PeP Link

# PePLink PolePoint

# 200BG / 400 BG

# User Manual

| | | |
|---|---|---|
| Document Revision | : | 1.2 |
| Firmware Version | : | 2.2 |
| Date | : | 2006-05-02 |

# Table of Content

# 1 Introduction

PePLink PolePoint is a carrier-grade 802.11b/g Wi-Fi access point. It is a powerful solution for building wholesale wireless networks. Each PePLink PolePoint is loaded with essential features such as Multiple SSID (virtual AP with distinct ESSID and BSSID), VLAN and a high-power antenna

One PePLink PolePoint can masquerade up to 16 different access points. Each virtual access point can have its own security policy (WEP, WPA, WPA2, 802.1x) and authentication mechanism. All these mean you can build your wholesale network much faster, easier and more cost-effective than ever before. PePLink PolePoint comes equipped with a high-power Wi-Fi transmitter (26 dBm for PolePoint 400BG, 23 dBm for PolePoint 200BG) which greatly enhances coverage and performance.

# 2 Feature Highlights

- Designed for wholesale wireless networks with multiple SSID and VLAN support
- Independent security policy and encryption mechanism per virtual AP.
- Hardware Watchdog increases service availability and guarantees firmware integrity ownership
- High-power output (up to 26 dBm) enhances coverage and lowers cost of ownership

# 3 Product Package

The following items are included in the PePLink PolePoint package:

1 x PePLink PolePoint

1 x Reverse-Polarity TNC Antenna

1 x Power Adapter (output: DC 5V)

1 x User’s Manual (this manual)

# 4 Installation

The PePLink PolePoint is acted as an Ethernet Bridge between the wireless and the Ethernet interface.  The network setup is typically like this:

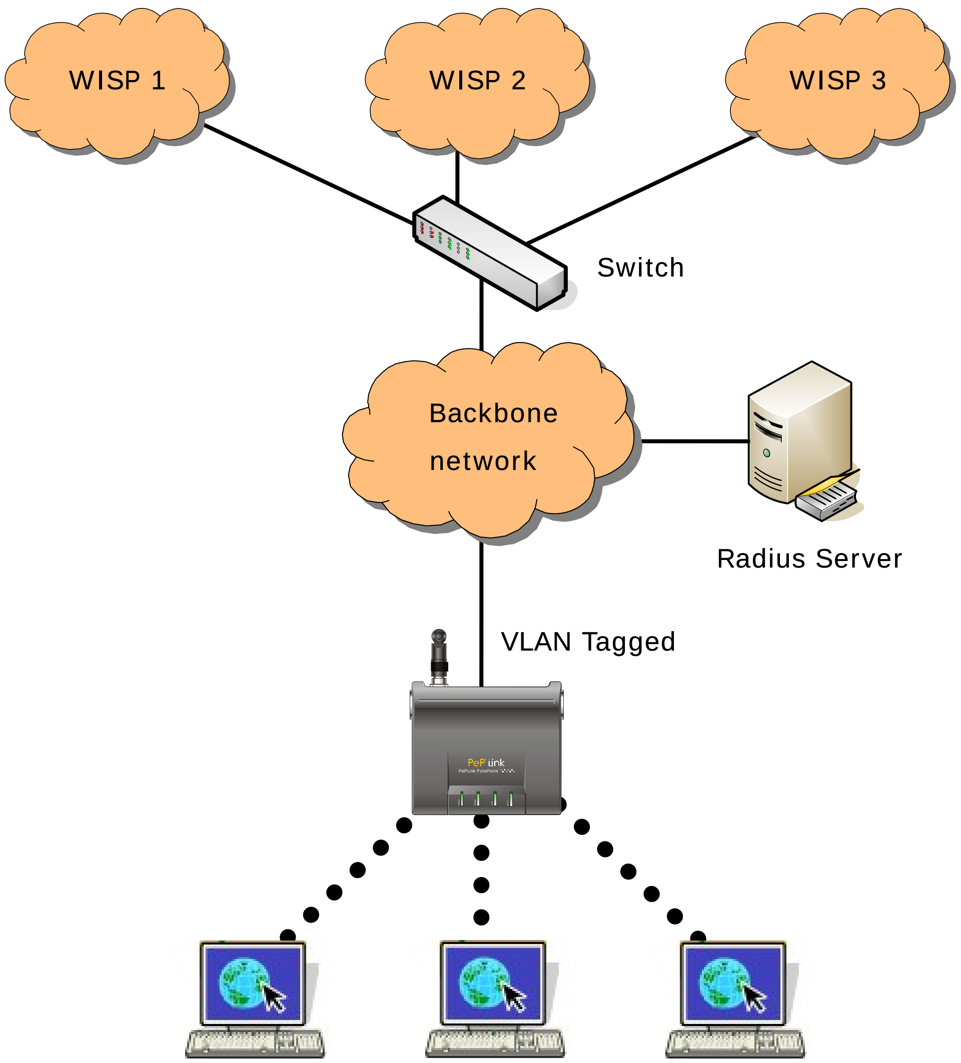
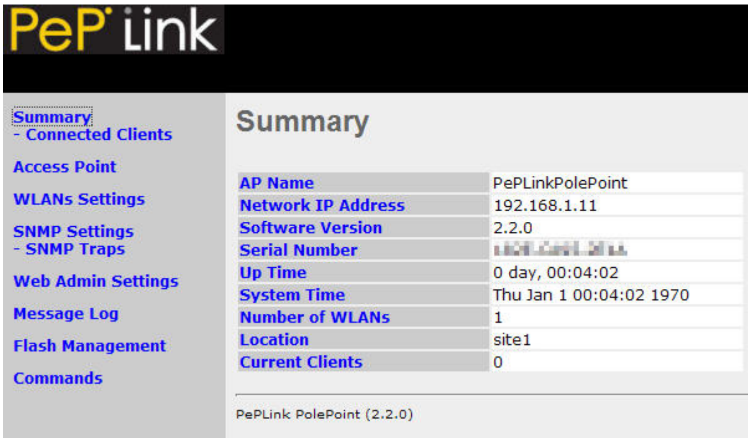


Figure 1

## 4.1 Procedures

- Attach the antenna to the PePLink PolePoint unit.
- Connect its LAN port with the backbone network using either a straight-through or cross-over cable.
- Plug the power adapter to a power socket and also the power input jack on the unit.
- Wait until the status LED turns green
- Connect a PC to the backbone network, configure its IP address to be any IP address between `192.168.0.4` to `192.168.0.254` with subnet mask of `255.255.255.0`
- Visit the URL `https://192.168.0.3/` (note that it is "HTTPS" based) using Microsoft Internet Explorer 5 or above, or Mozilla Firefox 1.0 or above. Accept all prompted questions
- You will be prompted for admin login ID and password. By default, they are "`admin`" and "`public`".
- You will see a page like this:



Summary

| | |
|---|---|
| AP Name | PePLinkPolePoint |
| Network IP Address | 192.168.1.11 |
| Software Version | 2.2.0 |
| Serial Number | [redacted] |
| Up Time | 0 day, 00:04:02 |
| System Time | Thu Jan 1 00:04:02 1970 |
| Number of WLANs | 1 |
| Location | site1 |
| Current Clients | 0 |

PePLink PolePoint (2.2.0)

Figure 2

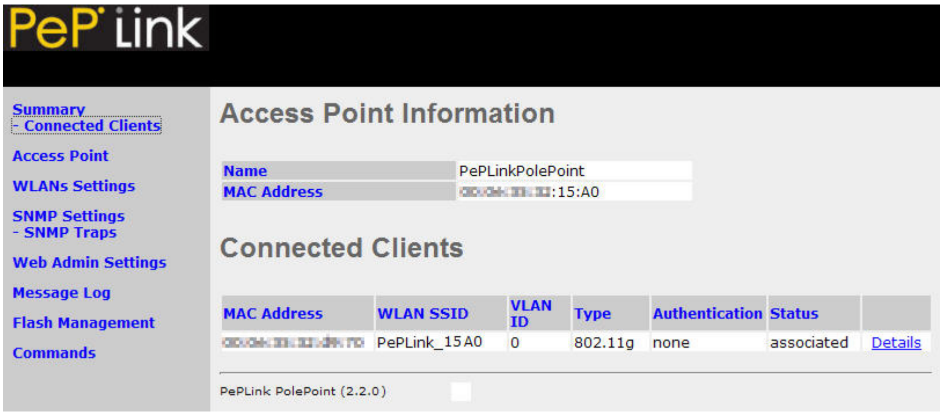
- You may now start to configure the PePLink PolePoint

> Tips: If you are unable to access the page, please refer to the Appendix A - FAQ for how to restore the settings to factory defaults.

## 4.2 Quick Start

With the default settings, an SSID is predefined, which is "PePLink_XXXX" where XXXX is the last 4 digits of the MAC Address. It has both encryption and VLAN tagging off. It bridges the wireless clients to the Ethernet port. So you may now access the Ethernet by associating to it with a Wi-Fi client.

After associated, you should see the session information shown on the PePLink PolePoint's web admin interface under the section "– Connected Clients".



Access Point Information

| | |
|---|---|
| Name | PePLinkPolePoint |
| MAC Address | [redacted]:15:A0 |

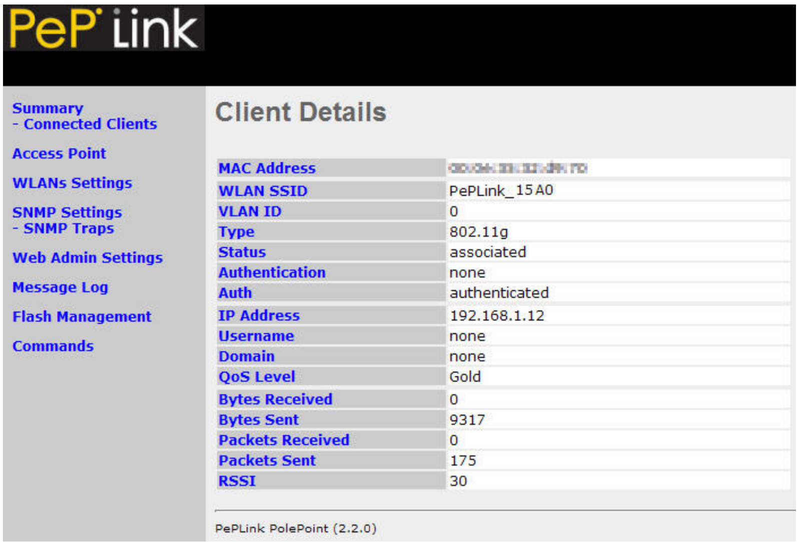
Connected Clients

| MAC Address | WLAN SSID | VLAN ID | Type | Authentication | Status | |
|---|---|---|---|---|---|---|
| [redacted] | PePLink_15A0 | 0 | 802.11g | none | associated | Details |

PePLink PolePoint (2.2.0)

Figure 3

When you click on the link "Details", you should see the client's details.



Client Details

| | |
|---|---|
| MAC Address | [redacted] |
| WLAN SSID | PePLink_15A0 |
| VLAN ID | 0 |
| Type | 802.11g |
| Status | associated |
| Authentication | none |
| Auth | authenticated |
| IP Address | 192.168.1.12 |
| Username | none |
| Domain | none |
| QoS Level | Gold |
| Bytes Received | 0 |
| Bytes Sent | 9317 |
| Packets Received | 0 |
| Packets Sent | 175 |
| RSSI | 30 |

PePLink PolePoint (2.2.0)

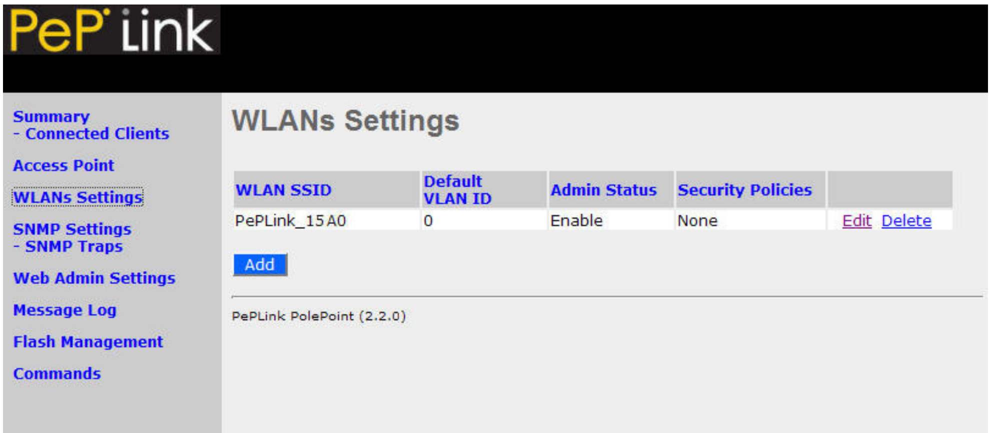
Figure 4

# 5 Configurations

## 5.1 WLANs Settings

Most of Wi-Fi related parameters are configurable in the “WLANs Settings” page accessible from the left side bar. The page is like this:

The column “WLAN SSID” shows the virtual APs’ SSID.



WLANs Settings

| WLAN SSID | Default VLAN ID | Admin Status | Security Policies | |
|---|---|---|---|---|
| PePLink_15A0 | 0 | Enable | None | Edit Delete |

PePLink PolePoint (2.2.0)

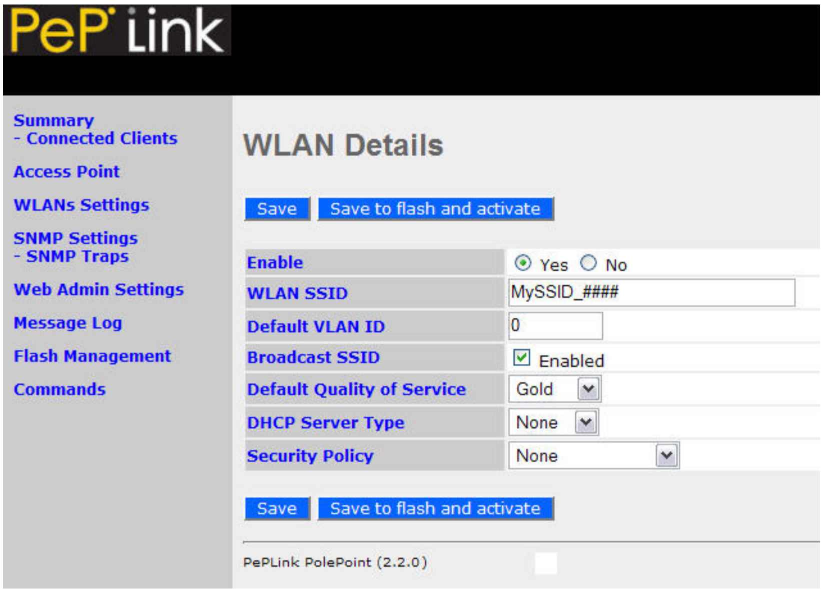
Figure 5

“Default VLAN ID” is the VLAN ID to be tagged on all outgoing packets (leave from the LAN port) generated from the virtual AP. The Default VLAN ID will be overridden if per-user VLAN ID is specified in the radius server’s authentication reply when 802.1x is enabled.

Admin Status shows the virtual AP is enabled or disabled.

Security Policies show the wireless authentication and encryption method configured.

To modify a virtual AP's setting, click the link "Edit" on the right of a WLAN SSID. Then you should see:



WLAN Details

| | |
|---|---|
| Enable | ● Yes ○ No |
| WLAN SSID | MySSID_#### |
| Default VLAN ID | 0 |
| Broadcast SSID | ☑ Enabled |
| Default Quality of Service | Gold |
| DHCP Server Type | None |
| Security Policy | None |

PePLink PolePoint (2.2.0)

Figure 6

**Enable**: select Yes to enable the virtual AP, select No to disable the virtual AP. The default is Yes.

**WLAN SSID**: the virtual APs' SSID. It is the SSID to be scanned by Wi-Fi clients. This value is case insensitive. The substring "####" in the SSID will be replaced by the last four digits of the BSSID / MAC address. By default, the value is "PePLink_####".

**Default VLAN ID**: the VLAN ID to be tagged on all outgoing packets (leave from the LAN port) generated from the virtual AP. If per-user VLAN ID is specified in radius server's authentication reply when 802.1x is enabled, the Default VLAN ID will be overridden. Possible value is from 0 to 4096. The default value is 0.

**Broadcast SSID**: to choose whether the virtual AP's ESSID to be able to be scanned by Wi-Fi clients or not. Note that BSSID (virtual AP's MAC address) cannot be hidden from scan. To associate with it, the client should specify the correct ESSID upon association. This is enabled by default.

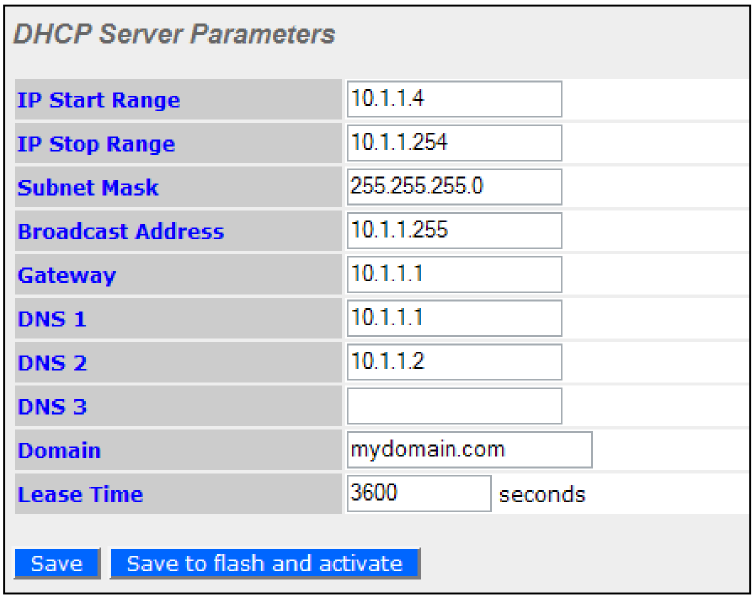
**Default Quality of Service**: the 802.1p QoS value to be marked to all outgoing packets (leave from the LAN port) generated from the virtual AP. If per-user or per-domain QoS value is specified, the Default Quality of Service value will be overridden. Possible values are Gold, Silver and Bronze.

**DHCP Server Type**: To choose to enable DHCP server, to enable DHCP relay or to just pass DHCP requests to the Ethernet port.

- None: DHCP requests will not be processed but will be passed to the Ethernet.

- Relay: the PolePoint will relay DHCP requests to a specified DHCP Server. This option could avoid broadcast messages being propagated on the backbone network.

- Server: the PolePoint will allocate and offer IP addresses locally.



DHCP Server Parameters

| | |
|---|---|
| IP Start Range | 10.1.1.4 |
| IP Stop Range | 10.1.1.254 |
| Subnet Mask | 255.255.255.0 |
| Broadcast Address | 10.1.1.255 |
| Gateway | 10.1.1.1 |
| DNS 1 | 10.1.1.1 |
| DNS 2 | 10.1.1.2 |
| DNS 3 | |
| Domain | mydomain.com |
| Lease Time | 3600 seconds |

Figure 7

If the type “Relay” is chosen, the DHCP Server IP address will be prompted.

If the type “Server” is chosen, the following information will be prompted:

**IP Start and Stop Range**: the IP address range to be offered to DHCP clients

**Subnet Mask**: the subnet mask the DHCP clients to be used

**Broadcast Address**: the broadcast address the DHCP clients to be used

**Gateway**: the default routing gateway the DHCP clients to be used

**DNS 1**, **2** and **3**: the DNS servers' IP address to be offered to the DHCP clients

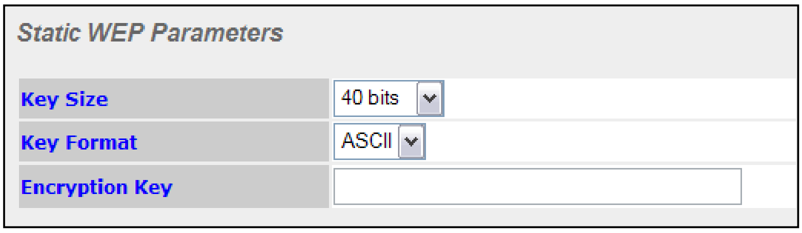
**Domain**: the domain name the clients to be used

**Lease Time**: the leased of DHCP records

**Security Policies:** to configure the wireless authentication and encryption method. Available options are: None, Static WEP, 802.1x and WPA.

**None**: to disable encryption. Data are sent over the air without any protection

**Static WEP**: to enable pre-shared WEP key encryption. Authentication is not supported by this method. The security level of this mode is known to be weak. When this is set, the following parameters have to be entered.



Static WEP Parameters

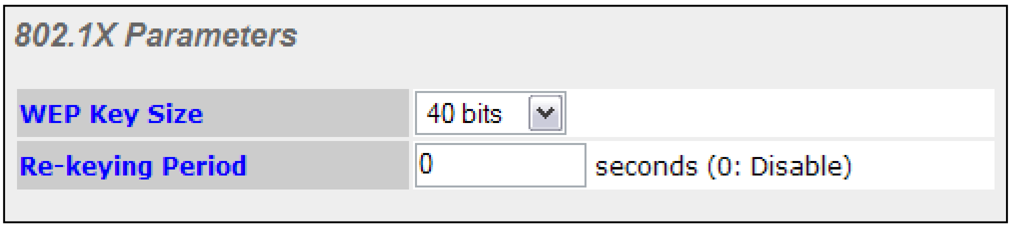
| | |
|---|---|
| Key Size | 40 bits |
| Key Format | ASCII |
| Encryption Key | |

**Key Size**: 40bits and 104 bits

**Key Format**: ASCII and HEX

**Encryption Key**: For ASCII format, key length is either 5 or 13. For HEX format, key length is either 10 or 26.

**802.1x**: to enable 802.1x radius-based authentication with dynamic WEP key. When it is set, the following parameters have to be entered:



802.1X Parameters

| | |
|---|---|
| WEP Key Size | 40 bits |
| Re-keying Period | 0 seconds (0: Disable) |

Figure 9

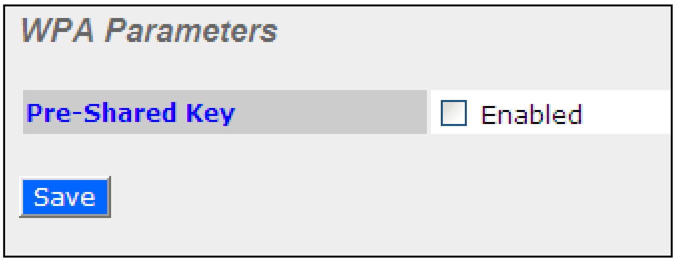
**Key Size**: 40bits and 104 bits

**Broadcast Key Index**: 1, 2, 3 or 4

**Re-keying Period**: Re-keying every this amount of seconds. The default is 14400 secs (4 hours). A value of 0 means disable re-keying.

**WPA-TKIP / WPA-AES:CCMP**: to enable WPA, WPA-PSK, WPA2 or WPA2-PSK. WPA-TKIP is for WPA and WPA-PSK. WPA-AES:CCMP is for WPA2 and WPA2-PSK

For WPA and WPA2, 802.1x radius-based authentication with TKIP encryption method will be used. The Pre-Shared Key option should be disabled. This method's security level is known to be very high



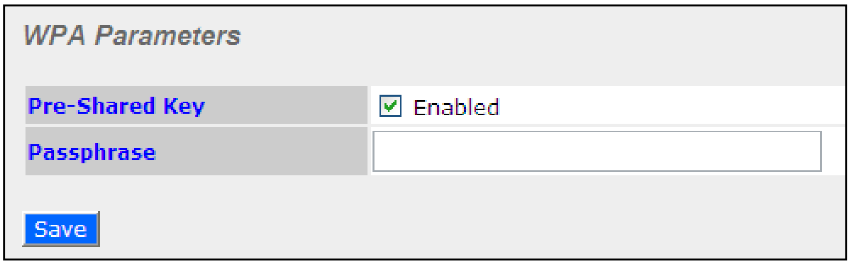
WPA Parameters

| | |
|---|---|
| Pre-Shared Key | □ Enabled |

Figure 10

For WPA-PSK and WPA2-PSK, a Pre-Shared Key, or Pass phrase, will be used for data encryption and authentication. "Pre-Shared Key" option should be enabled. Key length must be 8 to 63 characters. This method's security level is known to be high and is higher than Static WEP key.

After finished to modify the settings, press the “Save” button to make the changes effective.



WPA Parameters

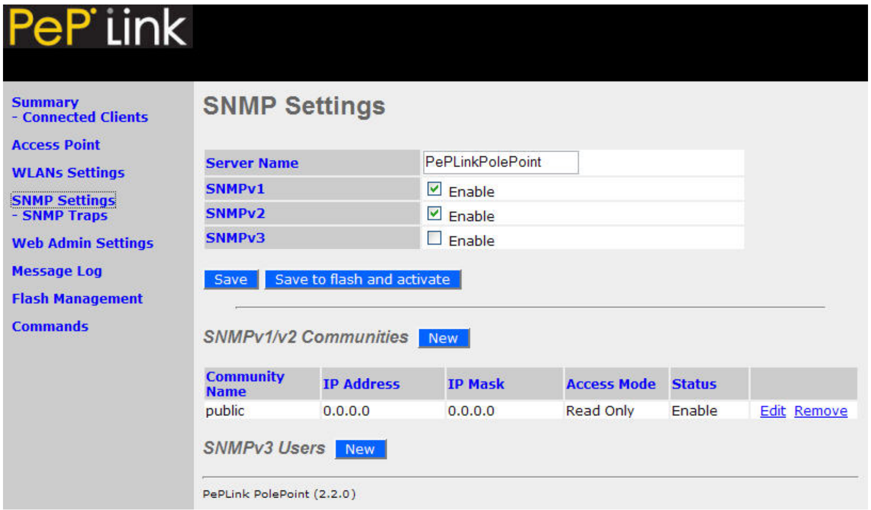
| | |
|---|---|
| Pre-Shared Key | ☑ Enabled |
| Passphrase | |

Figure 11

## 5.2 SNMP Settings

The PePLink PolePoint supports SNMP v1, v2 and v3. The SNMP Server Settings page allows you to configure the SNMP server settings.

When you click the “SNMP Settings” link on the left side bar, you will see this page:



SNMP Settings

| | |
|---|---|
| Server Name | PePLinkPolePoint |
| SNMPv1 | ☑ Enable |
| SNMPv2 | ☑ Enable |
| SNMPv3 | □ Enable |

SNMPv1/v2 Communities

| Community Name | IP Address | IP Mask | Access Mode | Status | |
|---|---|---|---|---|---|
| public | 0.0.0.0 | 0.0.0.0 | Read Only | Enable | Edit Remove |

SNMPv3 Users

PePLink PolePoint (2.2.0)

Figure 12

**Server Name**: the name to identify this SNMP server

**SNMP v1, v2, v3**: to enable or disable the support of each version of SNMP protocols.

You can control the access right by adding SNMPv1/v2 Communities and SNMPv3 Users.

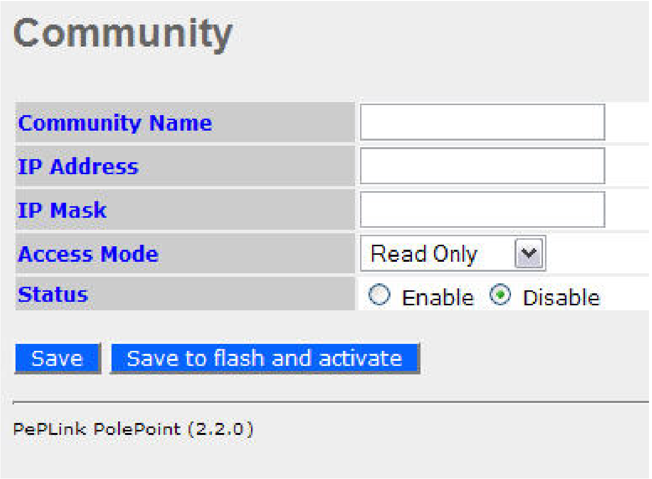
### 5.2.1 SNMPv1/v2 Communities

**Community Name**: the “password” for getting or setting SNMP values.

**IP Address and IP Mask**: the allowed subnet address who can access the SNMP server

**Access Mode**: choose the community name. Either “Read Only” or “Read & Write”.

**Status**: Enable or disable this community.



Community

| | |
|---|---|
| Community Name | |
| IP Address | |
| IP Mask | |
| Access Mode | Read Only |
| Status | ○ Enable ● Disable |

PePLink PolePoint (2.2.0)

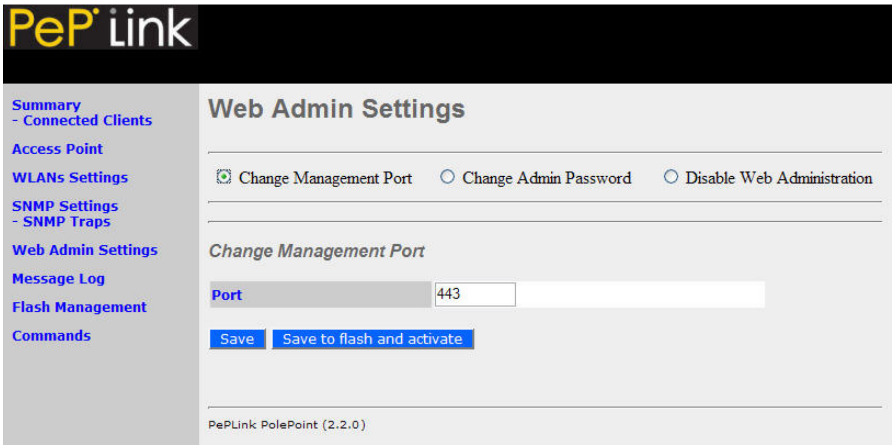
Figure 13

## 5.3 Web Admin Settings

In the Web Admin Settings section, you are allowed to change the management web site's parameters.

### 5.3.1 Change Management Port

Port: The TCP port number of the secure web server. The default is 443.



Web Admin Settings

● Change Management Port ○ Change Admin Password ○ Disable Web Administration

*Change Management Port*

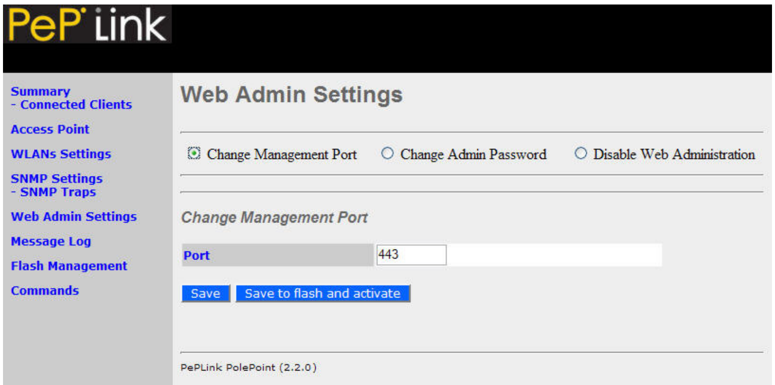
| | |
|---|---|
| Port | 443 |

PePLink PolePoint (2.2.0)

Figure 14

### 5.3.2 Change Admin Password

New Password/New Password (Retype): to enter the new password for entering this Web Admin Interface.



Web Admin Settings

● Change Management Port ○ Change Admin Password ○ Disable Web Administration

*Change Management Port*

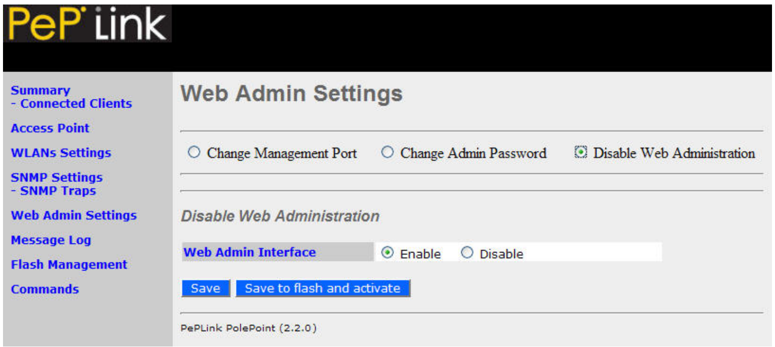
| | |
|---|---|
| Port | 443 |

PePLink PolePoint (2.2.0)

Figure 15

### 5.3.3 Disable Web Administration

The web administration interface can be disabled here. It can be turned on again by using SNMP.



○ Change Management Port ○ Change Admin Password ● Disable Web Administration

Disable Web Administration

Web Admin Interface ● Enable ○ Disable

Figure 16

## 5.4 Message Log

System message log is available. It is a good source of system status during troubleshooting. The message log page can be accessed from the "Message Log" section.

## 5.5 Commands

This section allows you to perform some system commands.

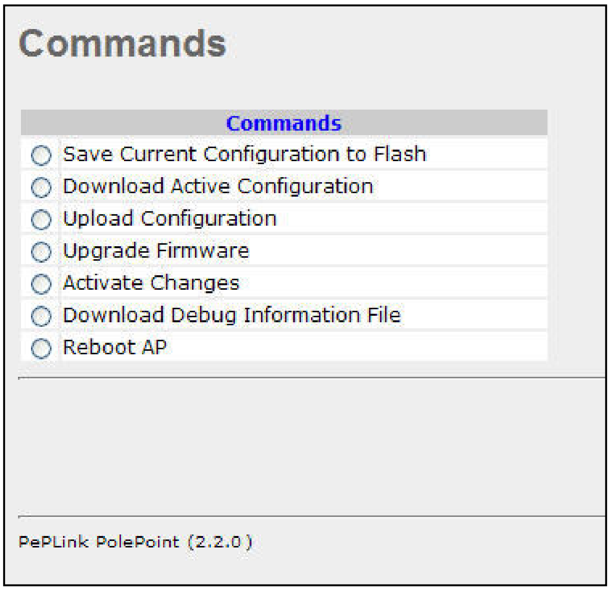

Commands
Commands
○ Save Current Configuration to Flash
○ Download Active Configuration
○ Upload Configuration
○ Upgrade Firmware
○ Activate Changes
○ Download Debug Information File
○ Reboot AP
PePLink PolePoint (2.2.0 )

Figure 16

- **Save Current Configuration to Flash** – The changes made are not saved to the flash. The configurations will be lost after reboot. To make the changes persistence across reboot, you can choose Save Current Configuration to Flash

- **Download Active Configuration** – Select this command to download the active configuration for backup purpose

- **Upload Configuration** – Select this command to upload a backed up configuration file. After uploaded, changes are not effectively immediately.

- **Upgrade Firmware** – Select this command to upload a firmware file for upgrading the system software. Upgrading the firmware requires a reboot.

- **Activate Changes** – This is for activating saved changes. But note that the configurations are not saved to the flash memory.

- **Download Debug Information File** – If you find some problems that need to get technical support from PePLink, please send along with a debug file with your e-mail request. This option is for you to download some debugging information. With the file, PePLink officers are able to get the running status of the PolePoint unit.

- **Reboot AP** – This option is for rebooting the PolePoint unit.

# 6 Per-session based VLAN tagging

The PePLink PolePoint supports VLAN tagging on per-client-session basis when 802.1x authentication is performed. The VLAN ID can be passed from the radius server.

The VLAN ID to be set on a client session is passed from the radius server in a vendor attribute in the Access-Accept response called "`Tunnel-Private-Group-ID`".

When such attribute is present, the per-SSID based default VLAN ID setting will be overwritten.

**Sample Radiator Setting**

This is a sample Radiator "users" file for enabling the attribute:

```
login_id User-Password=abc123
Tunnel-Type=1:VLAN,
Tunnel-Medium-Type=1:Ether_802,
Tunnel-Private-Group-ID=1:2,
Service-Type = Framed-User
```

The number "2" on the fourth line is the VLAN ID to be set to the user

# 7 Appendix A - FAQ

**Q. How can I restore the system to factory settings? I cannot find such option in the web admin interface.**

A. You can reset the system to factory settings by following this procedure:

1 Power on the unit, wait for 1 minute until the Status LED turns green

2 Press and hold the reset button at the rear pane for 5 seconds, then release

3 The Status LED will blink and then the unit will automatically reboot

4 Wait for 1 minute until the Status LED turns green

Now, the PolePoint has been restored to factory settings. By default the unit will acquire an IP address from DHCP server.

# 8 Appendix B – Radius Server Setup

The system has been proved to work with Radiator version 3.9, using EAP-TTLS protocol.

PePLink PolePoint settings:

Set the virtual Access Point’s authentication protocol to WPA-AES:CCMP.

Radiator configuration:

```
AuthPort        1812
AcctPort        1813
LogDir          /var/log/radius
DbDir           /etc/radiator
Trace          4
<Client DEFAULT>
        Secret  testing123
        DupInterval 0
</Client>
<Realm DEFAULT>
        <AuthBy FILE>
                Filename /etc/radiator/users
                EAPType TTLS
                EAPTLS_CAFile /etc/1x/cert/demoCA/cacert.pem
                EAPTLS_CertificateFile /etc/1x/cert/cert-srv.pem
                EAPTLS_CertificateType PEM
                EAPTLS_PrivateKeyFile /etc/1x/cert/cert-srv.pem
                EAPTLS_RandomFile /dev/urandom
                EAPTLS_PrivateKeyPassword whatever
                EAPTLS_MaxFragmentSize 1000
                AutoMPPEKeys
        </AuthBy>
        AcctLogFileName /etc/1x/radius_detail
</Realm>
```

# 9 Appendix C – Professional Installation

Outdoor PolePoint 200/400BG requires professional installation. It is not to be installed by the general public. You must be a Professional Installer. You must follow Part 15 of the FCC rules, and specifically Part 15.203 pertaining to antenna requirements of an intentional radiator.

If you are not a professional installer, STOP. Do not proceed any further with the installation.

Note: Installing the Outdoor PolePoint 200/400BG requires setting the antenna power, which required professional training. The installer must be trained to perform this configuration.

You must be a Professional Installer to connect an antenna to the Outdoor PolePoint 200/400BG, as specified in the Federal Communications Commission's part 15.203 for Radio Frequency Devices. The Outdoor PolePoint 200/400BG uses a single low-loss Female N-type antenna connector. You will need a Male N-type antenna to attach your antenna.

You will need a specialized RJ45 crimping device and RJ-45 connectors to prepare and connect LAN cable to backbone network for Data and POE power. Run the un-terminated RJ-45 cable through the Moisture proof Gland, terminate a RJ-45 connector, and connect to board. Hand tighten down on the gland nut until a good seal is provided around the Ethernet cable.

After the Ethernet is connected, close and seal the enclosure lid with the mounting screws provided. Please tighten with a screwdriver to make a positive seal.