



## **Tube-2H**

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

**User Guide**

## TABLE OF CONTENTS

INTRODUCTION .....	3
HARDWARE DESCRIPTION .....	錯誤! 尚未定義書籤。
HARDWARE INSTALLATION .....	3
INITIAL CONFIGURATION.....	4
CONNECTING TO THE LOGIN PAGE .....	4
STATUS PAGE .....	5
EASY SETUP.....	5
OPERATION MODE – AP ROUTER .....	6
SETTINGS – PPPoE(ADSL).....	6
SETTINGS – STATIC (FIXED IP) .....	7
SETTINGS – CABLE/DYNAMIC IP (DHCP) .....	8
SETTINGS – PPTP.....	9
SETTINGS – L2TP.....	11
OPERATION MODE – AP BRIDGE .....	12
OPERATION MODE – CLIENT ROUTER .....	13
OPERATION MODE – CLIENT BRIDGE.....	14
ADVANCED SETUP .....	16
MANAGEMENT .....	17
ADVANCED SETTINGS .....	19
OPERATION MODE .....	20
FIREWALL CONFIGURATION .....	21
MAC/IP/PORT FILTERING .....	21
VIRTUAL SERVER SETTINGS.....	22
DMZ.....	23
FIREWALL .....	24
CONTENT FILTERING.....	25
NETWORK SETTINGS.....	26
WAN .....	26
LAN.....	29
ADVANCED ROUTING .....	30
WIRELESS SETTINGS .....	31
BASIC.....	31
SECURITY .....	32

## INTRODUCTION

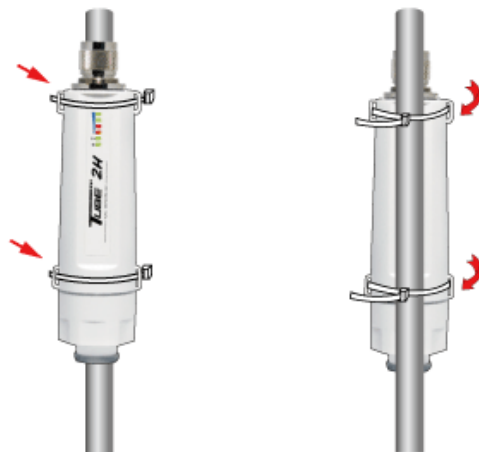
The Tube-2H is a 1X1 MIMO IEEE 802.11b/g/n wireless outdoor AP/CPE which support data rates up to 150Mbps. It is rain and splash proof when install in upright position. TUBE-2H also supports N type connector and passive PoE for simplify installation.

## HARDWARE INSTALLATION

- ◆ How to assembly the unit



- ◆ How to tie the strap on the pole



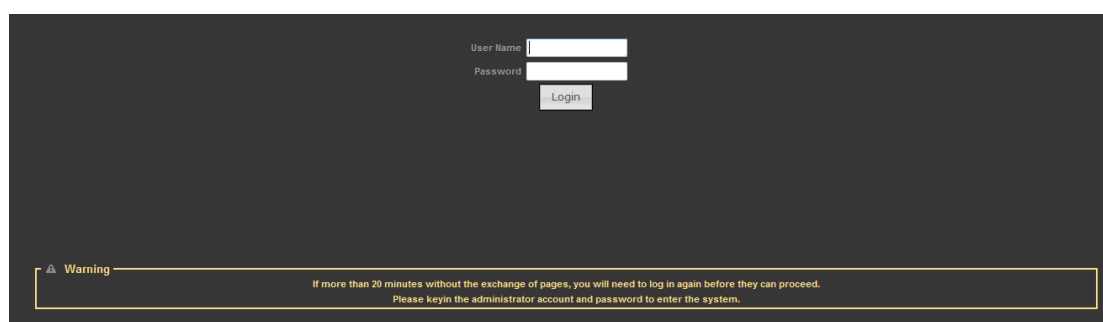
## INITIAL CONFIGURATION

The TUBE-2H, outdoor 2.4GHz AP/CPE offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a 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 a PC directly to the TUBE-2H's Ethernet port. The TUBE-2H has a default IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. You must set your PC IP address to be on the same subnet as the TUBE-2H (that is, the PC and TUBE-2H addresses must both start 192.168.2.x). To access the TUBE-2H's management GUI interface, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.2.1.
2. Log into the interface by entering the default username "admin" and password "admin," then click OK.



User Name

Password

Login

**Warning** If more than 20 minutes without the exchange of pages, you will need to log in again before they can proceed. Please keyin the administrator account and password to enter the system.

## STATUS PAGE

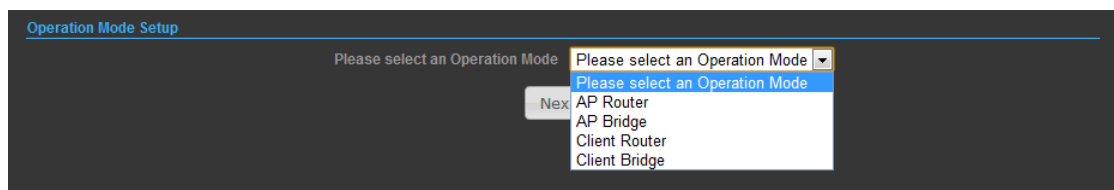
After logging in to the web interface, the Status page displays. The Home page top-menu-bar shows the Status, Easy Setup, Advanced and Language.

LAN Configuration	
LAN IP Address <b>192.168.2.1</b>	LAN Netmask <b>255.255.255.0</b>
MAC Address <b>00:C0:CA:60:9D:3C</b>	
System Info	
Firmware Version <b>V2.5 2012-06-27-13:35</b>	System Time <b>Sun, 01 Jan 2012 12:04:39</b>
Operation Mode <b>AP Bridge mode</b>	Wireless MAC Address <b>00:C0:CA:60:9D:3E</b>

## EASY SETUP

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

Click on Easy Setup to bring up the wizard



The screenshot shows the 'Operation Mode Setup' page. It features a label 'Please select an Operation Mode' followed by a dropdown menu. The dropdown menu is open, displaying four options: 'AP Router', 'AP Bridge', 'Client Router', and 'Client Bridge'. A 'Next' button is visible to the left of the dropdown menu.

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](#)

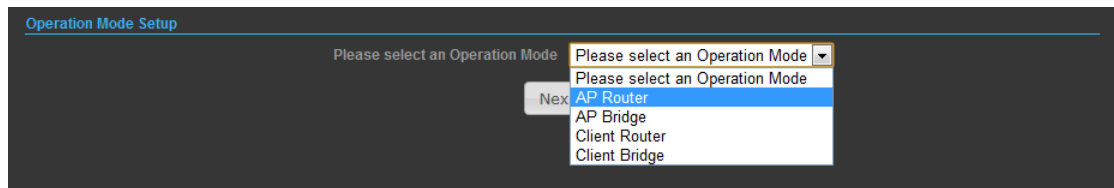
If you want to configure to WISP, please select [Client Router](#)

If you want to configure to WiFi client, please select [Client Bridge](#)

## OPERATION MODE – AP ROUTER

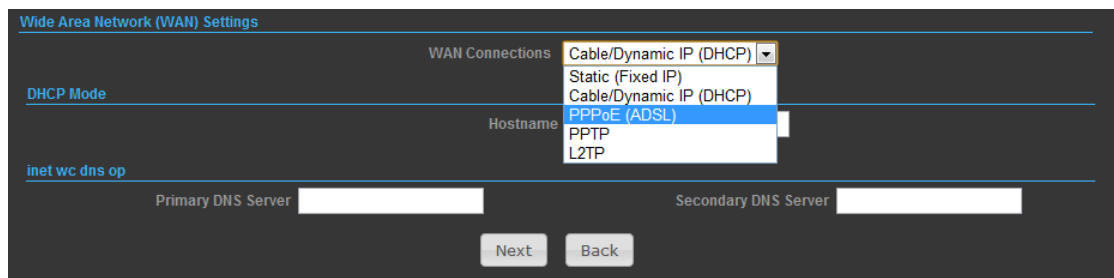
Choose menu “Easy Setup” and select AP Router if you want to configure a router connection.

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

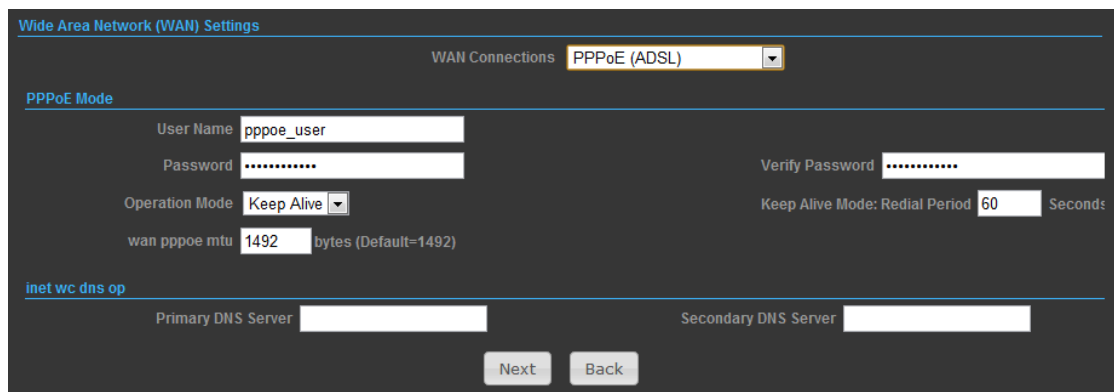


## SETTINGS – PPPoE(ADSL)

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).



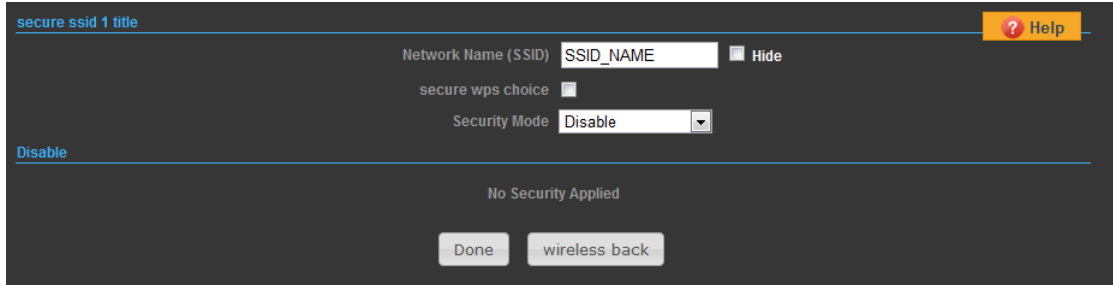
2)



- ◆ **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)



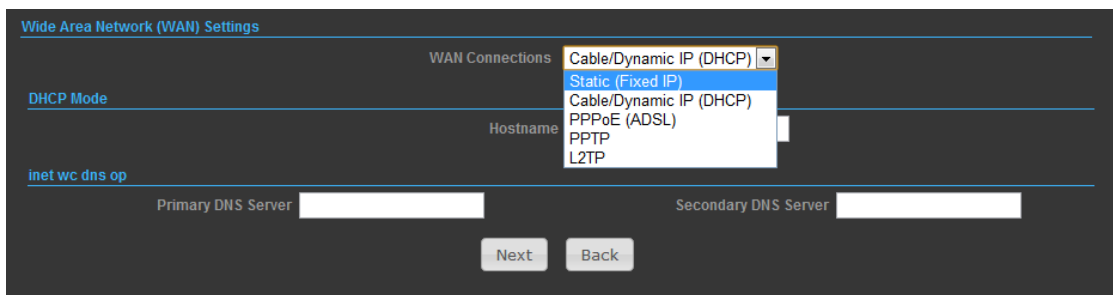
### Security Setup

**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 – 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)

Wide Area Network (WAN) Settings

WAN Connections: Static (Fixed IP)

Static Mode

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Default Gateway: [ ]

DNS Settings (Optional)

Primary DNS Server: [ ]

Secondary DNS Server: [ ]

Next Back

- ◆ **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 Domain Name Server.

3)

secure ssid 1 title

Network Name (SSID): SSID\_NAME  Hide

secure wps choice:

Security Mode: Disable

Disable

No Security Applied

Done wireless back

### 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.

Wide Area Network (WAN) Settings

WAN Connections: Cable/Dynamic IP (DHCP) (selected)  
Static (Fixed IP)  
Cable/Dynamic IP (DHCP)  
PPPoE (ADSL)  
PPTP  
L2TP

DHCP Mode

Hostname: \_\_\_\_\_

Primary DNS Server: \_\_\_\_\_ Secondary DNS Server: \_\_\_\_\_

Next Back

2)

Wide Area Network (WAN) Settings

WAN Connections: Cable/Dynamic IP (DHCP)

DHCP Mode

Hostname: DHCP

Primary DNS Server: \_\_\_\_\_ Secondary DNS Server: \_\_\_\_\_

Next Back

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

3)

secure ssid 1 title

Network Name (SSID): SSID\_NAME  Hide

secure wps choice

Security Mode: Disable

Disable

No Security Applied

Done wireless back

### 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.

Wide Area Network (WAN) Settings

WAN Connections: Cable/Dynamic IP (DHCP) (selected), Static (Fixed IP), Cable/Dynamic IP (DHCP) (highlighted), PPPoE (ADSL), PPTP, L2TP

DHCP Mode: [ ]

Hostname: [ ]

inet wc dns op

Primary DNS Server: [ ] Secondary DNS Server: [ ]

Next Back

2)

Wide Area Network (WAN) Settings

WAN Connections: PPTP (selected)

PPTP Mode

Server IP: pptp\_server

User Name: pptp\_user Password: [ ]

Address Mode: Dynamic

Operation Mode: Keep Alive Keep Alive Mode: Redial Period: 60 Seconds

inet wc dns op

Primary DNS Server: [ ] Secondary DNS Server: [ ]

Next Back

- ◆ **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)

secure ssid 1 title

Network Name (SSID): SSID\_NAME [ Hide ]

secure wps choice: [ ]

Security Mode: Disable

Disable

No Security Applied

Done wireless back

**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.

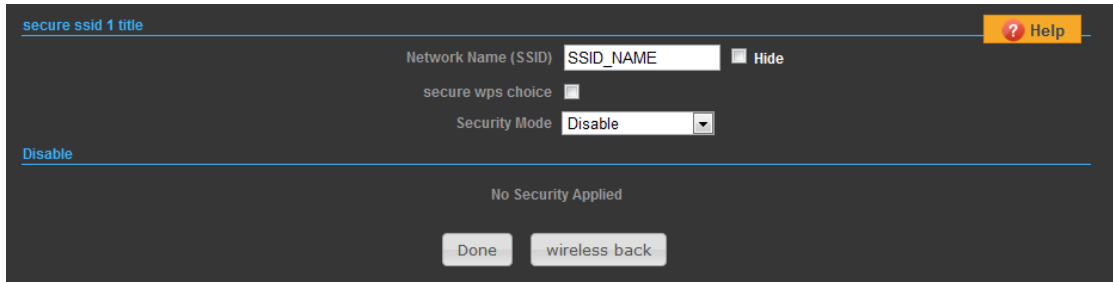
The screenshot shows the 'Wide Area Network (WAN) Settings' interface. The 'WAN Connections' dropdown menu is open, displaying the following options: Cable/Dynamic IP (DHCP), Static (Fixed IP), Cable/Dynamic IP (DHCP), PPPoE (ADSL), PPTP, and L2TP. The 'L2TP' option is highlighted in blue. Below the dropdown, there are fields for 'DHCP Mode', 'Hostname', 'Primary DNS Server', and 'Secondary DNS Server'. At the bottom, there are 'Next' and 'Back' buttons.

2)

The screenshot shows the 'Wide Area Network (WAN) Settings' interface with 'L2TP' selected in the 'WAN Connections' dropdown. The 'L2TP Mode' section contains the following fields: 'Server IP' (l2tp\_server), 'User Name' (l2tp\_user), 'Password' (masked with dots), 'Address Mode' (Static), 'IP Address', 'Subnet Mask', 'Operation Mode' (Keep Alive), and 'Keep Alive Mode: Redial Period' (60 Seconds). Below this, there are fields for 'Primary DNS Server' and 'Secondary DNS Server'. At the bottom, there are 'Next' and 'Back' buttons.

- ◆ **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 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)

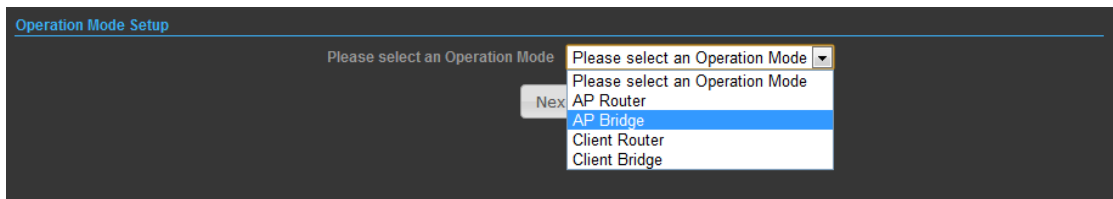


**Network Name (SSID)** — SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

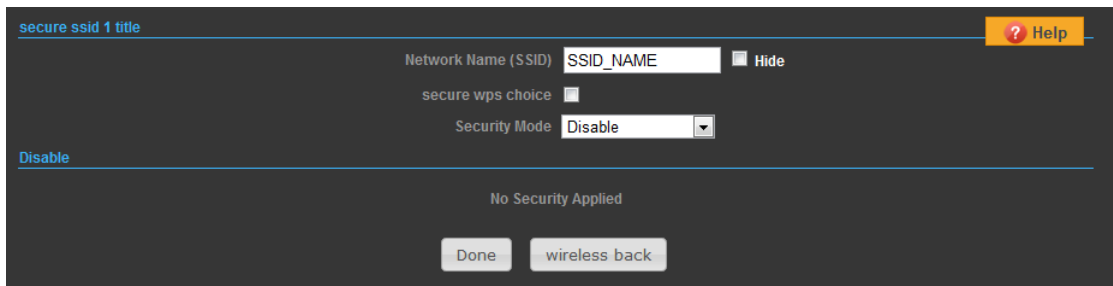
**Security Mode** — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

## OPERATION MODE – AP BRIDGE

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



2)

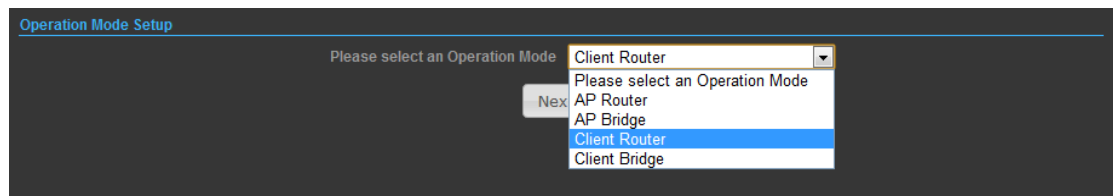


**Network Name (SSID)** — SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

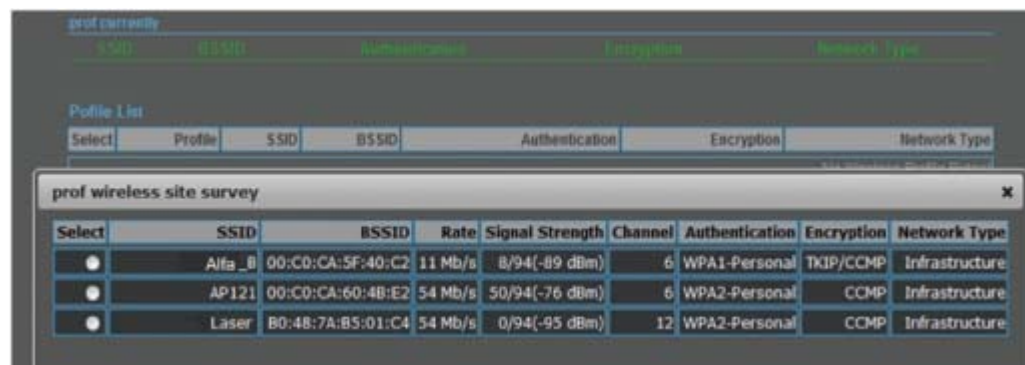
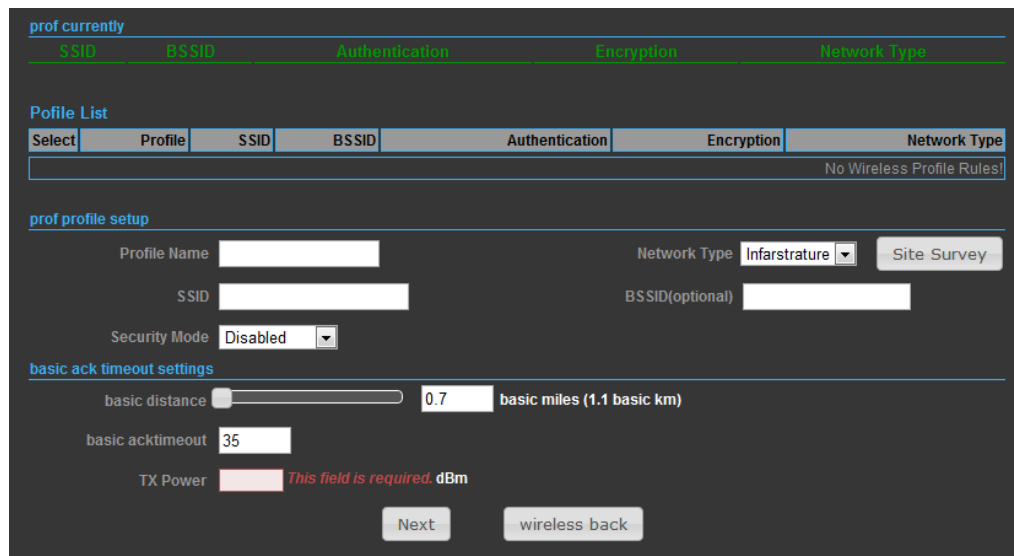
**Security Mode** — Select the security method and then configure the required parameters. (Options: Disabled, Open, Shared, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-PSK\_WPA2-PSK, WPA, WPA2, WPA1\_WPA2, 802.1X;

## OPERATION MODE – CLIENT ROUTER

In the Client Router mode is also known as WISP. The TUBE-2H wireless 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 network then 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 the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Next** button to continue.

prof currently

SSID	BSSID	Authentication	Encryption	Network Type
------	-------	----------------	------------	--------------

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
No Wireless Profile Rules						

prof profile setup

Profile Name:  Network Type:

SSID:  BSSID(optional):

Security Mode:  Encryption:

Pass Phrase:

basic ack timeout settings

basic distance:  basic miles (1.1 basic km)

basic acktimeout:

TX Power:  *This field is required. dBm*

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.

Wide Area Network (WAN) Settings

WAN Connections:

DHCP Mode

Hostname:

inet wc dns op

Primary DNS Server:

Secondary DNS Server:

## OPERATION MODE – CLIENT BRIDGE

In the Client Bridge mode your TUBE-2H will 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.

Operation Mode Setup

Please select an Operation Mode:

- Please select an Operation Mode
- AP Router
- AP Bridge
- Client Router
- Client Bridge

- 2) Press **Site Survey** button and look for available wireless network then 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.

prof currently

SSID	BSSID	Authentication	Encryption	Network Type
------	-------	----------------	------------	--------------

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
No Wireless Profile Rules						

prof profile setup

Profile Name  Network Type

SSID  BSSID(optional)

Security Mode

basic ack timeout settings

basic distance  basic miles (1.1 basic km)

basic acktimeout

TX Power  *This field is required. dBm*

prof currently

SSID	BSSID	Authentication	Encryption	Network Type
------	-------	----------------	------------	--------------

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
No Wireless Profile Rules						

prof wireless site survey

Select	SSID	BSSID	Rate	Signal Strength	Channel	Authentication	Encryption	Network Type
<input type="radio"/>	Alfa_B	00:C0:CA:5F:40:C2	11 Mb/s	8/94(-89 dBm)	6	WPA1-Personal	TKIP/CCMP	Infrastructure
<input type="radio"/>	AP121	00:C0:CA:60:4B:E2	54 Mb/s	50/94(-76 dBm)	6	WPA2-Personal	CCMP	Infrastructure
<input type="radio"/>	Laser	B0:48:7A:85:01:C4	54 Mb/s	0/94(-95 dBm)	12	WPA2-Personal	CCMP	Infrastructure

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

prof currently

SSID	BSSID	Authentication	Encryption	Network Type
------	-------	----------------	------------	--------------

Profile List

Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
No Wireless Profile Rules						

prof profile setup

Profile Name  Network Type

SSID  BSSID(optional)

Security Mode  Encryption

Pass Phrase

basic ack timeout settings

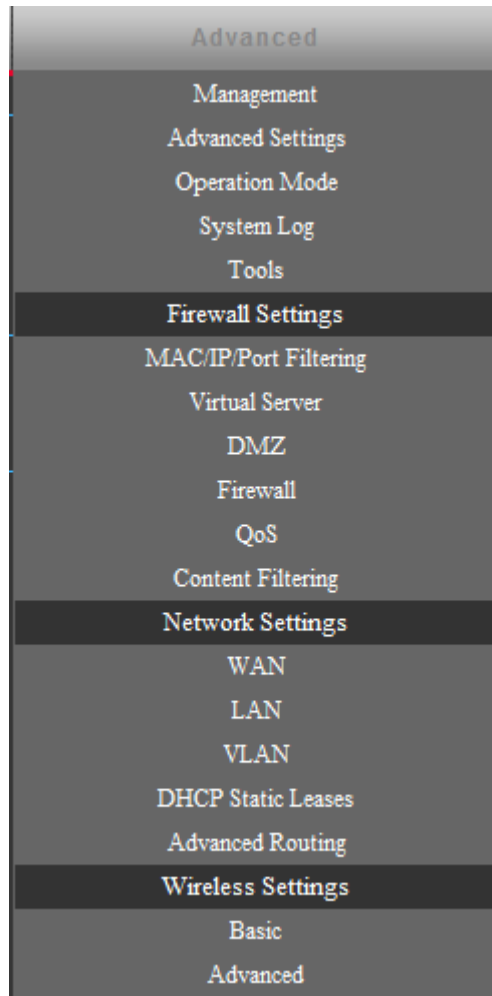
basic distance  basic miles (1.1 basic km)

basic acktimeout

TX Power  *This field is required. dBm*

## ADVANCED SETUP

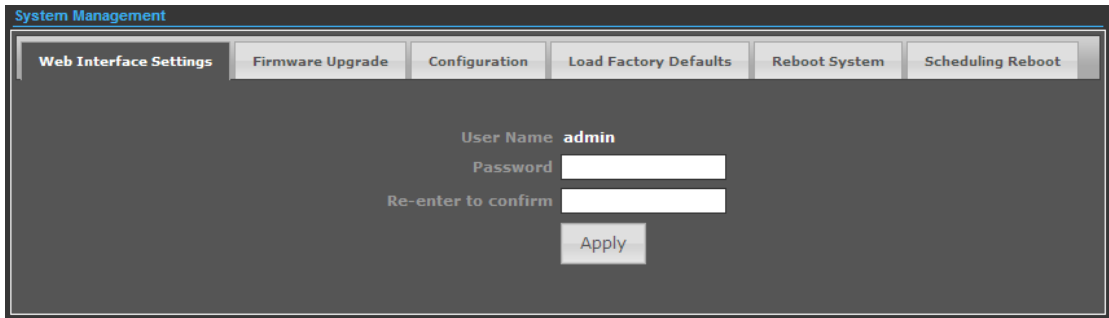
In the Advanced Manual Bar, it includes all the settings such as firmware upgrade, LAN, WAN and wireless settings that change the RF behaviors. It is important to read through this section before attempting to make changes.





## 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.



System Management

Web Interface Settings | Firmware Upgrade | Configuration | Load Factory Defaults | Reboot System | Scheduling Reboot

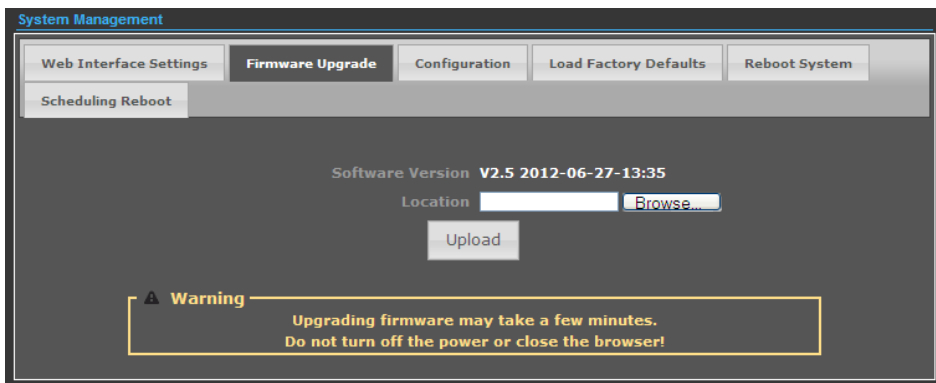
User Name **admin**

Password

Re-enter to confirm

Apply

- ◆ **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.



System Management

Web Interface Settings | **Firmware Upgrade** | Configuration | Load Factory Defaults | Reboot System

Scheduling Reboot

Software Version **V2.5 2012-06-27-13:35**

Location

Upload

**Warning**  
Upgrading firmware may take a few minutes.  
Do not turn off the power or close the browser!

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

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

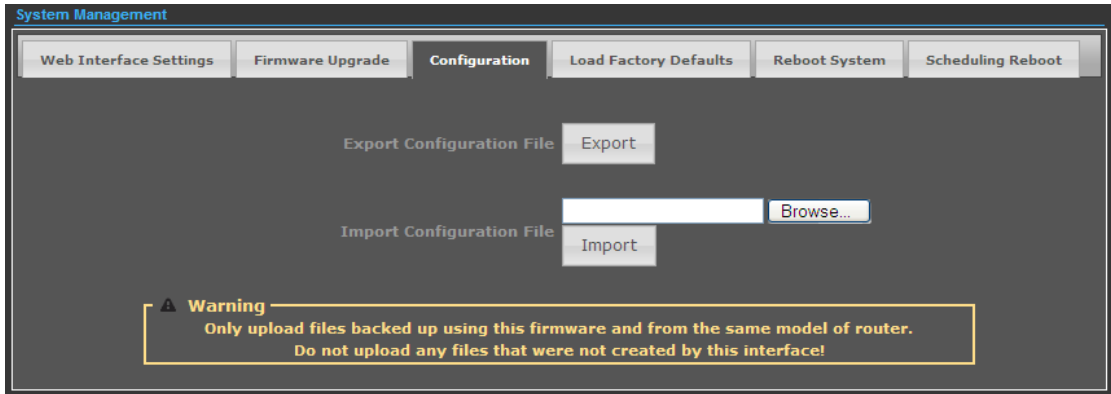
1. Download a more recent firmware upgrade file from our website.
2. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

### Note:

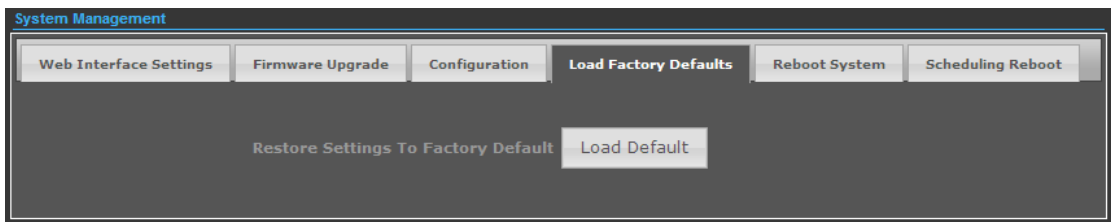
1. New firmware versions are posted at our website and can be downloaded for free.  
There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.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

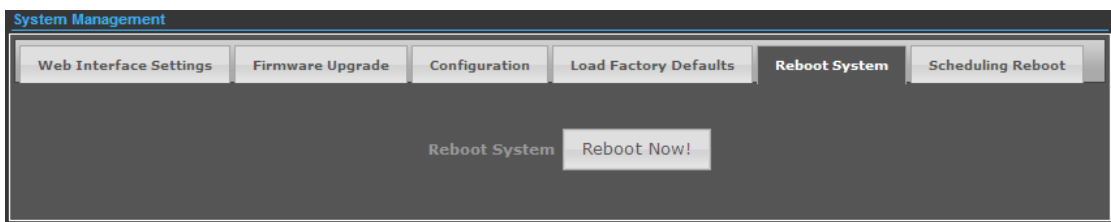
3. Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.
4. The Router will reboot after the upgrading has been finished.



- ◆ **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.



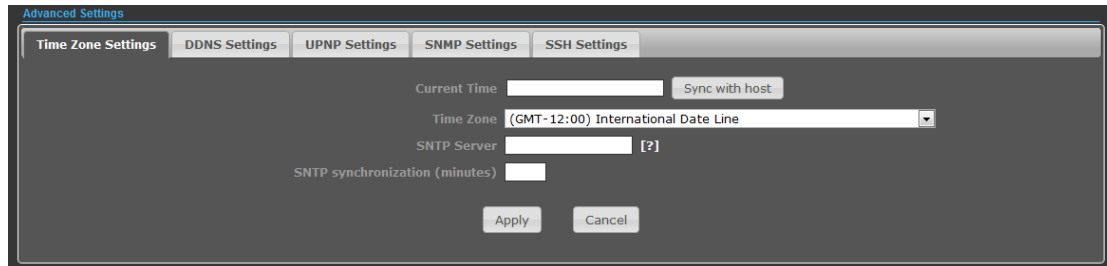
- ◆ **Load Factory Defaults** — If you have problems with TUBE-2H, which might be a result from changing some settings, but you are unsure what settings exactly, you can restore the factory defaults by click the Load Default Button.



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

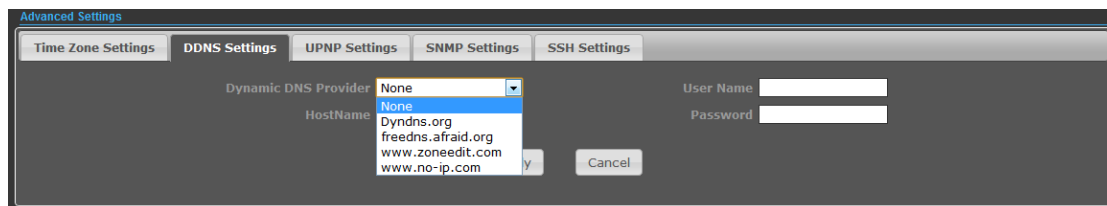
## ADVANCED SETTINGS

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



The screenshot shows the 'Advanced Settings' window with the 'Time Zone Settings' tab selected. The interface includes a 'Current Time' text box with a 'Sync with host' button, a 'Time Zone' dropdown menu currently set to '(GMT-12:00) International Date Line', an 'SNTP Server' text box with a help icon, and an 'SNTP synchronization (minutes)' text box. 'Apply' and 'Cancel' buttons are at the bottom.

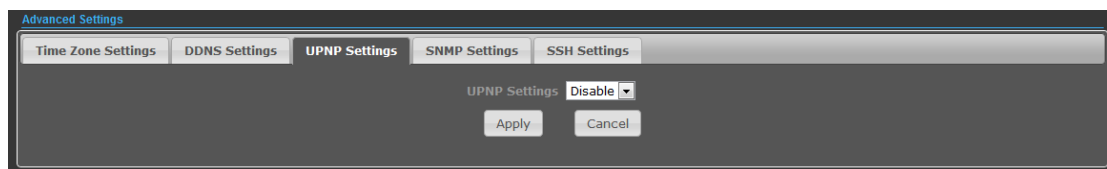
- ◆ **Time Zone Settings** — The Time Zone Settings allows you to configure, update and maintain the correct time on the TUBE-2H's internal system clock.
- ◆ **SNTP Server** — Enter the address of an SNTP server to receive time updates.
- ◆ **SNTP synchronization (minutes)** — Specify the interval between SNTP server updates.



The screenshot shows the 'Advanced Settings' window with the 'DDNS Settings' tab selected. A dropdown menu for 'Dynamic DNS Provider' is open, showing options: 'None', 'Dyndns.org', 'freedns.afraid.org', 'www.zoneedit.com', and 'www.no-ip.com'. To the right are 'User Name' and 'Password' text boxes. 'Apply' and 'Cancel' buttons are at the bottom.

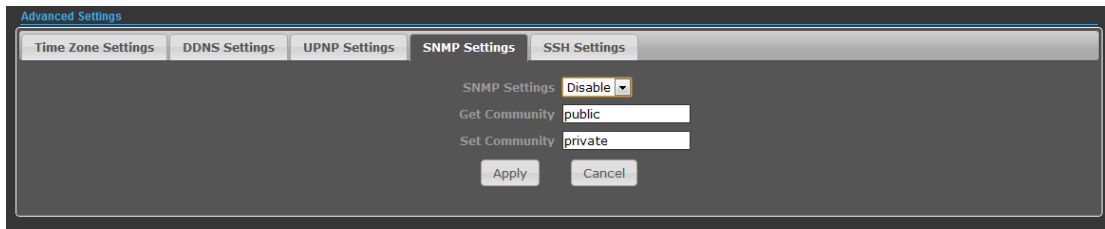
**DDNS Settings** — DDNS lets you assign a fixed host and domain name to dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the TUBE-2H. Before using this feature, you need to sign up for DDNS service at [www.dyndns.org](http://www.dyndns.org)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

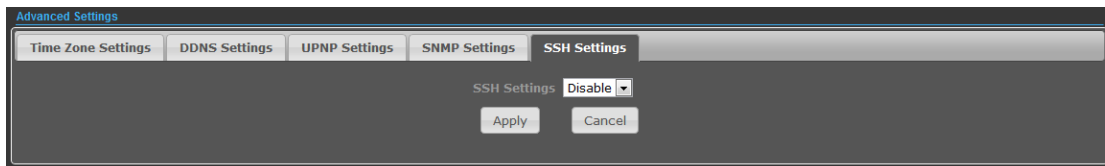


The screenshot shows the 'Advanced Settings' window with the 'UPNP Settings' tab selected. The 'UPNP Settings' dropdown menu is set to 'Disable'. 'Apply' and 'Cancel' buttons are at the bottom.

**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.



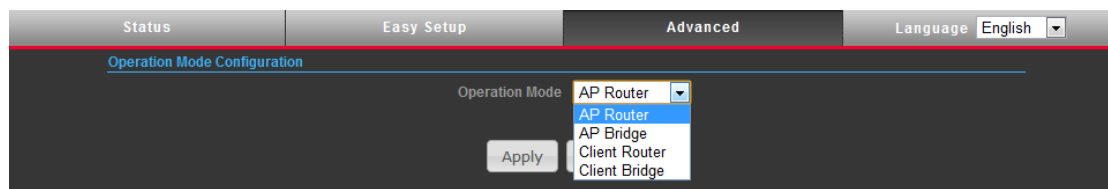
**SNMP Settings** – Managing devices on IP networks. Default setting is Disabled.



**SSH Settings** – Secure Shell. Enable your TUBE-2H unit 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** — The TUBE-2H will 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** — The TUBE-2H will 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.

## 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-2H allows 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.

No.	MAC address	DIP	SIP	Protocol	DPR	SPR	Action	Comment
Others would be accepted								

- ◆ **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 NAT enabled router.

Virtual Server

Virtual Server Settings

IP Address

Private Port

Public Port

Protocol

Comment

(The maximum rule count is 32.)

Current Virtual Servers in system

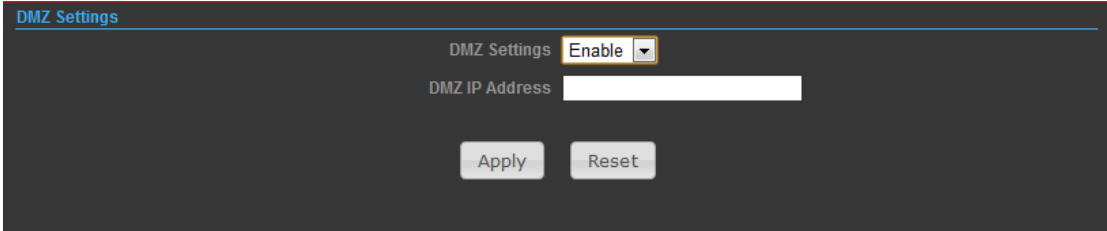
No.	IP Address	Port Mapping	Protocol	Comment

- ◆ **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-2H'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 a static IP address (which is mapped to its MAC address) and this must be configured as the DMZ IP address.



The screenshot shows a 'DMZ Settings' window with a dark background. At the top left, the title 'DMZ Settings' is displayed in blue. Below the title, there are two main settings: 'DMZ Settings' with a dropdown menu currently set to 'Enable', and 'DMZ IP Address' with an empty white text input field. At the bottom of the window, there are two buttons: 'Apply' and 'Reset'.

- ◆ **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 utilize firmware functions to protect your network from hackers and malicious intruders.

The screenshot displays a configuration page with the following sections and settings:

- Remote Management Access:** Remote Management (via WAN) is set to **Deny**. Remote Management Port is set to **2020**.
- Ping from WAN Filter:** Ping from WAN Filter is set to **Allow**.
- Stateful Packet Inspection (SPI):** SPI Firewall is set to **Disable**.
- Network Address Translation Settings:** Network Address Translation is set to **Enable**.
- PPPoE Passthrough Settings:** PPPoE Passthrough Setup is set to **Disable**.

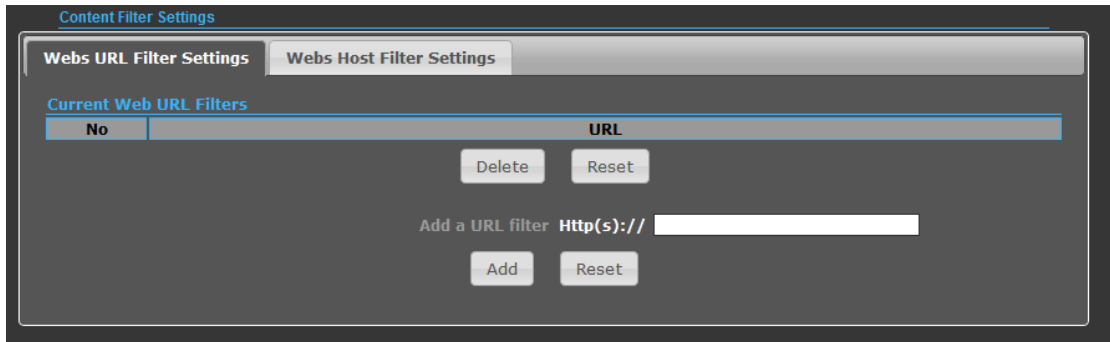
At the bottom of the page, there are **Apply** and **Reset** buttons.

- ◆ **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-2H from Internet, you would use a URL of the form:  
`http://xxx.xxx.xxx.xxx:2020/`
- ◆ **Ping from WAN Filter** — When Allow, the TUBE-2H does 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.

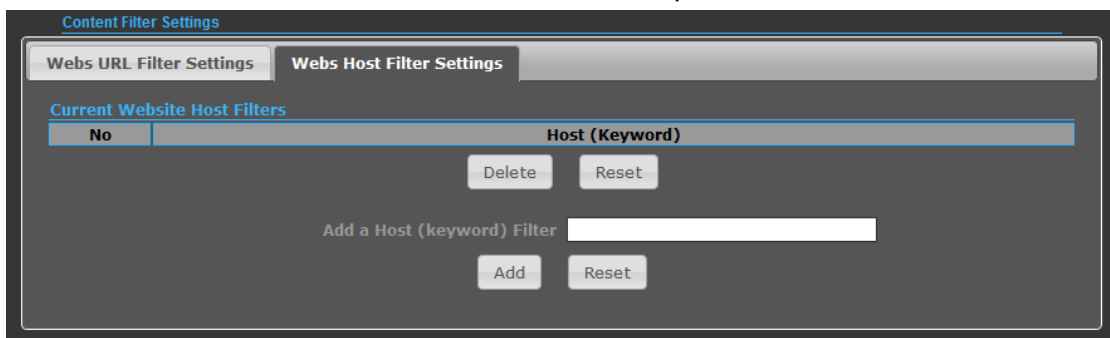


## CONTENT FILTERING

The TUBE-2H provides 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** — Allows Internet 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)

The screenshot shows the 'Wide Area Network (WAN) Settings' window. At the top, 'WAN Connections' is set to 'Cable/Dynamic IP (DHCP)'. Below this, the 'DHCP Mode' section is active, showing 'Hostname' set to 'DHCP'. The 'DNS Settings (Optional)' section has empty text boxes for 'Primary DNS Server' and 'Secondary DNS Server'. At the bottom are 'Apply' and 'Cancel' buttons.

- ◆ **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)

The screenshot shows the 'Wide Area Network (WAN) Settings' window. At the top, 'WAN Connections' is set to 'PPPoE (ADSL)'. Below this, the 'PPPoE Mode' section is active. It includes fields for 'User Name' (pppoe\_user), 'Password' (masked with dots), and 'Verify Password' (masked with dots). The 'Operation Mode' is set to 'Keep Alive' with a dropdown arrow. Below it, 'MTU' is set to '1492 bytes (Default=1492)'. To the right, 'Keep Alive Mode: Redial Period' is set to '60 Seconds'. The 'DNS Settings (Optional)' section has empty text boxes for 'Primary DNS Server' and 'Secondary DNS Server'. At the bottom are 'Apply' and 'Cancel' buttons.

- ◆ **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)

The screenshot shows the 'Wide Area Network (WAN) Settings' window. At the top, 'WAN Connections' is set to 'Static (Fixed IP)'. Below this, the 'Static Mode' section contains three input fields: 'IP Address' with the value '192.168.3.1', 'Subnet Mask' with the value '255.255.255.0', and 'Default Gateway' which is empty. A 'DNS Settings' section below has 'Primary DNS Server' and 'Secondary DNS Server' fields, both empty. At the bottom are 'Apply' and 'Cancel' buttons.

- ◆ **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 Domain Name Server.

## PPTP

The screenshot shows the 'PPTP Mode' configuration window. It includes several fields: 'Server IP' (pptp\_server), 'User Name' (pptp\_user), 'Password' (masked with dots), 'Address Mode' (Static IP), 'IP Address' (empty), 'Subnet Mask' (empty), 'Operation Mode' (Keep Alive), and 'Keep Alive Mode: Redial Period' (60 Seconds). Below these is a 'DNS Settings (Optional)' section with 'Primary DNS Server' and 'Secondary DNS Server' fields, both empty. 'Apply' and 'Cancel' buttons are at the bottom.

- ◆ **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

The screenshot shows the 'Wide Area Network (WAN) Settings' page with the 'WAN Connections' dropdown set to 'IPSEC'. Below this, the 'wan ipsec mode' section is expanded, showing various configuration options. The 'Connection address family' is set to 'IPv4'. The 'IPSec Connection Type' is 'Road Warrior Tunnel'. 'IPSec Authentication' is 'SHA-1'. 'SA connection Life Time' is set to 1 hour. 'Local IP Address', 'Local Subnet', and 'Local Gateway' are empty fields. 'IPSec Tunnel Name' is 'accCONN'. 'IPSec Key Life time' is '12h'. 'NAT Transversal' and 'IPSec Compression' are unchecked. 'IPSec Operation Mode' is 'add'. 'PFS/DH Group' is 'modp1024'. 'IPSec Encryption' is 'AES'. 'IKE Key Tries' is '3'. 'Peer IP Address', 'Peer Subnet', and 'Peer Gateway' are empty fields. 'IPSec Secret Key' is 'PSK'. 'Perfect Forward Secrets' and 'IPSec Conn. Keep Alive' are unchecked. At the bottom, there are 'Apply' and 'Cancel' buttons. Below the main settings, there is a 'DNS Settings (Optional)' section with 'Primary DNS Server' and 'Secondary DNS Server' fields, both empty.

Verify the desired 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 through, 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

**L2TP Mode**

Server IP: l2tp\_server

User Name: l2tp\_user Password: .....

Address Mode: Static IP

IP Address:

Subnet Mask:

Operation Mode: Keep Alive Keep Alive Mode: Redial Period: 60 Seconds

**DNS Settings (Optional)**

Primary DNS Server: Secondary DNS Server:

Apply Cancel

- ◆ **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 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.

## 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.

**LAN Setup**

MAC Address: 00:C0:CA:60:B8:AC

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

**DHCP Setup**

DHCP Server: DHCP Server

Local Domain Name (Optional):

Start IP Address: 192.168.2.100

End IP Address: 192.168.2.199

Lease Time: One day

Apply Cancel

- ◆ **IP Address** — The IP address of TUBE-2H on the local area network.  
( Default: 192.168.2.1 )
- ◆ **Subnet Mask** — The subnet mask of TUBE-2H on the local area network
- ◆ **DHCP Server** — The DHCP Server is to assign private IP address to the TUBE-2H in 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-2H.

**Advanced Routing Settings**

Add a routing rule

Destination

Type

Gateway

Interface

Comment

**Current Routing table in the system**

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	192.168.2.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	

**Dynamic Routing Protocol**

RIP

- ◆ **Destination** — The IP address of 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

Basic Wireless Settings

Wireless Mode: Access Point

Multiple SSID:

Country Code: Germany

Frequency (Channel): 2437 MHz (Channel 6)

Site Survey:

Network Mode: WiFi 11gn HT20

Extension Channel: Upper Channel

Distance:  0.8 miles (km)

ACK Timeout: 35

SSID Security Settings

Network Name (SSID): SSID NAME  Hide

WPS Choice:

Encryption Settings: Disable

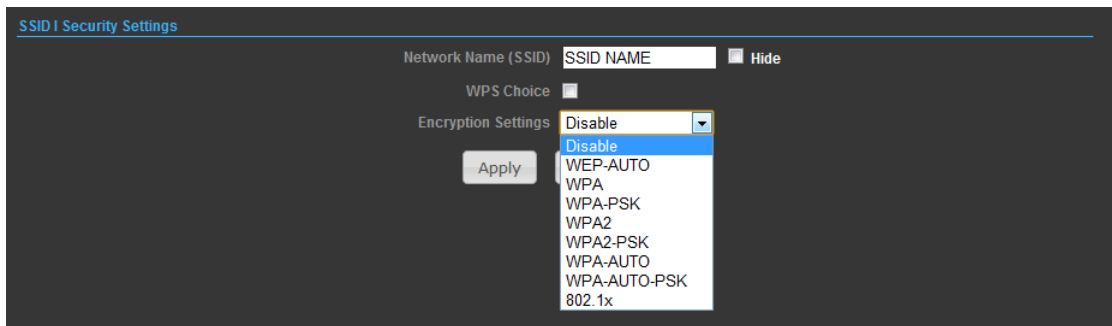
- ◆ **Wireless On/Off** — Enables or Disable the radio. (Default: Turn On)
- ◆ **Wireless Mode** — There are 4 wireless mode, those are Access Point, WDS Access Point, WDS Repeater and WDS Client

#### Note.

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

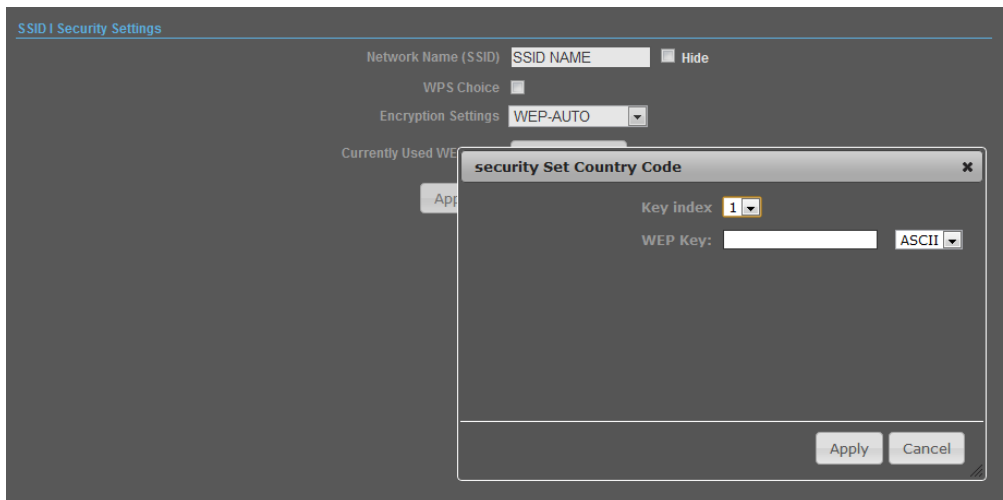
- ◆ **Network Name (SSID)** — The name of the wireless network service provided by the TUBE-2H. Clients that want to connect to the network must set their SSID to the same as that of TUBE-2H.
- ◆ **Multiple SSID** — One additional VAP interface supported on the device.
- ◆ **Frequency (Channel)** — The radio channel that the TUBE-2H uses to communicate with wireless clients.
- ◆ **Network Mode** — Defines the radio operating mode.

## SECURITY



### WIRED EQUIVALENT PRIVACY (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.



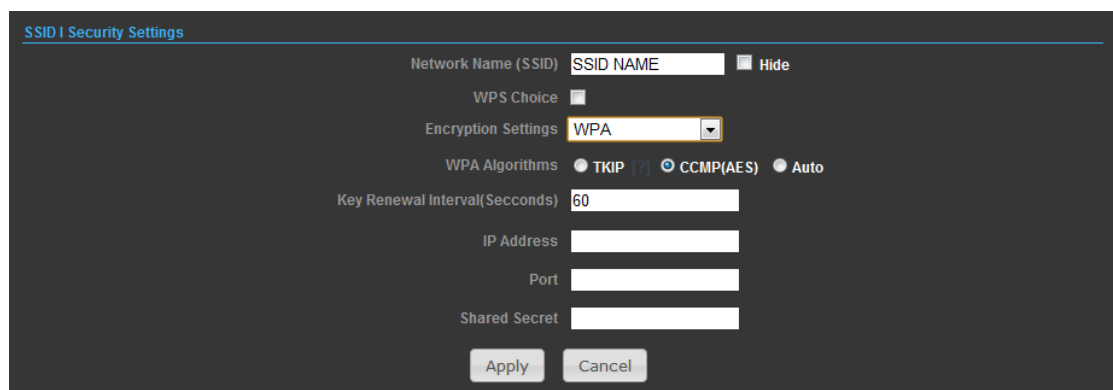
◆ **WEP Keys** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 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.



The screenshot shows the 'SSID Security Settings' window. It includes the following fields and options:

- Network Name (SSID): SSID NAME (with a 'Hide' checkbox)
- WPS Choice:
- Encryption Settings: WPA (dropdown menu)
- WPA Algorithms:  TKIP,  CCMP(AES),  Auto
- Key Renewal Interval(Seconds): 60
- IP Address: [empty text box]
- Port: [empty text box]
- Shared Secret: [empty text box]
- Buttons: Apply, Cancel

- ◆ **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.

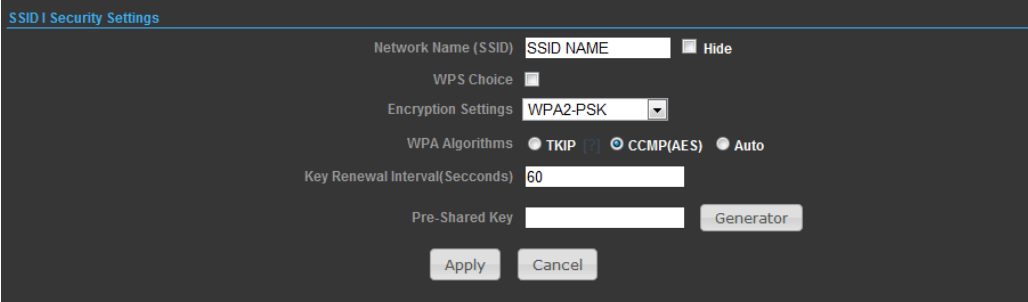
- ◆ **IP Address** — Specifies the IP address of the RADIUS server.

- ◆ **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.



The screenshot shows the 'SSID Security Settings' configuration window. It includes the following fields and options:

- Network Name (SSID): SSID NAME (with a 'Hide' checkbox)
- WPS Choice: [checkbox]
- Encryption Settings: WPA2-PSK (dropdown menu)
- WPA Algorithms: TKIP (radio button), CCMP(AES) (radio button), Auto (radio button)
- Key Renewal Interval(Seconds): 60 (text input)
- Pre-Shared Key: [text input] (with a 'Generator' button)
- Buttons: Apply, Cancel

- ◆ **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 AND RADIUS

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.

The screenshot shows the 'SSID Security Settings' configuration page. It includes the following fields and options:

- Network Name (SSID): SSID NAME (with a 'Hide' checkbox)
- WPS Choice:
- Encryption Settings: 802.1x (dropdown menu)
- IP Address: [Text Input]
- Port: [Text Input]
- Shared Secret: [Text Input]
- Buttons: Apply, Cancel

**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.

The screenshot shows the 'WPS Summary' section of the 'SSID Security Settings' page. It includes the following fields and options:

- WPS Choice:  (highlighted with a red box)
- WPS SSID: SSID NAME
- AP PIN: [Text Input]
- Device Name: [Text Input]
- Encryption Settings: WPA-PSK (dropdown menu)
- WPA Algorithms:  TKIP,  CCMP(AES),  Auto
- Key Renewal Interval(Seconds): 60
- Pre-Shared Key: [Text Input] (with a 'Generator' button)
- Buttons: Apply, Cancel

- ◆ **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) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCAMP) 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)