

your carrier.

The default and recommended Operator Settings is **Auto**.

**APN / Login /
Password / SIM
PIN**

When **Auto** is selected, the information in these fields will be filled automatically. Select the option **Custom** and you may customize these parameters. The parameters values are determined by and can be obtained from the ISP.

General Settings	
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
Standby State	<input checked="" type="radio"/> Remain Connected <input type="radio"/> Disconnected
Idle Disconnect	<input checked="" type="checkbox"/> <input type="text" value="3"/> minutes <small>Time value is global. A change will affect all WAN profiles.</small>

General Settings

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 put custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

Standby State

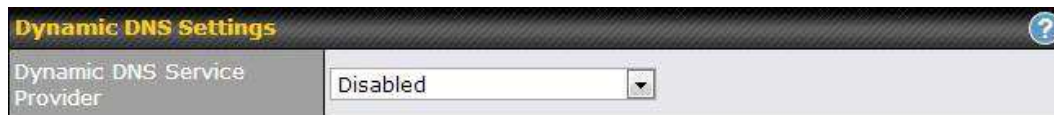
This option allows you to choose whether to remain the connection connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, upon bringing up this WAN connection to active, it will be immediately available for use.

Idle Disconnect

When Internet traffic is not detected within the user specified timeframe, the modem will automatically disconnect. Once the traffic is resumed by the LAN host, the connection will be re-activated,

Health Check Settings	
Health Check Method	<input type="text" value="SmartCheck"/>
Timeout	<input type="text" value="5"/> second(s)
Health Check Interval	<input type="text" value="10"/> second(s)
Health Check Retries	<input type="text" value="3"/>
Recovery Retries	<input type="text" value="3"/>

Health Check Settings	
Heath Check Method	This setting allows you to specify the health check method for the Cellular connection. The as available options are Disabled , Ping , DNS Lookup , HTTP , and SmartCheck . The default method is DNS Lookup . See Section for configuration details .
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the time interval between each health check test.
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



Dynamic DNS Settings ?

Dynamic DNS Service Provider:

Dynamic DNS Settings	
Dynamic DNS Service Provider	<p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> <ul style="list-style-type: none"> • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic <p>Select Disabled to disable this feature. See Section for configuration details.</p>



Bandwidth Allowance Settings

Bandwidth Allowance Monitor:

MTU:

Bandwidth Allowance Settings	
Bandwidth Allowance Monitor	This option allows you to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.

See Section **for configuration details.**

MTU

This setting specifies the Maximum Transmission Unit.

By default, MTU is set to **Custom 1440**.

You may adjust the MTU value by editing the text field. Click **Default** to restore the default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. The auto-detection will run each time when the WAN connection establishes

Configuring the LAN Interface

- WAN Configuration

For basic configuration, refer to Section , **Basic Configuration**.

For advanced configuration, refer to Section , **Configuring the WAN Interface(s)**.

8 Basic Configuration

8.1 Connecting to the Web Admin Interface

1. Start a Web browser on a computer that is connected with the Peplink Balance through the LAN.
2. To connect to the Web Admin of the Peplink Balance, enter the following LAN IP address in the address field of the web browser:

http://192.168.1.1

(This is the default LAN IP address of the Peplink Balance.)

3. Enter the following to access the Web Admin Interface.

User Name: admin

Password: admin

(This is the default Admin User login of the Peplink Balance. The Admin and Read-only User Password can be changed at **System > Admin Security**.)



4. After successful login, the **Dashboard** of the Web Admin Interface will be displayed. It looks similar to the following:



Important Note

The **Save** button causes the changes to be saved. Configuration changes (e.g., WAN, LAN, admin settings, etc.) take effect after clicking the **Apply Changes** button on each page's top right corner.

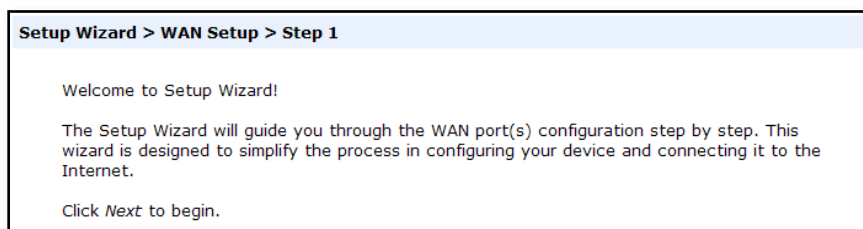
8.2 Configuration with the Setup Wizard

The Setup Wizard simplifies the task of configuring WAN connection(s) by guiding the configuration process step-by-step.

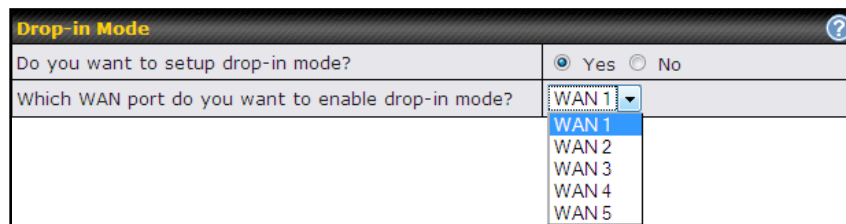
To begin, click **Setup Wizard** after connecting to the Web Admin Interface.



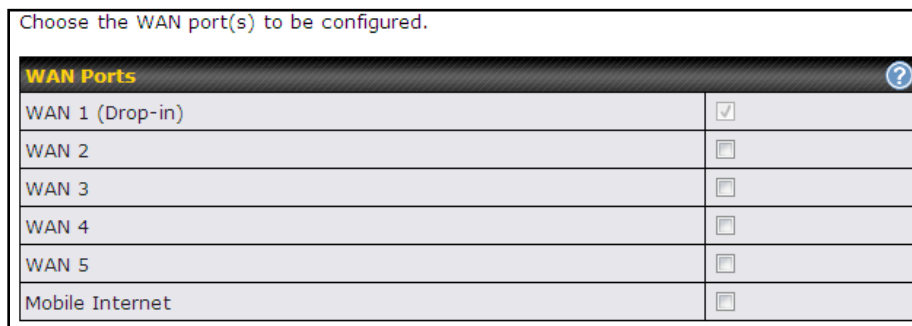
Click **Next** to begin.



Select **YES** if you want to set up Drop-in Mode using the setup wizard (note: Drop-in Mode is available on the Peplink Balance 210+).



Click on the appropriate checkbox(es) to select the WAN connection(s) to be configured. If you have chosen to configure Drop-in Mode using the setup wizard, the box of WAN port that is to be configured in Drop-in Mode will be checked by default.



WAN Ports	
WAN 1 (Drop-in)	<input checked="" type="checkbox"/>
WAN 2	<input type="checkbox"/>
WAN 3	<input type="checkbox"/>
WAN 4	<input type="checkbox"/>
WAN 5	<input type="checkbox"/>
Mobile Internet	<input type="checkbox"/>

If Drop-in Mode is going to be configured, the setup wizard will move on to **Drop-in Settings**.

Setup Wizard > WAN Setup > Step 4

Enter the parameters of Drop-in Settings for WAN 1.

Drop-in Settings	
IP Address	<input type="text"/>
Subnet Mask	255.255.255.0 (/24) ▼
Default Gateway	<input type="text"/>
DNS Servers	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
Upload Bandwidth	100 <input type="text"/> Mbps ▼
Download Bandwidth	100 <input type="text"/> Mbps ▼

Select the connection type for WAN connection(s) from the following screen:

Setup Wizard > WAN Setup > Step 3

Choose a connection method for WAN1.

Connection Method	
Method	Select
Static IP	<input type="radio"/>
DHCP	<input checked="" type="radio"/>
PPPoE	<input type="radio"/>
Disable	<input type="radio"/>

Depending on the selection of connection type, further configuration may be needed. For example, PPPoE and Static IP require additional settings for the selected WAN port. Please refer to **Section , Configuring the WAN Interface(s)** for details on setting up DHCP, static IP, and PPPoE.

If **Mobile Internet Connection** is checked, the setup wizard will move on to **Operator Settings**.

Setup Wizard > WAN Setup > Step 3

Select whether Operator Settings for Mobile Internet will be automatically detected or customized.

Operator Settings (for HSPA/EDGE/GPRS only)	
Settings	Select
Auto	<input type="radio"/>
Custom	<input checked="" type="radio"/>

If **Custom Mobile Operator Settings** is selected, APN parameters are required to be entered. Some service providers may charge a fee for connecting to a different APN. Please consult your service provider for the correct settings.

Setup Wizard > WAN Setup > Step 4

Enter the parameters of Mobile Operator Settings for Mobile Internet.

Mobile Operator Settings	
APN	<input type="text"/>
Login ID	<input type="text"/>
Password	<input type="text"/>
Dial Number	<input type="text"/>

Click on the appropriate check box(es) to select the preferred WAN connection(s). Connection(s) not selected in this step will be used as backup only. Click **Next>>** to continue.

Setup Wizard > WAN Setup > Step 6

Choose the preferred WAN Port(s) that is to be used as primary connection. The port(s) not selected in this step will only be used when none of the connection of the preferred port is up.

Preferred WAN Port Selection	
Port	Preferred
WAN 1	<input checked="" type="checkbox"/>
WAN 2	<input checked="" type="checkbox"/>
WAN 3	<input checked="" type="checkbox"/>
Mobile Internet	<input type="checkbox"/>

Choose the time zone of your country/region. Check the box **Show all** to display all time zone options.

Setup Wizard > WAN Setup > Step 6

Choose time zone of your Country / Region.

Time Zone Settings	
Time Zone	
	(GMT-08:00) Pacific Time (US & Canada)
	<input checked="" type="checkbox"/> Show all

Check in the following screen to make sure all settings have been configured correctly, and then click **Save Settings** to confirm.

Setup Wizard > WAN Setup > Final Step

Confirm the WAN connection(s) configuration below. Click *Back* to modify the configuration settings in previous steps. Click *Save Settings* when you are done.

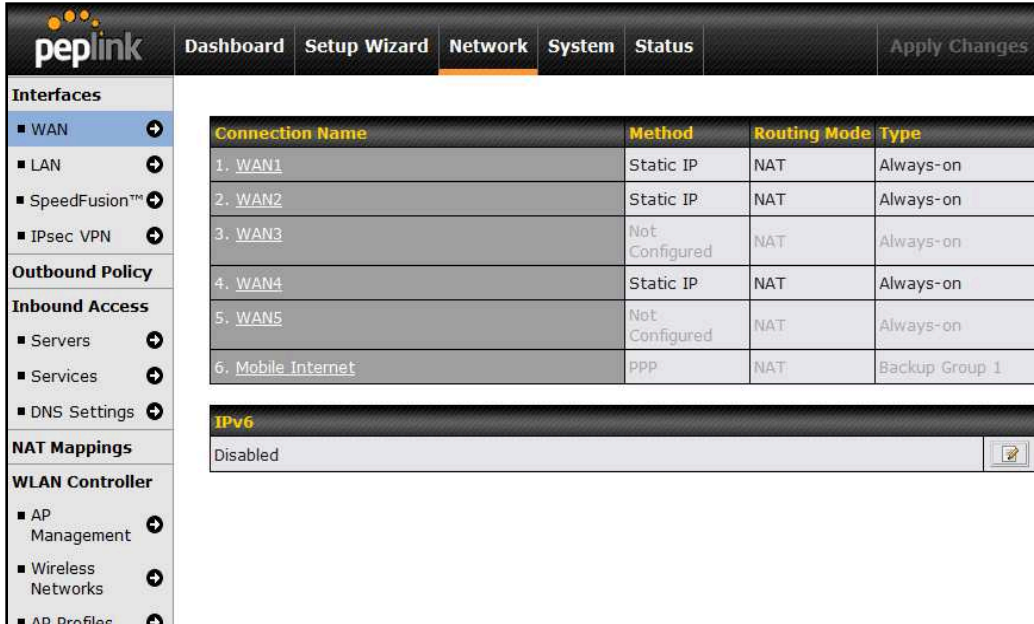
Summary of WAN Connection(s) Configuration	
2. WAN2	
Enable	No
4. Mobile Internet	
Connection Method	PPP
Operator Settings	Auto
Preferred WAN Connection(s)	
Connections	1. WAN1 3. WAN3
Time Zone Settings	
Time Zone	(GMT-08:00) Pacific Time (US & Canada)

After finishing the last step in the setup wizard, click **Apply Changes** on the page header to allow the configuration changes to take effect.

8.3 Advanced Setup

Advanced settings can be configured from the **Network** menu.

WAN connections can be configured by entering the corresponding WAN connection information at **Network > Interfaces > WAN**.



Connection Name	Method	Routing Mode	Type
1. WAN1	Static IP	NAT	Always-on
2. WAN2	Static IP	NAT	Always-on
3. WAN3	Not Configured	NAT	Always-on
4. WAN4	Static IP	NAT	Always-on
5. WAN5	Not Configured	NAT	Always-on
6. Mobile Internet	PPP	NAT	Backup Group 1

IPv6
Disabled

Tip

Please refer to **Section ,Configuring the WAN Interface(s)**, for details on setting up DHCP, static IP, PPPoE, and mobile Internet connections.

8.4 Cellular WAN

Network>WAN> Click on Detail [Details](#)


WAN Connection Status ?		
Priority 1 (Highest)		
1 WAN 1	■ Connected	Details
2 WAN 2	■ Connected	Details
Priority 2		
1 Cellular 1	■ Standby	Details
Priority 3		
Drag desired (Priority 3) connections here		
Disabled		
Wi-Fi WAN	<input type="checkbox"/> Disabled	Details
2 Cellular 2	<input type="checkbox"/> Disabled	Details


(Available on the Peplink 30 LTE only)


Cellular 1 Status ?	
IMSI	No SIM Card Detected
MEID	HEX: DEC:
ESN	
IMEI	

Cellular Status	
IMSI	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
MEID	The Pepwave MAX supports both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
ESN	This serves the same purpose as MEID HEX but uses an older format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.

WAN Connection Settings	
WAN Connection Name	Cellular 1 Default
Network Mode	<input checked="" type="radio"/> HSPA <input type="radio"/> Sprint, EV-DO <input type="radio"/> Verizon Wireless, EV-DO
Routing Mode ?	<input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding

WAN Connection Settings	
WAN Connection Name	This field is for defining a name to represent this WAN connection.
Network Mode	Users have to specify the Network they are on accordingly.
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 <i>NAT</i> (Network Address Translation) or <i>IP Forwarding</i> . Click the  button to enable IP Forwarding.

Cellular Settings	
3G/2G 	Auto <input type="text"/>
Authentication	Auto <input type="text"/>
Data Roaming	<input type="checkbox"/>
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
SIM PIN (Optional)	<input type="text"/>

Cellular Settings	
3G/2G	Band selection to restrict cellular on particular band. Click on the  button to enable the selection of specific bands.
Data Roaming	This checkbox enables data roaming on this particular SIM card. Please check your service provider's data roaming policy before proceeding.
Operator Settings	<p>This setting applies to 3G / EDGE / GPRS modem only. It does not apply to EVDO / EVDO Rev. A modem.</p> <p>This allows you to configure the APN settings of your connection. If Auto is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically afterwards. If there is any difficulty in making connection, you may select Custom to enter your carrier's APN, Login, Password, and Dial Number settings manually. The correct values can be obtained from your carrier.</p> <p>The default and recommended Operator Settings is Auto.</p>
APN / Login / Password / SIM PIN	<p>When Auto is selected, the information in these fields will be filled automatically.</p> <p>Select the option Custom and you may customize these parameters. The parameters values are determined by and can be obtained from the ISP.</p>

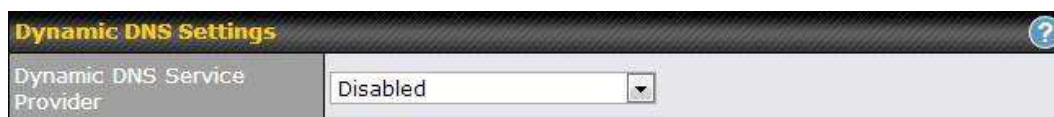
General Settings	
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
Standby State	<input checked="" type="radio"/> Remain Connected <input type="radio"/> Disconnected
Idle Disconnect	<input checked="" type="checkbox"/> <input type="text" value="3"/> minutes <small>Time value is global. A change will affect all WAN profiles.</small>

General Settings	
DNS Servers	<p>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.</p> <p>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.)</p> <p>When Use the following DNS server address(es) is selected, you can put custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields.</p>
Standby State	<p>This option allows you to choose whether to remain the connection connected or disconnected 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.</p>
Idle Disconnect	<p>When Internet traffic is not detected within the user specified timeframe, the modem will automatically disconnect. Once the traffic is resumed by the LAN host, the connection will be re-activated,</p>

Health Check Settings	
Health Check Method	<input type="text" value="SmartCheck"/>
Timeout	<input type="text" value="5"/> second(s)
Health Check Interval	<input type="text" value="10"/> second(s)
Health Check Retries	<input type="text" value="3"/>
Recovery Retries	<input type="text" value="3"/>

Health Check Settings	
Heath Check Method	<p>This setting allows you to specify the health check method for the Cellular connection. The as available options are Disabled, Ping, DNS Lookup, HTTP, and SmartCheck</p>

	The default method is DNS Lookup . See Section for configuration details.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the time interval between each health check test.
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



Dynamic DNS Settings	
	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:
Dynamic DNS Service Provider	<ul style="list-style-type: none"> • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic
	Select Disabled to disable this feature. See Section for configuration details.



Bandwidth Allowance Settings	
Bandwidth Allowance Monitor	<p>This option allows you to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.</p> <p>See Section for configuration details.</p>
MTU	<p>This setting specifies the Maximum Transmission Unit.</p> <p>By default, MTU is set to Custom 1440.</p> <p>You may adjust the MTU value by editing the text field. Click Default to restore the</p>

default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. The auto-detection will run each time when the WAN connection establishes

9 Configuring the LAN Interface

LAN Interface settings are located at **Network > Interfaces > LAN**.



IP Settings ?

IP Address:

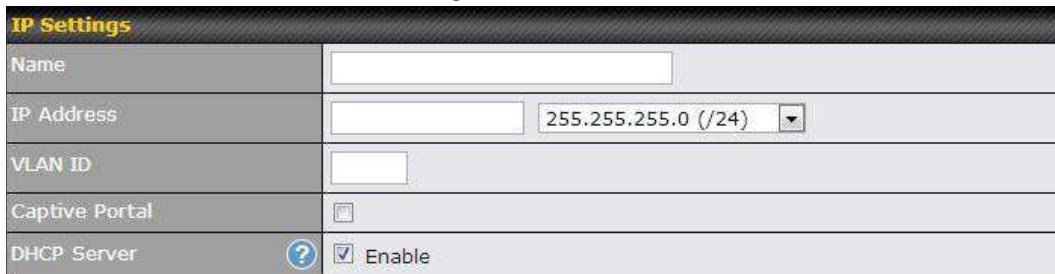
IP Settings	
IP Address & Subnet Mask	Enter Peplink Balance's IP address and subnet mask values to be used on the LAN.
Speed	<p>This setting specifies the speed of the LAN Ethernet port.</p> <p>By default, Auto is selected and the appropriate data speed is automatically detected by Peplink Balance.</p> <p>In the event of negotiation issues, the port speed can be manually specified to circumvent the issues. You can also choose whether or not to advertise the speed to the peer by selecting the Advertise Speed checkbox.</p>

To enable VLAN configuration, press the ? button under **IP Settings**. After clicking the link, the following screen will appear:



LAN	VLAN	Network	
Untagged LAN	None	192.168.1.1/24	?
<input type="button" value="New LAN"/>			

Click the **New LAN** button to reach the following screen:



IP Settings

Name:

IP Address:

VLAN ID:

Captive Portal:

DHCP Server: ? Enable

VLAN-enabled IP Settings	
Name	This field specified the name of this particular VLAN
IP Address	Enter Peplink Balance's IP address and subnet mask values to be used on the VLAN.
VLAN ID	Please enter a numerical value to identify this VLAN.
Captive Portal	This options switches on captive portal for users connected to this VLAN. Users on open networks will receive a splash screen, while users on closed networks will receive a login screen.
DHCP Server	Check the Enable box to enable the built-in DHCP server which serves DHCP requests on

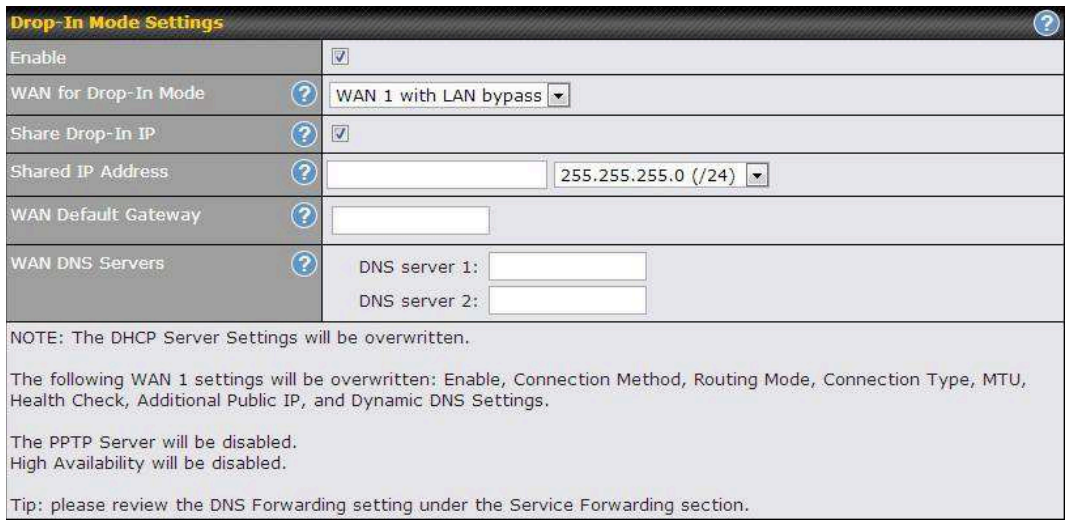
the LAN.



The screenshot shows the 'Port Settings' configuration page. On the left, there is a 'Ports' section with a help icon. The main area contains a list of ports: LAN (checked), WAN 3, WAN 4, WAN 5, WAN 6, and WAN 7. To the right of the LAN entry is a dropdown menu currently set to 'Auto'.

Port Settings

Ports To choose a physical Ethernet port to act as a LAN interface (in addition to the dedicated LAN port or ports), check the appropriate box and choose a speed setting from the drop-down menu immediately to the right of the listing. The default setting is Auto, which allows the Balance to detect and apply an appropriate data speed setting.



The screenshot shows the 'Drop-In Mode Settings' configuration page. It includes several settings: 'Enable' (checked), 'WAN for Drop-In Mode' (set to 'WAN 1 with LAN bypass'), 'Share Drop-In IP' (checked), 'Shared IP Address' (set to '255.255.255.0 (/24)'), and 'WAN Default Gateway'. Below these are fields for 'WAN DNS Servers' (DNS server 1 and 2). A note states: 'NOTE: The DHCP Server Settings will be overwritten. The following WAN 1 settings will be overwritten: Enable, Connection Method, Routing Mode, Connection Type, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings. The PPTP Server will be disabled. High Availability will be disabled. Tip: please review the DNS Forwarding setting under the Service Forwarding section.'

Drop-in Mode Settings (Available on Peplink Balance 210+)

Enable Drop-in Mode eases the installation of the Peplink Balance 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. Please refer to **Section, Drop-in Mode** for details.

WAN for Drop-In Mode Select the WAN port to be used for Drop-in Mode. If **WAN 1 with LAN Bypass** is selected, the High Availability feature will be disabled automatically.

Shared Drop-In Mode^A When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Balance will listen for this IP address when WAN hosts access services provided by the Balance (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 Balance will listen for this IP address when LAN hosts access services provided by the Balance (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, check the I have other host(s) on 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.



Note: Drop-in Mode and VLAN functionality are mutually exclusive.







The screenshot shows the DHCP Server Settings configuration page. It includes fields for:

- DHCP Server:** A checkbox labeled 'Enable'.
- IP Range:** Two input boxes containing '192.168.1.10' and '192.168.1.250'.
- Subnet Mask:** A dropdown menu showing '255.255.255.0 (/24)'.
- Lease Time:** Input boxes for '1' Days, '0' Hours, and '0' Mins.
- DNS Servers:** A checkbox labeled 'Assign DNS server automatically'.
- WINS Server:** A checkbox labeled 'Assign WINS server'.
- Extended DHCP Option:** A table with columns 'Option' and 'Value', and an 'Add' button below it.
- DHCP Reservation:** A table with columns 'Name', 'MAC Address', and 'Static IP', and a '+' button to add new entries.

DHCP Server Settings	
DHCP Server	When this setting is enabled, the Peplink Balance's DHCP server automatically assigns an IP address to each computer that is connected via LAN and is configured to obtain an IP address via DHCP. The Peplink Balance's DHCP server can prevent IP address collisions on the LAN.
IP Range & Subnet Mask	These settings allocate a range of IP address that will be assigned to LAN computers by the Peplink Balance's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of Lease Time , the assigned IP address will no longer be valid and the IP address assignment must be renewed.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Peplink Balance's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Server	This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's

	<p>built-in WINS server by entering this unit's LAN IP address in their DHCP WINS Servers setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at Status > WINS Clients.</p>
Extended DHCP Option	<p>In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts.</p> <p>To define an extended DHCP option, click the Add button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.</p>
DHCP Reservation	<p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses.</p> <p>The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p>Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of 00:AA:BB:CC:DD:EE. Press  to create a new record. Press  to remove a record. Reserved clients information can be imported from the Client List, located at Status > Client List. For more details, please refer to section .</p>

Static Route Settings			
Static Route		Destination Network	Subnet Mask
			255.255.255.0 (/24)
		Gateway	

Static Route Settings	
Static Route	<p>This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in w.x.y.z format.</p> <p>The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press  to create a new route. Press  to remove a route.</p>

WINS Server Settings	
Enable	<input type="checkbox"/>

WINS Server Settings	
Enable	Check the box to enable the WINS Server. A list of WINS clients will be displayed at Status > WINS Clients .

DNS Proxy Settings			
Enable	<input checked="" type="checkbox"/>		
DNS Caching	<input type="checkbox"/>		
Include Google Public DNS Servers	<input type="checkbox"/>		
Local DNS Records	Host Name	IP Address	
			<input type="button" value="+"/>

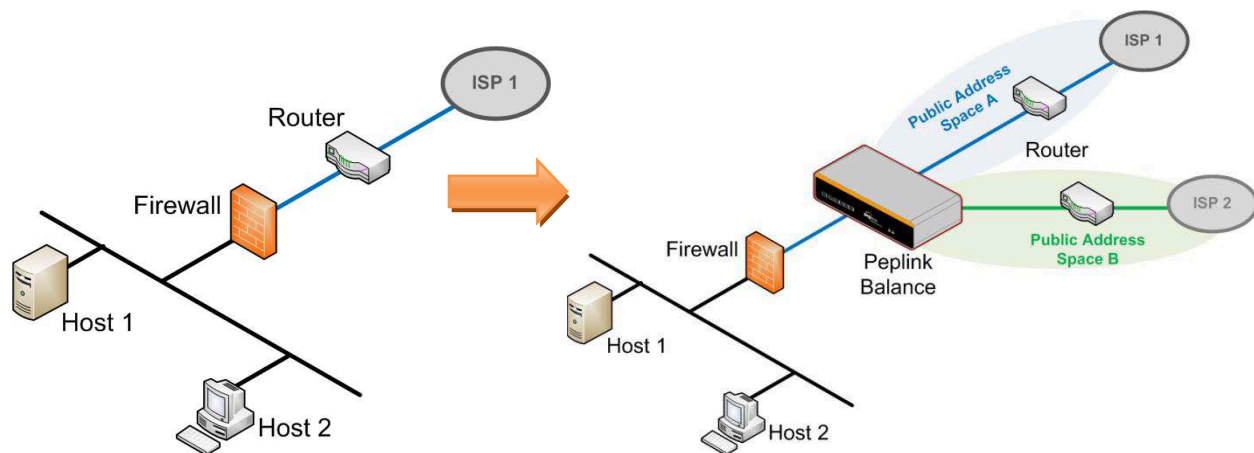
DNS Proxy Settings	
Enable	<p>To enable the DNS Proxy feature, check this box, and then set up the feature at Network > LAN > DNS Proxy Settings table.</p> <p>A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the DNS servers/resolvers defined for each WAN connection.</p>
DNS Caching	<p>This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can improve DNS response time by storing all received DNS results for faster DNS lookup. However, it cannot return the most updated result for frequently updated DNS records. By default, DNS Caching is disabled.</p>
Include Google Public DNS Servers	<p>When this option is enabled, the DNS proxy server will forward DNS requests to Google's Public DNS Servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.</p>
Local DNS Records	<p>This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP Address. When looking up the host name from the LAN to LAN IP of the Peplink Balance, the corresponding IP address will be returned. Press <input type="button" value="+"/> to create a new record. Press <input type="button" value="X"/> to remove a record.</p>
DNS Resolvers ^A	<p>Check the box to enable the WINS Server. A list of WINS clients will be displayed at Network > LAN > DNS Proxy Settings > DNS Resolvers.</p> <p>This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected.</p> <p>If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es).</p> <p>Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.</p>

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

10 Drop-in Mode

Drop-in Mode (or transparent bridging mode) eases the installation of the Peplink Balance on a live network between the firewall and router, such that changes to the settings of existing equipment are not required. Note that Drop-in Mode is **NOT** applicable to the Balance 20, 30 or 30 LTE.

The following diagram illustrates Drop-in Mode setup:



Check the checkbox to **Enable** Drop-in Mode. After enabling this feature and selecting the WAN for Drop-in mode, various settings, including the WAN's connection method and IP address, will be automatically updated.

When Drop-in Mode is enabled, the LAN and the WAN for Drop-in Mode ports will be bridged. Traffic between the LAN hosts and WAN router will be forwarded between the devices. In this case, the hosts on both sides will not notice any IP or MAC address changes.

After successfully setting up the Peplink Balance as part of the network using Drop-in Mode, a Peplink Balance 210 will accommodate one additional WAN connection; a 310, 305 or 380 will accommodate two, a 580 will accommodate four, a 710 will accommodate six, a 1350 will accommodate twelve, and a 2500 will accommodate eleven additional WAN connections.

IMPORTANT NOTE for customers using Drop-in Mode and planning to upgrade from firmware 4.8.2 or below to 5.0+

MAC address passthrough for Drop-in Mode is implemented in firmware 5.0 and above. If Drop-in Mode is enabled when upgrading from a previous firmware version, the ARP tables on hosts on LAN and WAN segments must be flushed once. Alternately, the hosts may be rebooted. Otherwise, hosts on one side may not be able to reach hosts on the other side of the Peplink Balance until old ARP records expire. Units not using Drop-in Mode are not affected.

NOTE

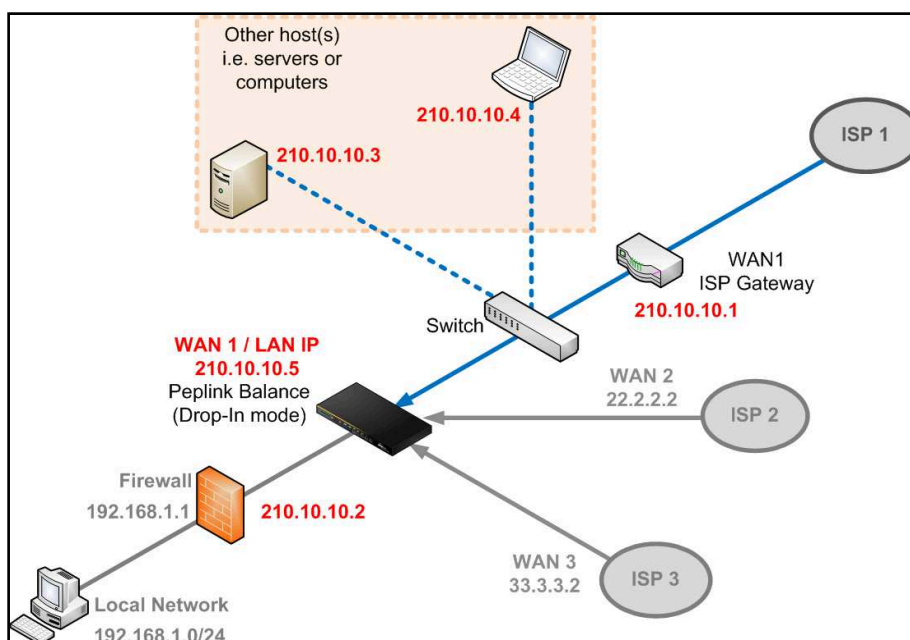
The PPTP server will be disabled in Drop-in Mode.

To enable Drop-in Mode, perform the following steps:

Drop-In Mode Settings	
Enable	<input checked="" type="checkbox"/>
WAN for Drop-In Mode	WAN 1
Do not Consume IP	<input type="checkbox"/>
WAN Default Gateway	210.10.10.1 <input checked="" type="checkbox"/> I have other host(s) on WAN segment Host IP Address(es) 210.10.10.3 - <input type="text"/> <input type="button" value="↓"/> 210.10.10.4 210.10.10.3 <input type="button" value="Delete"/>
WAN DNS Servers	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
NOTE: The DHCP Server Settings will be overwritten. The following WAN 1 settings will be overwritten: Enable, Connection Method, Routing Mode, Connection Type, 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.	

1. Check the **Enable** box under Drop-in Mode located at: **Network > Interfaces > LAN**. (After checking the **Enable** box, most network settings for WAN1 will be hidden in the Web Admin Interface.)
2. Enter the IP address of the WAN1 router in the **WAN Default Gateway** field. Ensure that the Peplink Balance subnet is the same as the firewall's WAN port and the router's LAN port.
3. If there are hosts other than the router on the WAN segment of Peplink Balance, check the **have other host(s) on WAN segment** box, enter the IP address(es) of the host(s), and then click the down-arrow to add the hosts.

The following diagram illustrates:

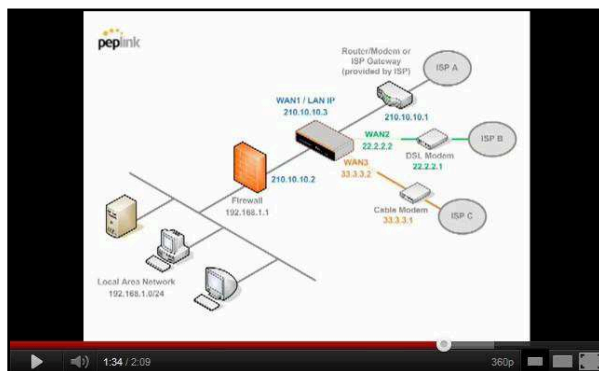


Important Note

Starting from Firmware version 5.0, Drop-in mode can be configured on any WAN port. Please note that only one WAN port can be configured in Drop-in mode. If you have selected the LAN bypass port (which is currently available on WAN1 of the Balance 1350 and WAN5 of the Balance 580) as the WAN for Drop-in Mode, the High Availability feature will be DISABLED automatically.

Tip

Want to know more about Drop-in mode? Visit our [YouTube Channel](#) for video tutorials!




<http://youtu.be/IZG2-VPmI5w>









11 Configuring the WAN Interface(s)

WAN interface settings are located at: *Network > Interfaces > WAN*

Connection Name	Method	Routing Mode	Type
1. WAN1	Static IP	NAT	Always-on
2. WAN2	Static IP	NAT	Always-on
3. WAN3	Not Configured	NAT	Always-on
4. WAN4	Static IP	NAT	Always-on
5. WAN5	Not Configured	NAT	Always-on
6. Mobile Internet	PPP	NAT	Backup Group 1

IPv6
Disabled 

By clicking a **connection name**, connection settings of that WAN can be modified. The connection method and details can be obtained from your ISP.

Connection Settings	
WAN Connection Name *	<input type="text" value="WAN1"/>
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Connection Method 	<input type="text" value="DHCP"/>  Click here to edit Connection settings
Routing Mode 	<input checked="" type="radio"/> NAT
Connection Type 	<input type="radio"/> Always-on <input checked="" type="radio"/> Backup Priority <input type="text" value="Group 1 (Highest)"/> 
Reply to ICMP PING 	<input checked="" type="checkbox"/> Enable
Upload Bandwidth * 	<input type="text" value="100"/> <input type="text" value="Mbps"/>
Download Bandwidth * 	<input type="text" value="100"/> <input type="text" value="Mbps"/>

Connection Settings	
WAN Connection Name	This field is for defining a name to represent this WAN connection.
Enable	This field is for choosing whether to enable this WAN connection.
Connection Method	<p>This option allows you to select the connection method for this WAN connection. Available options are:</p> <ol style="list-style-type: none"> DHCP Static IP PPPoE Mobile Internet Connection <p>See sections , , , and for configuration details pertaining to each connection method.</p>
Routing Mode	This field shows that NAT (Network Address Translation) will be applied to the traffic routing over this WAN connection. IP Forwarding is also available when you click the link in the help text. For further details, please refer to , Routing under DHCP, Static IP, and PPPoE.
Connection Type	This setting specifies the utilization of the WAN connection.

Always-on results in the WAN connection being used whenever it is available. If **Backup Priority** and a priority group are selected, the WAN connection is treated as a backup connection and is used only in the absence of available always-on WAN connection(s) and higher priority backup connection(s).

Connection Type	<input type="radio"/> Always-on	<input checked="" type="radio"/> Backup Priority	Group 1 (Highest)
Reply to ICMP PING	<input checked="" type="checkbox"/> Enable		Group 1 (Highest)
			Group 2
			Group 3 (Lowest)

The default and recommended connection type is **Always-on**.

Reply to ICMP Ping

If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is **enabled**.

Upload Bandwidth

This setting specifies the data bandwidth in the outbound direction from the LAN through the WAN interface. This value is provided by your ISP and should reflect the actual speed of the WAN.

This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. Setting the correct value here can result in effective traffic prioritization and efficient use of upload bandwidth.

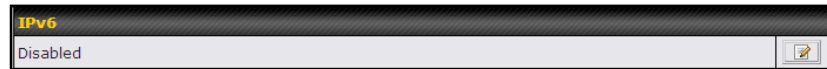
Download Bandwidth

This setting specifies the data bandwidth in the inbound direction from the WAN interface to the LAN. This value is provided by your ISP and should reflect the actual speed of the WAN.

This value is referenced as the default weight value when using the **Least Used** or **Persistence (Auto)** algorithms in **Outbound Policy** with **Managed by Custom Rules** chosen (see **Section**).

IPv6

IPv6 support can be enabled on one of the available Ethernet WAN ports. On this screen, you can choose which WAN will support IPv6.



IPv6

To enable IPv6 support on a WAN, the WAN router must respond to stateless address auto configuration advertisements and DHCPv6 requests. IPv6 clients on the LAN will acquire their IPv6, gateway, and DNS server addresses from it. The device will also acquire an IPv6 address for performing ping/traceroute checks and accepting Web Admin accesses.

11.1 Connection Method(s)

There are four possible connection methods:

1. DHCP
2. Static IP
3. PPPoE
4. Mobile Internet Connection (for USB WAN)

11.1.1 DHCP Connection

The DHCP connection method is suitable if your ISP provides an IP address automatically using DHCP (e.g., cable, metro Ethernet, etc.).


DHCP Settings	
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
Hostname (Optional) ?	<input type="text"/> <input type="checkbox"/> Use custom hostname

DHCP Settings	
DNS Servers	<p>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.</p> <p>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.)</p> <p>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.</p>
Hostname (Optional)	<p>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 a hostmane, you can safely bypass this option.</p>

Please refer to sections , , and for details about **WAN Health Check**, **Bandwidth Allowance Monitor**, **Additional Public IP Settings**, and **Dynamic DNS Settings**.

11.1.2 Static IP Connection

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

Static IP Settings 	
IP Address *	<input type="text"/>
Subnet Mask *	255.255.255.0 (/24) ▾
Default Gateway *	<input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>

Static IP Settings	
IP Address / Subnet Mask / Default Gateway	<p>These settings specify the information required in order to communicate on the Internet via a fixed Internet IP address.</p> <p>The information is typically determined by and can be obtained from your ISP.</p>
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This field specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>You can input the ISP-provided DNS server addresses into the DNSserver 1 and DNSserver 2 fields. If no address is entered here, this link will not be used for DNS lookups.</p>

Please refer to Section , , , and for details about **WAN Health Check**, **Bandwidth Allowance Monitor**, **Additional Public IP Settings**, and **Dynamic DNS Settings** respectively.

11.1.3 PPPoE Connection

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

PPPoE Settings ?	
PPPoE User Name *	<input type="text"/>
PPPoE Password	<input type="password"/>
Confirm PPPoE Password	<input type="password"/>
Service Name (optional)	<input type="text"/> <small>Leave it blank unless it's provided by ISP</small>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>

PPPoE Settings	
PPPoE User Name / Password	Enter the required information in these fields in order to connect via PPPoE to your ISP. The parameter values are determined by and can be obtained from your ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service Name is a PPPoE parameter which is provided by your ISP. <i>Note: Leave this field blank unless it is provided by your ISP.</i>
DNS Servers	<p>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.</p> <p>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.)</p> <p>When Use the following DNS server address(es) is selected, you can put custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>

Please refer to section , , and for details about **WAN Health Check**, **Bandwidth Allowance Monitor**, **Additional Public IP Settings**, and **Dynamic DNS Settings**.

Note

A PPPoE connection made from a firewall does not work with Drop-in Mode.

11.1.4 Mobile Internet Connection

The Mobile Internet Connection method is suitable for USB modem mobile connections, such as 3G, WiMAX, LTE, EVDO, EDGE, and GPRS. Currently, it only applies to connections made via the Balance's USB mobile WAN port, except in the case of the Balance 30 LTE, which includes a built-in 4G LTE modem. For a list of supported modems, please refer to Peplink Modem Support page at <http://www.peplink.com/modem>.

Connection Settings	
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Connection Type	<input type="radio"/> Always-on <input checked="" type="radio"/> Backup Priority Group 1 (Highest) ▾
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Idle Disconnect	<input checked="" type="checkbox"/> 3 minutes Time value is global. A change will affect all WAN profiles.
GRE	<input checked="" type="checkbox"/> Enable
Reply to ICMP PING	<input checked="" type="checkbox"/> Enable
Operator Settings (for HSPA/EDGE/GPRS only)	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Mobile Operator Settings APN: <input type="text"/> Login ID: <input type="text"/> Password: <input type="text"/> Dial Number: <input type="text"/>
Remote GRE Host	<input type="text"/>
Tunnel Local IP Address	<input type="text"/>
Tunnel Remote IP Address	<input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>

Mobile Internet Connection Settings	
Enable	Select Yes to enable the connection.
Connection Type	This setting specifies the utilization of the WAN connection. Always-on results in the WAN connection being used whenever it is available. If Backup is selected, the WAN connection is treated as a backup connection and is used only in the absence of an available always-on WAN. The default and recommended connection type is Always-on .
Standby State	This option allows you to choose whether to remain connected or disconnect when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen and this WAN connection is made active, the WAN connection will be immediately available for use.
Idle Disconnect	With this option enabled, an idle connection will be disconnected after a specified period of time. This time value specified is global and will affect all WAN profiles. The mobile connection will re-establish on demand.
Reply to ICMP Ping	If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled .

Operator Settings	<p>This setting applies to 3G/LTE/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems.</p> <p>Operator Settings allows you to configure the APN settings of your connection. If Auto is selected, the Peplink Balance will automatically detect the APN, configure the modem, and make a connection. You may change the APN settings by selecting Custom Mobile Operator Settings. The default and recommended Operator Settings value is Auto. The correct values can be obtained from your mobile Internet service provider.</p>
SIM PIN (Optional)	<p>This is an optional field which is only needed when there is SIM lock for your SIM card service.</p>
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This field specifies the DNS servers to be used when a DNS lookup is routed through this connection. You can input the ISP-provided DNS server addresses into the DNS server 1 and DNS server 2 fields. If no address is entered here, this link will not be used for DNS lookups.</p>

Please refer to sections , , , and for details about **WAN Health Check**, **Bandwidth Allowance Monitor**, **Additional Public IP Settings**, and **Dynamic DNS Settings**.

11.1.4.1 Modem Specific Custom Settings

The following settings may be available, depending on the modem model. The example below is for a 3G modem.

Modem Specific Custom Settings	
Modem Model	xxx Modem
IMSI	123400005678900
Network Type	? 3G preferred ▾
GSM Frequency Band	All Bands ▾

Modem Specific Custom Settings	
Modem Model	This field displays the manufacturer name of the connected mobile modem.
IMSI	This field shows the IMSI number associated with the SIM inside the mobile modem.
Network Type	<p>This setting allows you to define your preference for using 3G and/or 2G networks. 3G networks include HSPA/UMTS. 2G networks include EDGE/GPRS.</p> <p>If 3G only or 2G only is chosen, only the HSPA/UMTS or EDGE/GPRS network will be used, respectively. If the chosen network is not available, no other network will be used, regardless of its availability. The modem connection will remain offline.</p> <p>If 3G preferred or 2G preferred is chosen, the chosen network will be used when it is available. If the chosen network is not available, the other network will be used whenever available.</p> <p>The default network type is 3G preferred.</p>
GSM Frequency Band	<p>This setting allows you to specify which GSM frequency band will be used.</p> <p>GSM1900 is used in the United States, Canada, and many other countries in the Americas.</p> <p>GSM900 / GSM1800 / GSM2100 are used in Europe, the Middle East, Africa, Asia, Oceania, and Brazil.</p> <p>If All Bands is chosen, the appropriate frequency band will be used automatically.</p> <p>The default GSM frequency band is All Bands.</p>

11.1.4.2 WiMAX Settings

If a WiMAX modem is present in the system, its settings user interface can be accessed at **Network > Interfaces > WAN > Mobile Internet**.

The example shown here relates to Sprint's 250U or 600U WiMAX modems.

Modem Specific Custom Settings	
Modem Model	Sprint Modem
ESN	C7B1C7B1
Network Type	<input type="text" value="4G only"/> 4G only 3G only

Modem Specific Custom Settings	
Modem Model	The brand of the modem is automatically detected and appears here.
ESN	The modem's electronic serial number (ESN) is also auto-detected and appears here.
Network Type	This is to specify the network type (e.g., 3G or 4G) to be used with the modem.

11.2 Physical Interface Settings

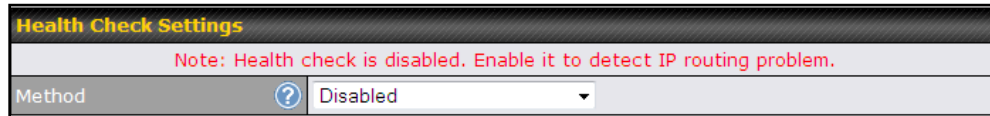
Physical Interface Settings	
Speed	<input type="radio"/> ? Auto
MTU	<input type="radio"/> ? Auto <input checked="" type="radio"/> Custom 1440 <input type="button" value="Default"/>
MSS	<input checked="" type="radio"/> ? Auto <input type="radio"/> Custom
MAC Address Clone	<input type="radio"/> ? Default <input checked="" type="radio"/> Custom 00 : 11 : 11 : 11 : 22 : BB
VLAN	<input type="checkbox"/> ? Enable

Physical Interface Settings	
Speed	This setting specifies port speed and duplex configurations of the WAN port. By default, Auto is selected and the appropriate data speed is automatically detected by the Peplink Balance. In the event of negotiation issues, the port speed can be manually specified to circumvent the issues. You can also choose whether or not to advertise the speed to the peer by selecting the Advertise Speed checkbox.
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to Custom 1440 . You may adjust the MTU value by editing the text field. Click Default to restore the default MTU value. Select Auto and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes.
MSS	This setting should be configured based on the maximum payload size that the local system can handle. The MSS (maximum segment size) is computed by taking the MTU and subtracting 40 bytes for TCP over IPv4. If MTU is set to Auto , MSS will also be set automatically. By default, MSS is set to Auto .
MAC Address Clone	This setting allows you to configure the MAC address. Some service providers (e.g., cable providers) identify the client's MAC address and require the client to always use the same MAC address to connect to the network. In such cases, change the WAN interface's MAC address to the original client PC's MAC address via this field. The default MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking the Default button restores the MAC address to the default value.
VLAN	Some service providers require the router to enable VLAN tagging for Internet traffic. If it is required by your service provider, you can enable this field and enter the VLAN ID that the provider requires. <i>Note: leave this field disabled if you are not sure.</i>

11.3 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Peplink Balance can periodically check the health of each WAN connection.

Health Check settings for each WAN connection can be independently configured via **Network > Interfaces > WAN > Health Check Settings**.

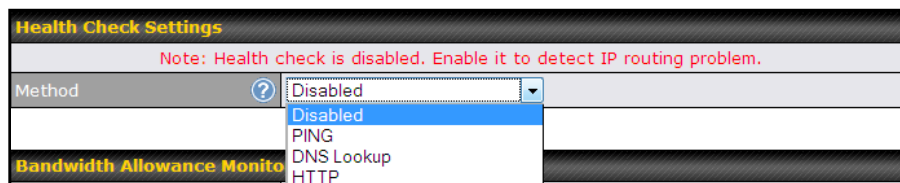


Health Check Settings

Note: Health check is disabled. Enable it to detect IP routing problem.

Method ? Disabled

Enable Health Check by selecting **PING**, **DNS Lookup**, or **HTTP** from the **Health Check Method** drop-down menu.



Health Check Settings

Note: Health check is disabled. Enable it to detect IP routing problem.

Method ? Disabled


- Disabled
- PING
- DNS Lookup
- HTTP

Bandwidth Allowance Monito

Health Check Settings

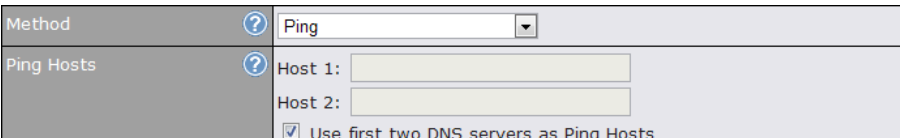
Method This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, or **DNS Lookup**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

Health Check Disabled



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



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

Method	?	DNS Lookup
Health Check DNS Servers	?	Host 1: <input type="text"/>
		Host 2: <input type="text"/>
		<input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers
		<input type="checkbox"/> 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

Health Check Settings		
Method	?	HTTP
Web 1		URL: http:// <input type="text"/>
		String to Match: <input type="text"/> (optional)
Web 2		URL: http:// <input type="text"/>
		String to Match: <input type="text"/> (optional)
Timeout	?	5 <input type="text"/> second(s)
Health Check Interval	?	5 <input type="text"/> second(s)
Health Retries	?	3 <input type="text"/>
Recovery Retries	?	3 <input type="text"/>

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

URL1

WAN Settings > WAN Edit > Health Check Settings > URL1

The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the 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.

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

Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is set to 5 seconds .
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. 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 Balance is to 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 Balance treats a previously down WAN connection as up again. By default, Recovery 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.

Note

If a WAN connection goes down, all of the WAN connections not set with a **Connection Type** of **Always-on** will also be brought up until any one of higher priority WAN connections is up and found to be healthy. This design could increase overall network availability.

For example, if WAN1, WAN2, and WAN3 have the connection types of **Always-on**, **Backup Priority Group 1**, and **Backup Priority Group 2**, respectively, when WAN1 goes down, WAN2 and WAN3 will try to connect. If WAN3 is connected first, WAN2 will still be kept connecting. If WAN2 is connected, WAN3 will disconnect or abort making connection.

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and checks fail, the Balance will automatically perform DNS lookups on some 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.

11.4 Bandwidth Allowance Monitor

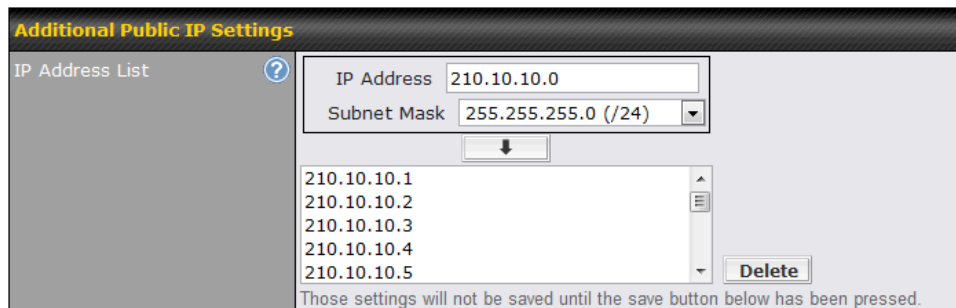
The Bandwidth Allowance Monitor helps track your network usage. Please refer to section to view usage statistics.

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

Bandwidth Allowance Monitor	
Action	<p>If Email Notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance.</p> <p>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.</p>
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	
<p>Due to different network protocol overheads and conversions, the amount of data as 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.</p>	

11.5 Additional Public IP Settings



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**.

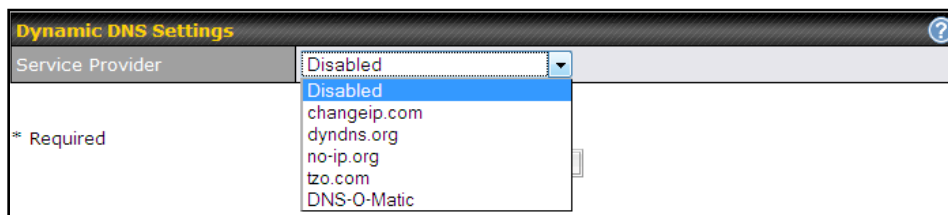
11.6 Dynamic DNS Settings

The Peplink Balance allows registering 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 hostname. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address externally even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

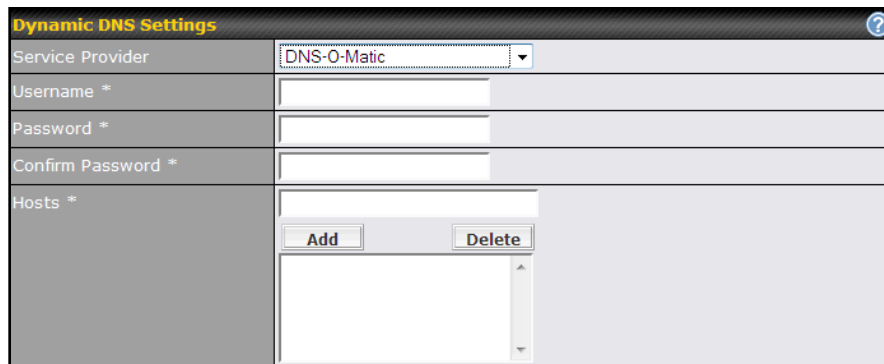
If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

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

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



If your desired provider is not listed, you may check with [DNS-O-Matic](#). This service supports updating 30 other dynamic DNS service providers. (Note: Peplink is not affiliated with DNS-O-Matic.)



Dynamic DNS Settings	
Service Provider	<p>This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:</p> <ul style="list-style-type: none"> • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic <p>Select Disabled to disable this feature.</p>
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.
Password / Pass / TZO Key	This setting specifies the password for the dynamic DNS service.
Hosts / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note

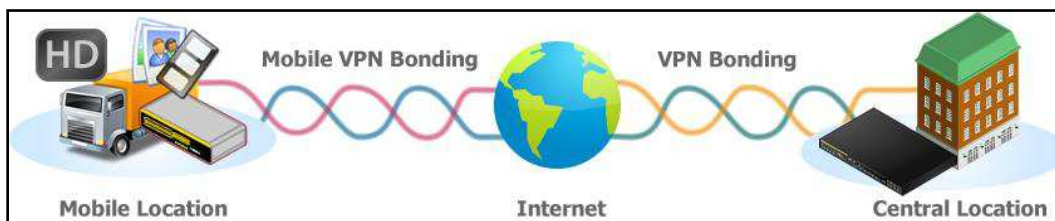
In order to use dynamic DNS services, appropriate hostname registration(s), as well as a valid account with a supported dynamic DNS service provider, are required.

A dynamic DNS update is performed whenever a WAN's IP address is changed, such as when an IP is changed after a DHCP IP refresh or reconnection.

Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a WAN's IP address did not change.

12 Bandwidth Bonding SpeedFusion™

(Available on the Peplink Balance 210+)



Peplink Balance Bandwidth Bonding SpeedFusion™ functionality securely connects one or more branch offices to your company's main headquarters or to other branches. The data, voice, and video communications between these locations are kept confidential across the public Internet.

The Bandwidth Bonding SpeedFusion™ of the Peplink Balance is specifically designed for multi-WAN environments. The Peplink Balance can bond all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, the Peplink Balance can keep the VPN up and running. Bandwidth Bonding is enabled by default.

12.1 SpeedFusion™ Settings

Peplink Balance 380, 580, 710, 1350 and 2500 support making multiple SpeedFusion™ connections with a remote Peplink Balance 210, 310, 380, 580, 710, 1350, 2500, or a Pepwave MAX mobile router. The Peplink Balance 210 and 310 support making two SpeedFusion™ connections with a remote Peplink Balance 210, 310, 380, 580, 710, 1350, 2500, or a Pepwave MAX mobile router.


A Peplink Balance that supports multiple VPN connections can act as a central hub which connects branch offices. For example, if branch office A and branch office B make VPN connections to headquarters C, both branch office LAN subnets and the subnets behind them (i.e., static routes) will also be advertised to the headquarters C and the other branches. So branch office A will be able to access branch office B via headquarters C in this case.


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 with 256-bit AES encryption standard. To configure this, navigate to **Network > SpeedFusion™**.



PepVPN with SpeedFusion™

 InControl management enabled. Settings can now be configured on [InControl](#).




Profile	Remote ID	Remote Address(es)	
 FL Office	Balance_20D3		
 NY Office	Balance_FBDB		

SpeedFusion™

Local ID	 Balance_8B8E	
----------	--	---

Link Failure Detection

Link Failure Detection Time 

- Recommended (Approx. 15 secs)
- Fast (Approx. 6 secs)
- Faster (Approx. 2 secs)
- Extreme (Under 1 sec)

Shorter detection time incurs more health checks and higher bandwidth overhead

To configure a new SpeedFusion™ profile, navigate to **Network > SpeedFusion™ > New Profile**

This will open a page similar to the one as shown below:

PepVPN Profile	
Name	<input type="text"/>
Active	<input checked="" type="checkbox"/>
SpeedFusion™	Supported
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF
Remote ID	<input type="text"/>
Authentication	<input checked="" type="radio"/> By Remote ID only <input type="radio"/> Preshared Key <input type="radio"/> X.509
NAT Mode	<input type="checkbox"/>
Remote IP Address / Host Names (Optional)	<input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small>
Data Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>
Layer 2 Bridging	<input checked="" type="checkbox"/>
Bridging Port	<input checked="" type="radio"/> LAN
VLAN Tagging	No VLAN <input type="button" value="More..."/>
STP	<input type="checkbox"/>
Preserve LAN Settings Upon Connected	<input type="checkbox"/> <small>After this VPN profile is established, most routing functionalities will cease to work. The device will practically become an Ethernet extender of the remote unit.</small>
Configure	Using DHCP <input type="button" value="v"/>

A list of defined SpeedFusion™ connection profiles and **aLink 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 Balance via the available WAN connections. Each profile is for making a VPN connection with one remote Peplink Balance.

PepVPN 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 ().
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
SpeedFusion™	This field indicates whether this device supports SpeedFusion or not.
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.
Remote ID	To allow the Peplink Balance to establish a VPN connection with a specific remote peer using a unique identifying number, enter the peer's ID or serial number here.
Authentication	Select from By Remote ID Only , Preshared Key , or X.509 to specify the method the Peplink Balance 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.

Pre-shared Key	This optional field becomes available when Pre-shared Key is selected as the Peplink Balance'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. If you would like to prevent the display of the pre-shared key, check Hide Characters .
X.509	This optional field becomes available when X.509 is selected as the Peplink Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into this field. To get more information on a listed X.509 certificate, click the Show Details link below the field.
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 Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance 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.
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.
Layer 2 Bridging^A	To make this option visible, click the question mark icon appearing at the top right of the PepVPN Profile settings section, and then click the displayed link. When this check box is unchecked, traffic between local and remote networks will be IP forwarded. To bridge the Ethernet network of an Ethernet port on a local and remote network, select Layer 2 Bridging. When this check box is selected, the two networks will become a single LAN, and any broadcast (e.g., ARP requests) or multicast traffic (e.g., Bonjour) will be sent over the VPN.
Bridge Port^A	When Layer 2 bridging is enabled, this field specifies the port to be bridged to the remote site. If you choose WAN , the selected WAN will be dedicated to bridging with the remote site and will be disabled for WAN purposes. The LAN port will remain unchanged.
VLAN Tagging^A	This field specifies the VLAN ID with which the VPN's traffic should be tagged before sending the traffic to the bridge port. If no VLAN tagging is needed, select No VLAN . To define a new VLAN ID, click More... and input the VLAN ID. VLAN IDs that are not referenced by any VPN profiles will be removed from the list automatically. The default value for this field is No VLAN .
STP^A	Checking this box enables spanning tree protocol, used to prevent loops in bridged Ethernet LANs.
Preserve LAN	The LAN port is chosen as the bridge port. Selecting this option preserves LAN settings


Settings Upon Connected^A

(e.g., LAN port IP address, DHCP server, etc.) when the Layer 2 VPN is connected. Uncheck this option if the LAN IP address and gateway will use remote LAN settings. Check this option if the LAN IP address and local DHCP server should remain unchanged after the VPN is up. If you choose not to preserve LAN settings when the VPN is connected, the device will not act as a router and most Layer 3 routing functions will cease to work.

Configure^A

This setting specifies how a management IP address is acquired for the bridge port in the specified VLAN (if defined) when the Layer 2 bridge is connected. Choosing **As None** will result in no IP address being assigned to the bridge port for the Layer 2 connection.

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

WAN Connection Priority 		
1. WAN1	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>
2. WAN2	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>
3. WAN3	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>
4. WAN4	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>
5. WAN5	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>
6. WAN6	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>
7. WAN7	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>
8. Mobile Internet	Priority: 1 (Highest) <input type="button" value="v"/>	Connect to Remote: All <input type="button" value="v"/>

WAN Connection Priority


WAN Connection Priority

These settings specify the priority of the WAN connections to be used in making VPN bonding connections. A WAN connection will never be used when OFF is selected. Only available WAN connections with the highest priority will be utilized.

To allow connection mapping to remote WANs, click the question mark icon found at the top right of this section, and then click the displayed link to reveal the **Connect to Remote** drop-down menu.

Send All Traffic To	
VPN Connection 2	

Send All Traffic To

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

Send All Traffic	
Send All Traffic To	<input checked="" type="checkbox"/> VPN Connection 2 <input type="button" value="v"/>
DNS Server	135.36.14.0 <input type="text"/>
	<input type="text"/>

You could also specify a DNS server to resolve incoming DNS requests

Link Failure Detection

Link Failure Detection Time ?

- Recommended (Approx. 15 secs)
- Fast (Approx. 6 secs)
- Faster (Approx. 2 secs)
- Extreme (Under 1 sec)

Shorter detection time incurs more health checks and higher bandwidth overhead

Link Failure Detection

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.

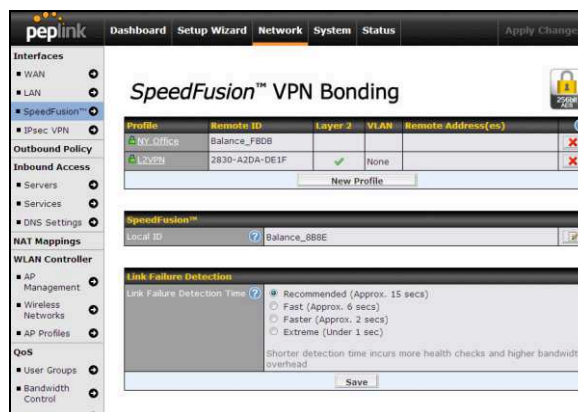
When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

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 Balance 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

Watch a video walkthrough of setting up a SpeedFusion™ VPN on our [YouTube Channel!](#)



http://youtu.be/xNaq13FWu_g

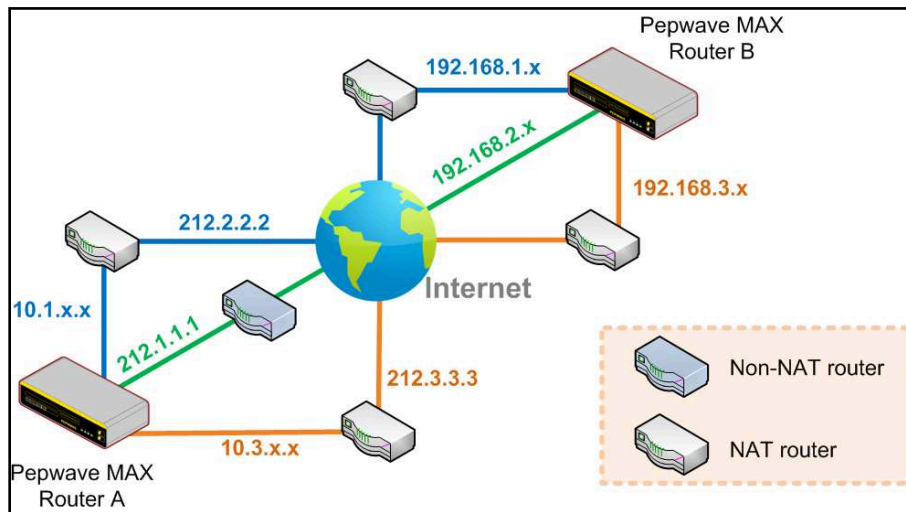
12.2 The Peplink Balance Behind a NAT Router

The Peplink Balance supports 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 Balance.

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

12.3 SpeedFusion™ Status

SpeedFusion™ Status is shown in the **Dashboard**. The connection status of each connection profile is shown as below.



SpeedFusion™		Status
FL Office		Established
NY Office		Established

SpeedFusion™ connection status is also shown on the LCD panel of the Peplink Balance 380, 580, 710, 1350, and 2500.

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



Profile	Remote Networks
 NY Office	192.168.3.0/24 
 FL Office	192.168.50.0/24 

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.

13 IPsec VPN

Peplink Balance 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.

IPsecVPN on the Peplink Balance is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for his 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.

13.1 IPsec VPN Settings

All Peplink products can make multiple IPsec VPN connections with Peplink routers, as well as 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, navigate to **Network > IPsec VPN**.

NAT-Traversal		Enabled	
IPsec VPN Profiles	Remote Networks		
Profile 1	192.167.11.193/28		
<input type="button" value="New Profile"/>			

A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown.

NAT-Traversal should be enabled if your system is behind a NAT router.

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

Name	Profile 1											
Active	<input checked="" type="checkbox"/>											
Remote Gateway IP Address / Host Name	12.12.12.12											
Local Networks	<input checked="" type="checkbox"/> 192.168.1.0/24 <input type="checkbox"/> <input type="text"/>											
Remote Networks	<table border="1"> <thead> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td>192.167.11.193</td> <td>255.255.255.240 (/28)</td> <td><input type="button" value="X"/></td> </tr> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24)</td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Network	Subnet Mask		192.167.11.193	255.255.255.240 (/28)	<input type="button" value="X"/>	<input type="text"/>	255.255.255.0 (/24)	<input type="button" value="+"/>		
Network	Subnet Mask											
192.167.11.193	255.255.255.240 (/28)	<input type="button" value="X"/>										
<input type="text"/>	255.255.255.0 (/24)	<input type="button" value="+"/>										
Authentication	<input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate											
Mode	<input checked="" type="radio"/> Main Mode (All WANs need to have Static IP) <input type="radio"/> Aggressive Mode											
Force UDP Encapsulation	<input type="checkbox"/>											
Preshared Key	<input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters											
Local ID	<input type="text"/>											
Remote ID	<input type="text"/>											
Phase 1 (IKE) Proposal	1 AES-256 & SHA1 2 -----											
Phase 1 DH Group	<input checked="" type="checkbox"/> Group 2: MODP 1024 <input type="checkbox"/> Group 5: MODP 1536											
Phase 1 SA Lifetime	<input type="text" value="3600"/> seconds <input type="button" value="Default"/>											
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 2 -----											
Phase 2 PFS Group	<input checked="" type="radio"/> None <input type="radio"/> Group 2: MODP 1024 <input type="radio"/> Group 5: MODP 1536											
Phase 2 SA Lifetime	<input type="text" value="28800"/> seconds <input type="button" value="Default"/>											

IPsec VPN 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.
Remote Gateway IP Address	Enter the remote peer's public IP address. For Aggressive Mode , this is optional.
Local Networks	Enter the local LAN subnets here. If you have defined static routes, they will be shown here.
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 methods of authentication.
Mode	Choose Main Mode if both IPsec peers use static IP addresses. Choose Aggressive Mode if one of the IPsec peers uses dynamic IP addresses.
Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Local ID	In Main Mode , this field can be left blank. In Aggressive Mode , if Remote Gateway IP Address is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Remote ID	In Main Mode , this field can be left blank. In Aggressive Mode , if Remote Gateway IP Address is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Phase 1 (IKE) Proposal	In Main Mode , this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In Aggressive Mode , only one selection is permitted.
Phase 1 DH Group	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. Group 2 - 1024-bit is the default value. Group 5 - 1536-bit is the alternative option.
Phase 1 SA Lifetime	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at 3600 seconds.
Phase 2 (ESP) Proposal	In Main Mode , this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In Aggressive Mode , only one selection is permitted.
Phase 2 PFS Group	Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. None - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. Group 2 - 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. Group 5 - 1536-bit is the third option.
Phase 2 SA Lifetime	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at 28800 seconds.