PEPWAVE

Broadband Possibilities

User Manual

AP One Enterprise AX / AP One ENT AX / APO-ENT-AX / PRB-11AX

Pepwave AP One Enterprise AX / Peplink AP One Enterprise AX
AP One AX / APO-AX / Pepwave AP One AX / Peplink AP One AX

Pepwave Firmware 3.7.2

May 2020

Table of Contents

1 Introduction and Scope

Our AP Series of enterprise-grade 802.11ax/ac/a/b/g/n Wi-Fi access points is engineered to provide fast, dependable, and flexible operation in a variety of environments, all controlled by an easy-to-use centralized management system.
From the small but powerful AP One AC mini to the top-of-the-line AP Pro Duo our AP Series offers wireless networking solutions to suit any business need, and every access point is loaded with essential features such as multiple SSIDs, VLAN, WDS, and Guest Protect.

A single access point provides as many as 32 virtual access points (16 on single-radio models), each with its own security policy (WPA, WPA2, etc.) and authentication mechanism (802.1x, open, captive portal, etc.), allowing faster, easier, and more cost-effective network builds.
Each member of the AP Series family also features a high-powered Wi-Fi transmitter that greatly enhances coverage and performance while reducing equipment costs and maintenance.

2 Product Features and Benefits

Key features and benefits of AP Series access points:

- High-powered Wi-Fi transmitter enhances coverage and lowers cost of ownership.
- Independent security policies and encryption mechanisms for each virtual access point allow fast, flexible, cost-effective network builds.
- Centralized management via InControl reduces maintenance expense and time.
- WDS support allows secure and fast network expansion.
- Guest Protect support guards sensitive business data and subnetworks.
- WMM (Wi-Fi Multimedia) and QoS (Quality of Service) support keeps video and other bandwidth-intensive data flowing fast and lag-free.

3 Package Contents

AP One Enterprise AX

1x AP One Enterprise
1 x Mounting Bracket

4 Hardware Overview

4.1 AP One Enterprise AX

Top

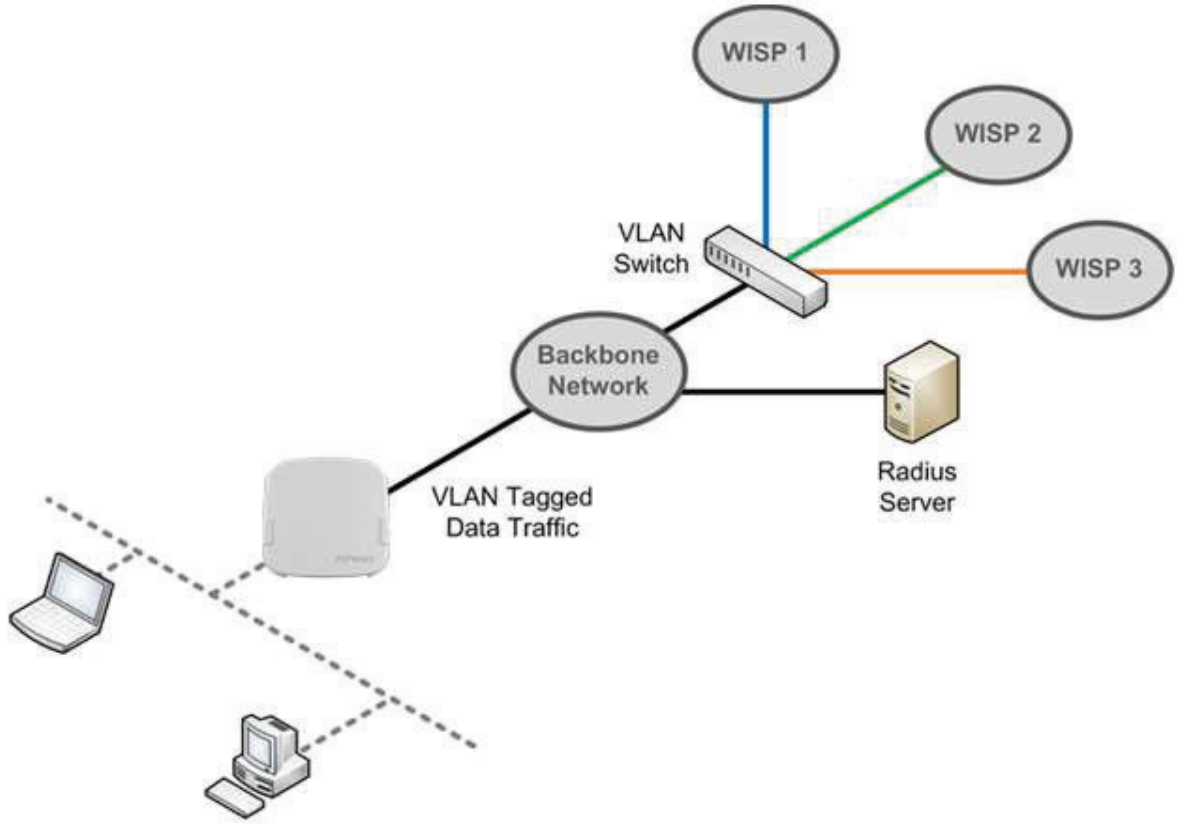
Bottom

Side

LED Indicators	
Status	RED – Access point initializing GREEN – Access point ready
LAN 1	OFF – No device connected to Ethernet port BLINKING – Ethernet port sending/receiving data ON – Powered-on device connected to Ethernet port Note that LAN 5 displays the status of the uplink connection

5 Installation

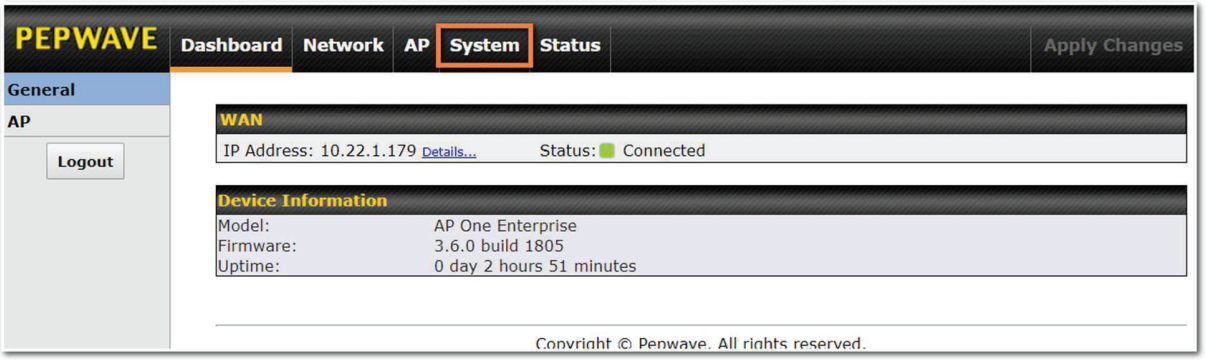
Your access point acts as a bridge between wireless and wired Ethernet interfaces.
A typical setup follows:



Installation Procedures

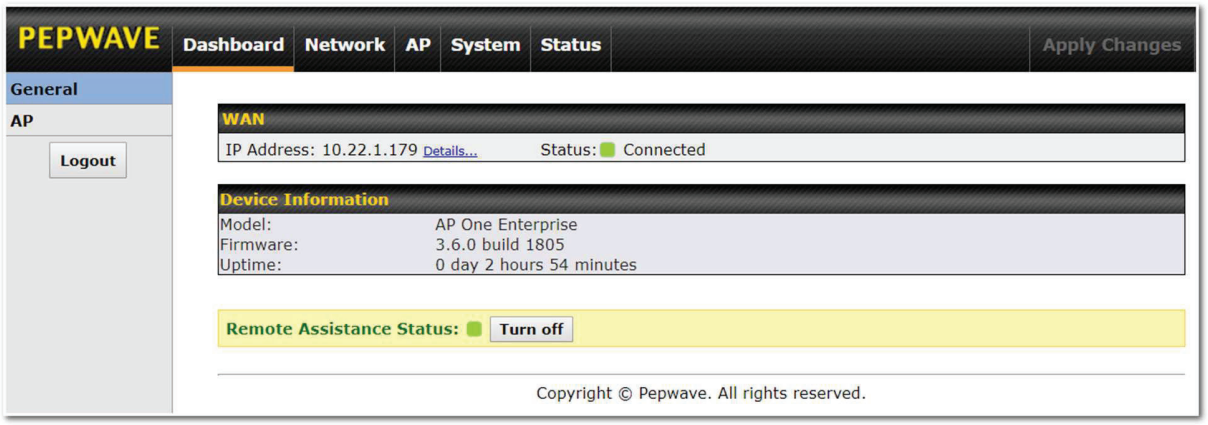
1. Connect the Ethernet port on the unit to the backbone network using an Ethernet cable. The port should auto sense whether the cable is straight-through or crossover.
2. Connect the power adapter to the power connector of the unit. Plug the power adapter into a power source.
3. Wait for the status LED to turn green.

4. Connect a PC to the backbone network. Configure the IP address of the PC to be any IP address between 192.168.0.4 and 192.168.0.254, with a subnet mask of 255.255.255.0.
5. Using your favourite browser, connect to https://192.168.0.3.
6. Enter the default admin login ID and password, **admin** and **public** respectively.
7. After logging in, the Dashboard appears. Click the **System** tab to begin setting up your access point.

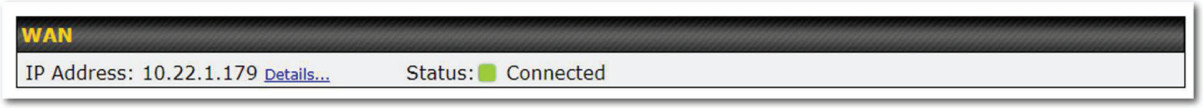


6 Dashboard

The **Dashboard** section contains a number of displays to keep you up-to-date on your access point's status and operation. Remote assistance can also be turned off here, if it has been enabled.

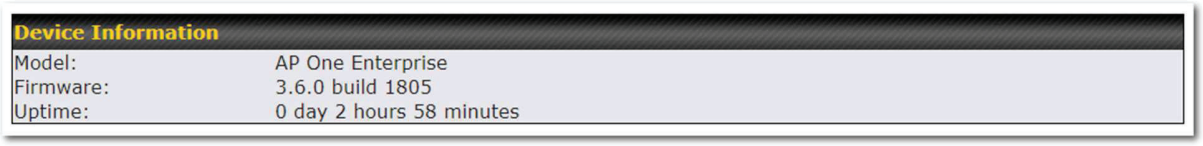


6.1 General



This section contains WAN status and general device information.

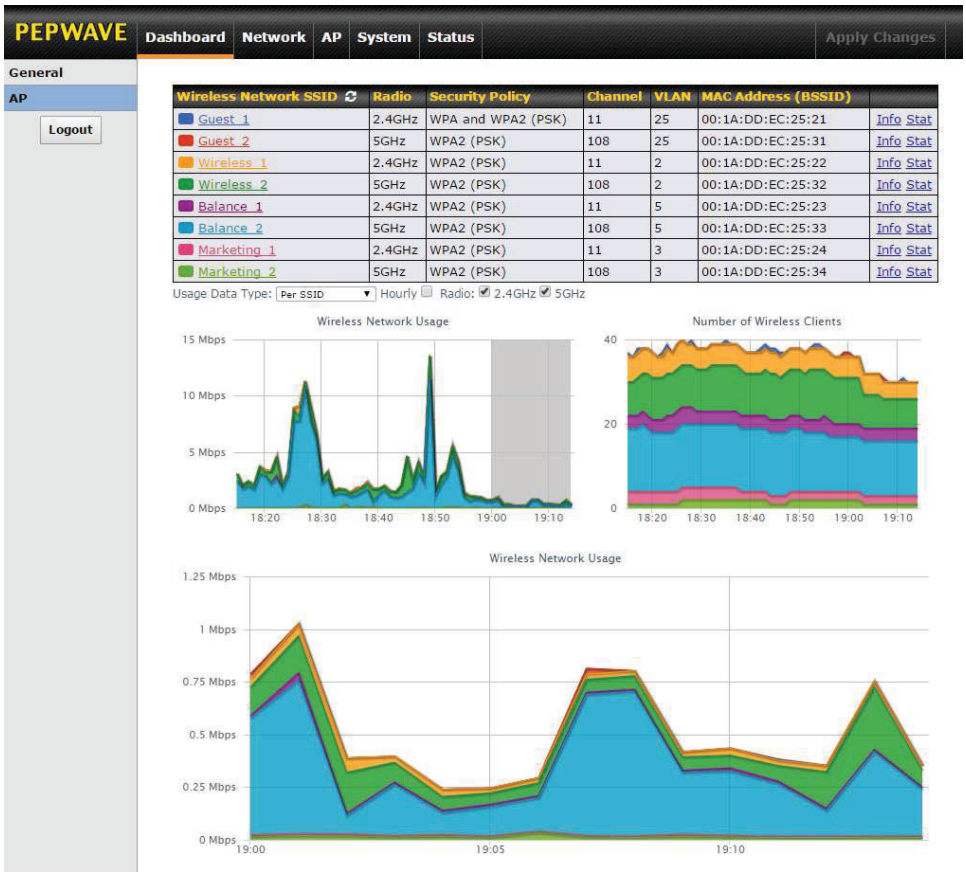
WAN	
IP Address	When your access point is connected to a WAN, this field displays the WAN IP address. For more information, click the **Details** link which shows connection type details
Status	This field displays the current WAN connection status.



Device Information	
Model	This field displays your access point's model number.
Firmware	The firmware version currently running on your access point appears here.
Uptime	This field displays your access point's uptime since the last reboot or shutdown.

6.2 AP

This section displays a variety of information about your wireless network.



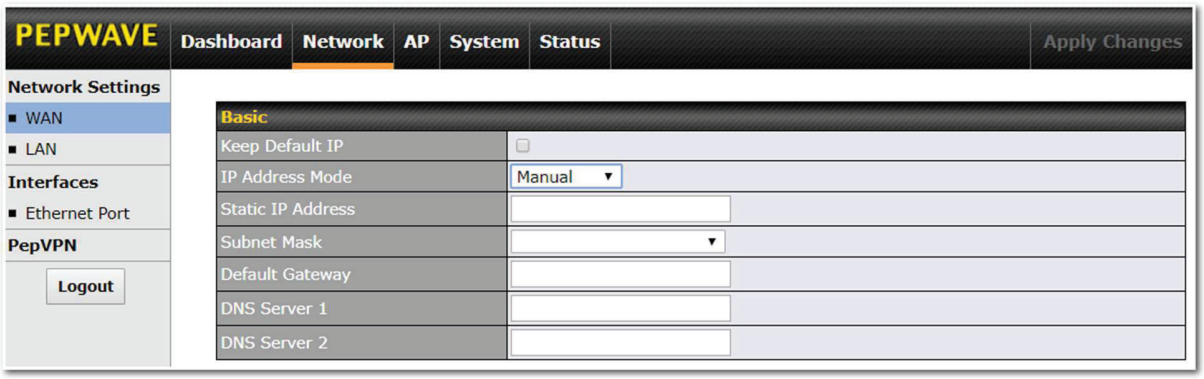
AP Status	
Wireless Network SSID	This field displays your access point's SSID.
Radio	The radio frequency currently used by your access point appears here. If you're using the AP One AC mini or the AP One In-Wall and have configured both radios, this displays both radios in use.
Security Policy	This field displays the security policy your access point is currently using. If you're using the AP One AC mini and have configured both radios, this displays channels in use for the 2.4GHz and 5GHz bands.
Channel	The channel currently used by your access point is displayed in this field.

VLAN	If your access point is using a VLAN ID for management traffic, it will appear here. A value of **0** indicates that a VLAN ID is not being used.
MAC Address (BSSID)	Your access point's MAC address appears here. If you're using the AP One AC mini and have configured both radios, this displays a MAC address for both the 2.4GHz and 5GHz radio.
Info	Click this link to display the following information panel: **INFO** Close Broadcast SSID: Enable Web Portal Login: Disable MAC Filter: None Bandwidth Control: Disable Layer 2 Isolation: Disable
Stat	Click this link to display the following statistics panel: **STAT** Close Packets Sent: 0 Bytes Sent: 0 Packets Received: 0 Bytes Received: 0
Usage Data Type	Select **Per SSID** or **AP Send / Recv** to determine the data displayed in the graphs below.
Hourly	Check this box to graph wireless network usage on an hourly basis.
Wireless Network Usage/Number of Wireless Clients	These graphs detail recent wireless network usage.

7 Network

The settings on the **Network** tab control WAN and LAN settings, as well as allow you to set up PepVPN profiles.

7.1 WAN

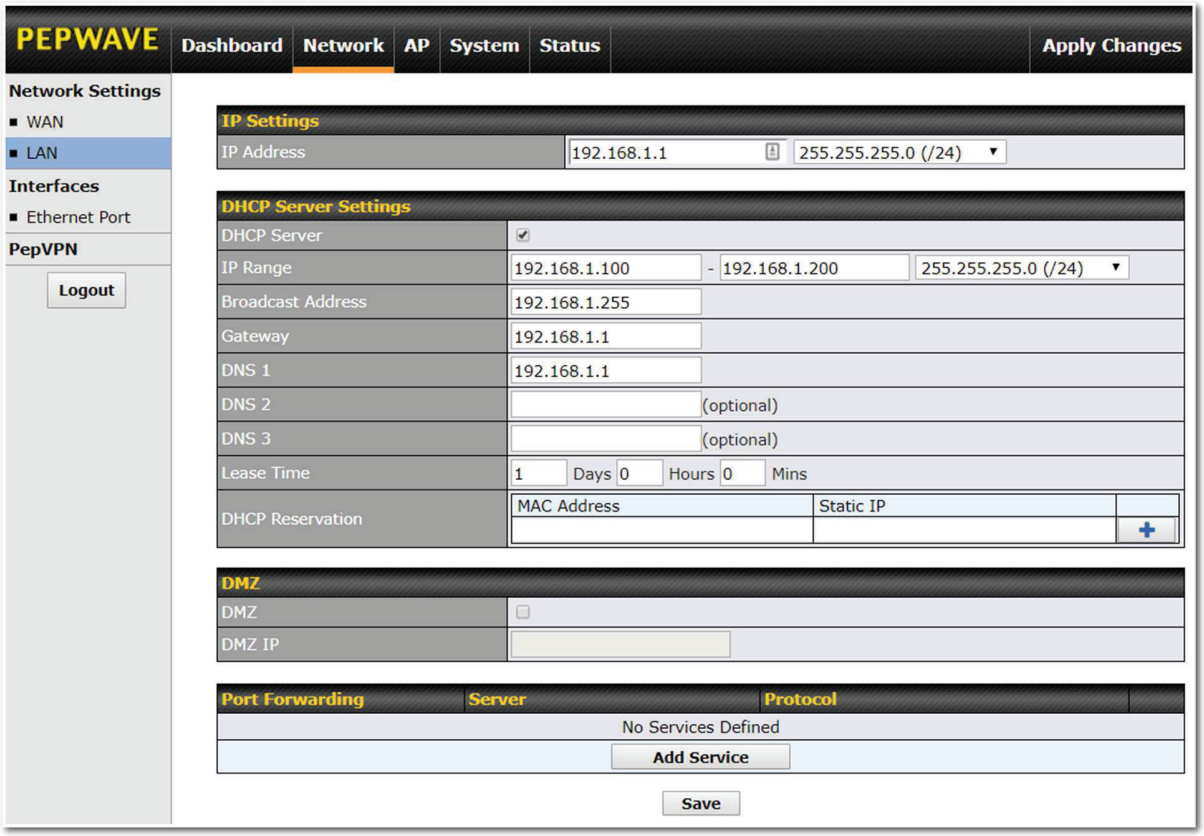


This section provides basic and advanced WAN settings.

Basic	
Keep Default IP	When enabled, this option maintains **192.168.0.3** as your access point's IP address.
IP Address Mode	**IP Address Mode** options are **Automatic** and **Manual**. In **Automatic** mode, the IP address of your access point is acquired from a DHCP server on the Ethernet segment. In **Manual** mode, a user-specified IP address is used for your access point, as described below.
Static IP Address / Subnet Mask	You can use these fields to specify a unique IP address that your access point will use to communicate on the Ethernet segment. This IP address is distinct from the admin IP address (192.168.0.3) on the Ethernet segment.
Default Gateway	Enter the IP address of the default gateway to the internet.
DNS Server	Enter the DNS server address that your access point will use to resolve host names.

7.2 LAN

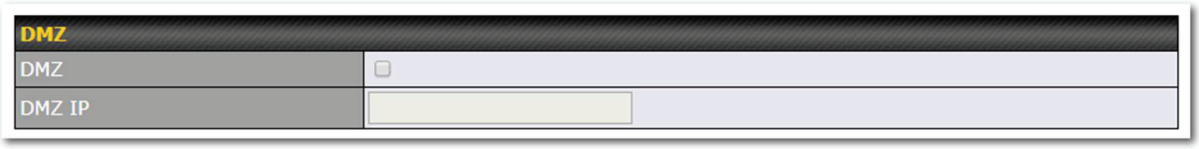
This section offers a variety of settings that affect your access point's operation on the LAN, such as settings for DHCP, DMZ, and port forwarding. Note that the following settings will be available only when your access point is operating in router mode.



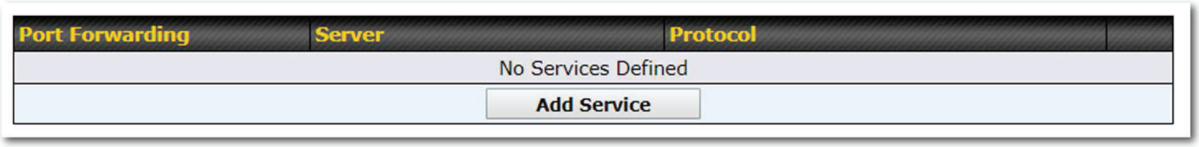
IP Settings	
IP Address	Enter the LAN IP address and subnet mask to assign to your access point on the LAN.

DHCP Server Settings	
DHCP Server	Check to enable the DHCP server feature of your access point. Enabling DHCP is the best option for most users. The following options will be enabled once you have checked and enabled the DHCP server.
IP Range	Enter the first and last IP addresses of the range of addresses that your access point will make available to DHCP clients. The default range is from **192.168.1.100** to **192.168.1.200**, with 24-bit subnet mask.

Broadcast Address	Enter the broadcast address that DHCP clients will use when communicating with the entire LAN segment. The default value is **192.168.1.255**.
Gateway	Enter the default gateway address that DHCP clients will use to access the internet. By default, this address will be the same as your access point's IP address on the LAN.
DNS 1/2/3	In **DNS 1**, enter the IP address of the primary DNS server offered to DNS clients or accept the default of **192.168.1.1**, which is your access point's address on the LAN. You can also specify up to two additional DNS servers to use when the primary server is busy or down.
Lease Time	Specify the length of time that an IP address of a DHCP client remains valid. When an address lease time has expired, the assigned IP address is no longer valid, and renewal of the IP address assignment is required. By default, this value is set to one day.
DHCP Reservation	To reserve certain addresses for specific clients, such as network printers, enter the device's MAC Address and a static IP to be assigned to the device. Click + to add the DHCP reservation. To delete a DHCP reservation, click ✖.

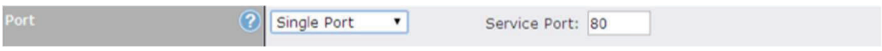


DMZ	
DMZ	Check this box to forward traffic sent to the WAN IP address to the DMZ IP address.
DMZ IP	Enter an IP address clients will use to connect to the DMZ.

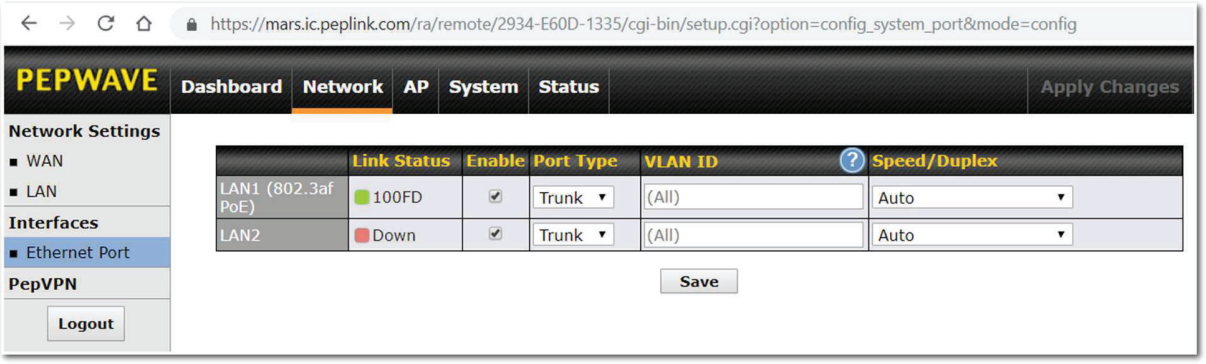


To create a port forwarding rule, first click the **Add Service** button, located in the **Port Forwarding** section..

Port Forwarding	
Service Name	Enter a name for the new port forwarding rule. Valid values for this setting consist of alphanumeric and underscore "_" characters only.
IP Protocol	The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service

	as TCP, UDP, ICMP, or IP. Traffic that is received by your access point via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g., HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.
Port	The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: **Single Port**, **Port Range**, **Port Mapping**  **Single Port**: Traffic that is received by your access point via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Server IP Address** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.  **Port Range**: Traffic that is received by your access point via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Server IP Address** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.  **Port Mapping**: Traffic that is received by your access point via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Server IP Address** setting. For example, with **IP Protocol** set to **TCP**, and Port set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on Port 80 is forwarded to the configured server via Port 88.
Server IP Address	Enter the LAN IP address of the server that handles requests for the forwarded service.

7.3 Interfaces > Ethernet Port

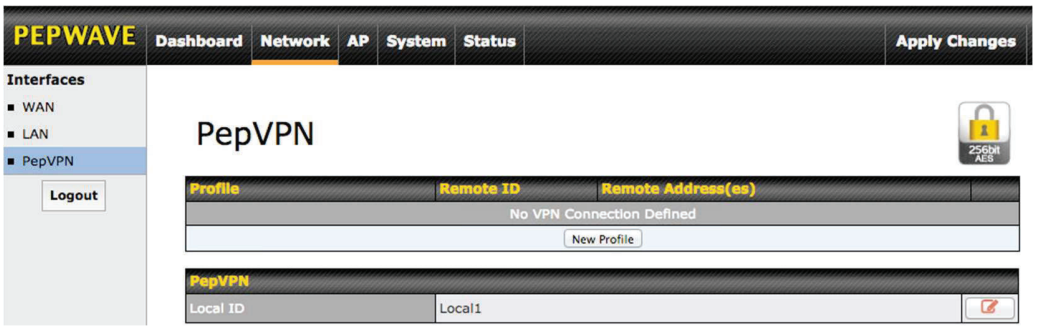


Assign one (or more) specific VLAN(s) to one of the LAN ports.
Configure the port as Access- or Trunk-port .

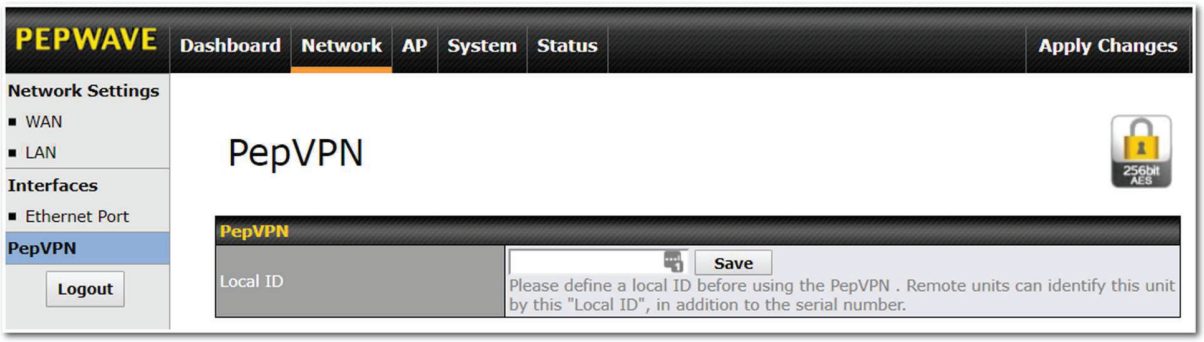
For Trunk port, enter multiple VLAN IDs for VLAN filtering (e.g. 1,5-8,10) or keep the field empty for accepting all VLANs.
For Access port, only a single VLAN ID is supported.

7.4 PepVPN

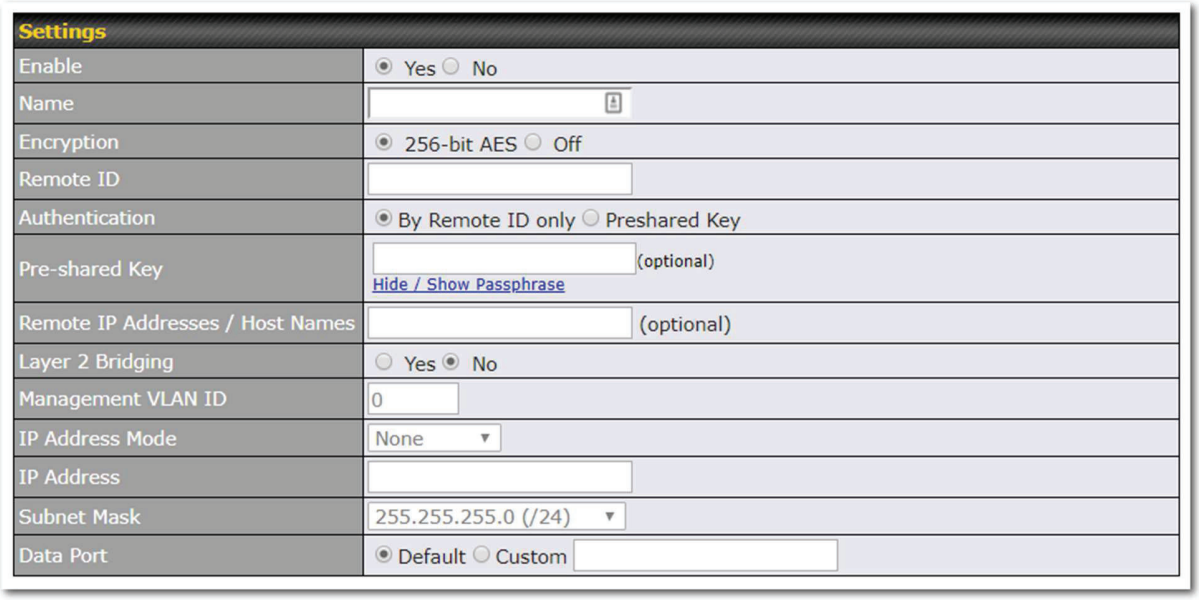
PepVPN securely connects one or more remote sites to the site running your access point.



To set up PepVPN, first give your site a local PepVPN ID. To modify an existing local ID, click 



Once you've specified a local ID, click the **New Profile** button to configure PepVPN.



PepVPN Profile Settings	
Enable	Check this box to enable PepVPN.
Name	Enter 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 ( ).
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 your access point 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 **By Remote ID Only** or **Preshared Key** to specify the method your access point 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 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. Click **Hide / Show Passphrase** to toggle passphrase visibility.
Remote IP Address / Host Names (Optional)	Optionally, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote client 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. With this field filled, your access point will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, your access point 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.
Layer 2 Bridging	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.
Management VLAN ID	This field specifies the VLAN ID that will be tagged to management traffic, such as AP-to-AP controller communication traffic. A value of 0 indicates that no VLAN tagging will be applied.
IP Address Mode	Choose **Automatic** or **Manual**. In automatic mode, your access point acquires an IP from a DHCP server on the Ethernet segment. In manual mode, your access point uses a user-specified IP address.
IP Address/Subnet Mask	When using manual IP addressing (above), enter an IP address and subnet mask in these fields.
Data Port	This field specifies the outgoing UDP port number for transporting VPN data. If **Default** is selected, port 4500 will be used by default. Port 32015 will be used if port 4500 is unavailable. If **Custom** is selected, you can input a custom outgoing port number between 1 and 65535.