms
DTIM	1
RTS Threshold	0
Fragmentation Threshold	0 (0: Disable)
Distance / Time Converter	4050 m Note: Input distance for recommended values
Slot Time	☐ Auto ☒ Custom 9 μ s
ACK Timeout	48 μ s

AP Settings

SSID

These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Peplink MAX does not detect whether the AP is capable of transmitting at

	both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.
Operating Country	This drop-down menu specifies the national / regional regulations which the AP should follow. - If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). - If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). Note: Users are required to choose an option suitable to local laws and regulations. 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.
Preferred Frequency	These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies.
Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are 802.11ng and 802.11na . By default, 802.11ng is selected.
Channel Width	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
Channel	This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
Output Power	This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When Dynamic settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance. The Dynamic: Auto setting will set the AP to do this automatically. Otherwise, the Dynamic: Manual setting will set the AP to dynamically adjust only if instructed to do so. If you have set Dynamic:Manual, you can go to AP>Toolbox>Auto Power Adj. to give your AP further instructions. If you click the Boost checkbox, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to increased interference.