MultiAP 700g

Professional Installation Manual

Dated June 27, 2006

Table of Contents

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B & Class C digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Installation only by Professional Installers:

MultiAP 700G requires professional installation. It is not to be installed by the general public. It is not available through retail or mail order. 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. A 2 dBi or less dipole antenna must be used.

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

1 Introduction

The ValuePoint Networks MultiAP 700g is a MultiSSID/VLAN 802.11b/g Rugged Access point. It is a powerful solution for building wireless networks. Each MultiAP 700g is loaded with essential features such as Multiple SSID (virtual AP), VLAN, and advanced security options.

One MultiAP 700g can act as up to 8 independent virtual access points. Each virtual access point can have its own security policy (WEP, WPA, WPA2, 802.1x) and authentication mechanism. This means you can build your network much faster, easier and more cost-effective than ever before. The MultiAP 700g comes equipped with a high-power Wi-Fi transmitter (25 dBm) which greatly enhances coverage and performance.

2 Feature Highlights

- Designed for outdoor 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 25 dBm) enhances coverage and lowers cost of installation

3 Product Package

MultiAP 700g is provided in the standard configuration that requires onsite final assembly and installation only by a Professional Installer. Special tools must be purchased separately and are required to professionally install the 700g such as

- RJ-45 cable crimping tool for connecting the Ethernet cable for data and power.
- Spectrum analyzer or RF power meter for measuring RF output power.

The following items are included in the MultiAP 700g package:

- N-female connector for 2 dBi or less dipole antenna, compliant with Part 15.203 (ordered separately)
- IP68 rated Gland for Ethernet cable.
- Six screws for mounting lid.
- Six M6 mount holes for pole mount
- 1 x Professional Installer's Manual on CD (this manual)

The latest Firmware is pre-loaded on 700g. Firmware updates are available at http://www.valuepointnet.com/DOWNLOADS. You must be a Professional Installer to

access the Downloads Page.

4 MultiAP 700g Overview

4.1 LEDs on board (hidden inside enclosure)

Power	OFF – Power off ON (Green) – Power on
Status	OFF –Initializing system Red – Booting up or busy Orange – Power on self test Green – Ready state
Ethernet	OFF – Port is not connected ON – Port is connected Blinking - Data is transferring
Wireless	On – No data transfer Blinking - Data is transferring

LEDs are visible only prior to assembly, and following disassembly. Professional Installers only can view the LEDs. They are not visible during normal product operation.

4.2 Connectors:

Commercial Grade N-bulkhead Antenna Connector	Specialized N-female bulkhead connector for connecting the antenna cable. Only professional installers may install or service the antenna, and only antennas complying with Part 15.203 may be used. Antennas are not available through retail or mail order. A 2 dBi or less dipole antenna must be used.
LAN	Supports one 10/100BaseT Ethernet connection, normally to be connected to back haul network, and for POE power. This connection is sealed inside the enclosure, and available only to professional installers.
Reset	Concealed behind set screw, specialized equipment required to access it. Only a professional installer may access the reset button. Hold it for 5 sec. to restore the system to factory defaults (see Appendix)

INSTALLATION TO BE DONE ONLY BY PROFESSIONAL INSTALLERS:

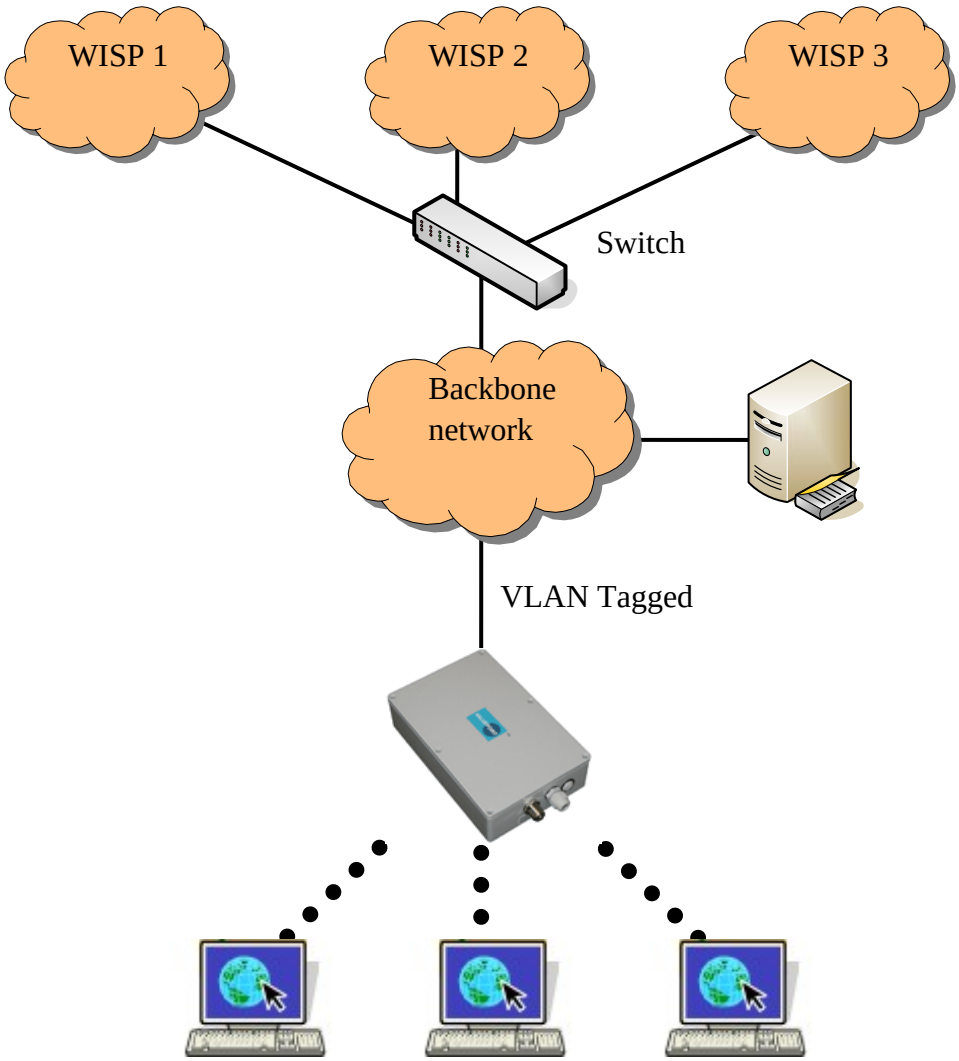
You must be a Professional Installer to connect an antenna to the MultiAP 700g, as specified in the Federal Communications Commission's Part 15.203 for Radio Frequency Devices.

The 700g uses a single low-loss **Female N-type** antenna connector. You will need a Male

N-type antenna or Male antenna extension cable (pigtail) to attach your 2 dBi or less dipole antennas to the access point. You must comply with Part 15.203 of the FCC rules.

5 Professional Installation

The MultiAP 700g acts as an Ethernet Bridge between the wireless and the LAN interface. The network setup is typically like this:



5.1 Procedures:

- Connecting antennas

You must be a Professional Installer to connect an antenna to the MultiAP 700g, as specified in the Federal Communications Commission's Part 15.203 for Radio Frequency Devices.

The 700g uses a single low-loss **Female N-type** antenna connector. You will need a specialized Male N-type antenna or Male antenna extension cable (pigtail) to attach your antennas to the access point. Your antenna must comply with Part 15.203, and must be 2 dBi or less dipole antenna.

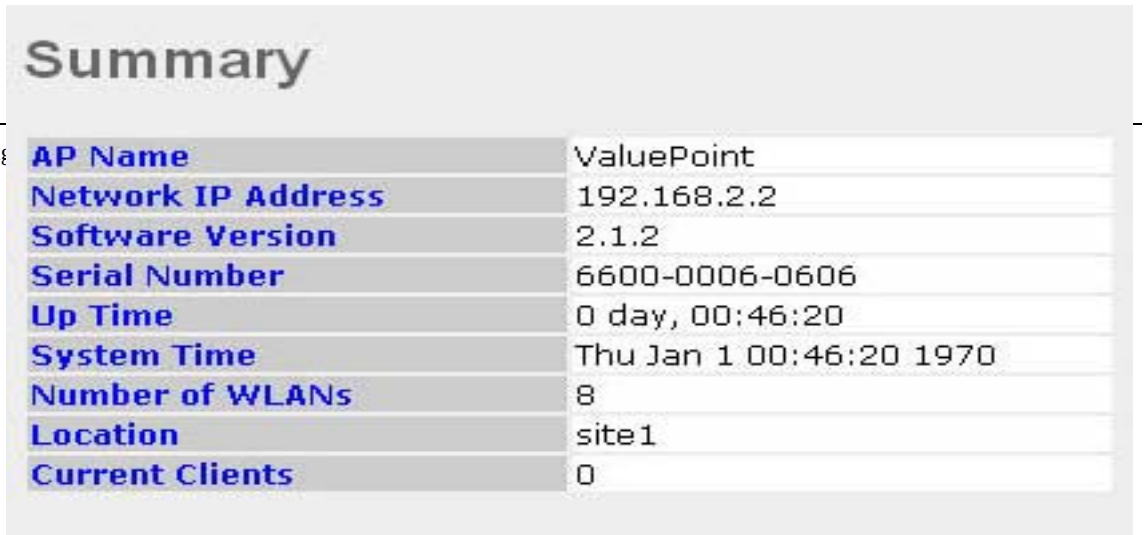
- Connecting LAN and Power

You will need a specialized RJ-45 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. If POE power is not being provided, remove the #2 hole plug and install the optional Moisture proof Gland, run the power cord through the gland, and connect to DC jack on board.

- Closing and Sealing the Enclosure

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

- 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`
- Open browser to `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 the Summary page.

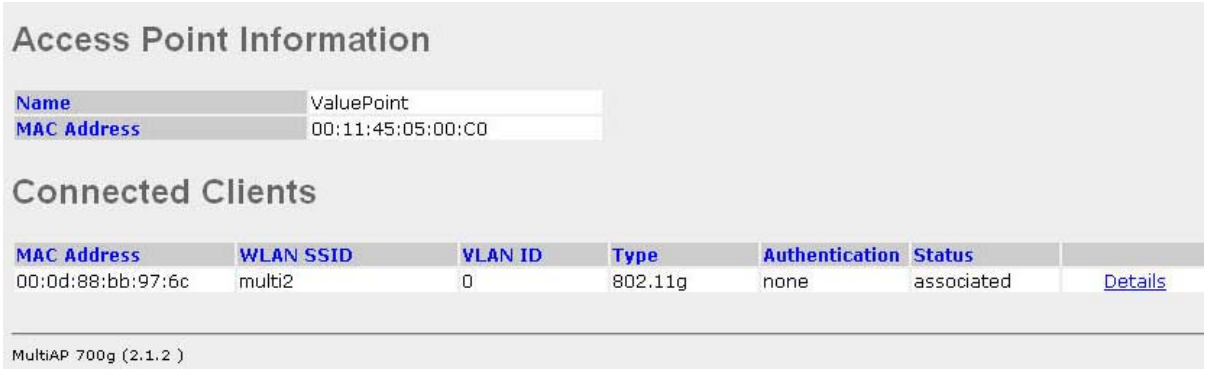


- You may now start to configure the MultiAP 700g

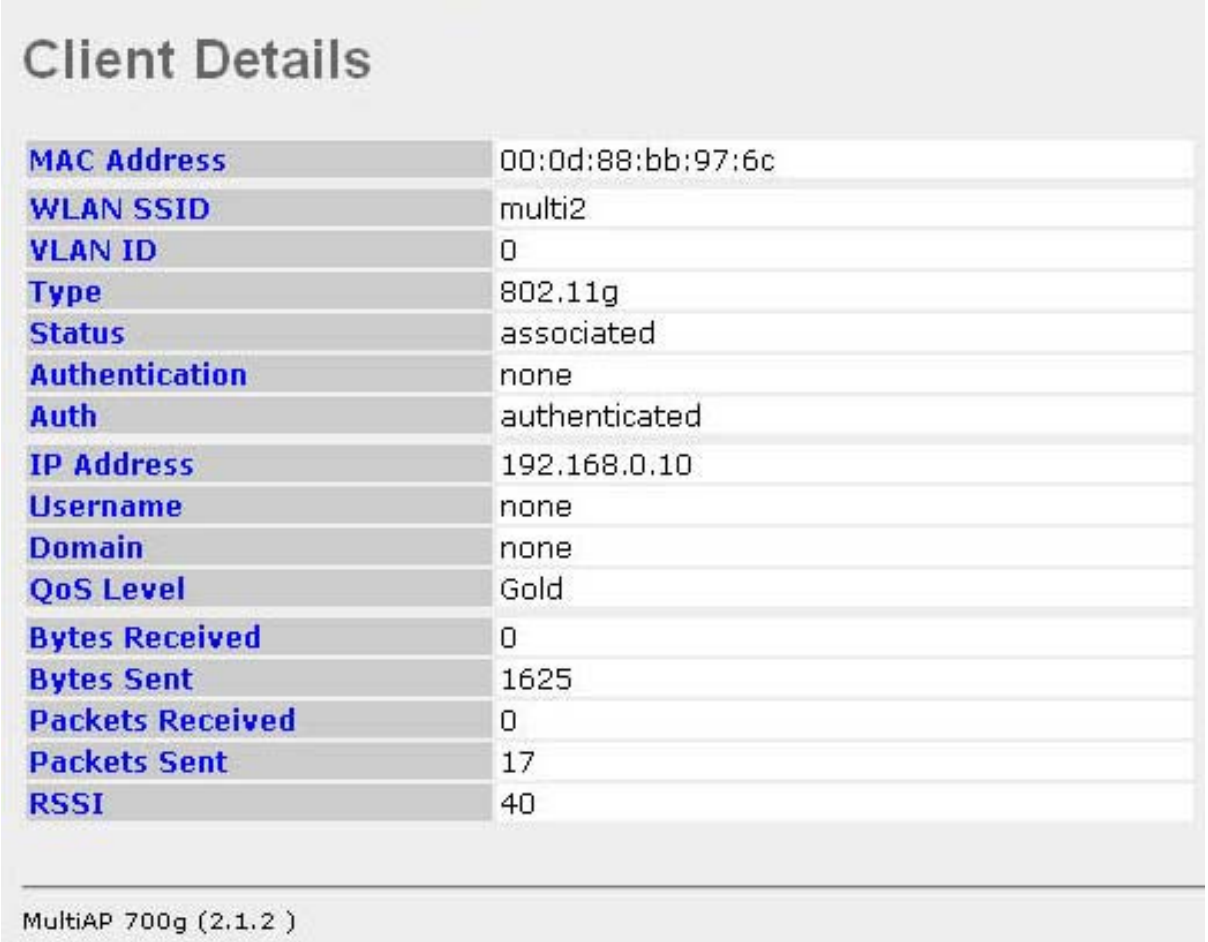
5.2 Quick Start

With the default settings, an SSID is predefined, which is "`wireless`". 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 associating, you should see the session information shown on the MultiAP 700g's web admin interface

under the section “Summary – Connected Clients”.

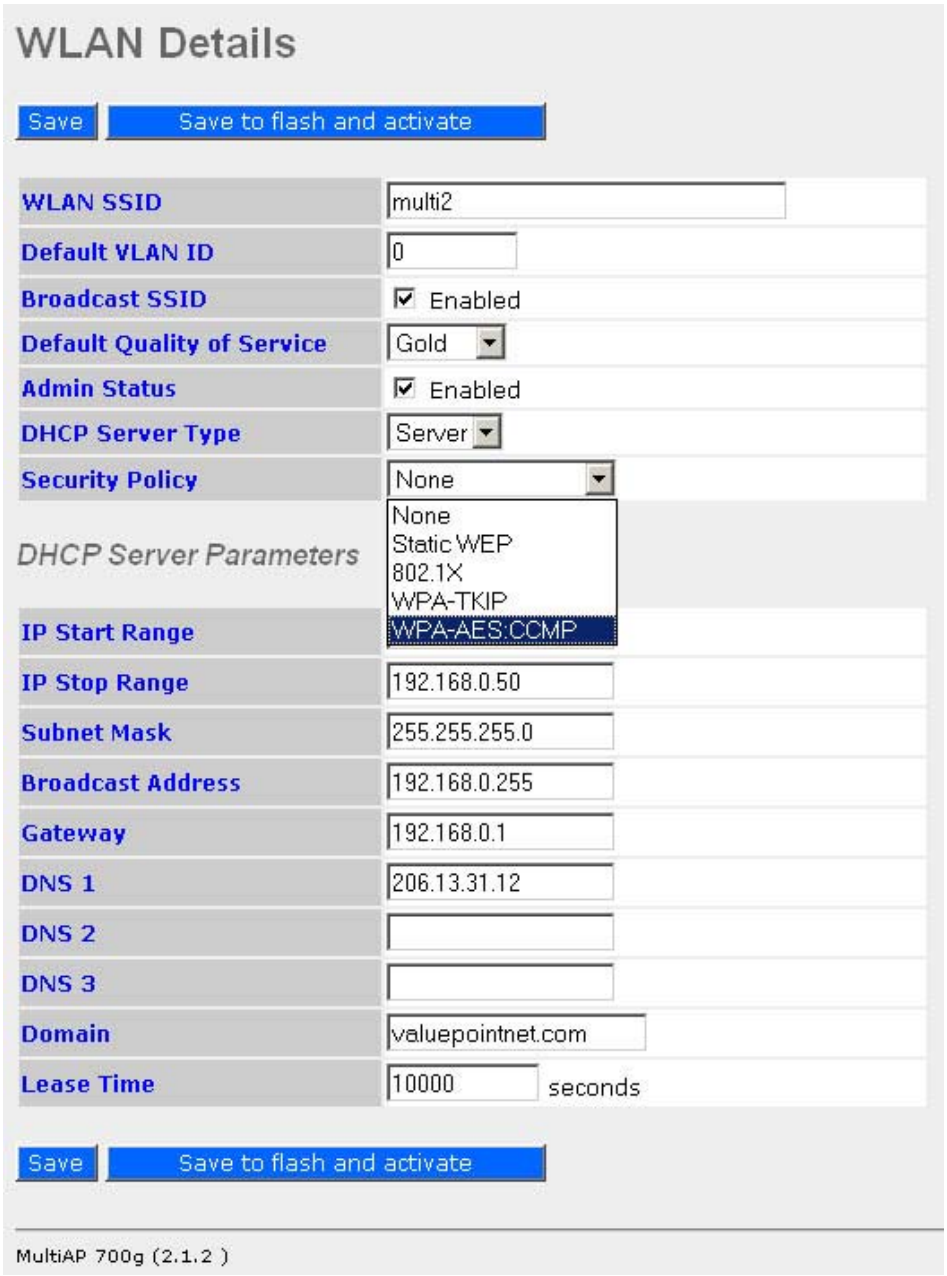


When you click on the link “Details”, you will see the client’s details.



5.3 WLANs Settings

Most of Wi-Fi related parameters are configurable in the “WLANs Settings”.



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

“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.

To modify a virtual AP’s setting, click the link “Edit” on the right of a WLAN SSID.

WLAN SSID: the virtual APs’ SSID. It is the SSID to be scanned by Wi-Fi clients. This value is case insensitive.

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.

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.

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.

Admin Status: to enable or disable the virtual AP.

DHCP Server Type: To choose to disable the DHCP service, to enable DHCP relay or to enable DHCP server. If "Relay" is chosen, the DHCP Server IP address has to be entered. If "Server" is chosen, DHCP server parameters will be requested.

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.

Key Size: 40bits and 104 bits

Figure 1

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 rotation. When it is set, the following parameters have to be entered:

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 sec. (4 hours). A value of 0 disables re-keying.

WPA-TKIP / WPA-AES:CCMP: to enable WPA, WPA-PSK, WPA2 or WPA-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 very high

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.

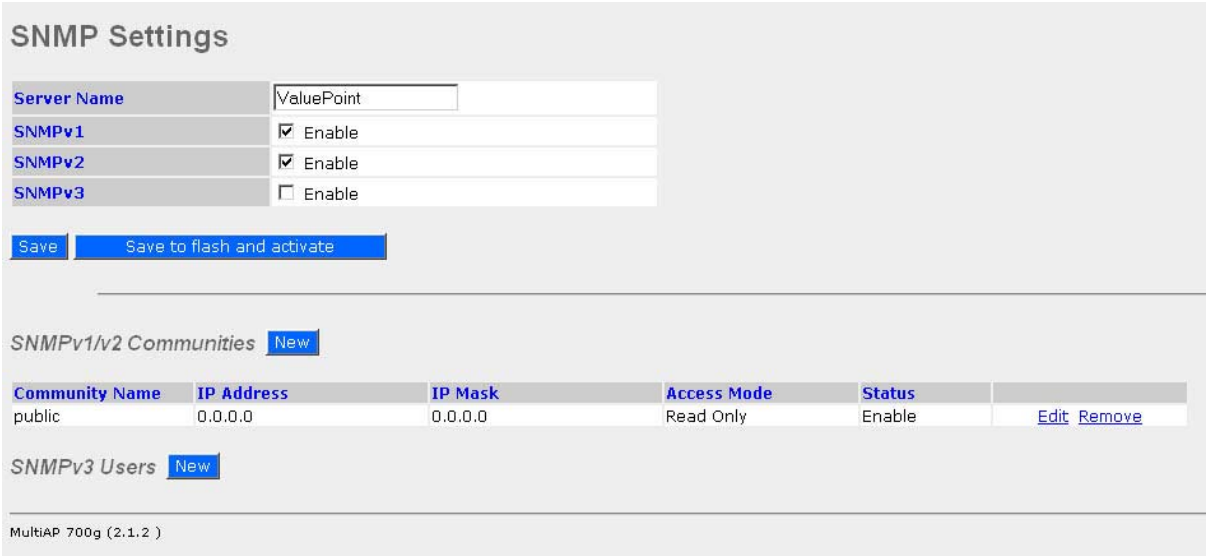
This method's security level is higher than Static WEP.

After modifying the settings, press the "Save" button to make the changes effective.

5.4 SNMP Settings

The MultiAP 700g 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 these parameters:



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 change the access rights by adding SNMPv1/v2 Communities and SNMPv3 Users.

5.4.1 SNMPv1/v2 Communities

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

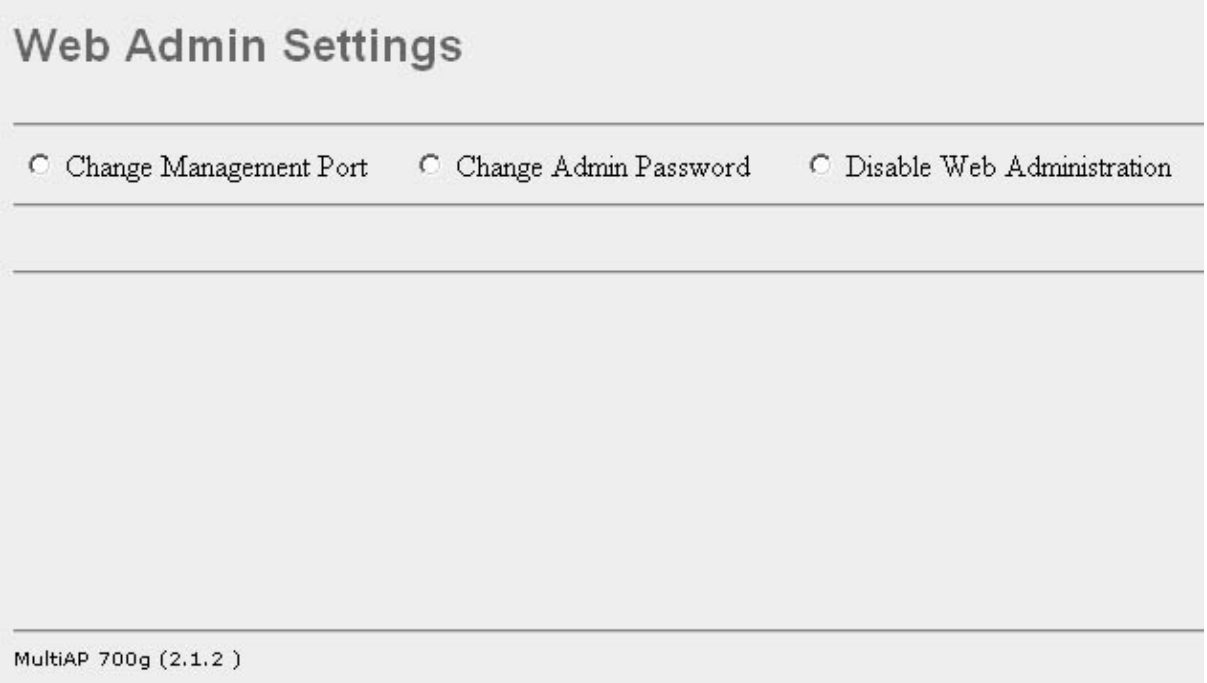
IP Address and IP Mask: the allowed subnet address who can access the SNMP server

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

Status: Enable or disable this community.

5.5 Web Admin Settings

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



5.5.1 Change Management Port

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

5.5.2 Change Admin Password

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

5.5.3 Disable Web Administration

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

5.6 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.

5.7 Commands

This section allows you to Save Current Configuration to the Flash, Download Active Configuration, Activate the Changes and Reboot the MultiAP 700g.

Before saving configurations to the flash, the configurations will be lost after the MultiAP 700g is rebooted.

Appendix A - FAQ

Q. How can I restore the system to factory settings? I cannot find this 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 of the unit 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 board has been restored to factory settings. By default the unit will acquire an IP address from a DHCP server.

Q2. How can I get shell access to the MultiAP 700g?

A2. The SSH remote shell service is enabled by default. You can use an SSH v2 client to connect to the MultiAP 700g using the default admin IP 192.168.0.3 (see section 5.2 Quick Start). Default login name and password are "`root`" and "`public`".

Appendix B – Radius Server Setup

The system has been tested with Radiator version 3.9, using EAP-TTLS protocol.

MultiAP 700g settings:

Set the virtual Access Point's authentication protocol to 802.1x.

Sample 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_MaxFragmentSiz 000

                AutoMPPEKeys
        </AuthBy>
        AcctLogFileName /etc/1x/radius_detail
</Realm>
```

