

Drop-In Mode Settings								
Enable	☒							
WAN for Drop-In Mode	WAN ▾ ☒ Apply NAT on VLAN networks outgoing Internet traffic VLAN network(s) may route their outgoing Internet traffic to this unit. When this checkbox is checked their traffic will be NAT'd before forwarding out of this WAN. Leave this checkbox checked if you are not sure.							
Share Drop-In IP	☒							
Shared IP Address	255.255.255.0 (/24) ▾							
Static Route	<table border="1"> <thead> <tr> <th>Destination Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>255.255.255.0 (/24) ▾</td> <td>+</td> </tr> </tbody> </table>		Destination Network	Subnet Mask			255.255.255.0 (/24) ▾	+
Destination Network	Subnet Mask							
	255.255.255.0 (/24) ▾	+						
WAN Default Gateway	☒ I have other host(s) on WAN segment IP Address - 							
WAN DNS Servers	DNS server 1: DNS server 2:							
NOTE: The DHCP Server Settings will be overwritten. The following WAN settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings. The PPTP Server will be disabled. Tip: please review the DNS Forwarding setting under the Service Forwarding section.								

Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of the Peplink MAX on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If WAN is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^A	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The MAX will listen for this IP address when WAN hosts access services provided by the MAX (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The MAX will listen for this IP address when LAN hosts access services provided by the MAX (web admin access from the WAN, DNS proxy, etc.).

Shared IP Address^A	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the  button next to "WAN Default Gateway" and check the other host(s) on the WAN segment box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

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

7.2 Port Settings

To configure port settings, navigate to **Network > Port Settings**

Port Settings						
ID	Name	Port Type	VLAN Networks	PVID	Speed	
1		Trunk	Any	Untagged LAN (1)	Auto	
2		Trunk	Any	Untagged LAN (1)	Auto	
3		Trunk	Any	Untagged LAN (1)	Auto	
4		Trunk	Any	Untagged LAN (1)	Auto	

On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, as well as which VLAN each link belongs to, if any.

Untagged frames received by the port are classified to a VLAN indicated by Port VLAN Identifier (PVID). All frames from the VLAN are untagged on egress. PVID option is only configurable when Port Type is set to "Trunk".

7.3 Captive 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 > LAN > Captive Portal**.

Captive Portal

General Settings

Name			
Enable	☒ Untagged LAN		
Hostname		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	☒ Daily at 00 :00 ☐ 1440 minutes after quota reached
Inactive Timeout	0 minutes (0: No Timeout)
Allowed Networks	Domain Name / IP Address / Network +
Allowed Clients	MAC / IP Address / Host Identifier +
Splash Page	☒ Built-in ☐ External, URL: http://
Popup Handling	☐ Bypass Popup (Redirection only takes place on normal browser) ☐ Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	(Not configured)

Click [here](#) to preview / customize built-in splash page

Save

Cancel

Captive Portal Settings	
Name	Enter the name for the Captive Portal.
Enable	Check Enable 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 Default .

Access Mode

Click **Open Access** to allow clients to freely access your router. Click **User Authentication** to force your clients to authenticate before accessing your router.

Select **External Server** to use the Captive Portal with a HotSpot system.

As described in the following knowledgebase article:

<https://forum.peplink.com/t/using-hotspotsystem-wi-fi-on-Peplink-max-routers/>

Authentication

When selecting the “**User Authentication**” in the Access Mode field, you will see the available option for the Authentication via drop-down list:

- RADIUS Server

Access Mode	☐ Open Access ☒ User Authentication ☐ External Server
Authentication	RADIUS Server ▼

RADIUS Settings		
	Primary	Secondary
Authentication Protocol	PAP ▼	
	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
CoA-DM	☐	
Accounting Interim Interval	?	
NAS-Identifier	?	

- LDAP Server

Access Mode	☐ Open Access ☒ User Authentication ☐ External Server
Authentication	LDAP Server ▼

LDAP Settings	
LDAP Server	Port Default
	☐ Use DN/Password to bind to LDAP Server
Base DN	
Base Filter	

Fill in the necessary information to complete your connection to the server and enable authentication.

External Server

When selecting the “**External Server**” in the Access Mode field, you will see the available option for the Service Type via drop-down list:

- CoovaChilli

	Access Mode ☐ Open Access ☐ User Authentication ☒ External Server Server Type CoovaChilli CoovaChilli Settings UAM Secret ☒ Hide Characters HotspotSystem Access Mode ☐ Open Access ☐ User Authentication ☒ External Server Server Type HotspotSystem HotspotSystem Settings Operator Username Location ID Splash Page Domain customer.hotspotsystem.com Fill in the necessary information to complete your connection to the server and enable authentication.
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to Daily will reset it at a specified time every day. Setting a number of minutes after quota reached establish a timer for each user that begins after the quota has been reached.
Inactive Timeout	Clients will get disconnected when the inactive the configured time is reached. Default 0: no timeout
Allowed Networks	Add networks that can bypass the captive Portal in this field. To whitelist a network, enter the domain name / IP address here and click . To delete an existing network from the list of allowed networks, click the  button next to the listing.
Allowed Clients	Add MAC address and /or IP addresses for client devices that are allowed to bypass the Captive Portal. Clients accessing these domains and IP addresses will not be redirected to the splash page.
Splash Page	Here, you can choose between using the Peplink router'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 Hostname	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



PEPWAVE

☐ Use uploaded Logo Image
☒ Use default Logo Image
☐ No file chosen

NOTE: Size max: 512KB. Supported images types: JPEG, PNG and GIF.

EMPTY STRING

☒ I have read and agree to the [terms and conditions](#) ?

You must accept the terms and conditions before you can proceed

Agree

Powered by Pepwave.

Portal Configuration

Show Quota Status	☒
Custom Landing Page	☐

Page: Login ▼

Edit mode ON ?

Save

8 Configuring the WAN Interface(s)

WAN Interface settings are located at **Network > WAN**. To reorder WAN priority, drag on the appropriate WAN by holding the left mouse button, move it to the desired priority (the first one would be the highest priority, the second one would be lower priority, and so on), and drop it by releasing the mouse button.

WAN Connection Status

Priority 1 (Highest)		
Orbit 1	Connected via Starlink	192.168.100.25
Orbit 2	Connected	10.9.2.235
Orbit 3	Connected via Oneweb	192.168.100.26
Orbit 4	No Cable Detected	(No IP Address)
LAN 2	No Cable Detected	(No IP Address)
Priority 2		
Drag desired (Priority 2) connections here		
Disabled		
Wi-Fi WAN on 2.4 GHz	Disabled	(No IP Address)
Wi-Fi WAN on 5 GHz	Disabled	(No IP Address)
VLAN WAN 1	Disabled	(No IP Address)

Click [here](#) to show all disabled as LAN Connections.

DNS over HTTPS
Disabled

WAN Quality Monitoring
Auto

Synergy Controller
Disabled

Orbit WAN

Starlink	Orbit 1
OneWeb	Orbit 3

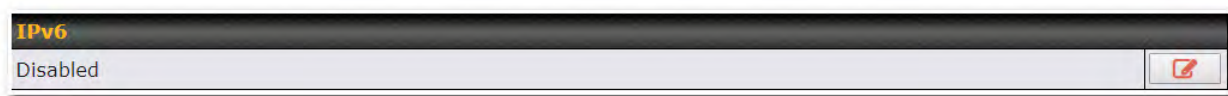
To enable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it to the **Disabled** row, and drop it by releasing the mouse button.

You can also set priorities on the **Dashboard**. Click the **WAN** button in the corresponding row to modify the connection setting.

Important Note

Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.

IPv6

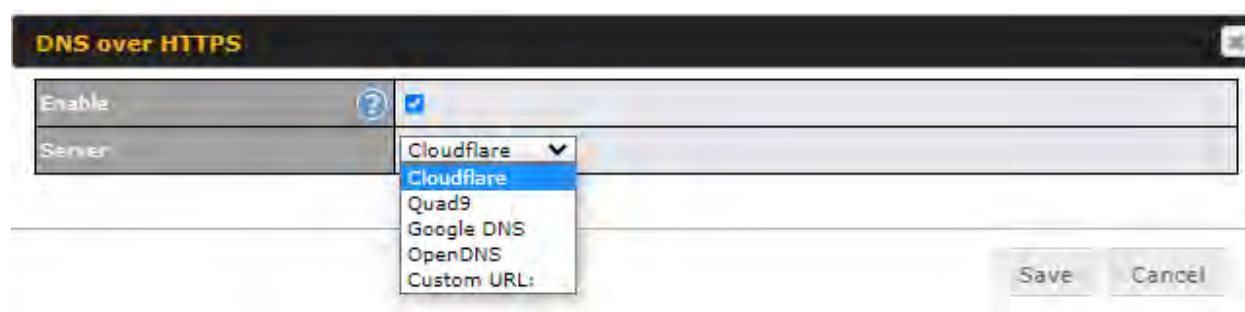


You can also enable IPv6 support in this section.

DNS over HTTPS (DoH)



You can enable DoH (DNS over HTTPS) support in this section.



DNS over HTTPS	
Enable	When this option is enabled, the DNS proxy server will use HTTPS connections to forward DNS requests to the DoH resolver; it will not fallback to traditional UDP DNS options.
Server	The options to configure DoH with a predefined server are: - Cloudflare - The DNS server IP addresses for Cloudflare will be using 1.1.1.1, which is unfiltered. - Quad9 - The DNS server IP addresses for Quad9 will be using 9.9.9.9 and 142.112.112.112, which is malware blocking and DNSSEC. - Google DNS - The DNS server IP addresses for Google DNS will be using 8.8.8.8 and 8.8.4.4, which is RFC8484 standard. - OpenDNS - The DNS server IP addresses for OpenDNS will be using 208.67.222.222 and 208.67.220.220, which is standard DNS. - Custom URL - You may select Custom URL:, and enter the resolver URL and IP address.

WAN Quality Monitoring

This settings advice how WAN Quality information is being gathered.

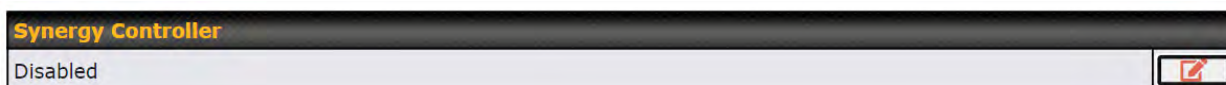


The screenshot shows a settings window titled "WAN Quality Monitoring". It has a search bar with the text "Auto" and a red edit icon in the top right corner.

By default, WAN Quality will always be observed and gathered automatically. With customized choice of WAN connections, the device will always observe WAN Quality of those selected WAN connections. Other WAN connections may stop observing WAN Quality information if it is not necessary for the underlying features.

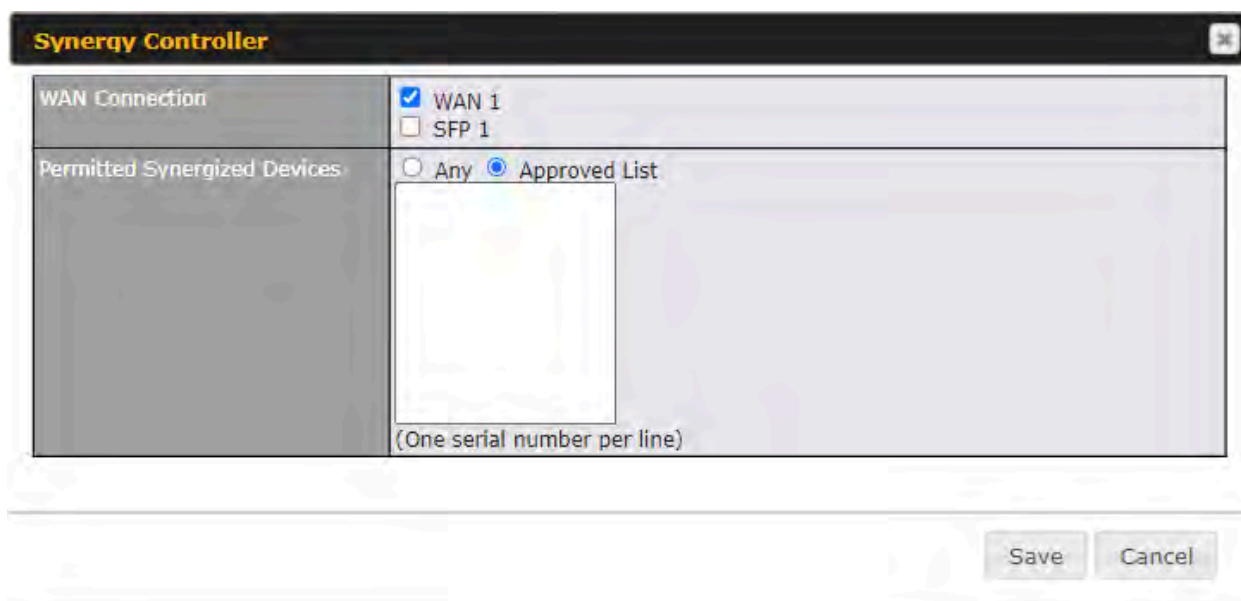
Synergy Mode

You can enable the Synergy Controller in this section.



The screenshot shows a settings window titled "Synergy Controller". It has a search bar with the text "Disabled" and a red edit icon in the top right corner.

You may click this  to enable the Synergy Controller. By default, the setting is disabled.



The screenshot shows the "Synergy Controller" configuration window. It has a title bar with the text "Synergy Controller" and a close button. The window is divided into two main sections. The top section, labeled "WAN Connection", contains two checkboxes: "WAN 1" (checked) and "SFP 1" (unchecked). The bottom section, labeled "Permitted Synergized Devices", contains two radio buttons: "Any" (unchecked) and "Approved List" (checked). Below the radio buttons is a text area for entering device serial numbers, with a note "(One serial number per line)". At the bottom right of the window are "Save" and "Cancel" buttons.

You may select the WAN connection to use as a Synergy Link which will connect to synergized devices.

Orbit WAN

The option is to enable Starlink / OneWeb management on the selected WAN connection.

Orbit WAN		
Starlink	Orbit 1 Orbit 3	
OneWeb	Disabled	

You may click this to show the WAN connection list to select which WAN connection to enable the management.

Orbit WAN

Starlink

WAN Connection

Clear

All

☒ Orbit 1
☐ Orbit 2
☒ Orbit 3
☐ Orbit 4
☐ LAN 1
☐ LAN 2
☐ USB
☐ Wi-Fi WAN on 2.4 GHz
☐ Wi-Fi WAN on 5 GHz
☐ VLAN WAN 1

Ignore Outages ☐

OneWeb

WAN Connection

Clear

All

☐ Orbit 1
☐ Orbit 2
☐ Orbit 3
☐ Orbit 4
☐ LAN 1
☐ LAN 2
☐ USB
☐ Wi-Fi WAN on 2.4 GHz
☐ Wi-Fi WAN on 5 GHz
☐ VLAN WAN 1

Starlink	
WAN connection	WAN option to enable Starlink management.
Ignore Starlink Outages	Enable the device to ignore all outages (e.g., obstructed, no downlink, no pings). The WAN will only go down when its health check fails.
OneWeb	
WAN connection	WAN option to enable OneWeb management.

<https://www.peplink.com>

54

Copyright @ 2026 Peplink

8.1 Orbit WAN / Ethernet WAN

There are four possible connection methods for the Ethernet WAN connection:

1. DHCP
2. Static IP
3. PPPoE
4. L2TP
5. GRE

8.1.1 DHCP Connection

The DHCP connection method is suitable if the ISP provides an IP address automatically using DHCP (e.g., satellite modem, WiMAX modem, cable, Metro Ethernet, etc.).

WAN Connection Settings	
WAN Connection Name	WAN
Enable	☒
Connection Priority	☒ Always-on (Priority 1) ☐ Backup
Independent from Backup WANs	☐
Connection Method	DHCP
Routing Mode	☒ NAT ☐ IP Forwarding
Management IP Address	255.255.255.0 (/24)
Custom Hostname	☐
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	☐
Standby State	☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	☒ Yes ☐ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

DHCP Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Enable	This setting enables the WAN connection. If schedules have been defined,

	you will be able to select a schedule to apply to the connection.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help  icon in this field, you can display the IP Forwarding option, if your network requires it.
Management IP Address	Management IP Address is available for configuration when you click here for other DHCP settings. This option allows you to configure the management IP address for the DHCP WAN connection.
Custom Hostname	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields.

IP Passthrough	When this IP Passthrough option is active, after the ethernet WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT. Regardless the WAN connection's state, the router always binds to the LAN IP address (Default: 192.168.50.1). So when the ethernet WAN is connected, the LAN client could access the router's web admin by manually configuring its IP address to the same subnet as the router's LAN IP address (e.g. 192.168.50.10). Note: when this option is firstly enabled, the LAN client may not be able to refresh its IP address to the ethernet WAN IP address in a timely fashion. The LAN client may have to manually renew its IP address from DHCP server. After this option is enabled, the DHCP lease time will be 2 minutes. I.e. the LAN client could refresh its IP address and access the network at most one minute after the ethernet WAN connection goes up.
Standby State	This option allows you to choose whether to remain connected when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, upon bringing up this WAN connection to active, it will be immediately available for use. If this WAN connection is charged by connection time, you may want to set this option to Disconnect so that connection will be made only when needed. SpeedFusion VPN may use connected standby WAN for failover if link failure detected on the higher priority WAN, you can set this option to Disconnect to avoid data passing through.
Reply to ICMP PING	If the checkbox is unticked, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: ticked (Yes)
Upload Bandwidth	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

8.1.2 Static IP Connection

The Static IP connection method is suitable if your ISP provides a static IP address to connect directly.

Connection Method	 Static IP ▼
Routing Mode	 ☒ NAT ☐ IP Forwarding
IP Address	
Subnet Mask	255.255.255.0 (/24) ▼
Default Gateway	
DNS Servers	☒ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

Static IP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server. When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields.

8.1.3 PPPoE Connection

The PPPoE connection method is suitable if your ISP provides a login ID/password to connect via PPPoE.

Connection Method	 PPPoE ▼
Routing Mode	 ☒ NAT ☐ IP Forwarding
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	 Leave it blank unless it is provided by ISP
IP Address (Optional)	 Leave it blank unless it is provided by ISP
Keep-Alive Interval	 6 seconds(s)
Keep-Alive Retry	 6
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it.
PPPoE Username / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service name is provided by the ISP. Note: Leave this field blank unless it is provided by your ISP.
IP Address (Optional)	If your ISP provides a PPPoE IP address, enter it here. Note: Leave this field blank unless it is provided by your ISP.
Keep Alive Interval	This is the time interval between each Keep-Alive packet.
Keep-Alive Retry	This is the number of consecutive Keep-Alive check failures before treating PPPoE connection as down.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.

Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.)

When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

8.1.4 L2TP Connection

L2TP has all the compatibility and convenience of PPTP with greater security. Combine this with IPsec for a good balance between ease of use and security.

Connection Method	 L2TP
Routing Mode	 ☒ NAT ☐ IP Forwarding
L2TP User Name	
L2TP Password	
Confirm L2TP Password	
Server IP Address / Host	
Address Type	☒ Dynamic IP ☐ Static IP
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

L2TP Settings

Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it.
L2TP Username / Password	Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.
Confirm L2TP Password	Verify your password by entering it again in this field.
Server IP Address / Host	L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
Address Type	Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.

DNS Servers

Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.

Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection.

(The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)

When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

8.1.5 GRE Connection

This connection method is suitable if your ISP provides a static WAN IP and Tunnel IP via GRE.

Connection Method	 GRE ▼
Routing Mode	 ☒ NAT ☐ IP Forwarding
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24) ▼
WAN Default Gateway	
Remote GRE Host	
Tunnel Local IP Address	
Tunnel Remote IP Address	
Outgoing NAT IP Address	
DNS Servers	☒ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

GRE Settings

Routing Mode

NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.

WAN IP Address / Subnet Mask / Default Gateway

These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.

Remote GRE Host

This field allows you to enter the IP address of the remote GRE.

Tunnel Local IP Address	This field allows you to enter the IP address of the local tunnel for the GRE tunnel connection.
Tunnel Remote IP Address	This field allows you to enter the IP address of the remote tunnel for the GRE tunnel connection.
Outgoing NAT IP Address	This field is to enter the NAT IP address for outgoing via GRE tunnel.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.) When Use the following DNS server address(es) is selected, you can enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.

8.2 Wi-Fi WAN

Disabled	
⋮  Cellular	☐ Disabled (No IP Address)
⋮  1 Wi-Fi WAN on 2.4 GHz 	☐ Disabled (No IP Address) 
⋮  2 Wi-Fi WAN on 5 GHz	☐ Disabled (No IP Address) 

To access/configure the Wi-Fi WAN settings, click **Network > Wi-Fi WAN Connection Name**.

WAN Connection Settings	
WAN Connection Name	Wi-Fi WAN on 2.4 GHz
Enable	☒
Connection Priority	☒ Always-on (Priority 1) ☐ Backup
Independent from Backup WANs	☐
Routing Mode	☒ NAT ☐ IP Forwarding
Standby State	☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	☒ Yes ☐ No

WAN Connection Settings	
WAN Connection Name	Enter a name to represent this Wi-Fi WAN connection.
Enable	Click the checkbox to toggle the on and off state of this connection.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.

Routing Mode	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding. In the case if you need to choose IP Forwarding for your scenario. Click the button to enable IP Forwarding.
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are Remain Connected and Disconnect.
Reply to ICMP PING	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

Wi-Fi WAN Settings

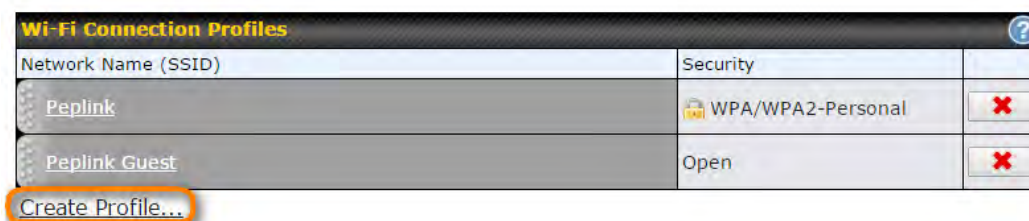
Channel Width	Auto
Channel	☒ Auto ☐ Custom
Output Power	Max ☐ Boost
Data Rate	☒ Auto ☐ Fixed
Roaming	☐ Enable
Connect to Any Open Mode AP	☐ Yes ☒ No
Beacon Miss Counter	5
Channel Scan Interval	50 ms

Wi-Fi WAN Settings	
Channel Width	Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz
Channel	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:
Output Power	If you are setting up a network with many Wi-Fi devices in close proximity, then you can configure the output power here. Click the “boost” button for additional power. However, with that option ticked, output power may exceed local regulatory limits.

Data Rate	Selecting Auto will enable the router to automatically determine the best data rate, while manually selecting a rate will force devices to connect using the fixed rate.
Roaming	Checking this box will enable Wi-Fi roaming. Click the  icon for additional options.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.
Beacon Miss Counter	This sets the threshold for the number of missed beacons.
Channel Scan Interval	Configure Channel Scan Interval in ms.

8.2.1 Creating Wi-Fi Connection Profiles

You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden-SSID access points. Click **Network > Wi-Fi WAN > Create Profile...** to get started.



This will open a window similar to the one shown below

Create Wi-Fi Connection Profile

Wi-Fi Connection

Network Name (SSID)	
Security	WPA2/WPA3-Personal
Shared Key	☒ Hide Characters
Preferred BSSID	☐
Connection Method	DHCP Static IP
	Click here for other DHCP settings
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

OK

Cancel

Wi-Fi Connection Profile Settings	
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network. Available options: • Open • WEP • Enhanced Open (OWE) • WPA3 -Personal • WPA2/WPA3 -Personal • WPA/ WPA2 – Personal • WPA/ WPA2 – ENTERprise • 802.1X with dynamic WEP key
Shared Key	Enter the password for the wireless network.
Preferred BSSID	Configure the BSSID. The BSSID is the MAC address of the wireless access point (WAP).
Connected Method	Choose DHCP or Static IP for the Wi-Fi WAN connection method.
DNS Servers	Configure the DNS servers that this WAN connection should use.

8.3 OpenVPN WAN

OpenVPN WAN is a standalone “WAN” which will appear in both your router and your InControl2 dashboards. You will be able to configure the priority of the physical WANs to connect to the OpenVPN server (similar to IPsec’s “WAN Connection Priority”). You can also customize OpenVPN’s outbound policy, firewall, etc.

* OpenVPN WAN license is required. Click on the below link for more details.

<https://forum.peplink.com/t/introducing-the-openvpn-wan-license-partner-discussion/30291>

WAN Connection Settings ✕

WAN Connection Settings	
WAN Connection Name	OpenVPN WAN 1
Enable	☐
Connection Method	OpenVPN ▼
Routing Mode	● NAT
OpenVPN Profile	 Choose a file or drag it here
Login Credential (Optional)	Username: Password: ☒ Hide Characters
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2: Click here to set this WAN's DNS servers as Preferred DNS resolvers for DNS leak protection. You can unset this setting in LAN Network Settings page.
Standby State	○ Remain connected ● Disconnect
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	1 Gbps ▼
Download Bandwidth	1 Gbps ▼

WAN Connection Settings

WAN Connection Name	Enter a name to represent this WAN connection.
Enable	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.
Connection Method	OpenVPN.
Routing Mode	This field shows that NAT (network address translation) will be applied to the traffic routed over this WAN connection. IP Forwarding is available when you click the link in the help  icon.
OpenVPN Profile	Upload the OpenVPN profile (.ovpn) from the OpenVPN server.
Login Credential (Optional)	This field is optional to key in the respective username and password to connect to OpenVPN server if needed.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.

Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
Standby State	This option allows you to choose whether to remain connected when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, upon bringing up this WAN connection to active, it will be immediately available for use. If this WAN connection is charged by connection time, you may want to set this option to Disconnect so that connection will be made only when needed. SpeedFusion VPN may use connected standby WAN for failover if link failure detected on the higher priority WAN, you can set this option to Disconnect to avoid data passing through.
Reply to ICMP PING	If the checkbox is unticked, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: ticked (Yes)
Upload Bandwidth	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

Physical Interface Settings (OpenVPN)

Physical Interface Settings							
MTU	☐ Auto ☒ Custom 1440						
Uplink Connection Priority	<table border="1"> <thead> <tr> <th>Priority</th> <th>WAN Selection</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>WAN1-Maxis-30M-BF008867851</td> </tr> <tr> <td>2</td> <td>-----</td> </tr> </tbody> </table> ☐ Failback on Connection Recovery	Priority	WAN Selection	1	WAN1-Maxis-30M-BF008867851	2	-----
Priority	WAN Selection						
1	WAN1-Maxis-30M-BF008867851						
2	-----						

MTU

This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value. Default value is 1440.

Uplink Connection Priority

Specify the order of WAN connections to be used to establish this OpenVPN connection. The healthy WAN with highest priority will be used.

When Failback on Connection Recovery is enabled, once a higher priority WAN is recovered, OpenVPN connection will be disconnected and use that WAN to establish the connection again.

8.4 Physical Interface Settings (Common)

The remaining WAN-related settings are common to the WAN connection:

Physical Interface Settings	
Port Speed	Auto
MTU	☐ Auto ☒ Custom 1440
MSS	☒ Auto ☐ Custom
MAC Address Clone	☒ Default ☐ Custom 10:56:CA:15:92:5D
VLAN	☐

Physical Interface Settings

Speed

This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems.

When a static speed is set, you may choose whether to advertise its speed to the

	peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device. Default: Auto
MTU	This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value. Default value is 1440.
MSS	This field is for specifying the Maximum Segment Size of the WAN connection. When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections. Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections. Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size. Default: Auto
MAC Address Clone	Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.
VLAN	Check the box to assign a VLAN to the interface.

8.5 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Peplink router can periodically check the health of each WAN connection. The health check settings for each WAN connection can be independently configured via **Network > WAN Connection Name**

Health Check Settings	
Method	This setting specifies the health check method for the WAN connection. This value can be configured as Disabled, PING, DNS Lookup, or HTTP. The default method is DNS Lookup. For mobile Internet connections, the value of Method can be configured as Disabled or SmartCheck.
Health Check Disabled	

Health Check Method	?	Disabled
---------------------	---	----------

Health Check disabled. Network problem cannot be detected.

When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

Health Check Method: PING

Health Check Method	?	PING
PING Hosts	?	Host 1: Host 2: ☒ Use first two DNS servers as PING Hosts

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts

This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup

Health Check Method	?	DNS Lookup
Health Check DNS Servers	?	Host 1: Host 2: ☒ Use first two DNS servers as Health Check DNS Servers ☐ Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers

This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS lookup.

If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

Health Check Method	 HTTP
URL 1	 http:// Matching String: ☐
URL 2	 http:// Matching String: ☐

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

HTTP request will be sent according to the specified URL. Health check result is determined based on the HTTP response status code. Status code 2xx, 301 and 302 are classified as success. If Matching String is provided, health check will be determined as success only when the HTTP response content contains the specified string.

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

If URL2 is also provided, a health check will pass if either one of the tests passed.

Timeout	 10	second(s)
Health Check Interval	 5	second(s)
Health Check Retries	 3	
Recovery Retries	 3	

Other Health Check Settings

Timeout

This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.

Health Check Interval

This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.

Health Check Retries

This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink router will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.

Recovery Retries

This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink router treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and health checks fail, the Peplink router will automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:

⚠ Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.

8.6 Bandwidth Allowance Monitoring

Bandwidth Allowance Monitor	
Bandwidth Allowance Monitor	☒ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . ☒ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st of each month at 00:00 midnight
Monthly Allowance	GB

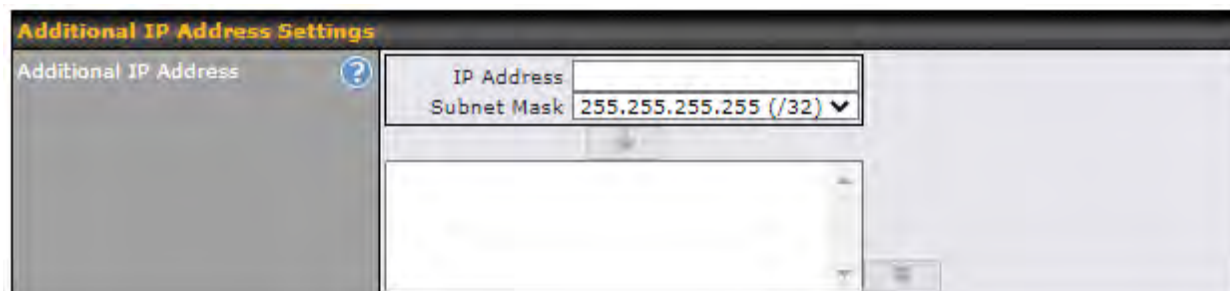
Bandwidth Allowance Monitor

Action	If Email Notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Disclaimer

Due to different network protocol overheads and conversions, the amount of data reported by this Peplink device is not representative of actual billable data usage as metered by your network provider. Peplink disclaims any obligation or responsibility for any events arising from the use of the numbers shown here.

8.7 Additional Public IP address



Additional Public IP Settings	
IP Address List	IP Address List represents the list of fixed Internet IP addresses assigned by the ISP in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the Down Arrow button to populate IP address entries to the IP Address List.

8.8 Dynamic DNS Settings

Peplink routers are capable of registering the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address from the external, even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

Either upon a change in IP addresses or every 23 days without link reconnection, the Peplink router will connect to the dynamic DNS service provider to perform an IP address update within the provider's records.

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network > WAN > Details > Dynamic DNS Service Provider/Dynamic DNS Settings**.

Dynamic DNS Service Provider	changeip.com
User ID	
Password	
Confirm Password	
Hosts	

Dynamic DNS Settings

Dynamic DNS

This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:

- Disabled
- changeip.com
- dyndns.org
- no-ip.org
- DNS-O-Matic
- Others...

Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.

Select **Disabled** to disable this feature.

User ID/ Username / Email

This setting specifies the registered user name for the dynamic DNS service.

Password

This setting specifies the password for the dynamic DNS service.

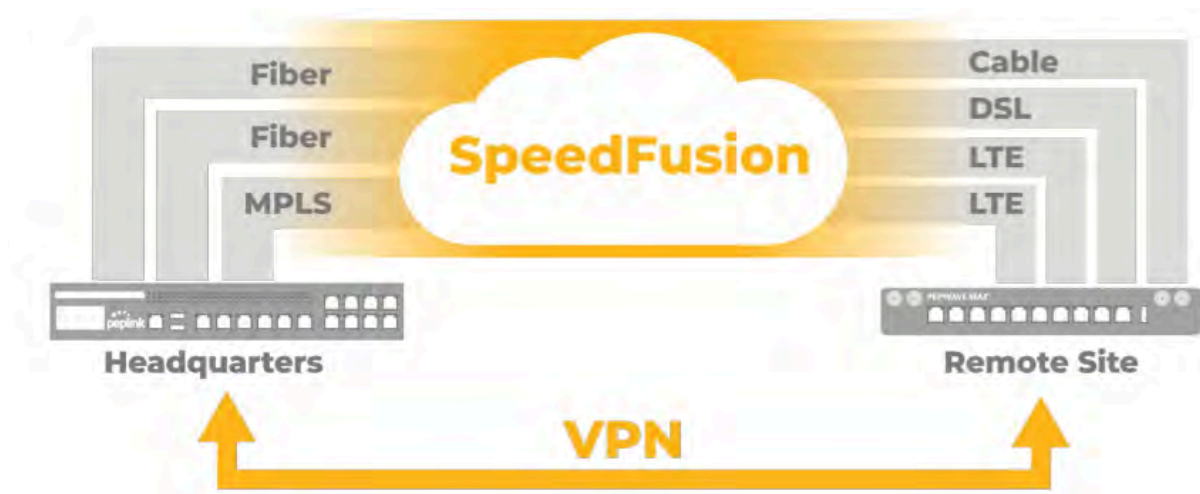
Hosts

This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

Important Note

In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN's IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service providers' policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long time. Therefore the Peplink router performs an update every 23 days, even if a WAN's IP address has not changed.

9 SpeedFusion VPN



Peplink bandwidth bonding SpeedFusion™ is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion functionality securely connects your Peplink router to another Peplink or Peplink device (Peplink Balance 210/310/380/580/710/1350 only). Data, voice, or video communications between these locations are kept confidential across the public Internet.

Bandwidth bonding SpeedFusion™ is specifically designed for multi-WAN environments. In case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic.

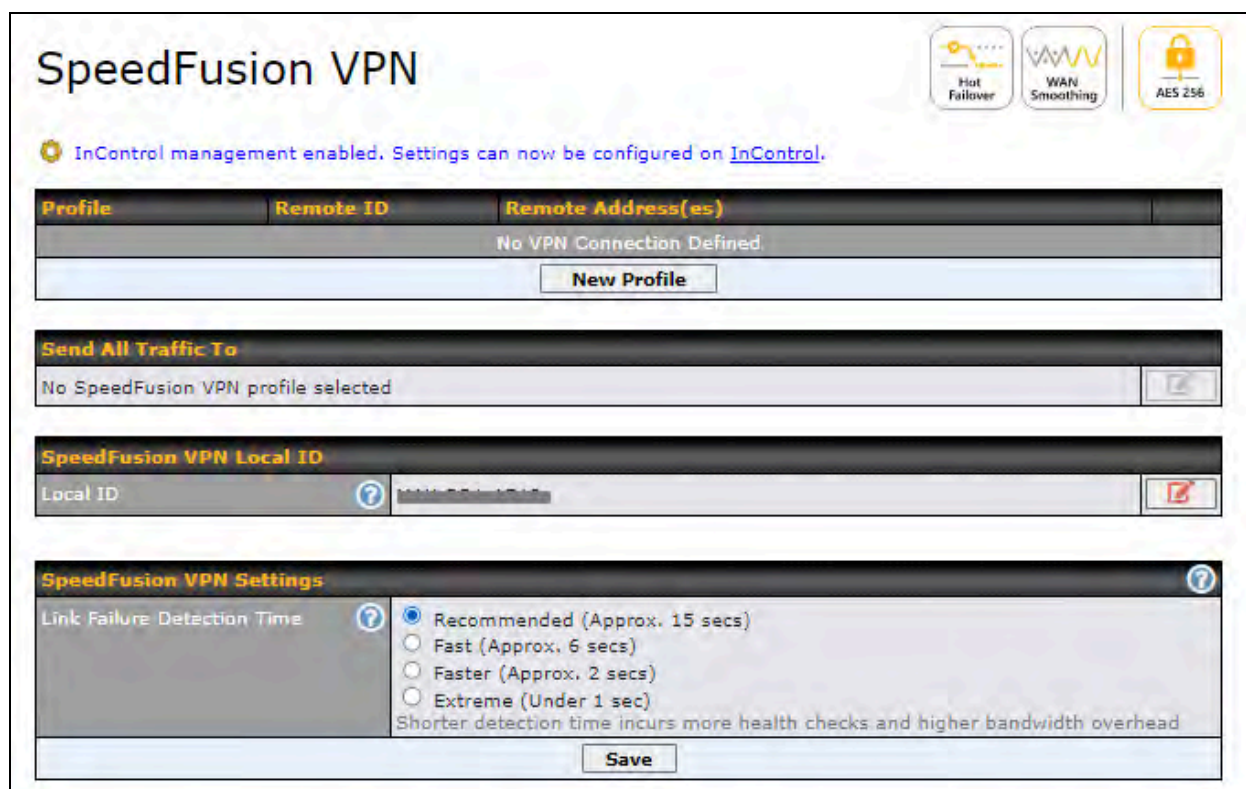
Different models of our SD-WAN routers have different numbers of site-to-site connections allowed. End-users who need to have more site-to-site connections can purchase a SpeedFusion license to increase the number of site-to-site connections allowed.

Peplink routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Peplink routers can keep the VPN up and running.

VPN bandwidth bonding is supported in Firmware 5.1 or above. All available bandwidth will be utilized to establish the VPN tunnel, and all traffic will be load balanced at packet level across all links. VPN bandwidth bonding is enabled by default.

9.1 SpeedFusion VPN

To configure SpeedFusion VPN, navigate to **Advanced > SpeedFusion VPN**.



The local LAN subnet and subnets behind the LAN (defined under **Static Route** on the LAN settings page) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to local subnets.

Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN using the 256-bit AES encryption standard. To configure, navigate to **Advanced > SpeedFusion VPN** and click the **New Profile** button to create a new VPN profile (you may have to first save the displayed default profile in order to access the **New Profile** button). Each profile specifies the settings for making VPN connection with one remote Peplink or Peplink device. Note that available settings vary by model.

A list of defined SpeedFusion connection profiles and a **Link Failure Detection Time** option will be shown. Click the **New Profile** button to create a new VPN connection profile for making a VPN connection to a remote Peplink or Peplink device via the available WAN connections. Each profile is for making a VPN connection with one remote Peplink or Peplink Device.

SpeedFusion VPN Profile					
Name					
Enable	☒				
Encryption	☒ 256-bit AES ☐ OFF				
Authentication	☒ Remote ID / Pre-shared Key				
Remote ID / Pre-shared Key	<table border="1"> <tr> <th>Remote ID</th> <th>Pre-shared Key</th> </tr> <tr> <td> </td> <td> </td> </tr> </table>	Remote ID	Pre-shared Key		
Remote ID	Pre-shared Key				
NAT Mode	☐				
Remote IP Address / Host Names (Optional)	 If this field is empty, this field on the remote unit must be filled				
Cost	10				
Data Port	☒ Auto ☐ Custom				
Bandwidth Limit	☐				
WAN Smoothing	Off				
Forward Error Correction	Off				
Receive Buffer	0 ms				
Packet Fragmentation	☒ Always ☐ Use DF Flag				
Use IP ToS	☐				
Latency Difference Cutoff	500 ms				

SpeedFusion VPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Enable	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from By Remote ID Only , Preshared Key , or X.509 to specify the method the Peplink MAX will use to authenticate peers. When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field.
Remote ID / Pre-shared Key	This optional field becomes available when Remote ID / Pre-shared Key is selected as the Peplink router's VPN Authentication method, as explained above. Pre-shared Key defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.

	Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the  icon next to the “Remote ID / Preshared Key” setting.
Remote ID/Remote Certificate	These optional fields become available when X.509 is selected as the Peplink MAX's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the Show Details link below the field.
Allow Shared Remote ID	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	If NAT Mode is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted. This field is optional. With this field filled, the Peplink MAX will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink MAX will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If Default is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If Custom is selected, enter an outgoing port number from 1 to 65535. Click the  icon to configure data stream using TCP protocol [EXPERIMENTAL]. In the case TCP protocol is used, the exposed TCP session option can be authorised to work with TCP accelerated WAN link.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use SpeedFusion VPN version 4.0.0 or above.
WAN Smoothing	While using SpeedFusion VPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN's available bandwidth.

	Off - Disable WAN Smoothing. Normal - The total bandwidth consumption will be at most 2x of the original data traffic. Medium - The total bandwidth consumption will be at most 3x of the original data traffic. High - The total bandwidth consumption depends on the number of connected active tunnels.
Forward Error Correction	Forward Error Correction (FEC) can help to recover packet loss by using extra bandwidth to send redundant data packets. Higher FEC level will recover packets on a higher loss rate link. The expected overhead of Low is 13.3% and High is 26.7%. Require peer using SpeedFusion VPN version 8.0.0 and above.
Receive Buffer	Receive Buffer can help to reduce out-of-order packets and jitter, but will introduce extra latency to the tunnel. Default is 0 ms, which disables the buffer, and maximum buffer size is 2000 ms.
Packet Fragmentation	If the packet size is larger than the tunnel's MTU, it will be fragmented inside the tunnel in order to pass through. Select Always to fragment any packets that are too large to send, or Use DF Flag to only fragment packets with Don't Fragment bit cleared. This can be useful if your application does Path MTU Discovery, usually sending large packets with DF bit set, if allowing them to go through by fragmentation, the MTU will not be detected correctly.
Use IP ToS^A	Checking this button enables the use of IP ToS header field.
Latency Difference Cutoff^A	Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)

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

To enable Layer 2 Bridging between SpeedFusion VPN profiles, navigate to **Network > LAN > Basic Settings > *LAN Profile Name*** and refer to instructions in section 9.1



Traffic Distribution		
Policy		Dynamic Weighted Bonding ▼
Congestion Latency Level		Default ▼
Ignore Packet Loss Event		☐
Disable Bufferbloat Handling		☐
Disable TCP ACK Optimization		☐
Packet Jitter Buffer		150 ms

Traffic Distribution	
Policy	This option allows you to select the desired out-bound traffic distribution policy: - Bonding - Aggregate multiple WAN-to-WAN links into a single higher throughput tunnel. - Dynamic Weighted Bonding - Aggregates WAN-to-WAN links with similar latencies. By default, Bonding is selected as a traffic distribution policy.
Congestion Latency Level	For most WANs, especially on satellite and wireless networks, the latency will increase when the link becomes more congested. Setting the Congestion Latency Level to Low will treat the link as congested more aggressively. Setting it to High will allow the latency to increase more before treating it as congested.
Ignore Packet Loss Event	By default, when there is packet loss, it is considered as a congestion event. If this is not the case, select this option to ignore the packet loss event.
Disable Bufferbloat Handling	Bufferbloat is a phenomenon on the WAN side when it is congested. The latency can become very high due to buffering on the uplink. By default, the Dynamic Weighted Bonding policy will try its best to mitigate bufferbloat by reducing TCP throughput when the WAN is congested. However, as a side effect, the tunnel might not achieve maximum bandwidth. Selecting this option will disable the bufferbloat handling mentioned above.
Disable TCP ACK Optimization	By default, TCP ACK will be forwarded to remote peers as fast as possible. This will consume more bandwidth, but may help to improve TCP performance as well. Selecting this option will disable the TCP ACK optimization mentioned above.
Packet Jitter Buffer	The default jitter buffer is 150ms, and can be modified from 0ms to 500ms. The jitter buffer may increase the tunnel latency. If you want to keep the latency as low as possible, you can set it to 0ms to disable the buffer. Note: If the Receive Buffer is set, the Packet Jitter Buffer will be automatically disabled.

WAN Connection Priority					
	Priority	Direction	Connect to Remote	Cut-off latency (ms)	Suspension Time after Packet Loss (ms)
1. WAN 1	1 (Highest) ▼	Up/Down ▼	All ▼		
2. WAN 2	1 (Highest) ▼	Up/Down ▼	All ▼		
3. Wi-Fi WAN	1 (Highest) ▼	Up/Down ▼	All ▼		
4. Cellular 1	1 (Highest) ▼	Up/Down ▼	All ▼		
5. Cellular 2	1 (Highest) ▼	Up/Down ▼	All ▼		
6. USB	1 (Highest) ▼	Up/Down ▼	All ▼		

WAN Connection Priority

WAN Connection Priority

If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used.

To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the button.

Send All Traffic To

No SpeedFusion VPN profile selected

Send All Traffic To

This feature allows you to redirect all traffic to a specified SpeedFusion VPN connection. Click the button to select your connection and the following menu will appear:

Send All Traffic To

☒ Balance 2942-1257-1241 ▼
 DNS Server
 8.8.8.8
 8.8.4.4
☒ Backup Site Balance-4810-1825-068E-4810 ▼
 DNS Server
 8.8.8.8
 8.8.4.4

You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main SpeedFusion VPN connection fail.

Outbound Policy/SpeedFusion VPN Outbound Custom Rules

Some models allow you to set outbound policy and custom outbound rules from **Advanced>SpeedFusion VPN**. See **Section 14** for more information on outbound policy settings.

The screenshot shows two configuration sections. The top section, 'Outbound Policy', has a dropdown menu set to 'According to custom rules' and a red edit icon. The bottom section, 'PepVPN Outbound Custom Rules', is a table with columns: Service, Algorithm, Source, Destination, and Protocol. The 'Algorithm' column has '(Auto)' selected. Below the table is an 'Add Rule' button.

SpeedFusion VPN Local ID

The screenshot shows the 'Local ID' field with a question mark icon and the text 'MAX-BR1-A712'. A red edit icon is visible on the right.

SpeedFusion VPN Local ID

The local ID is a text string to identify this local unit when establishing a VPN connection. When creating a profile on a remote unit, this local ID must be entered in the remote unit's **Remote ID** field. Click the icon to edit **Local ID**.

Link Failure Detection Settings

The screenshot shows the 'Link Failure Detection Settings' section. It includes a 'Cold Failover Mode' checkbox (unchecked) and a 'Link Failure Detection Time' section with radio button options: 'Follow Device Setting - Recommended (Approx. 15 secs)' (selected), 'Recommended (Approx. 15 secs)', 'Fast (Approx. 6 secs)', 'Faster (Approx. 2 secs)', and 'Extreme (Under 1 sec)'. A note at the bottom states: 'Shorter detection time incurs more health checks and higher bandwidth overhead'.

Link Failure Detection Settings

Cold Failover Mode

Enabling Cold Failover Mode turns off link failure detection for standby WAN-to-WAN links, helping to lower bandwidth consumption.

Link Failure Detection Time

The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed.

When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds.

When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds.

When **Faster** is selected, a health check packet is sent every second, and the

expected detection time is two seconds.

When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

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

Important Note

Peplink proprietary SpeedFusion™ uses TCP port 32015 and UDP port 4500 for establishing VPN connections. If you have a firewall in front of your Peplink devices, you will need to add firewall rules for these ports and protocols to allow inbound and outbound traffic to pass through the firewall.

Tip

Want to know more about VPN sub-second session failover? Visit our YouTube Channel for a video tutorial!



<http://youtu.be/TLQgdpPSY88>

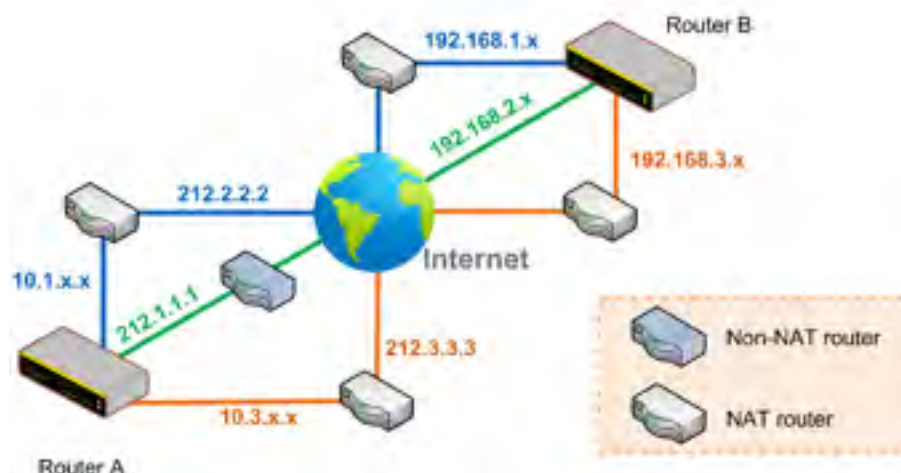
9.2 The Peplink Router Behind a NAT Router

Peplink routers support establishing SpeedFusion™ over WAN connections which are behind a NAT (network address translation) router.

To enable a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to inbound port-forward TCP port 32015 to the Peplink router.

If one or more WAN connections on Unit A can accept VPN connections (by means of port forwarding or not), while none of the WAN connections on the peer Unit B can do so, you should enter all of Unit A's public IP addresses or hostnames into Unit B's **Remote IP Addresses / Host Names** field. Leave the field in Unit A blank. With this setting, a SpeedFusion™ connection can be set up and all WAN connections on both sides will be utilized.

See the following diagram for an example of this setup in use:



One of the WANs connected to Router A is non-NAT'd (212.1.1.1). The rest of the WANs connected to Router A and all WANs connected to Router B are NAT'd. In this case, the **Peer IP Addresses / Host Names** field for Router B should be filled with all of Router A's hostnames or public IP addresses (i.e., 212.1.1.1, 212.2.2.2, and 212.3.3.3), and the field in Router A can be left blank. The two NAT routers on WAN1 and WAN3 connected to Router A should inbound port-forward TCP port 32015 to Router A so that all WANs will be utilized in establishing the VPN.

9.3 SpeedFusion VPN Status

SpeedFusion VPN status is shown in the Dashboard. The connection status of each connection profile is shown as below.

SpeedFusion VPN		Status
To MK2		Established

After clicking the **Status** button at the top right corner of the SpeedFusion™ table, you will be forwarded to **Status > SpeedFusion VPN**, where you can view subnet and WAN connection information for each VPN peer.

IP Subnets Must Be Unique Among VPN Peers

The entire interconnected SpeedFusion™ network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

10 IPsec VPN

IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

IPsec VPN on Peplink routers is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for a multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g., unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

10.1 IPsec VPN Settings

Many Peplink products can make multiple IPsec VPN connections with Peplink, Peplink, Cisco, and Juniper routers. Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other. All data can be routed over the VPN with a selection of encryption standards, such as 3DES, AES-128, and AES-256. To configure IPsec VPN on Peplink devices that support it, navigate to **Advanced>IPsec VPN**.

IPsec VPN Profiles		Remote Networks
No IPsec VPN Profile Defined.		
New Profile		

IPsec Settings	
DPD Interval	10 seconds
DPD Attempts	3
Save	

Peplink IPsec only supports network-to-network connection with Cisco, Juniper or Peplink devices.

Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Peplink, Cisco, or Juniper routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.

IPsec VPN Profile

Name									
Active	☒								
IKE Version	☒ IKEv1 ☐ IKEv2								
Connect Upon Disconnection of	☒	WAN 1							
Remote Gateway IP Address / Host Name									
IPsec Type	☒ Policy-based ☐ Route-based								
Local Networks	☒ 192.168.50.0/24 ☐								
Remote Networks	<table> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> <tr> <td> </td> <td>255.255.255.0 (/24)</td> <td> + </td> </tr> </table>	Network	Subnet Mask			255.255.255.0 (/24)	+		
Network	Subnet Mask								
	255.255.255.0 (/24)	+							
Authentication	☒ Preshared Key ☐ X.509 Certificate								
Mode	☒ Main Mode (All WANs need to have Static IP) ☐ Aggressive Mode								
Force UDP Encapsulation	☐								
Preshared Key	 ☒ Hide Characters								
Local ID									
Remote ID									
Phase 1 (IKEv1) Proposal	1 AES-CBC-256 & SHA1 2 -----								
Phase 1 DH Group	1 Group 2 2 -----								
Phase 1 SA Lifetime	3600	seconds							
Phase 2 (ESP) Proposal	1 AES-CBC-256 & SHA1 2 -----								
Phase 2 PFS Group	None								
Phase 2 SA Lifetime	28800	seconds							

IPsec VPN Profile Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
IKE Version	Two versions of the IKE standards are available: • IKEv1 • IKEv2

Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected.
Remote Gateway IP Address / Host Name	Enter the remote peer's public IP address. For Aggressive Mode , this is optional.
IPsec Type	Policy-based - (default) All the matched traffic as defined in Local Networks and Remote Networks will be routed to this IPsec connection, this cannot be overridden by other routing methods. Route-based - Outbound Policy rule is required to route traffic to this tunnel and comes with more flexibility to control how to route traffic compared to Policy-based. If you want to modify the traffic selector instead of using the default (0.0.0.0/0). Note: This option is available for certain following models only: MAX: BR1 ENT, Transit, 700 HW3 or above, HD2 HW5 or above, HD4
Local Networks	Enter the local LAN subnets here. If you have defined static routes, they will be shown here. Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allow you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site. Two types of NAT policies can be defined: One-to-One NAT policy: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too. Many-to-One NAT policy: if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 > 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Authentication	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the Preshared Key and X.509 Certificate methods of