Tube-2HQP

2.4GHz 802.11b/g/n Outdoor AP/CPE

User Guide

TABLE OF CONTENTS

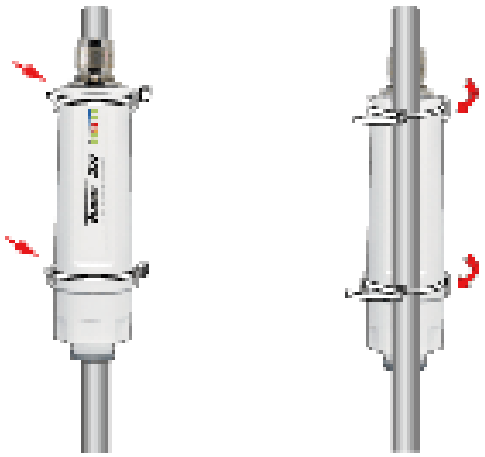
INTRODUCTION

The Tube-2HQP is a 1X1 MIMO IEEE 802.11b/g/n wireless outdoor AP/CPE which support data ratesup to 150Mbps. It is rain and splash proof when install in upright position. TUBE-2HQPalso supports N type connector and 802.3at/afStandard PoE for simplify installation.

HARDWARE INSTALLATION

◆□How to assembly the unit

◆□How to tie the strap on the pole



INITIAL CONFIGURATION

The TUBE-2HQP, outdoor 2.4GHz AP/CPE offers a user-friendly web-basedmanagement interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface usinga web browser, such as Internet Explorer (version 6.0 or above).

CONNECTING TO THE LOGIN PAGE

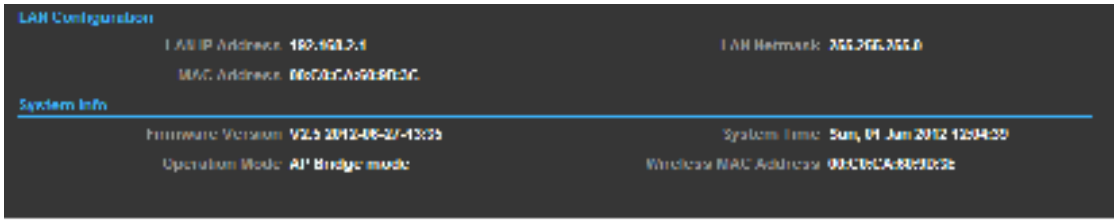
It is recommended to make initial configuration changes by connecting aPC directly to the TUBE-2HQP's Ethernet port. The TUBE-2HQPhas a default IP address of 192.168.2.1 and a subnetmask of 255.255.255.0. You must set your PC IP address to be on thesame subnet as the TUBE-2HQP(that is, the PC and TUBE-2HQPaddresses must both start 192.168.2.x).To access the TUBE-2HQP's management GUI interface, followthese steps:

1. Use your web browser to connect to the management interface usingthe default IP address of 192.168.2.1.

2. Log into the interface by entering the default username "admin" andpassword "admin," then click OK.

STATUS PAGE

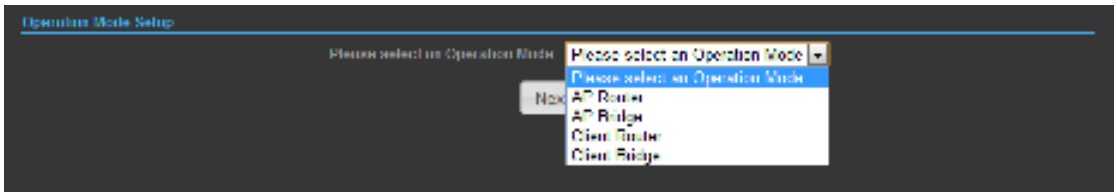
After logging in to the web interface, the Status page displays. The Homepage top-menu-bar shows the Status, Easy Setup, Advanced and Language.



EASY SETUP

The Easy Setup is designed to help you to configure the basic settings required to get the TUBE-2HQPup and running. There are only a fewbasic steps you need to set up theTUBE-2HQPto get the connection.

Click on Easy Setup to bring up the wizard



If you want to configure a router connection, please select **AP Router**

If you want to configure to an access point, please select **AP Bridge**

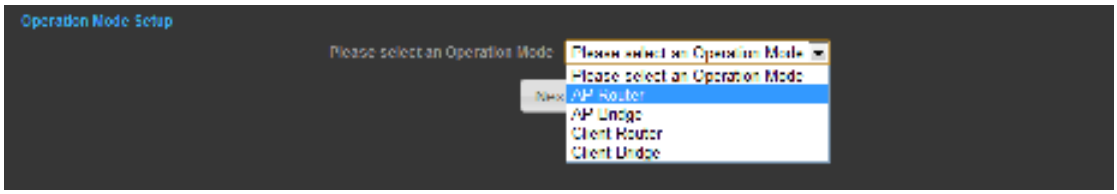
If you want to configure to WISP, please select **Client Router**

If you want to configure to WiFi client, please select **Client Bridge**

OPERATION MODE–AP ROUTER

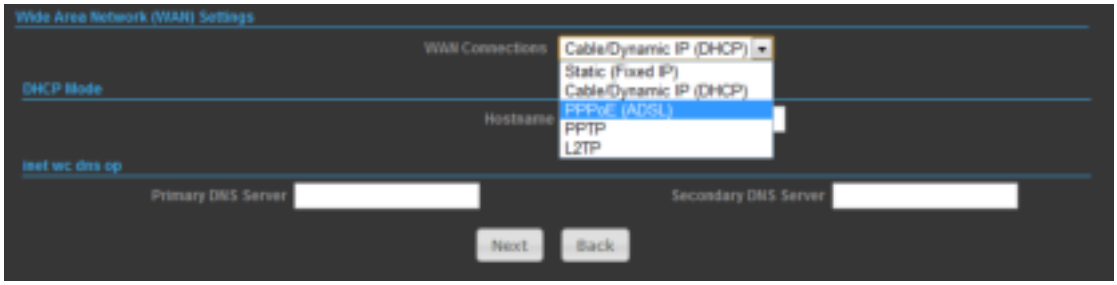
Choose menu "Easy Setup" and select AP Router if you want to configure a router connection.

NOTE: The Ethernet port will convert into WAN port requiring you to configure your CPE via WLAN.



SETTINGS – PPPOE(ADSL)

1) Select PPPoE to be assigned automatically from an Internet service provider (ISP) through a DSL modem using Point-to-Point Protocol over Ethernet (PPPoE).



2)

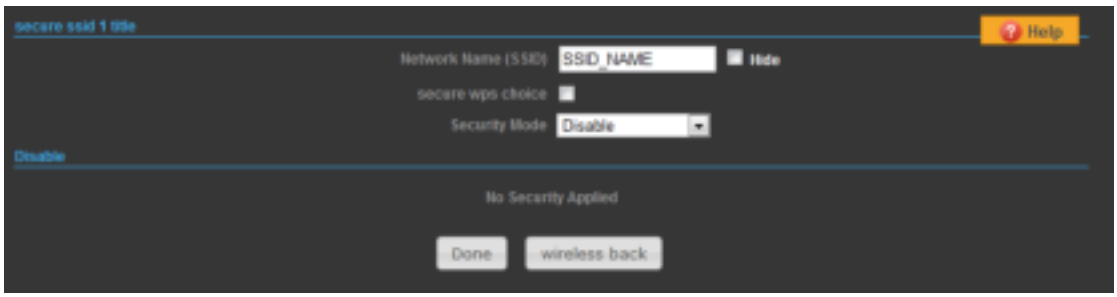
◆□**User Name** — Sets the PPPoE user name for the WAN port.

◆□**Password** — Sets a PPPoE password for the WAN port.

◆□**Verify Password** — Prompts you to re-enter your chosen password.

◆□**Operation Mode —** Enables and configures the keep alive time and configures the on-demand idle time.

3)



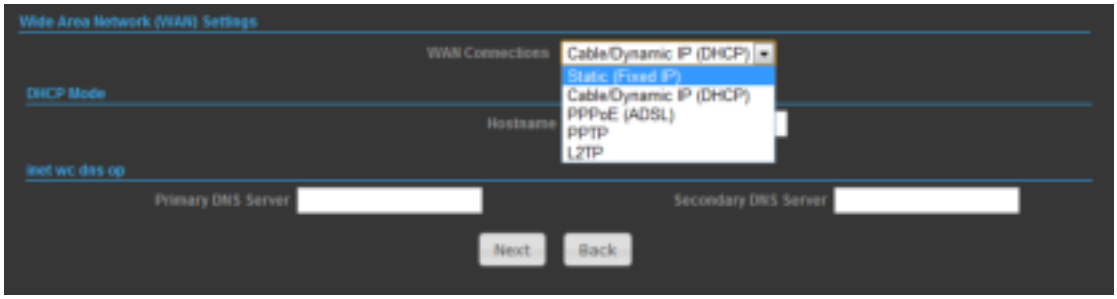
Security Setup

NetworkName (SSID)—SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

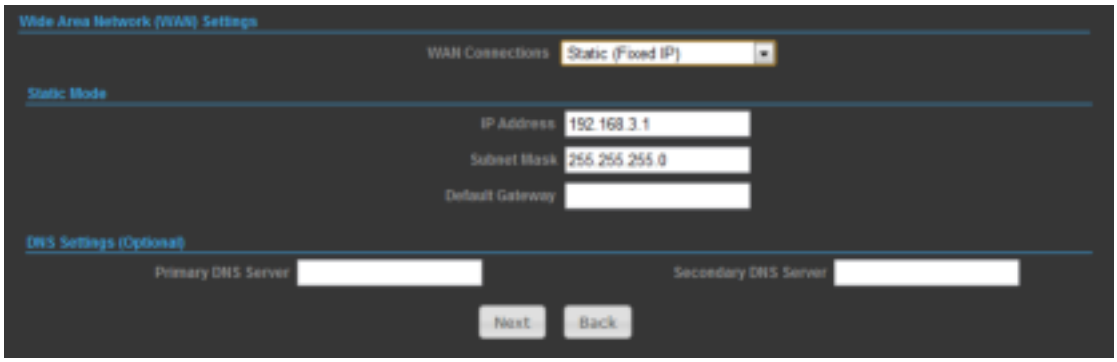
Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – STATIC (FIXED IP)

1) Select Static(Fixed IP), if your Internet service provider (ISP) to be permanent address on the Internet. A Static IP address is a number (in the form of a dotted quad)



2)



◆□**IP Address**—Sets the static IP address.

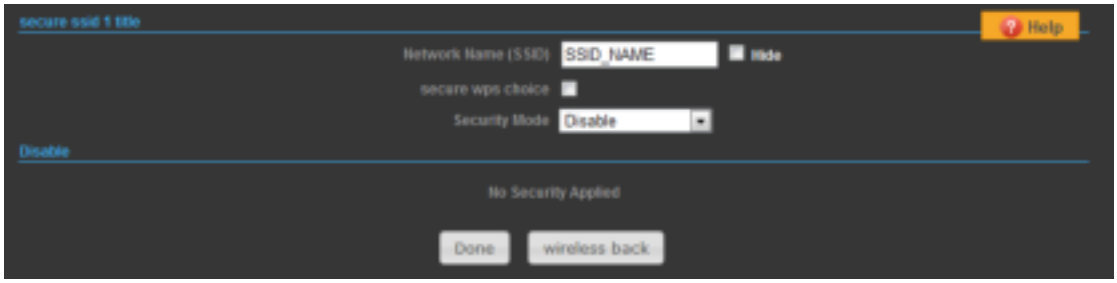
◆□**Subnet Mask**—Sets the static IP subnet mask. (Default: 255.255.255.0)

◆□**Default Gateway**—The IP address of a router that is used when the requested destination IP address is not on the local subnet.

◆□**Primary DNS Server**—The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□**Secondary DNS Server** —The IP address of the Secondary DomainName Server.

3)



Security Setup

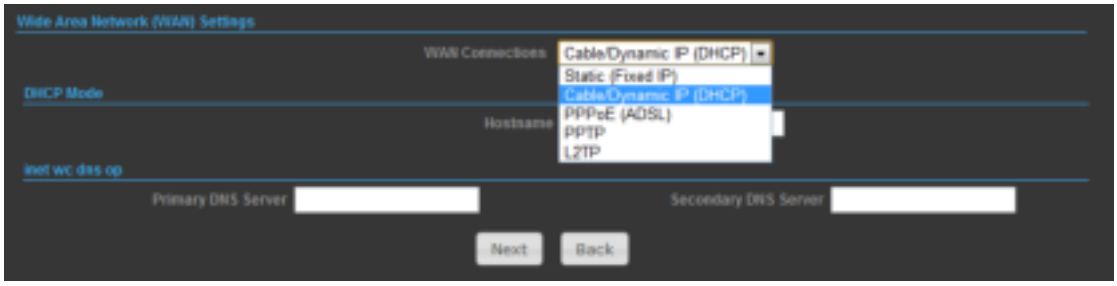
Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required

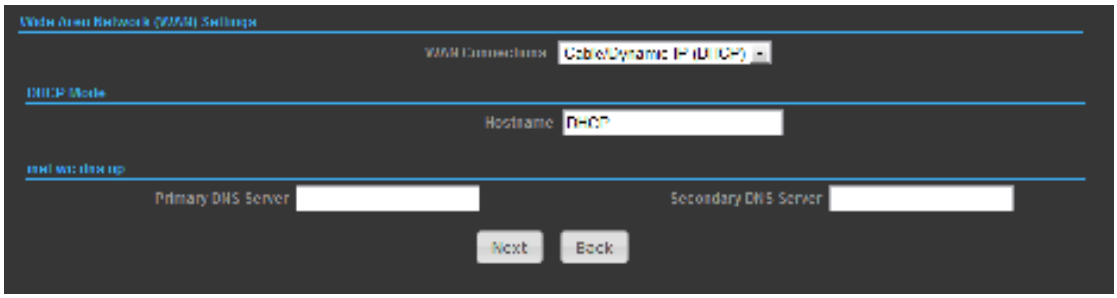
parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – CABLE/DYNAMIC IP (DHCP)

1) Select Cable/Dynamic IP (DHCP), if your Internet service provider (ISP) use a DHCP service to assign your Router an IP address when connecting to the Internet.

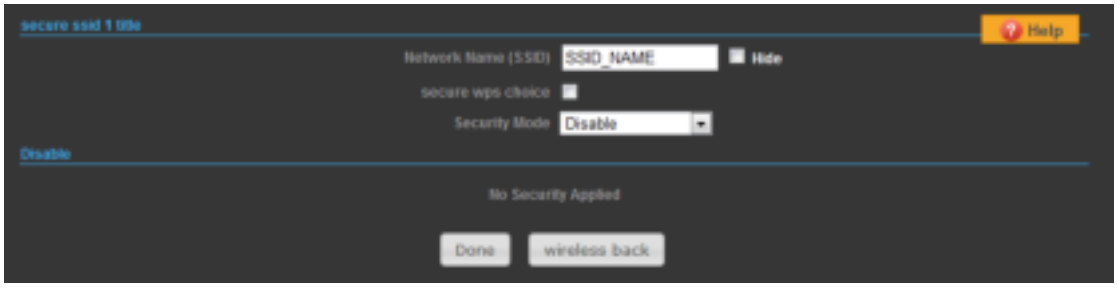


2)



The host name that you selected from the DHCP service provider.

3)



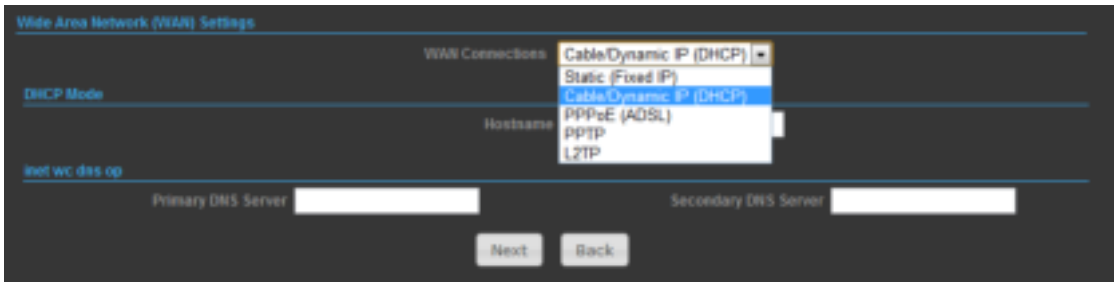
Security Setup

Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – PPTP

1) Select PPTP, if you are using PPTP service to gain connection to the Internet.



2)

◆□**Server IP** — Sets the PPTP server IP Address. (Default: pptp_server)

◆□**User Name** — Sets the PPTP user name for the WAN port.

◆□**Password** — Sets a PPTP password for the WAN port.

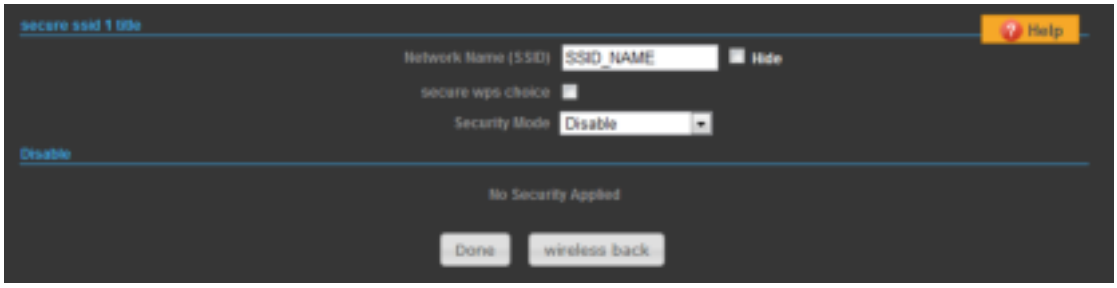
◆□**Address Mode** — Sets a PPTP network mode. (Default: Dynamic IP)

◆□**Operation Mode —** Enables and configures the keep alive time.

◆□**Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□**Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

3)

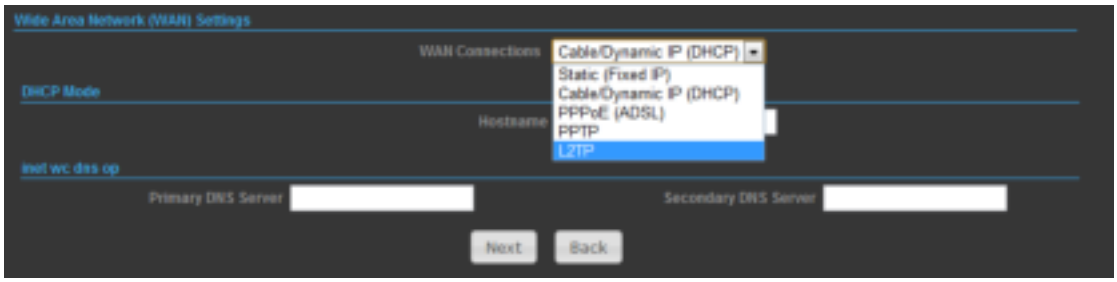


Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – L2TP

1) Select L2TP, if you are using PPTP service to gain connection to the Internet.



2)

◆□**Server IP** — Sets the L2TP server IP Address. (Default: l2tp_server)

◆□**User Name** — Sets the L2TP user name for the WAN port.

◆□**Password** — Sets a L2TP password for the WAN port.

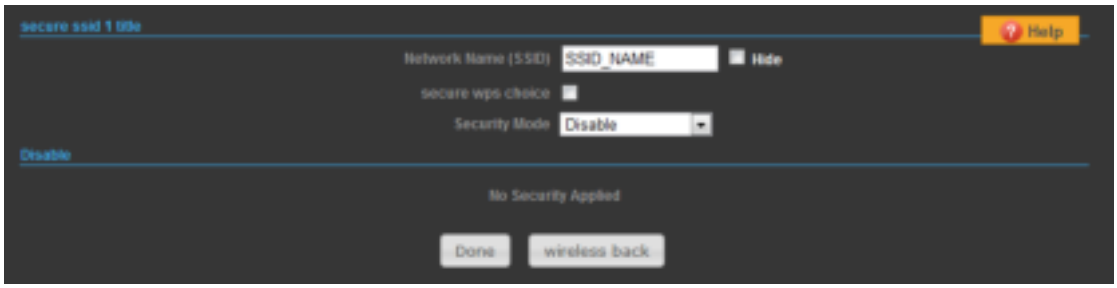
◆□**Address Mode** — Sets a L2TP network mode. (Default: Dynamic IP)

◆□**Operation Mode —** Enables and configures the keep alive time.

◆□**Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and canbe used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□**Secondary DNS Server** — The IP address of the Secondary DomainName Server.

3)

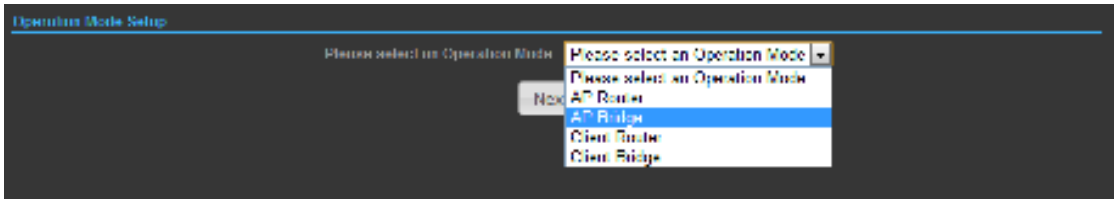


Network Name (SSID)—SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

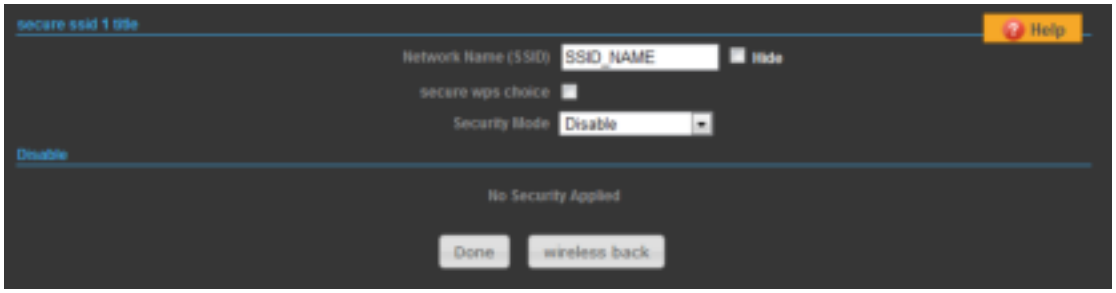
Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

OPERATION MODE–AP BRIDGE

Choose menu “Easy Setup” and select AP Bridge if you want to configure to an access point.



2)

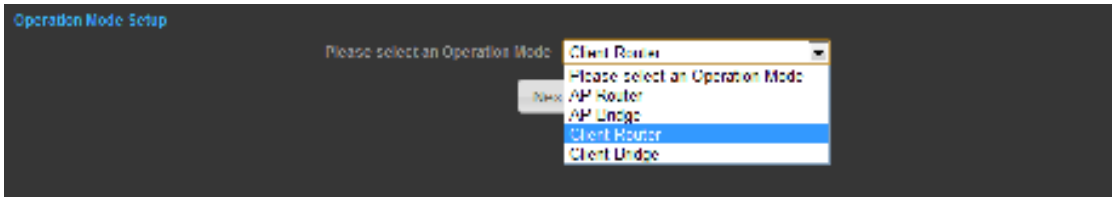


Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

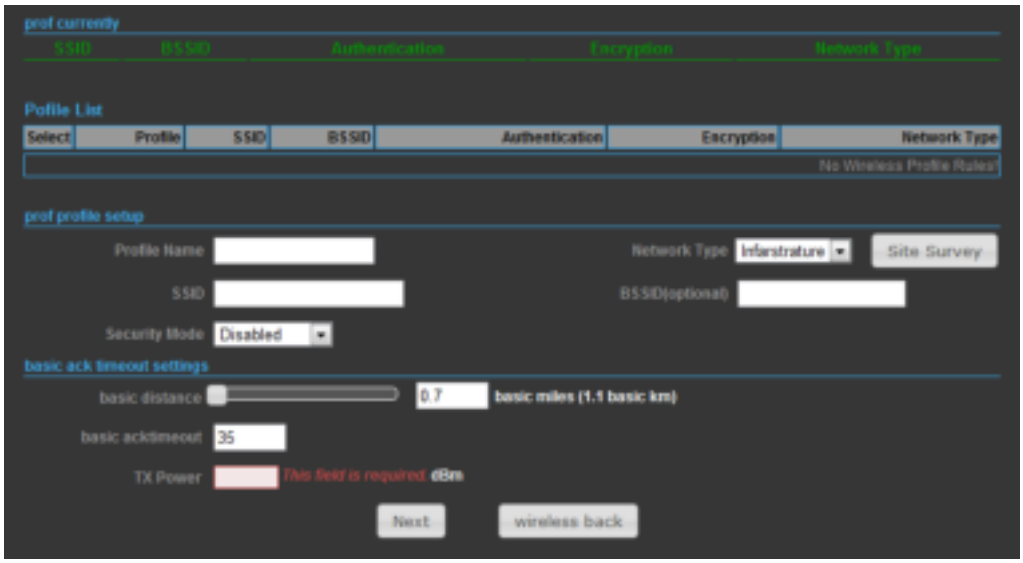
Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, Open, Shared, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-PSK_WPA2-PSK, WPA, WPA2, WPA1_WPA2, 802.1X;

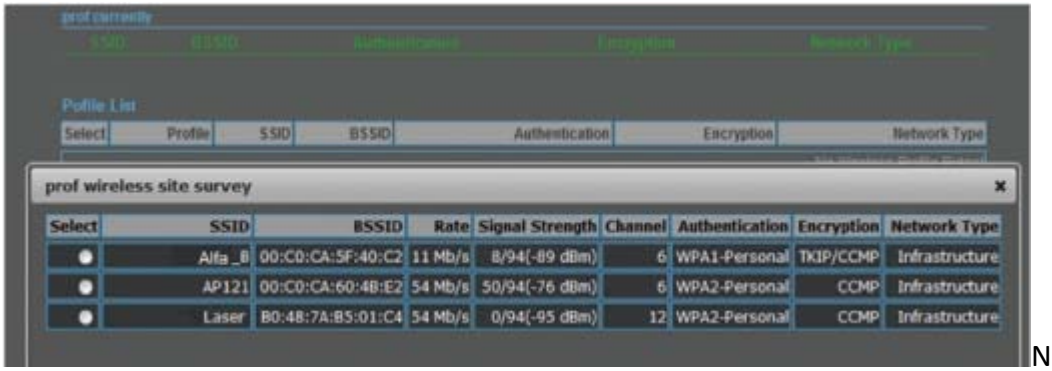
OPERATION MODE–CLIENT ROUTER

In the Client Router mode is also known as WISP. The TUBE-2HQPwireless side is connected to the remote AP (Base-Station) as in Client Infrastructure mode. Between the wireless and LAN is the IP sharing router function. This is used to share Client Router connection. The WAN is on the wireless side.

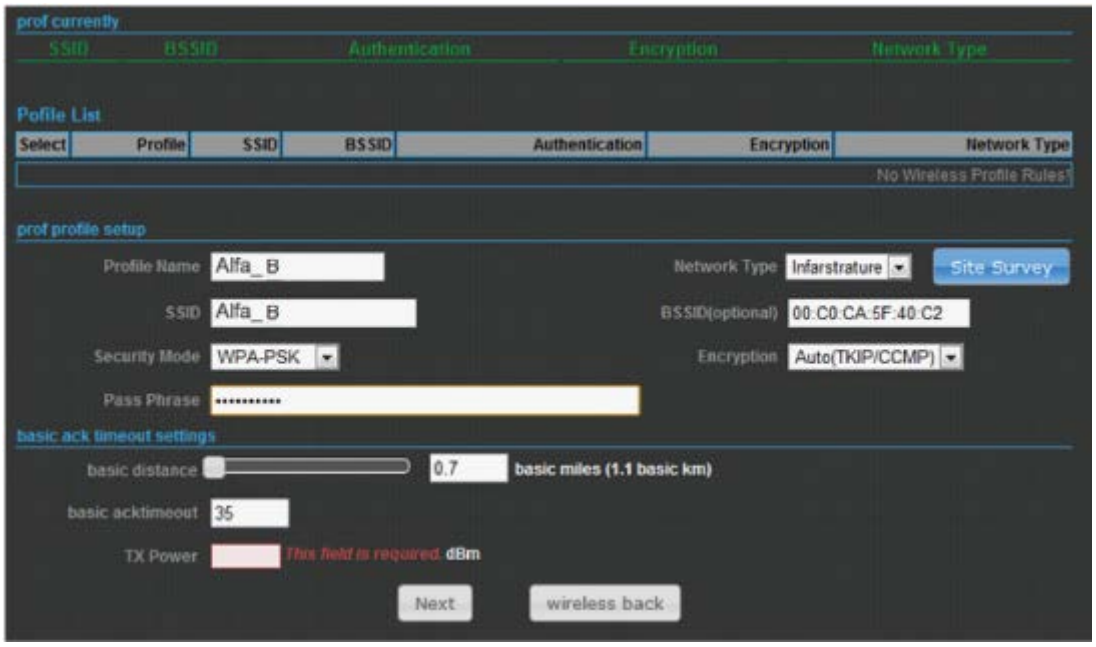


2) Press **Site Survey** button and look for available wireless networkthen click on the SSID that you attempt to connect to it; Alfa_B is the SSID that we are going to connect in this example. Press**Next**button when finished.



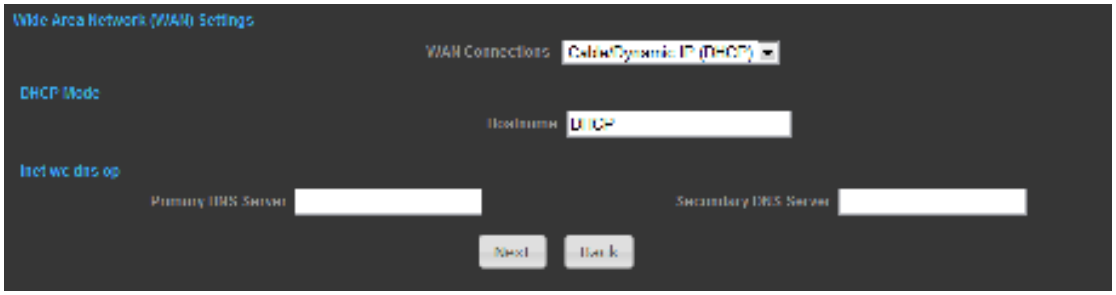


Now, it shows theProfile Name, SSID, BSSID, and encryption type received from your target network and press **Next** button to continue.



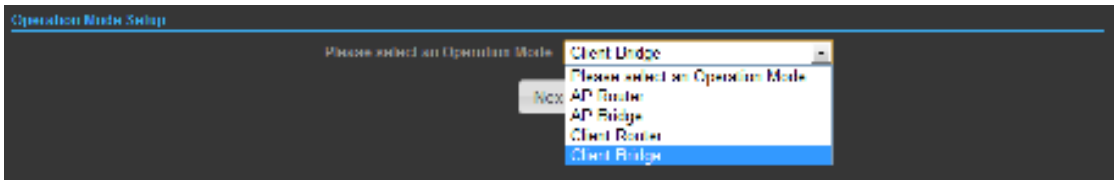
3) Finally, you need to tell the system about IP address received from WAN, DHCP

Hostname, and DNS Server then press **Next** button to finish the wizard.

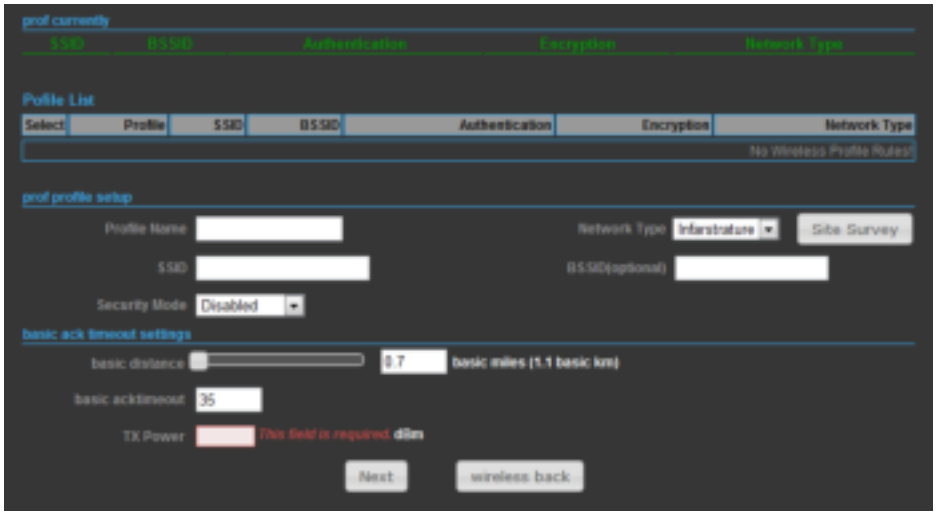


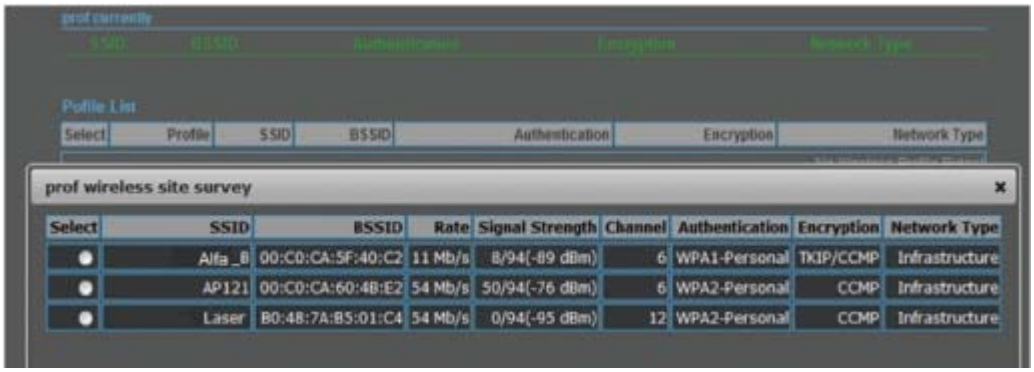
OPERATION MODE–CLIENT BRIDGE

In the Client Bridgemode yourTUBE-2HQPwill behave just the same as Wireless adapter. With Client Bridges, the WLAN and the LAN are on the same subnet. Consequently, NAT is no longer used and services that are running on the original network.

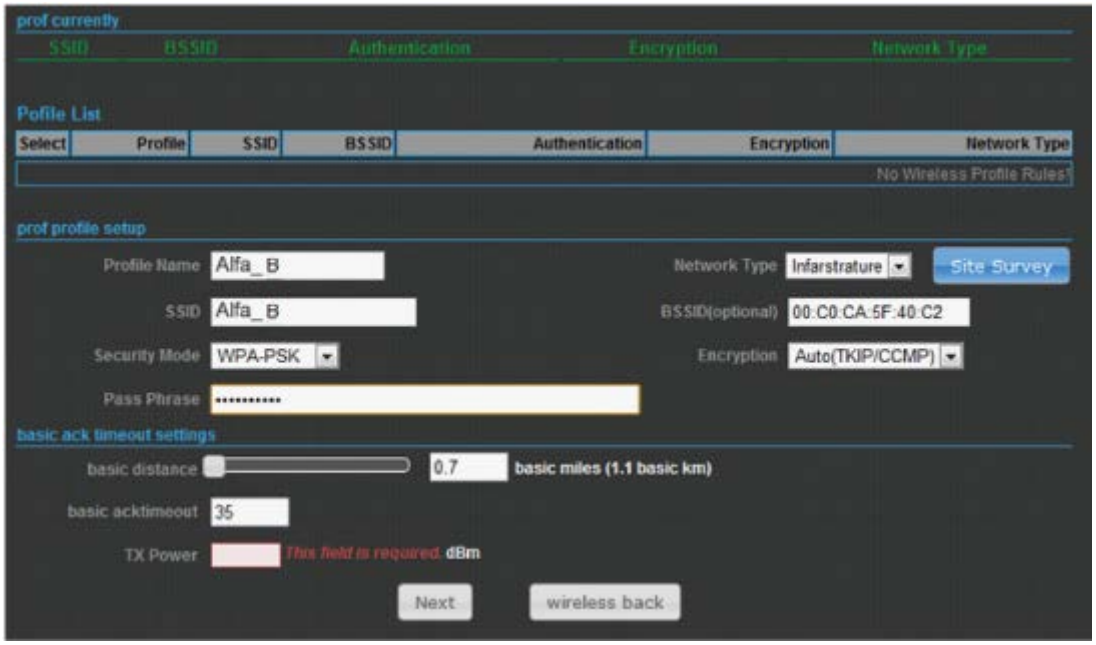


2) Press **Site Survey** button and look for available wireless networkthen click on the SSID that you attempt to connect to it; Alfa_B is the SSID that we are going to connect in this example. Press**Next**button when finished.



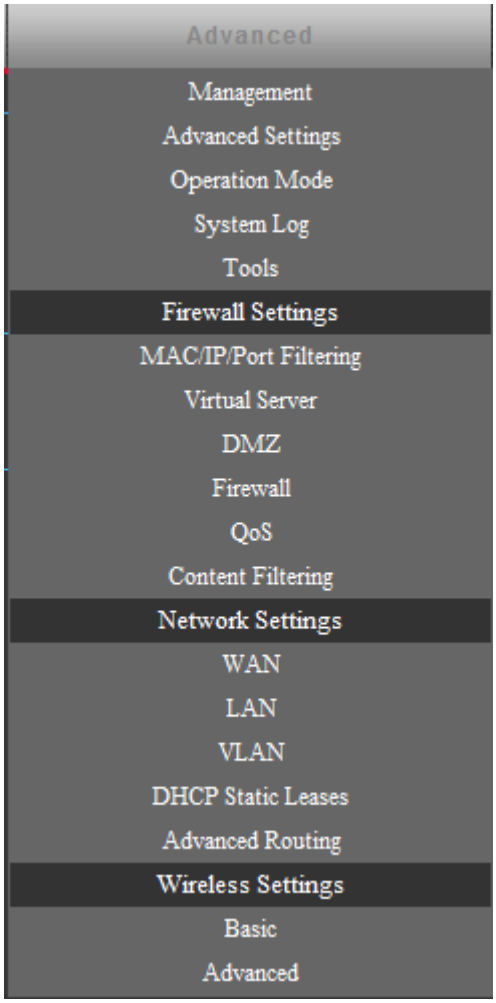


3) Now, it shows theProfile Name, SSID, BSSID, and encryption type received from your target network and press **Next** button to finish the wizard.



ADVANCED SETUP

Inthe Advanced Manual Bar, it includes all the settings such as firmware upgrade, LAN, WAN and wireless settings that change the RF behaviors. It is important to read through this section before attempting to make changes.



MANAGEMENT

The Management section is provided for configuration of administrative needs such as language type, user name / Password, firmware upgrade, export and import settings, load factory defaults and reboots system.

◆□**Password** — The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.

◆□**Software Version -** This displays the current firmware version.

To upgrade the Router's firmware, follow these instructions below:

1. Download a more recent firmware upgrade file from our website.

2. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.

3. Click the **Upgrade** button.

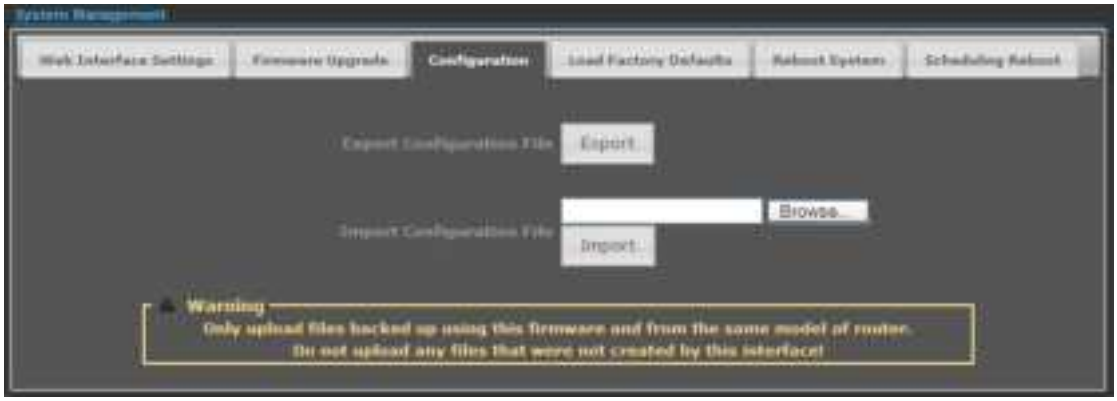
Note:

1. New firmware versions are posted at our website and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.

2. When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.

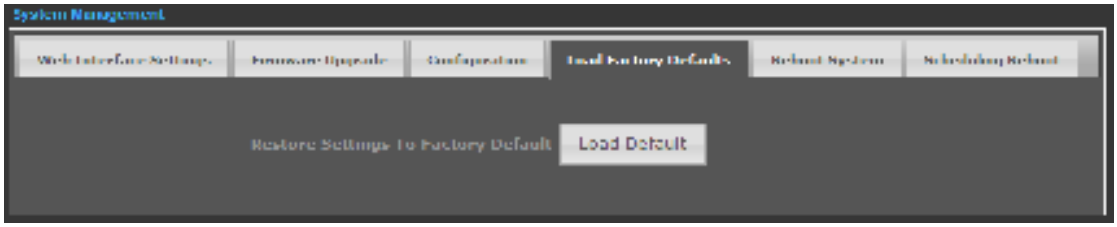
3. Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.

4. The Router will reboot after the upgrading has been finished.

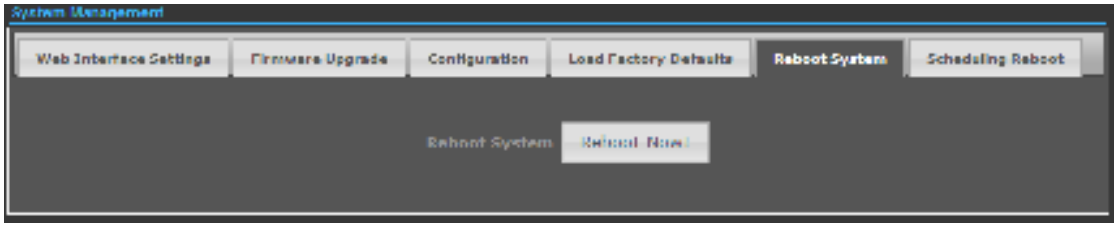


◆□**Export Settings** — Click the Export Button to download current router configuration to your PC.

◆□**Import Settings** — Click the Import Button to browse for the configuration file that is currently saved on your PC. Click Import to overwrite all current configurations with the one in the configuration file.



◆□**Load Factory Defaults** — If you have problems with TUBE-2HQP, which might be a result from changing some settings, but you are unsure what settings exactly, you can restore the factory defaults by click the Load Default Button.



◆□**Reboot System** — If you want to reboot the TUBE-2HQP, click the Reboot Now Button.

ADVANCED SETTINGS

The Advanced Settings section is provided for configuration of Time Zone, DDNS, UPnP, SNMP, and SSH.

◆□**Time Zone Settings**— The Time Zone Settings allows you to configure, update and maintain the correct time on the TUBE-2HQP's internal system clock.

◆□**SNTP Server** — Enter the address of an SNTP server to receive time updates.

◆□**SNTP synchronization (minutes)** — Specify the interval between SNTP server updates.

DDNS Settings — DDNS lets you assign a fixed host and domain name to dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the TUBE-2HQP. Before using this feature, you need to sign up for DDNS service at www.dyndns.org , a DDNS service provider.

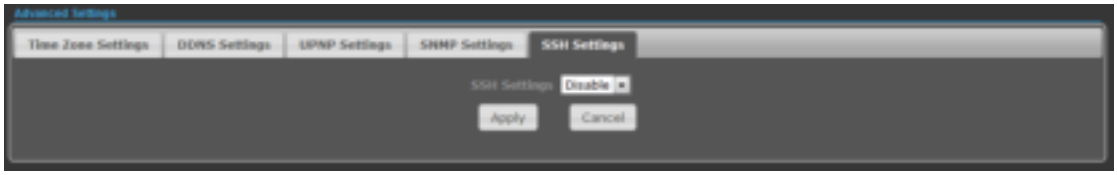
◆□**User Name** — Sets the DDNS user name for the connection.

◆□**Password** — Sets a DDNS password for the connection.

◆□**HostName —** The host name that you selected from the DDNS service provider.

UPNP Settings– UPnP permits network devices to discover other network device(s) preference and establish functional network services for data sharing, communication, and entrainment. Default setting is Disabled.

SNMP Settings–Managing devices on IP networks. Default setting is Disabled.



SSH Settings–Secure Shell. Enable your TUBE-2HQPunit to access secure shell (SSH) based network device. Default setting is Disabled.

OPERATION MODE

The Operation Mode content four modes: AP Bridge, AP Router, Client Router and Client Bridge.

◆□**AP Bridge**— The wired Ethernet and wireless are bridged together. Once the mode is selected, all WAN related functions will be disabled.

◆□**AP Router**—The Ethernet port will convert into WAN port requiring you to configure your CPE via WLAN.

◆□**Client Router**—TheTUBE-2HQPwill behave just the same as the client mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WSIP subscriber can share the WISP connection without the extra router.

◆□**Client Bridge**—TheTUBE-2HQPwill behave just the sameas Wireless adapter.With Client Bridges, the WLAN and the LAN are on the same subnet. Consequently, NAT is no longer used and services that are running on the original network.

FIREWALL CONFIGURATION

MAC/IP/PORT FILTERING

MAC/IP/Port filtering restricts connection parameters to limit the risk of intrusion

and defends against a wide array of common hacker attacks. MAC/IP/Port filtering allows the unit to permit, deny or proxy traffic through its MAC addresses, IP addresses and ports. The TUBE-2HQPallows you define a sequential list of permit or deny filtering rules. This device tests ingress packets against the filter rules one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is either accepted or dropped depending on the default policy setting.

◆□**MAC/IP/Port Filtering**— Enables or disables MAC/IP/Port Filtering. (Default: Disable)

◆□**Default Policy** — When MAC/IP/Port Filtering is enabled, the default policy will be enabled. If you set the default policy to “Dropped”, all incoming packets that don’t match the rules will be dropped. If the policy is set to "Accepted," all incoming packets that don't match the rules are accepted. (Default: Dropped)

◆□**MAC Address** — Specifies the MAC address to block or allow traffic from.

◆□**DIP**—Specifies the destination IP address to block or allow traffic from.

◆□**SIP**—Specifies the source IP address to block or allow traffic from.

◆□**Protocol** — Specifies the destination port type, TCP, UDP or ICMP.

◆□**Destination Port Range** — Specifies the range of destination port to block traffic from the specified LAN IP address from reaching.

◆□**Source Port Range** — Specifies the range of source port to block traffic from the specified LAN IP address from reaching.

◆□**Action** — Specifies if traffic should be accepted or dropped. (Default: Accept)

◆□**Comment** — Enter a useful comment to help identify the filtering rules.

◆□**Current Filtering rules**— The Current Filter Table displays the configured IP addresses and ports that are permitted or denied access to and from.

- **No.** — The table entry number.
- **MAC Address** — Displays a MAC address to filter.
- **Destination IP Address (DIP)**— Displays the destination IP address.
- **Source IP Address (SIP)**— Displays the source IP address.
- **Protocol** — Displays the protocol type.
- **Destination Port Range (DPR)** — Displays the destination port range.
- **Source Port Range (SPR)** — Displays the source port range.

- **Action** — Displays if the specified traffic is accepted or dropped.
- **Comment** — Displays a useful comment to identify the filter rules.

VIRTUAL SERVER SETTINGS

Virtual Server (sometimes referred to as Port Forwarding) is the act of forwarding traffic from one network node to another based on received protocol port number. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside through a NATenabled router.

◆□**Virtual Server** — Selects between enabling or disabling port forwarding the virtual server. (Default: Disable)

◆□**IP Address** — Specifies the IP address of a server on the local network to allow external access.

◆□**Private Port** — The protocol port number on the local server.

◆□**Public Port** — The protocol port number on the router's WAN interface.

◆□**Protocol** — Specifies the protocol to forward, either TCP, UDP, or TCP&UDP.

◆□**Comment** — Enter a useful comment to help identify the port forwarding service on the network.

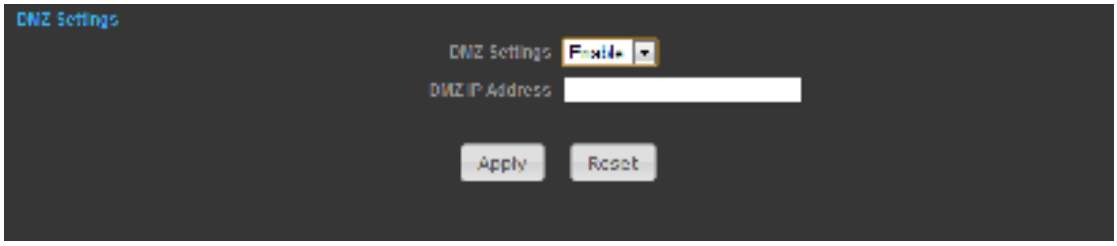
◆□**Current Virtual Servers in System**— The Current Port Forwarding Table displays the entries that are allowed to forward packets through the TUBE-2HQP's firewall.

- **No.** — The table entry number.
- **IP Address** — The IP address of a server on the local network to allow external access.

- **Port Mapping** — displays the port mapping for the server.
- **Protocol** — Displays the protocol used for forwarding this port.
- **Comment** — Displays a useful comment to identify the nature of the port to be forwarded.

DMZ

DMZ is to specified host PC on the local network to access the Internet without any firewall protection. Some Internet applications, such as interactive games or video conferencing, may not function properly behind the firewall. By specifying a Demilitarized Zone(DMZ) host, the PC's TCP ports are completely exposed to the Internet, allowing open two-way communication. The host PC should be assigned astatic IP address (which is mapped to its MAC address) and this must beconfigured as the DMZ IP address.

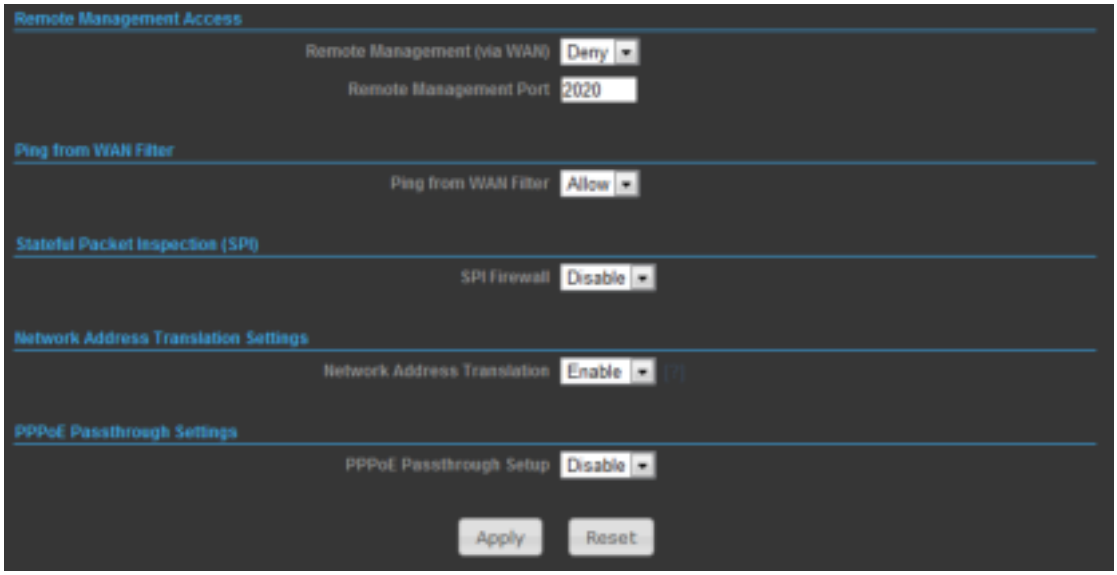


◆□**DMZ Settings** — Sets the DMZ status. (Default: Disable)

◆□**DMZ IP Address** — Specifies an IP address on the local network allowed unblocked access to the WAN.

FIREWALL

Firewall functions which will help to protect your network and computer. You can utilized firmware functions to protect your network from hackers and malicious intruders.



◆□**Remote Management (via WAN)**— allow or deny to manage the router from anywhere on the Internet.

◆□**Remote Management Port**— The port that you will use to address the management from the Internet. For example, if you specify port 2020, then to access the TUBE-2HQPfrom Internet, you would use a URL of the form: http://xxx.xxx.xxx.xxx:2020/

◆□**Ping from WAN Filter** — When Allow, the TUBE-2HQPdoes not respond to ping packets received on the WAN port.

◆□**SPI Firewall** — SIP firewall help to keep track of the state of network connections (such as TCP streams, UDP communication) traveling across it. It is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.

◆□**Network Address Translation** — NAT is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

CONTENT FILTERING

The TUBE-2HQPprovides a variety of options for blocking Internet access based on content, URL and host name.

◆□**Web URL Filter Settings** — By filtering inbound Uniform Resource Locators (URLs) the risk of compromising the network can be reduced. URLs are commonly used to point to websites. By specifying a URL or a keyword contained in a URL traffic from that site may be blocked.

◆□**Current URL Filters** — Displays current URL filter.

◆□**Add a URL Filter** — Adds a URL filter to the settings.

◆□**Delete a URL Filter** — Deletes a URL filter entry from the list.

◆□**Web Host Filter Settings** — AllowsInternet content access to be restricted based on web address keywords and web domains. A domain name is the name of a particular web site. For example, for the address www.HOST.com, the domain name is HOST.com. Enter the Keyword then click “Add.”

◆□**Current Host Filters** — Displays current Host filter.

◆□**Add a Host Filter** — Enters the keyword for a host filtering.

◆□**Delete a Host Filter** — Deletes a Host filter entry from the list.

NETWORK SETTINGS

WAN

In this section, there are several connection types to choose from; Static IP, DHCP, PPPoE, PPTP and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

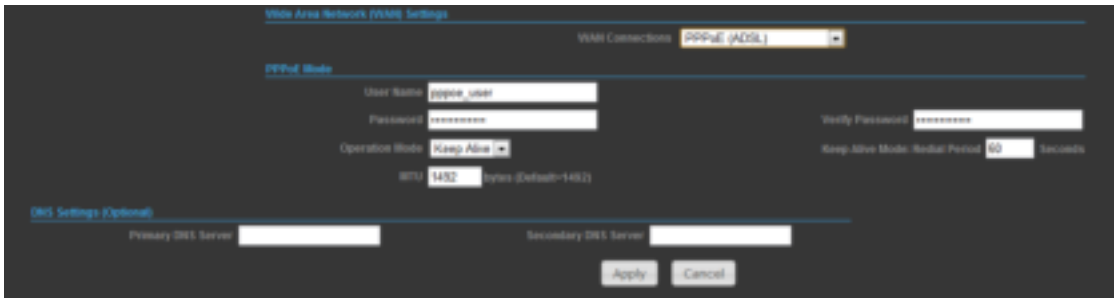
CABLE/DYNAMIC IP (DHCP)

◆□**Hostname** — Specifies the host name of the DHCP client.

◆□**Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□**Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

PPPoE (ADSL)



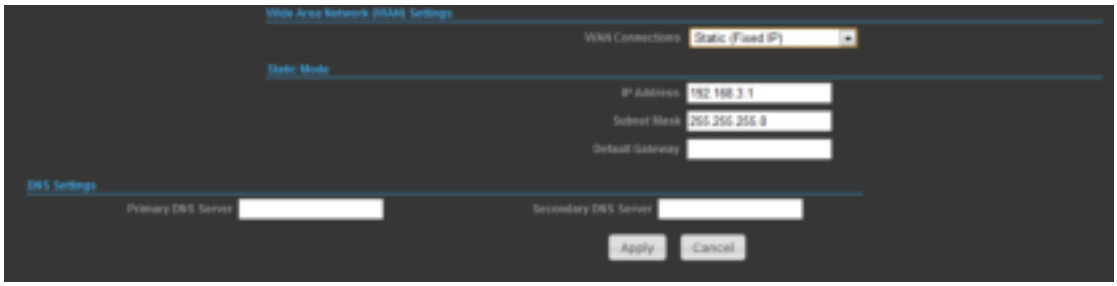
◆□**User Name** — Sets the PPPoE user name for the WAN port.

◆□**Password** — Sets a PPPoE password for the WAN port.

◆□**Verify Password** — Prompts you to re-enter your chosen password.

◆□**Operation Mode —** Enables and configures the keep alive time and configures the on-demand idle time.

STATIC IP (FIXED IP)



◆□**IP Address**—Sets the static IP address.

◆□**Subnet Mask**—Sets the static IP subnet mask. (Default: 255.255.255.0)

◆□**Default Gateway**—The IP address of a router that is used when the requested destination IP address is not on the local subnet.

◆□**Primary DNS Server**—The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□**Secondary DNS Server** —The IP address of the Secondary DomainName Server.

PPTP

◆□**Server IP** — Sets the PPTP server IP Address. (Default: pptp_server)

◆□**User Name** — Sets the PPTP user name for the WAN port.

◆□**Password** — Sets a PPTP password for the WAN port.

◆□**Address Mode** — Sets a PPTP network mode. (Default: Dynamic IP)

◆□**Operation Mode —** Enables and configures the keep alive time.

◆□**Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□**Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

IPSec

Verify the desire settings and use scroll down for more options.

◆□IPSec Connection Type –Use drop down menu to select from Road Warrior Tunnel, Host to Host Tunnel, Subnet to Subnet Tunnel, Host to Host Transport, Pass trough, Drop, or Reject. Default setting is Road Warrior Tunnel

◆□IPSec Authentication– Use drop down menu to select from SHA-1, or MD5. Default setting is SHA1.

◆□SA Connection Life Time –Specify how often each SA should be rekeyed, measured in hour.

◆□Local IP address / Subnet / Gateway–Local end point IP address, Subnet, and Gateway IP address.

◆□IPSec Operation Mode – Use drop down menu to select from Add, Route Start, Manual, or Ignore. Default setting is Add.

◆□IKE Key Retry–Specify maximum retry limits for negotiate key to Internet Key Exchange.

◆□Peer IP address / Subnet / Gateway –Remote end point IP address, Subnet, and Gateway IP address.

L2TP

◆□**Server IP** — Sets the L2TP server IP Address. (Default: l2tp_server)

◆□**User Name** — Sets the L2TP user name for the WAN port.

◆□**Password** — Sets a L2TP password for the WAN port.

◆□**Address Mode** — Sets a L2TP network mode. (Default: Dynamic IP)

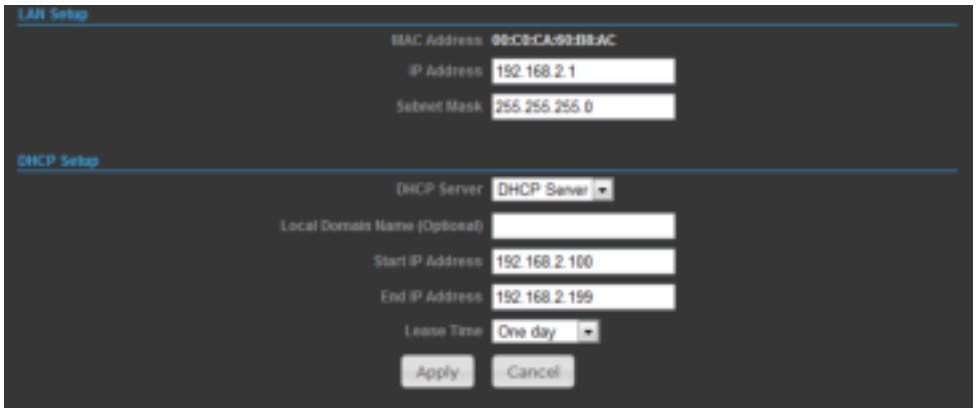
◆□**Operation Mode —** Enables and configures the keep alive time.

◆□**Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and canbe used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□**Secondary DNS Server** — The IP address of the Secondary DomainName Server.

LAN

In this section, the LAN settings are configured based on the IP Address and Subnet Mask. The IP address is also used to access this Web-based management interface. It is recommended to use the default settings if you do not have an existing network.



◆□**IP Address** — The IP address of TUBE-2HQPon the local area network.

(Default: 192.168.2.1)

◆□**Subnet Mask**— The subnet mask of TUBE-2HQPon the local area network

◆□**DHCP Server**— The DHCP Server is to assign private IP address to the TUBE-2HQPin your local area network(LAN). The default LAN IP address is 192.168.2.1, changing IP address will also change the DHCP server's IP subnet.

ADVANCED ROUTING

In this section, allow to configure routing feature in the TUBE-2HQP.

◆□**Destination** — The IP addressof packets that can be routed.

◆□**Type**— Defines the type of destination. (Host: Signal IP address / Net: Portion of Network)

◆□**Netmask**— Displays the subnetwork associated with the destination.

◆□**Gateway**— Defines the packets destination next hop

◆□**Interface**— Select interface to which a static routing subnet is to be applied

◆□**Comment**— Help identify the routing

◆□**RIP**—Enable or disable the RIP(Routing Information Protocol) for the WAN or LAN interface.

WIRELESS SETTINGS

BASIC

◆□**Wireless On/Off** — Enables or Disable the radio. (Default: Turn On)

◆□**Wireless Mode** — There are 4 wireless mode, those are Access Point, WDS Access Point, WDS Repeater and WDS Client

Note.

If WEP authentication is selected for WDS communication, you will then only have one set of encryption for the entire channel.

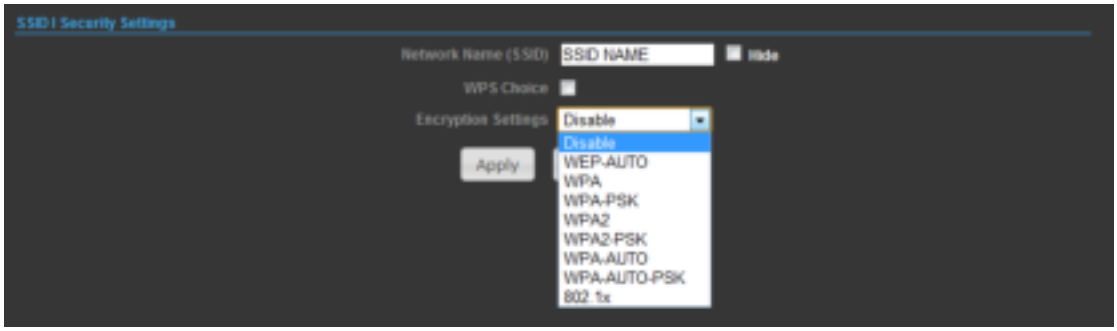
◆□**Network Name (SSID)** — The name of the wireless network service provided by the TUBE-2HQP. Clients that want to connectto the network must set their SSID to the same as that of TUBE-2HQP.

◆□**Multiple SSID** — One additional VAP interface supported on the device.

◆□**Frequency (Channel)** — The radio channel that the TUBE-2HQPuses to communicate with wireless clients.

◆□**Network Mode** — Defines the radio operating mode.

SECURITY



WIRED EQUIVALENTPRIVACY (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network. When you select to use WEP, be sure to define at least one static WEP key for user authentication or data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

◆□**WEP-AUTO** — Allows wireless clients to connect to the network using Open-WEP (uses WEP for encryption only) or Shared-WEP (uses WEP for authentication and encryption).

◆□**Encrypt Type** — Selects WEP for data encryption (OPEN mode only).

◆□**Security Key Index** — Selects the WEP key number to use for authentication or data encryption. If wireless clients have all four WEP keys configured to the same values, you can change the encryption key to any of the settings without having to update the client keys.

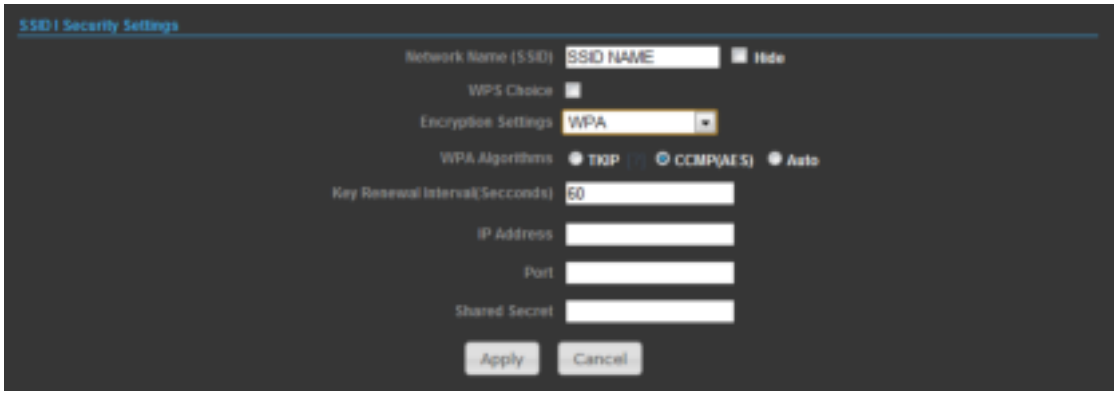
◆□**WEP Keys** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. (Default: Hex, no preset value)

Note.

If WEP authentication is selected for WDS communication, you will then only have one set of encryption for the entire channel.

WPA & WPA2

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA.



◆□**WPA** — Clients using WPA for authentication.

◆□**WPA2** — Clients using WPA2 for authentication.

◆□**WPA-Auto**— Clients using WPA or WPA2 for authentication.

◆□**WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

■□**TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

■□**AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to

WPA2-compliant hardware.

■□**Auto**— Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆□**Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients.

RADIUS Server — Configures RADIUS server settings.

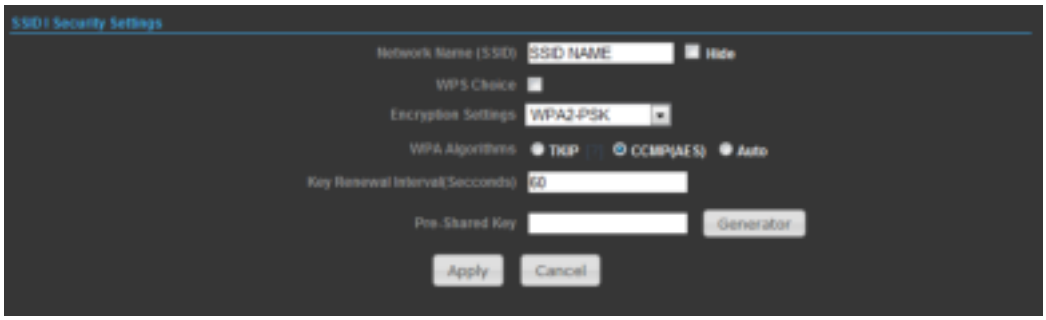
◆□**IP Address** — Specifies the IP address of the RADIUS server.

◆□**Port** — The User Datagram Protocol (UDP) port number used by the RADIUS server for authentication messages. (Range: 1024-65535;Default: 1812)

◆□**Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

WPA-PSK & WPA2-PSK

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. For small home or office networks, WPA and WPA2 provide a simple “personal” operating mode that uses just a pre-shared key for network access. The **WPA Pre-Shared Key (WPA-PSK)** mode uses a common password phrase for user authentication that is manually entered on the access point and all wireless clients. Data encryption keys are automatically generated by the access point and distributed to all clients connected to the network.



◆□**WPA-PSK** — Clients using WPA with a Pre-shared Key are accepted for authentication.

◆□**WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

◆□**WPA- Auto-PSK** — Clients using WPA or WPA2 with a Preshared

Key are accepted for authentication. The default data encryption type is TKIP/AES.

◆□**WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

■□**TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

■□**AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

■□**Auto**— Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆□**Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

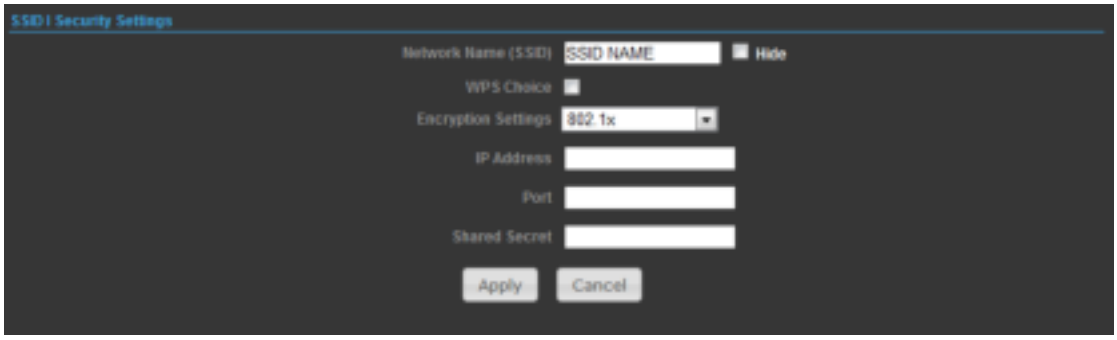
◆□**Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients.

IEEE 802.1X ANDRADIUS

IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the client can access the network. Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires network access.

The WPA and WPA2 enterprise security modes use 802.1X as the method of user authentication. IEEE 802.1X can also be enabled on its own as a security mode for

user authentication. When 802.1X is used, a RADIUS server must be configured and be available on the connected wired network.



RADIUS Server — Configures RADIUS server settings.

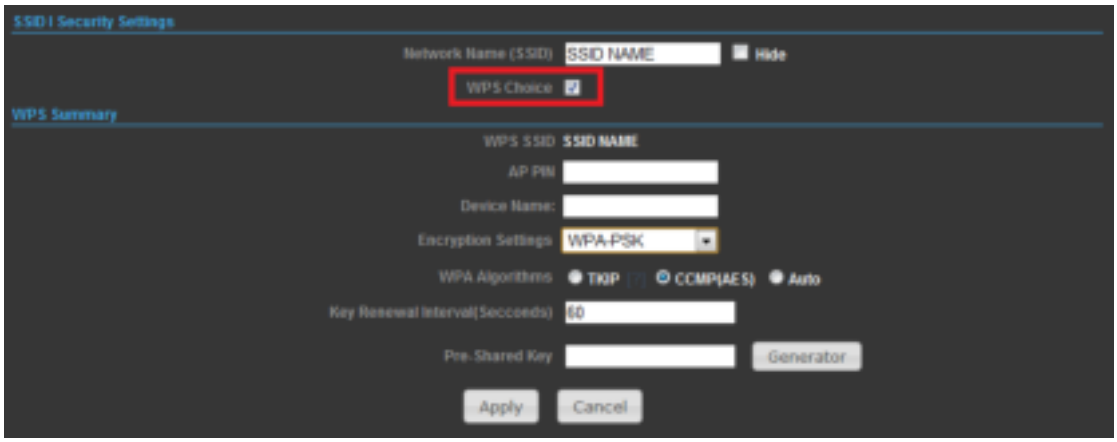
◆□**IP Address** — Specifies the IP address of the RADIUS server.

◆□**Port** — The User Datagram Protocol (UDP) port number used by the RADIUS server for authentication messages. (Range: 1024-65535;Default: 1812)

◆□**Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

WI-FI PROTECTED SETUP(WPS)

Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the Wireless Router can be pressed at any time to allow a single device to easily join the network. The WPS Settings page includes configuration options for setting WPS device PIN codes and activating the virtual WPS button.



◆□**WPS SSID** — The service set identifier for the unit.

◆□**AP PIN** — Displays the PIN Code for the Wireless Router.

◆□**Device Name**— WPS name for connecting to the device.

◆□**Encryption Settings**— Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network:

WPA Algorithms — Select the data encryption type to use. (Default is determined by the Security Mode selected.)

◆□**TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

◆□**AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) formessage integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

◆□**Auto**— Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆□**Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients.

◆□**Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

Federal Communications Commission (FCC) Statement

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

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 of the device.

This equipment has been tested and found to comply with the limits for a Class B 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 or more 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 RF 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 20cm between the radiator& your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.