

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

TABLE OF CONTENTS

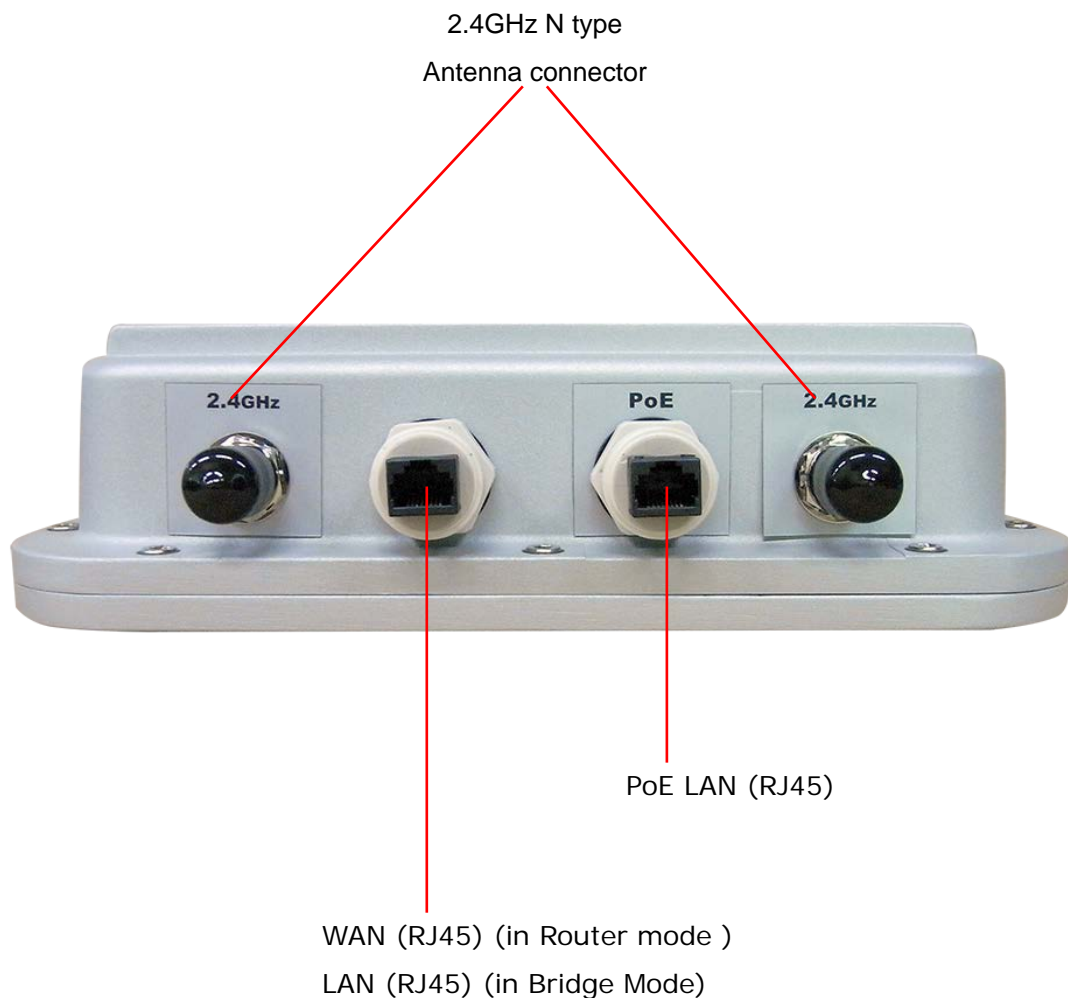
INTRODUCTION	3
HARDWARE DESCRIPTION	3
HARDWARE INSTALLATION	4
INITIAL CONFIGURATION	6
CONNECTING TO THE LOGIN PAGE	6
STATUS PAGE	6
EASY SETUP	7
OPERATION MODE – AP ROUTER	7
SETTINGS – PPPoE(ADSL)	8
SETTINGS – STATIC (FIXED IP)	9
SETTINGS – CABLE/DYNAMIC IP (DHCP)	10
SETTINGS – PPTP	11
SETTINGS – L2TP	12
OPERATION MODE – AP BRIDGE	14
OPERATION MODE – CLIENT ROUTER	14
OPERATION MODE – CLIENT BRIDGE	16
ADVANCED SETUP	17
MANAGEMENT	18
ADVANCED SETTINGS	21
OPERATION MODE	22
FIREWALL CONFIGURATION	23
MAC/IP/PORT FILTERING	23
VIRTUAL SERVER SETTINGS	24
DMZ	25
FIREWALL	26
CONTENT FILTERING	27
NETWORK SETTINGS	28
WAN	28
LAN	31
ADVANCED ROUTING	32
WIRELESS SETTINGS	33
BASIC	33
SECURITY	34

INTRODUCTION

The AP is a IEEE 802.11b/g/n wireless outdoor AP/CPE which support data rates up to 300Mbps. It is rain and splash proof when install in upright position. AP has two N-type connector for external antenna and passive PoE for simplify installation.

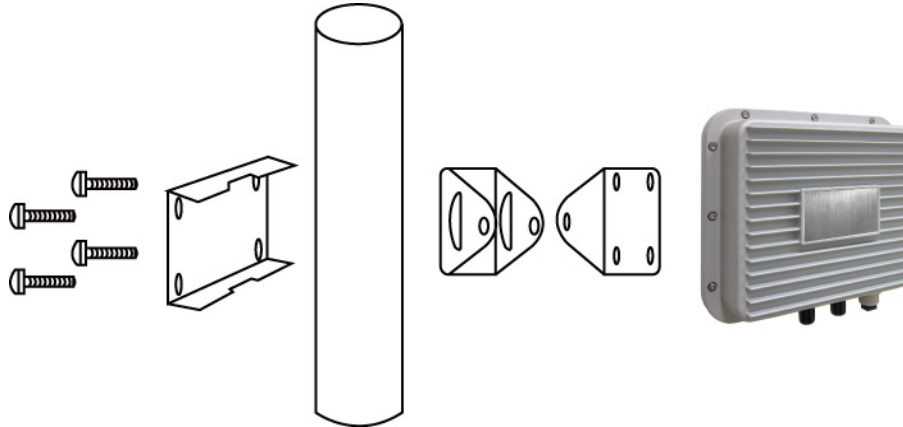
HARDWARE DESCRIPTION

Below are AP hardware descriptions

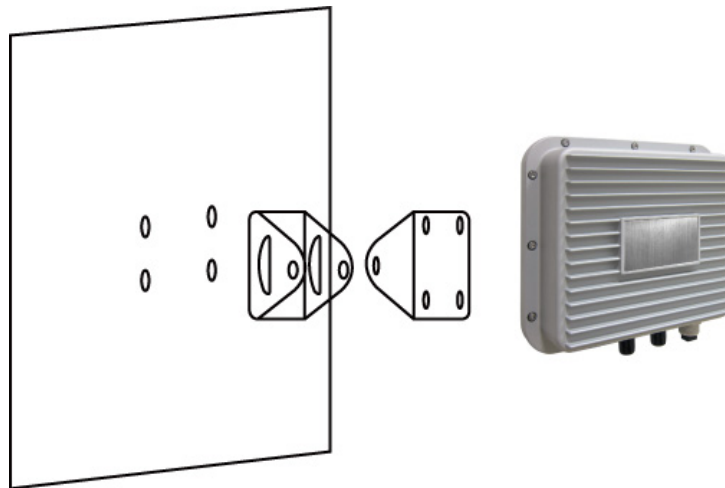


HARDWARE INSTALLATION

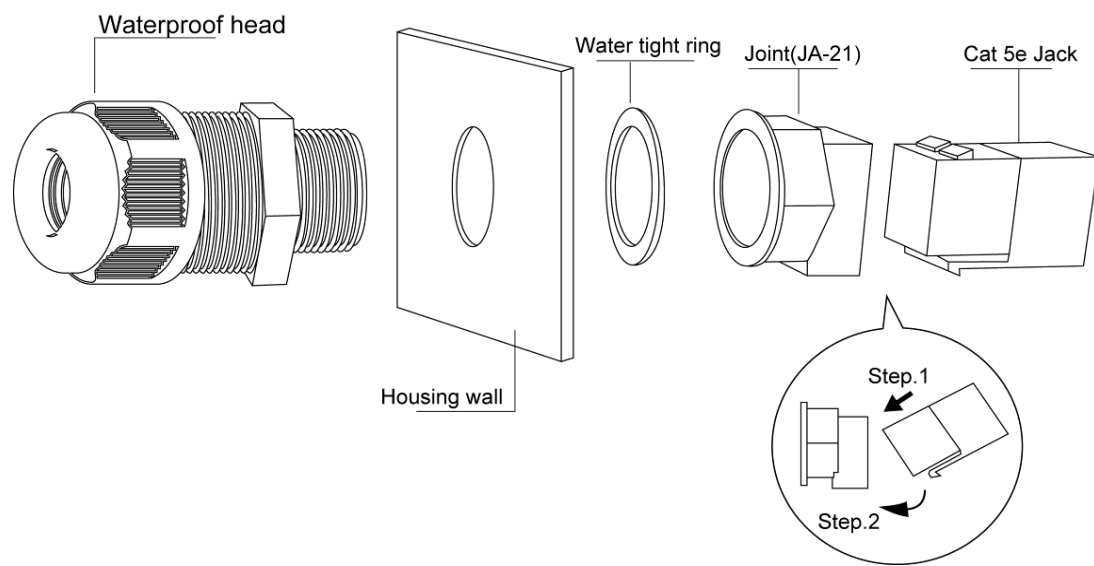
◆ □ Pipe Mounting Figure



◆ Wall Mounting Figure



◆ Waterproof wiring kit installation diagram



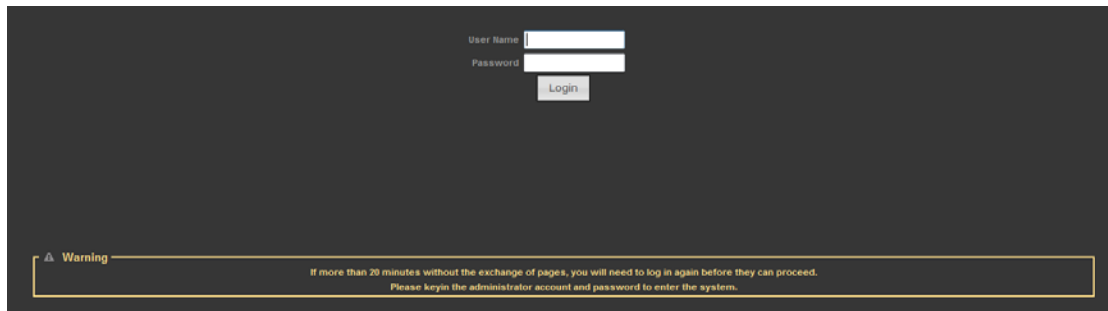
INITIAL CONFIGURATION

The AP, 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 AP's LAN port. The AP 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 AP (that is, the PC and AP addresses must both start 192.168.2.x). To access the AP'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 login 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.

Internet Configuration	
Connected Type DHCP	Connected Status Disconnected/Connecting...
WAN IP Address	Subnet Mask
Default Gateway	Primary Domain Name Server
Secondary Domain Name Server	MAC Address E0:8F:EC:60:B8:AD
LAN Configuration	
LAN IP Address 192.168.2.1	LAN Netmask 255.255.255.0
MAC Address E0:8F:EC:60:B8:AC	
System Info	
Firmware Version V2.1 2012-03-23-15:55	System Time Mon, 09 Apr 2012 20:39:12
Operation Mode AP Router mode	

EASY SETUP

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

Click on Easy Setup to bring up the wizard

Operation Mode Setup	
Please select an Operation Mode	<div> <div>Please select an Operation Mode</div> <div> <div>Please select an Operation Mode</div> <div>AP Router</div> <div>AP Bridge</div> <div>Client Router</div> <div>Client Bridge</div> </div> </div>

OPERATION MODE – AP ROUTER

In AP Router mode, your 11N AP unit is turned to a wireless router and wireless interface will become the LAN side; if your PC is connected to the PoE port, the management IP will change to the LAN IP (192.168.2.1). The remote management will be automatically turned on to allow you managing the device from the PoE LAN port.

Operation Mode Setup	
Please select an Operation Mode	<div> <div>Please select an Operation Mode</div> <div> <div>Please select an Operation Mode</div> <div>AP Router</div> <div>AP Bridge</div> <div>Client Router</div> <div>Client Bridge</div> </div> </div>

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).

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

2)

The screenshot shows the 'Wide Area Network (WAN) Settings' page with 'WAN Connections' set to 'PPPoE (ADSL)'. The 'PPPoE Mode' section contains fields for 'User Name' (pppoe_user), 'Password' (masked), 'Verify Password' (masked), 'Operation Mode' (Keep Alive), 'Keep Alive Mode: Redial Period' (60 seconds), and 'wan pppoe mtu' (1492 bytes). Below are 'Primary DNS Server' and 'Secondary DNS Server' fields, and 'Next' and 'Back' 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.

3)

The screenshot shows the 'secure ssid 1 title' page. It has a 'Network Name (SSID)' field with 'SSID_NAME' and a 'Hide' checkbox. Below are 'secure wps choice' and 'Security Mode' (set to 'Disable'). At the bottom, it says 'No Security Applied' and has 'Done' and 'wireless back' buttons.

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)

The screenshot shows the 'Wide Area Network (WAN) Settings' page. The 'WAN Connections' dropdown menu is open, displaying options: 'Cable/Dynamic IP (DHCP)', 'Static (Fixed IP)' (highlighted), 'Cable/Dynamic IP (DHCP)', 'PPPoE (ADSL)', 'PPTP', and 'L2TP'. Below the menu, the 'DHCP Mode' section is visible, followed by the 'inet wc dns op' section with fields for 'Primary DNS Server' and 'Secondary DNS Server'. 'Next' and 'Back' buttons are at the bottom.

- 2)

The screenshot shows the 'Wide Area Network (WAN) Settings' page with 'Static (Fixed IP)' selected in the 'WAN Connections' dropdown. The 'Static Mode' section is active, showing fields for 'IP Address' (192.168.3.1), 'Subnet Mask' (255.255.255.0), and 'Default Gateway'. Below this is the 'DNS Settings (Optional)' section with fields for 'Primary DNS Server' and 'Secondary DNS Server'. 'Next' and 'Back' buttons are at the bottom.

- ◆ ☐ **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)

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.

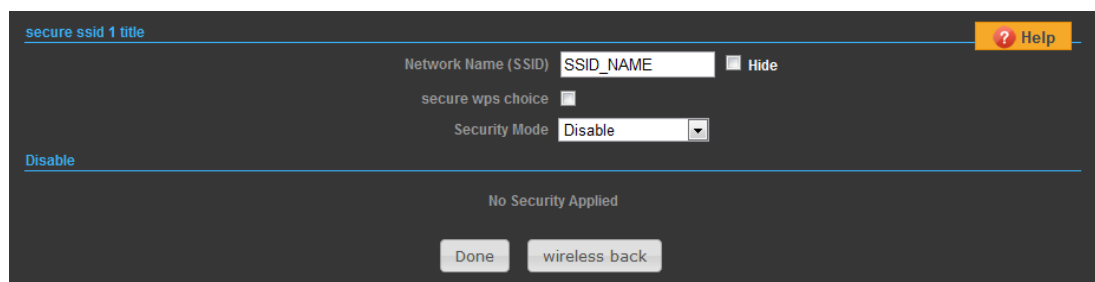
2)

- ◆ ☐ **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)

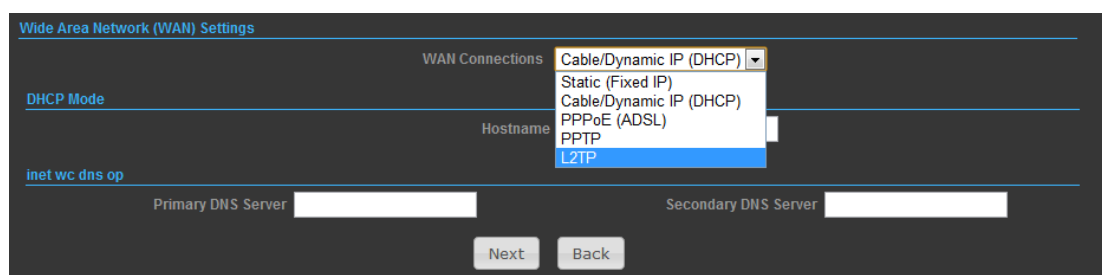


Network Name (SSID) — SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

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)

The screenshot shows the 'Wide Area Network (WAN) Settings' interface. At the top, 'WAN Connections' is set to 'L2TP'. Under the 'L2TP Mode' section, the following fields are visible: 'Server IP' (l2tp_server), 'User Name' (l2tp_user), 'Password' (masked with dots), 'Address Mode' (Static), 'IP Address' (empty), 'Subnet Mask' (empty), 'Operation Mode' (Keep Alive), and 'Keep Alive Mode: Redial Period' (60 seconds). Below this, the 'inet wc dns op' section shows 'Primary DNS Server' and 'Secondary DNS Server' fields, both empty. At the bottom 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.

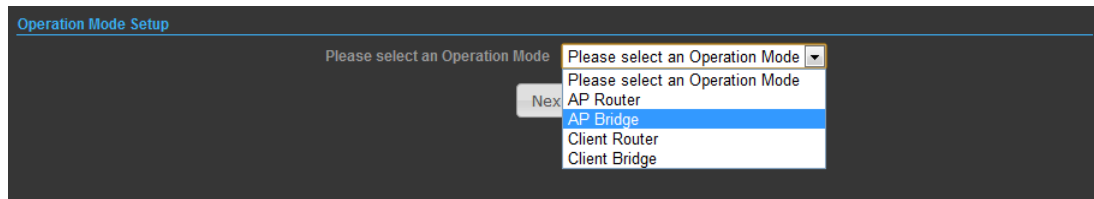
3)

The screenshot shows the 'secure ssid 1 title' interface. It includes a 'Network Name (SSID)' field with 'SSID_NAME' and a 'Hide' checkbox. Below this is a 'secure wps choice' checkbox and a 'Security Mode' dropdown menu set to 'Disable'. A 'Disable' link is on the left. At the bottom, it says 'No Security Applied' and has 'Done' and 'wireless back' buttons. A 'Help' button is in the top right corner.

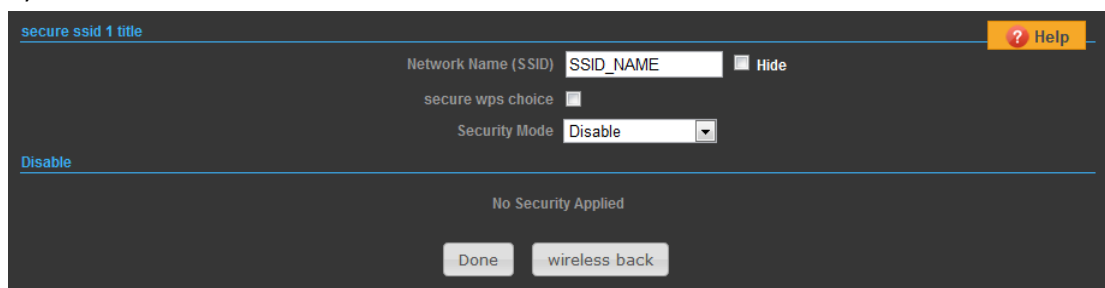
- Network Name (SSID)** — SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.
- Security Mode** — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

OPERATION MODE – AP BRIDGE

1) In this mode bridge your AP to another Access Point.



2)

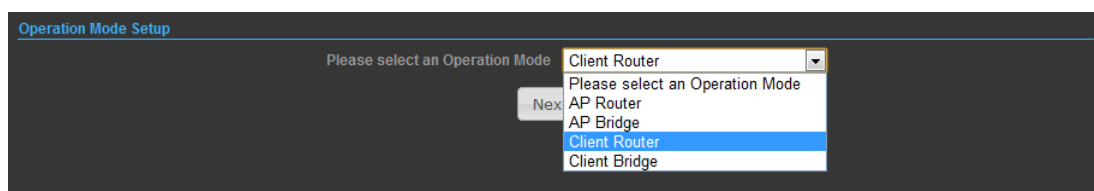


Network Name (SSID) — SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

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; Default: Disabled)

OPERATION MODE – CLIENT ROUTER

In the Client Router mode is also known as WISP. The AP 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; MikroTik_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"/>	MikroTik_B	E0:8F:EC:5F:40:C2	11 Mb/s	8/94(-89 dBm)	6	WPA1-Personal	TKIP/CCMP	Infrastructure
<input type="radio"/>	AP121	E0:8F:EC:60:4B:E2	54 Mb/s	50/94(-76 dBm)	6	WPA2-Personal	CCMP	Infrastructure
<input type="radio"/>	Laservideo TP-LINK	B0:48:7A:B5:01: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 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

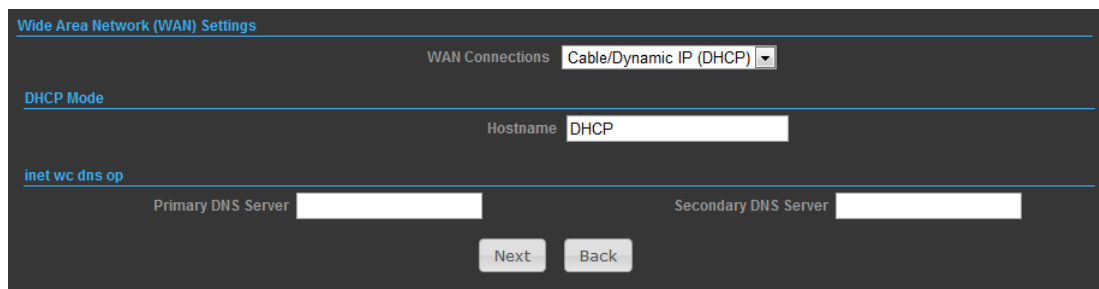
basic ack timeout settings

basic distance basic miles (1.1 basic km)

basic acktimeout

TX Power *This field is required. dBm*

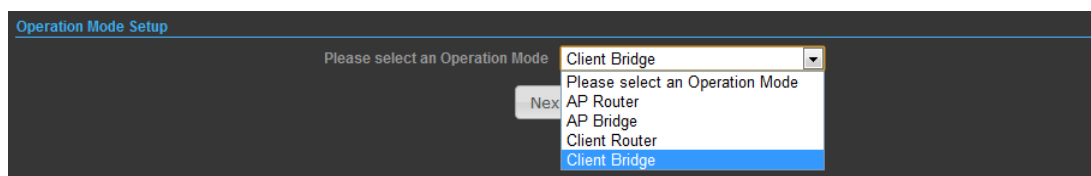
- 4) Finally, you need to tell the system about IP address received from WAN, DHCP Hostname, and DNS Server then press **Next** button to finish the wizard.



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 has a 'Hostname' field set to 'DHCP'. The 'inet wc dns op' section has fields for 'Primary DNS Server' and 'Secondary DNS Server', both currently empty. At the bottom, there are 'Next' and 'Back' buttons.

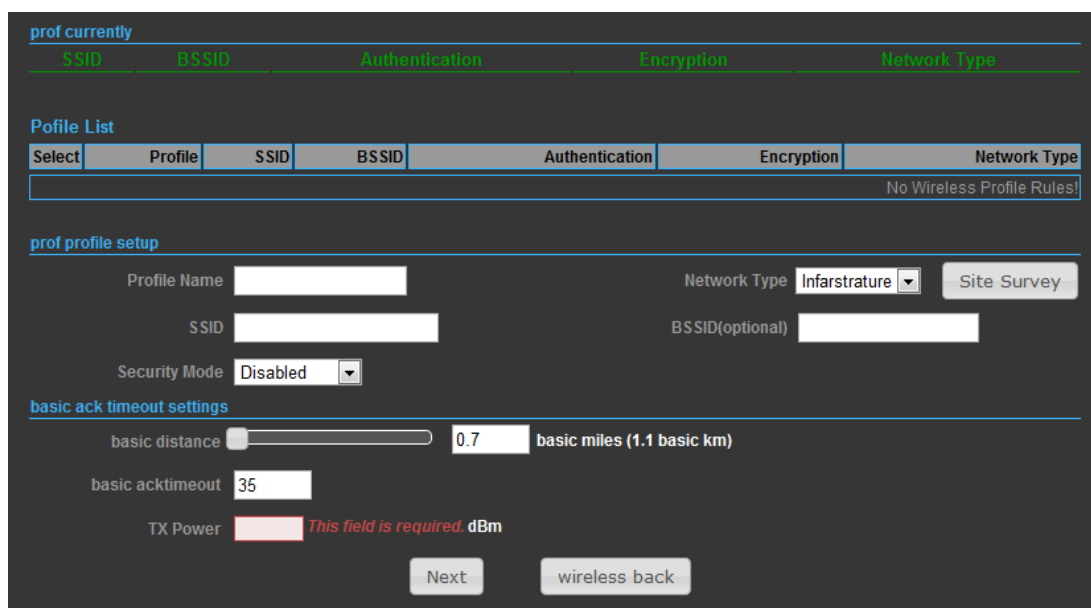
OPERATION MODE – CLIENT BRIDGE

In the Client Bridge mode your AP 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.

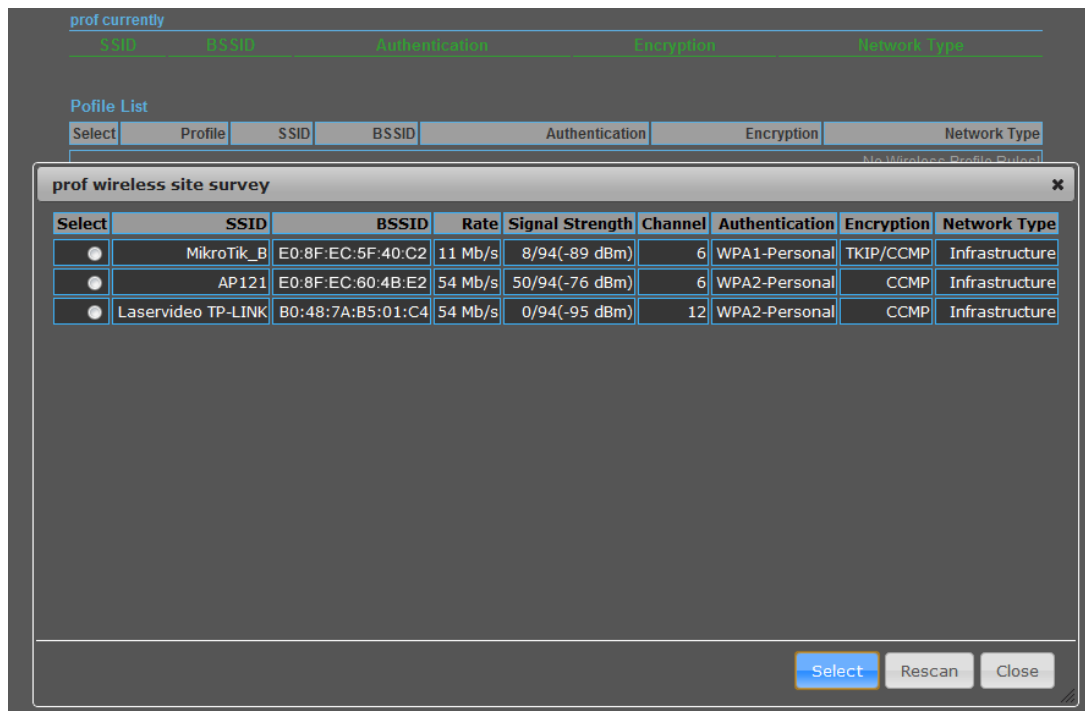


The screenshot shows the 'Operation Mode Setup' window. A dropdown menu is open, showing options: 'Client Bridge', 'Please select an Operation Mode', 'AP Router', 'AP Bridge', 'Client Router', and 'Client Bridge' (highlighted). A 'Next' button is visible to the left of the dropdown.

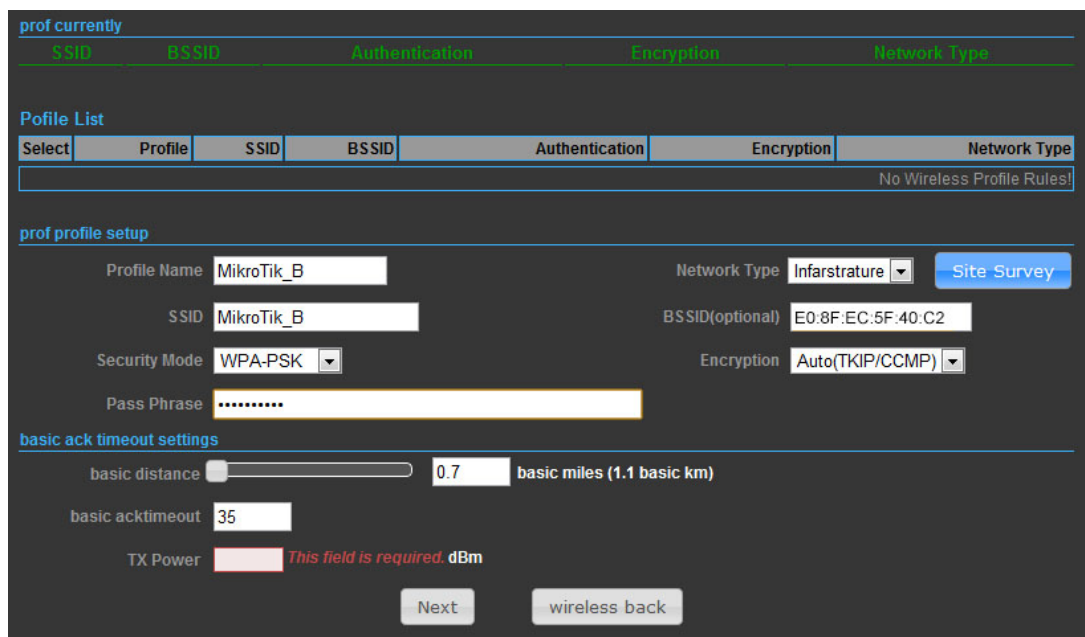
- 2) Press **Site Survey** button and look for available wireless network then click on the SSID that you attempt to connect to it; MikroTik_B is the SSID that we are going to connect in this example. Press **Next** button when finished.



The image contains two screenshots from the MikroTik WinBox interface. The top screenshot shows the 'Profile List' table, which is currently empty with the message 'No Wireless Profile Rules!'. The bottom screenshot shows the 'profile setup' window. It has fields for 'Profile Name', 'SSID', 'Security Mode' (set to 'Disabled'), 'Network Type' (set to 'Infrastructure'), and 'BSSID(optional)'. There is a 'Site Survey' button. Below this, the 'basic ack timeout settings' section includes a slider for 'basic distance' (set to 0.7), a text field for 'basic acktimeout' (set to 35), and a red text field for 'TX Power' with the message 'This field is required. dBm'. At the bottom, there are 'Next' and 'wireless back' buttons.



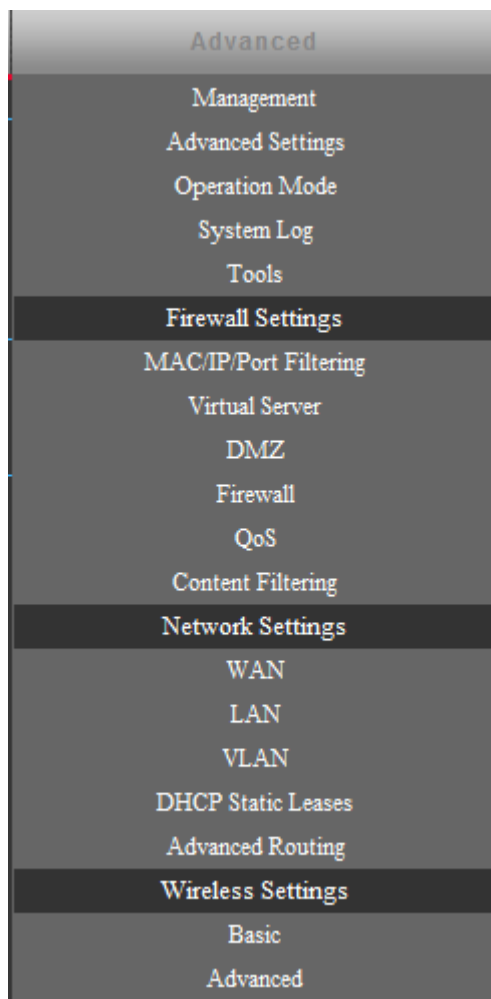
- 3) Now, it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Next** button to finish the wizard.



ADVANCED SETUP

In the Advanced Manual Bar, it includes all the settings such as firmware upgrade,

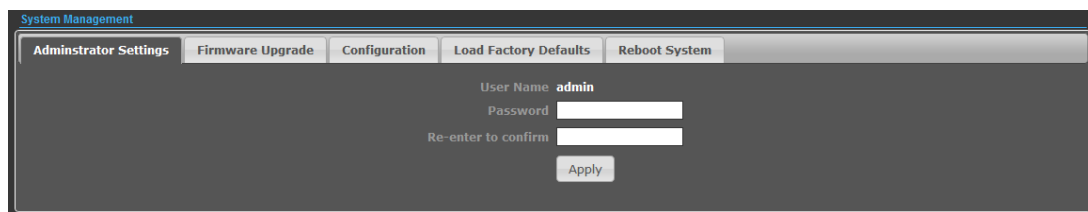
LAN, WAN and wireless settings that change the RF behaviors. It is important to read through this section before attempting to make changes.



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.



The screenshot shows the 'System Management' interface with the 'Administrator Settings' tab selected. It contains fields for 'User Name' (pre-filled with 'admin'), 'Password', and 'Re-enter to confirm'. An 'Apply' button is located at the bottom right of the form.

◆ ☐ **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.



The screenshot shows the 'System Management' interface with the 'Firmware Upgrade' tab selected. It displays the 'Software Version' as 'V2.2 2012-04-02-13:31' and the 'Location' as '選擇檔案' (Select File) and '未選擇檔案' (No file selected). An 'Upload' button is present. A warning message is shown in a yellow box: 'Warning: Upgrading firmware may take a few minutes. Do not turn off the power or close the browser!'.

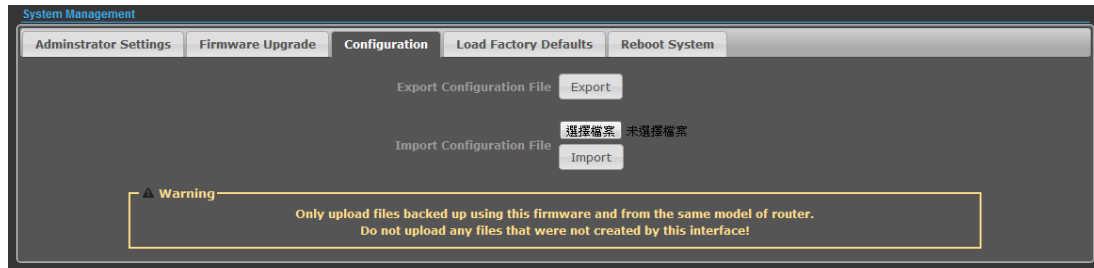
◆ ☐ **Software Version** - This displays the current firmware version.

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.

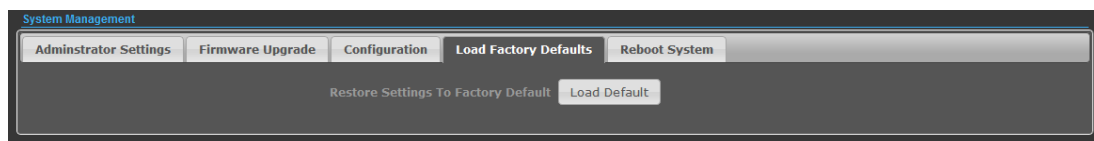
Note:

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.

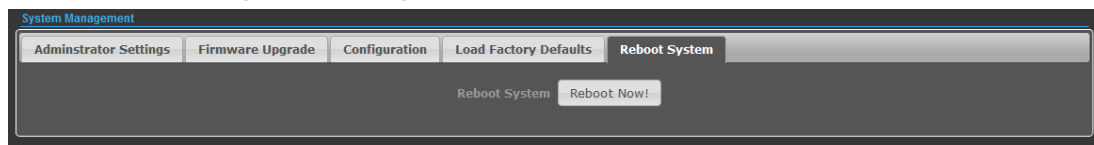


◆ ☐ **Export Settings** — Click the Export Button to download current router configuration to your PC.

◆ ☐ **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 AP, 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 AP, 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 window has a title bar 'Advanced Settings' and five tabs: 'Time Zone Settings', 'DDNS Settings', 'UPNP Settings', 'SNMP Settings', and 'SSH Settings'. The 'Time Zone Settings' tab contains the following fields: 'Current Time' with a text input and a 'Sync with host' button; 'Time Zone' with a dropdown menu showing '(GMT-12:00) International Date Line'; 'SNTP Server' with a text input and a '[?]' button; and 'SNTP synchronization (minutes)' with a text input. At the bottom are 'Apply' and 'Cancel' buttons.

◆ ☐ **Time Zone Settings** — The Time Zone Settings allows you to configure, update and maintain the correct time on the AP'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. The window has a title bar 'Advanced Settings' and five tabs: 'Time Zone Settings', 'DDNS Settings', 'UPNP Settings', 'SNMP Settings', and 'SSH Settings'. The 'DDNS Settings' tab contains the following fields: 'Dynamic DNS Provider' with a dropdown menu showing 'None' and a list of providers (DynDNS.org, freedns.afraid.org, www.zoneedit.com, www.no-ip.com); 'HostName' with a text input; 'User Name' with a text input; and 'Password' with a text input. At the bottom are 'Apply' and 'Cancel' buttons.

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 AP. Before using this feature, you need to sign up for DDNS service at www.dyndns.org, a DDNS service provider.

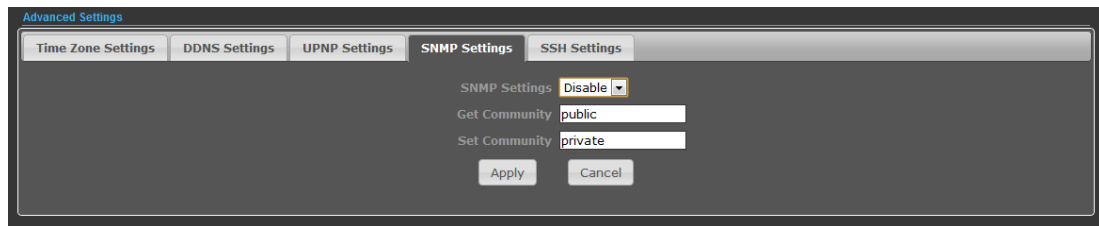
◆ ☐ **User Name** — Sets the DDNS user name for the connection.

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

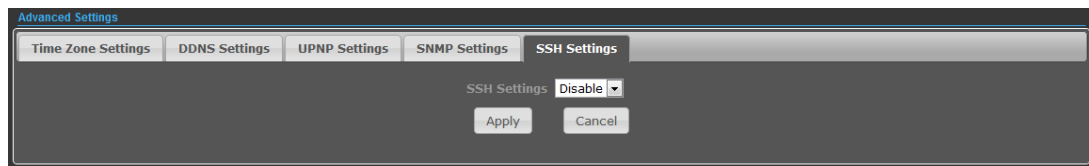
◆ ☐ **HostName** — The host name that you selected from the DDNS service provider.

The screenshot shows the 'Advanced Settings' window with the 'UPNP Settings' tab selected. The window has a title bar 'Advanced Settings' and five tabs: 'Time Zone Settings', 'DDNS Settings', 'UPNP Settings', 'SNMP Settings', and 'SSH Settings'. The 'UPNP Settings' tab contains a single field: 'UPNP Settings' with a dropdown menu showing 'Disable'. At the bottom are 'Apply' and 'Cancel' buttons.

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.



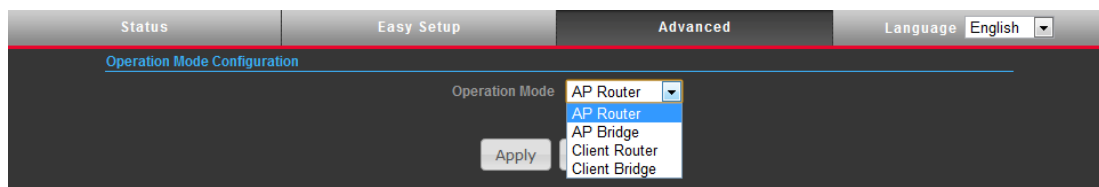
SNMP Settings – Managing devices on IP networks. Default setting is Disabled.



SSH Settings – Secure Shell. Enable your AP 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 WAN port is used to connect with ADSL/Cable modem and the wireless is used for your private WLAN. The NAT is existed between the 2 RJ45 ports and all wireless clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is DHCP client
- ◆ ☐ **Client Router** — The AP 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 AP 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 AP 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** — Destination IP Address. Specifies the destination IP address to block or allow traffic from.
- ◆ ☐ **SIP** — Source IP Address. 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. (Maximum 32 entries are allowed.)

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)

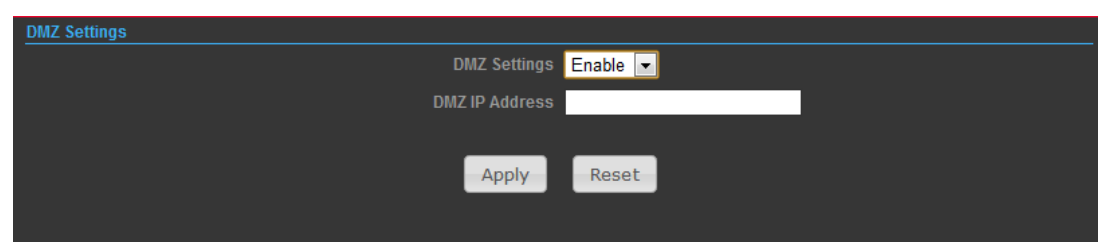
◆ ☐ **IP Address** — Specifies the IP address of a server on the local network to allow external access.

◆ ☐ **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 AP'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.



- ◆ ☐ **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 Access

Remote Management (via WAN)

Remote Management Port

Ping from WAN Filter

Ping from WAN Filter

Stateful Packet Inspection (SPI)

SPI Firewall

Network Address Translation Settings

Network Address Translation [?]

PPPoE Passthrough Settings

PPPoE Passthrough Setup

◆ ☐ **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 AP from Internet, you would use a URL of the form:
`http://xxx.xxx.xxx.xxx:2020/`

◆ ☐ **Ping from WAN Filter** — When Allow, the AP 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 AP provides a variety of options for blocking Internet access based on content, URL and host name.

The screenshot shows the 'Content Filter Settings' window with the 'Webs URL Filter Settings' tab selected. It features a 'Current Web URL Filters' section with a table containing one row with 'No' and 'URL' headers. Below the table are 'Delete' and 'Reset' buttons. At the bottom, there is an 'Add a URL filter' section with a text input field starting with 'Http(s)://', followed by 'Add' and 'Reset' buttons.

◆ **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.

The screenshot shows the 'Content Filter Settings' window with the 'Webs Host Filter Settings' tab selected. It features a 'Current Website Host Filters' section with a table containing one row with 'No' and 'Host (Keyword)' headers. Below the table are 'Delete' and 'Reset' buttons. At the bottom, there is an 'Add a Host (keyword) Filter' section with a text input field, followed by 'Add' and 'Reset' buttons.

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 a 'Hostname' field with the value 'DHCP'. The 'DNS Settings (Optional)' section at the bottom has empty fields for 'Primary DNS Server' and 'Secondary DNS Server'. 'Apply' and 'Cancel' buttons are at the bottom right.

- ◆ ☐ **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' (filled with 'pppoe_user'), 'Password' (masked with dots), and 'Verify Password' (also masked). The 'Operation Mode' is set to 'Keep Alive' from a dropdown menu. Below that, '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 at the bottom has empty fields for 'Primary DNS Server' and 'Secondary DNS Server'. 'Apply' and 'Cancel' buttons are at the bottom right.

- ◆ ☐ **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. The 'WAN Connections' dropdown is set to 'Static (Fixed IP)'. Under the 'Static Mode' section, there are 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. Below this is the 'DNS Settings' section with '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 fields for 'Server IP' (pptp_server), 'User Name' (pptp_user), and 'Password' (masked with dots). There is an 'Address Mode' dropdown set to 'Static IP', followed by 'IP Address' and 'Subnet Mask' input fields. The 'Operation Mode' dropdown is set to 'Keep Alive'. To the right, 'Keep Alive Mode: Redial Period' is set to '60' seconds. Below is the 'DNS Settings (Optional)' section with 'Primary DNS Server' and 'Secondary DNS Server' fields, both empty. At the bottom are 'Apply' and 'Cancel' buttons.

- ◆ ☐ **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' window with the 'IPSEC' tab selected. The 'wan ipsec mode' section contains the following fields and values:

- Connection address family: IPv4
- IPsec Connection Type: Road Warrior Tunnel
- IPsec Authentication: SHA-1
- SA connection Life Time: 12h
- Local IP Address: (empty)
- Local Subnet: (empty)
- Local Gateway: (empty)
- IPsec Tunnel Name: accCONN
- IPsec Key Life time: 12h
- NAT Transversal: ☐
- IPsec Compression: ☐
- IPsec Operation Mode: add
- PF S/DH Group: modp1024
- IPsec Encryption: AES
- IKE Key Tries: 3
- Peer IP Address: (empty)
- Peer Subnet: (empty)
- Peer Gateway: (empty)
- IPsec Secret Key: PSK
- Perfect Forward Secrets: ☐
- IPsec Conn. Keep Alive: ☐

At the bottom, there are fields for 'Primary DNS Server' and 'Secondary DNS Server', and buttons for 'Apply' and 'Cancel'.

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

Advanced Routing Settings

Add a routing rule

Destination
Type
Gateway
Interface
Comment

Apply Reset

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)	

Delete Reset

Dynamic Routing Protocol

RIP

Apply Reset

- ◆ ☐ **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:

Multiple SSID: ☐

Country Code:

Frequency (Channel):

Site Survey:

Network Mode:

Extension Channel:

Distance: miles (km)

ACK Timeout:

SSID | Security Settings

Network Name (SSID): ☐ Hide

WPS Choice: ☐

Encryption Settings:

◆ ☐ **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.

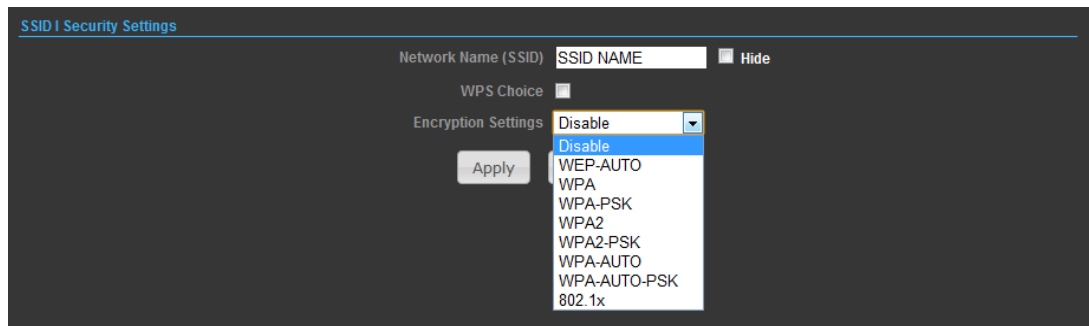
◆ ☐ **Network Name (SSID)** — The name of the wireless network service provided by the AP. Clients that want to connect to the network must set their SSID to the same as that of AP. (Range: 1-32 characters)

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

◆ ☐ **Frequency (Channel)** — The radio channel that the AP uses to communicate with wireless clients.

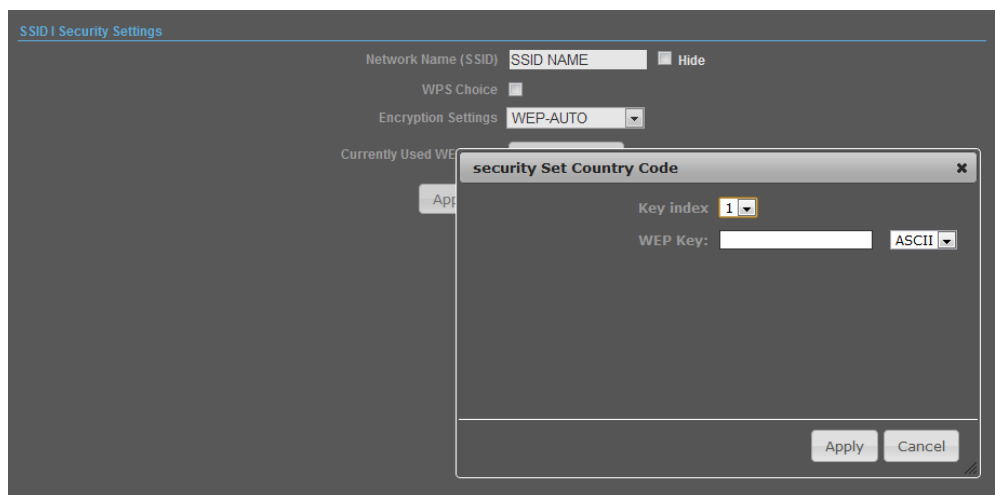
◆ ☐ **Network Mode** — Defines the radio operating mode.

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.

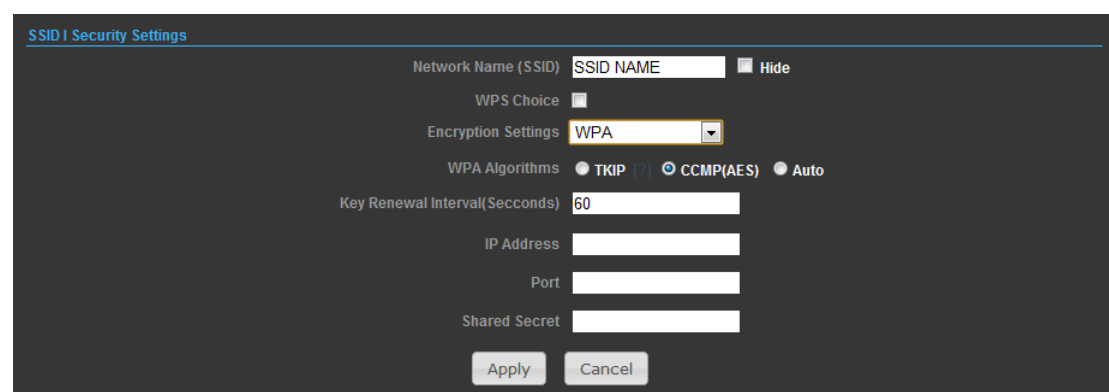
◆ ☐ **WEP Keys** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or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



◆ ☐ **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. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation. 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.

SSID | Security Settings

Network Name (SSID) ☐ Hide

WPS Choice ☐

Encryption Settings

WPA Algorithms ☒ TKIP ☒ CCMP(AES) ☐ Auto

Key Renewal Interval(Seconds)

Pre-Shared Key

◆ ☐ **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.

◆ ☐ **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 (AESCMP) 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.

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.
- ◆ ☐ **WPS Name** — WPS name for connecting to the device.
- ◆ ☐ **Security Mode** — Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network:

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.

◆ ☐ **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)