CHIPSIP

Technology Co., Ltd

CPRA02F

操作手冊

(Only for Internal Reference)

Revision 01

2013/07/01

Prepared By: Jeff Hsieh

Revision History

Revision	Date	Notes	Owner
01	2013/07/01	Initial Release	Jeff Hsieh

TABLE OF CONTENT

1. Preparation....4
1.1 Default settings....4
1.2 Pre-required configuration....4
2.1 Introduction....6
2.2 Gateway....6
2.3 Bridge....錯誤! 尚未定義書籤。
2.4 Wireless ISP....錯誤! 尚未定義書籤。
3.1 Basic Settings....7
3.2 Advanced Settings....10
3.3 Security....10
3.3.1 Security....10
3.3.2 WEP....11
3.3.3 WPA-PSK....11
3.3.4 WPA + 802.1x....12
3.3.5 WPA2-PSK....12
3.3.6 WPA2 + 802.1x....13
3.3.7 WPA2-Mixed-PSK....13
3.3.8 WPA-Mixed + 802.1x....14
3.4 Access Control....14
3.5 WDS Settings....15
3.6 WPS....15
3.7 Wireless Schedule....16
4.1 LAN Interface....17
4.2 WAN Interface....18
5.1 Port Filtering....19
5.2 IP Filtering....19
5.3 MAC Filtering....20
5.4 Port Forwarding....20
5.4 URL Filtering....21
5.5 DMZ....21
5.6 VLAN Settings....22
6.1 Status....23
6.2 Statistics....23
6.3 DDNS....24
6.4 Time Zone Setting....24
6.5 Denial of Service....25
6.5 System Log....26
6.5 Upgrade Firmware....27
6.5 Save/Reload Settings....27
6.5 Password....27

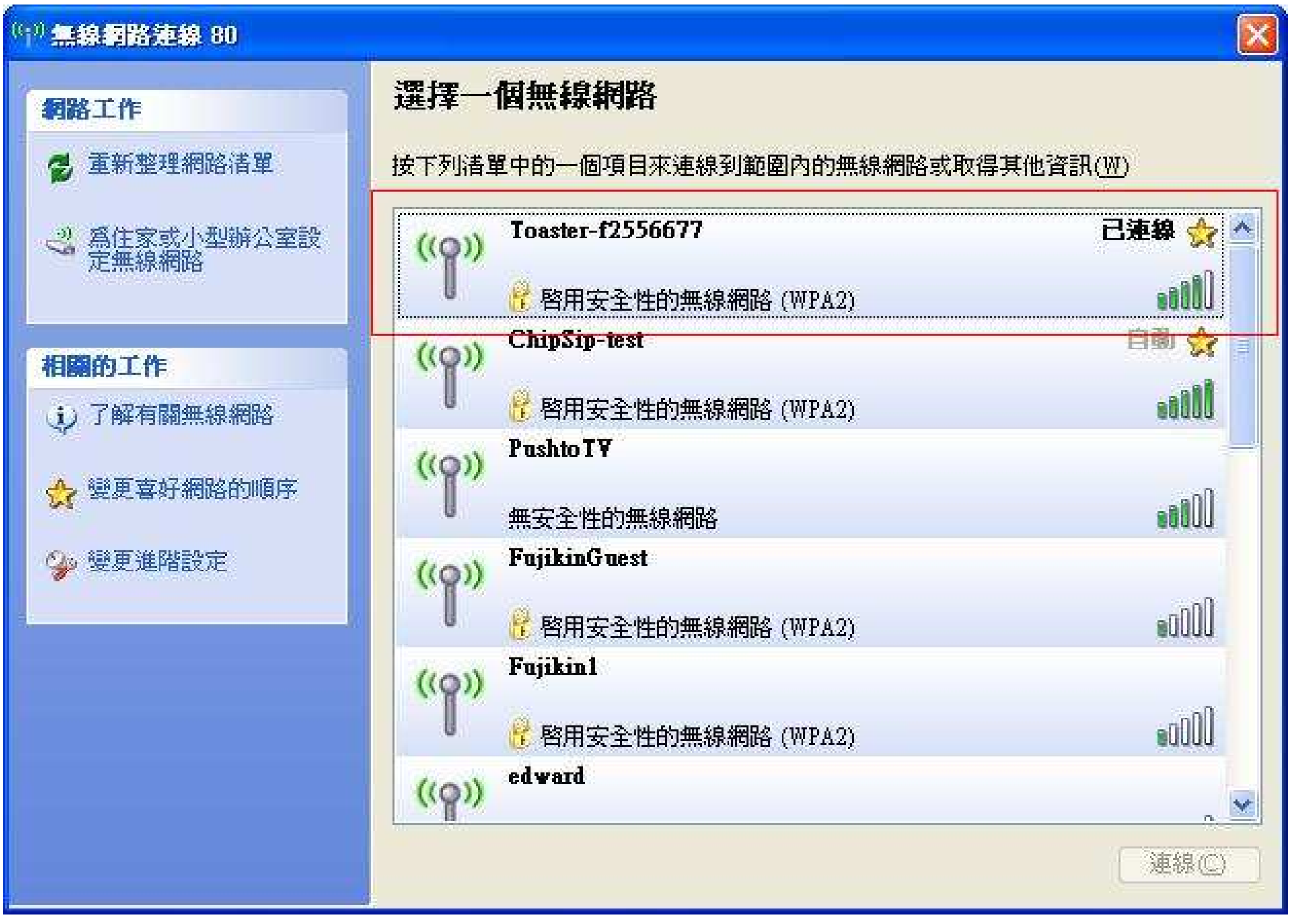
1. PREPARATION

1.1 Default settings

IP address	10.10.1.1
Subnet mask	255.255.255.0
Username	(Null)
Password	(Null)
Operation Mode	Gateway
DHCP	On
SSID	Wireless 11n AP-xxxxxxx (last 8 characters of MAC address)
Channel	Smart select
Security	Off

1.2 Pre-required configuration

1. Connect your Wireless LAN card to our device. Right click the “**Wireless Network Connection**” from the “**Start**” menu → “**Control Panel**” → “**Network Connections**” and select “**Wireless 11n AP -xxxxxxx**” to connect. Your Wireless LAN card will be automatically assigned an IP address.



無線網路連線 80

選擇一個無線網路

按下列清單中的一個項目來連線到範圍內的無線網路或取得其他資訊(W)

Toaster-f2556677 已連線
啓用安全性的無線網路 (WPA2)

ChipSip-test 自動
啓用安全性的無線網路 (WPA2)

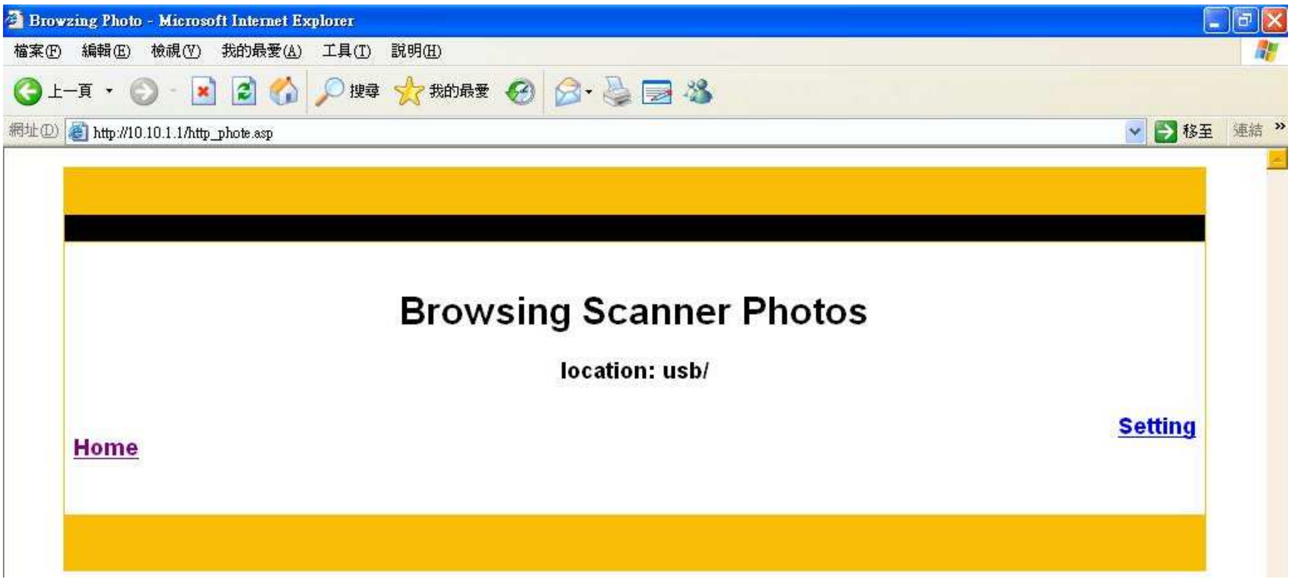
PushtoTV
無安全性的無線網路

FujikinGuest
啓用安全性的無線網路 (WPA2)

Fujikin1
啓用安全性的無線網路 (WPA2)

edward

2. Open Internet Explorer, enter **10.10.1.1**, the main page as below



Browzing Photo - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
http://10.10.1.1/http_phote.asp
移至
連結

Browsing Scanner Photos

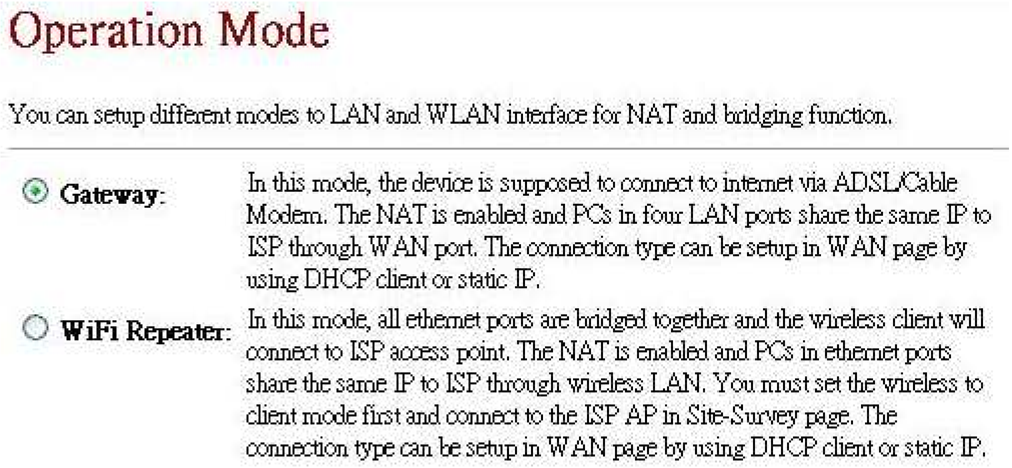
location: usb/

2. OPERATION MODE

2.1 Introduction

The operation mode web page allows you to setup different modes to LAN and WLAN interface for NAT and bridging function. It can be configured at 2 modes.

- Gateway
- WiFi Repeater



Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

● **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using DHCP client or static IP.

○ **WiFi Repeater:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using DHCP client or static IP.

2.2 Gateway

In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

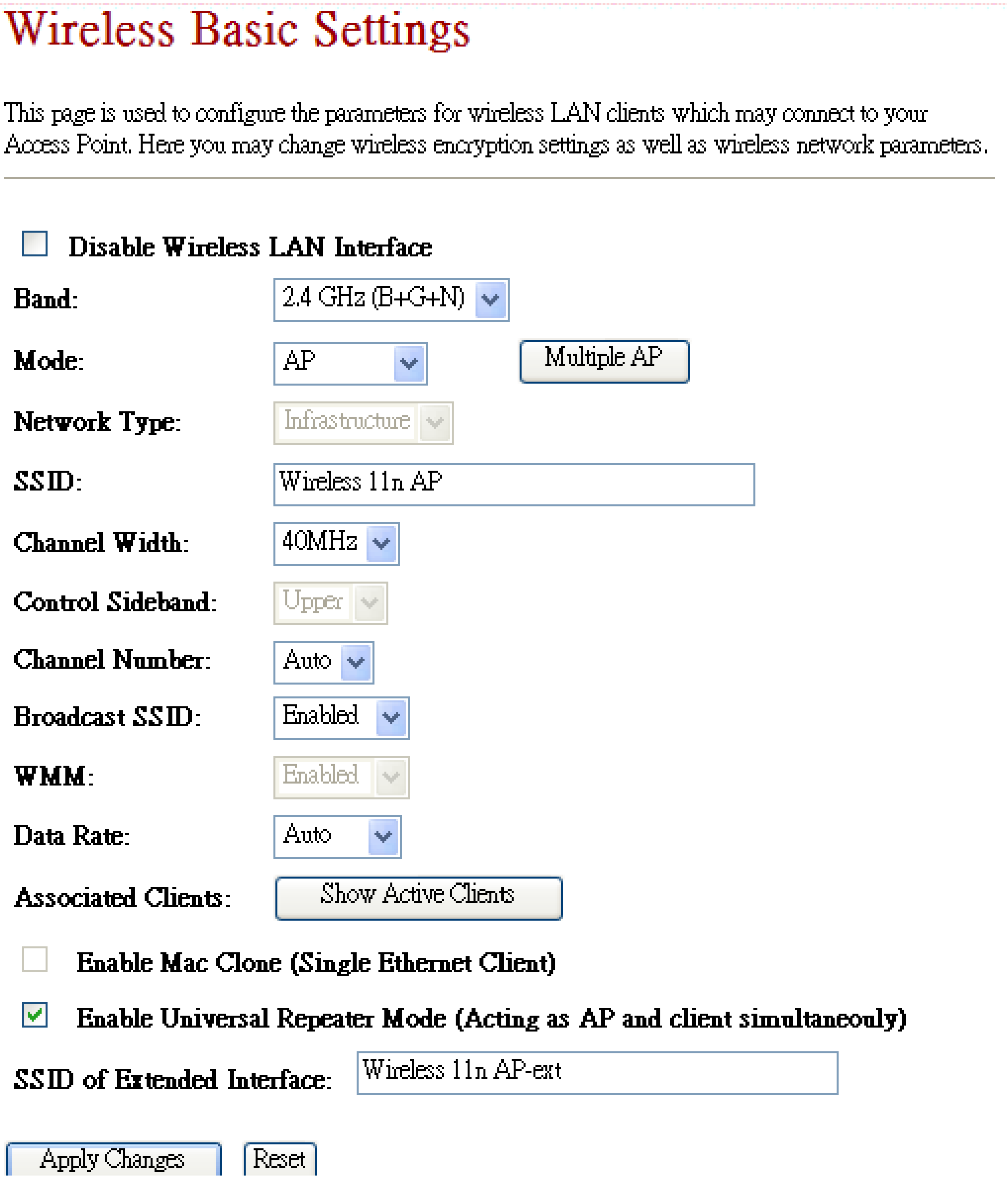
2.3 WiFi Repeater

In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

3. WIRELESS

3.1 Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	Wireless 11n AP
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	Auto
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	

□ Enable Mac Clone (Single Ethernet Client)

☑ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface: Wireless 11n AP-ext

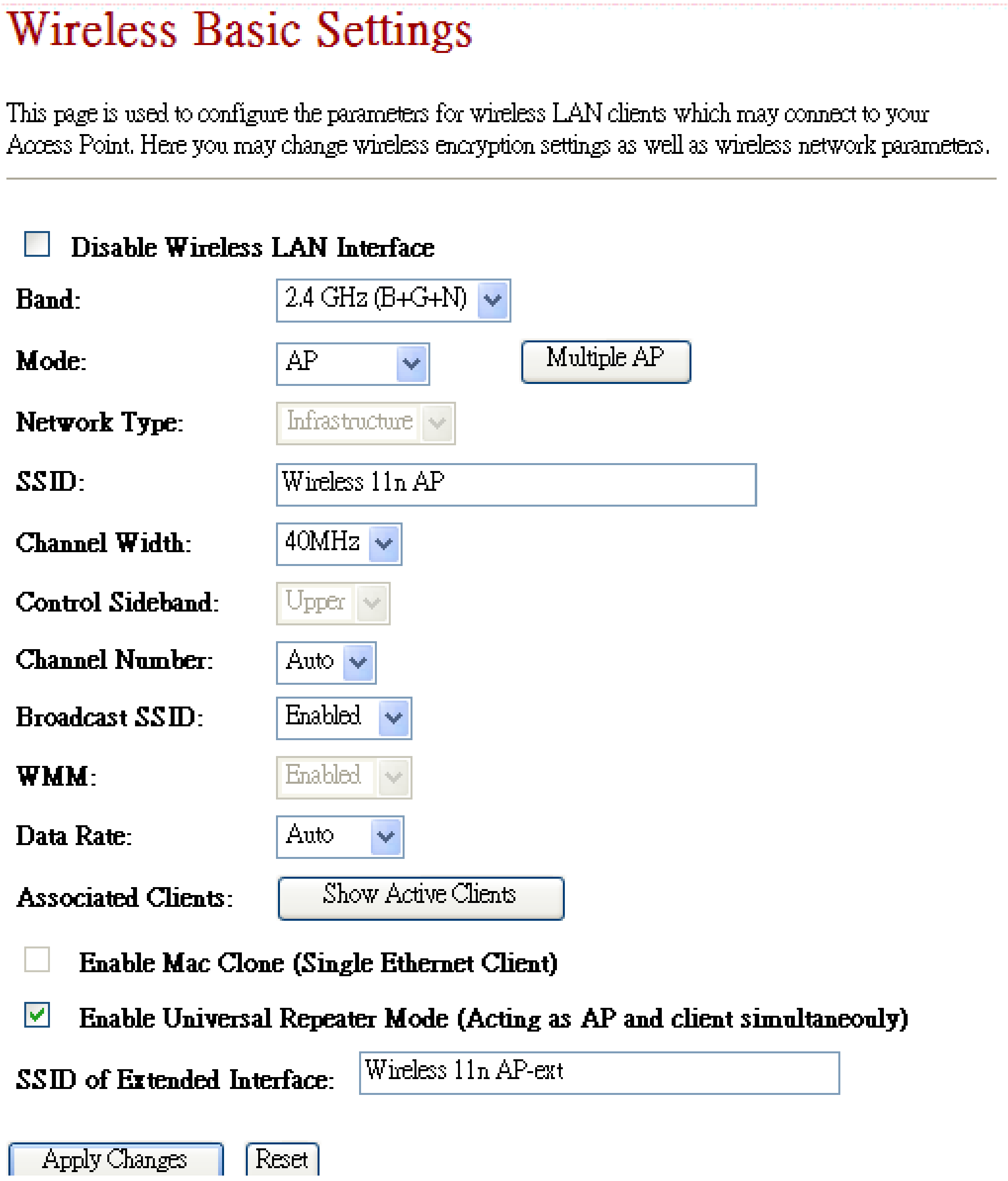
3.1 Extended Function

When the device is in AP, it can extend Client mode which is able to connect to other wireless AP.

When the device is in Client mode, it can extend AP mode so that other station cards are able to connect to extended-AP

3.1.1 AP + Extended Client

(1) If user would like to enable extended Client in AP mode, check “Enable Universal Repeater Mode (Acting as AP and client simultaneously) and assign SSID that user would like to connect



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

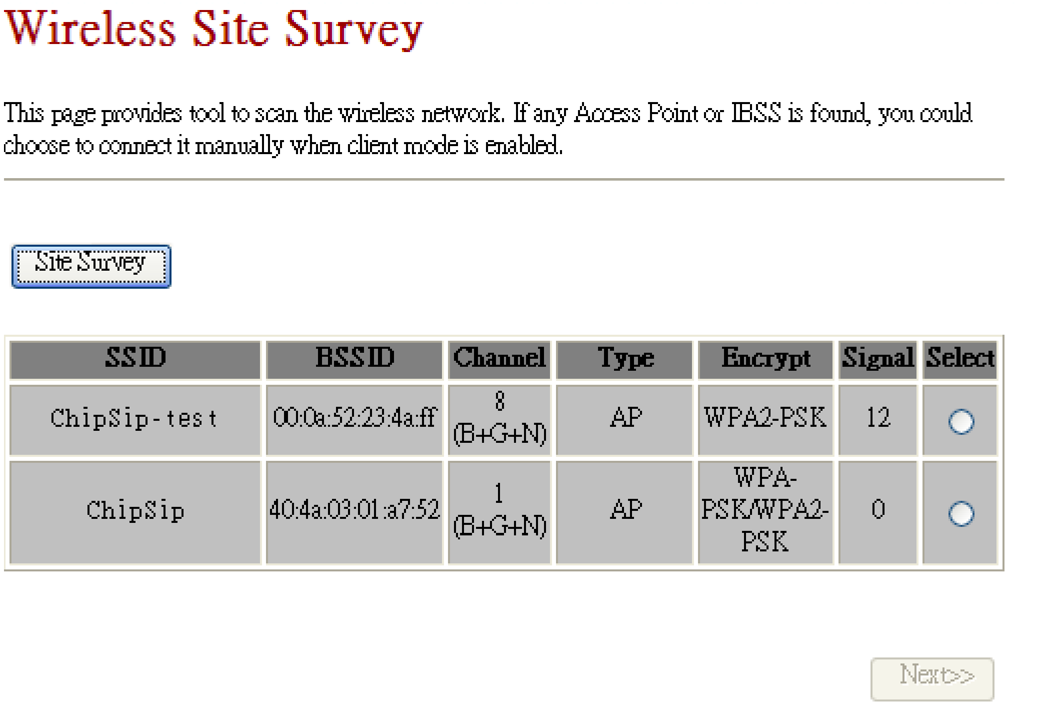
Band:	2.4 GHz (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	Wireless 11n AP
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	Auto
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☑ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface: Wireless 11n AP-ext

(2) User can select the desired AP from “Site Survey” WEB page, click “Select”, then click “Next”

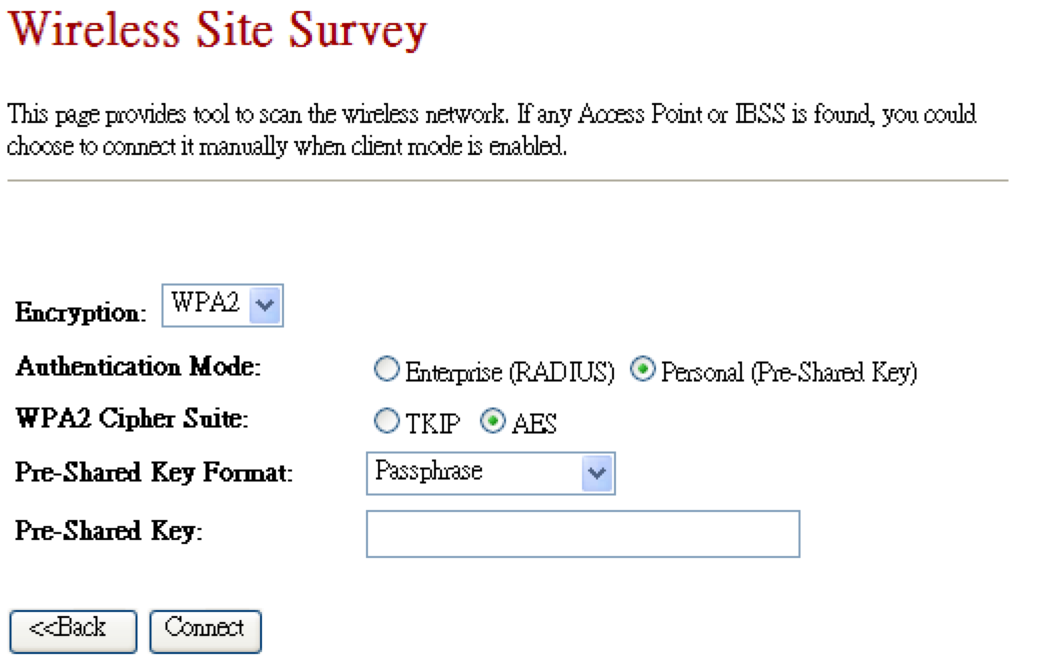


Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
ChipSip-test	00:0a:52:23:4a:ff	8 (B+G+N)	AP	WPA2-PSK	12	○
ChipSip	40:4a:03:01:a7:52	1 (B+G+N)	AP	WPA-PSK/WPA2-PSK	0	○

(3) You will be asked to configure security parameters



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Encryption: WPA2

Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA2 Cipher Suite: ○ TKIP ● AES

Pre-Shared Key Format: Passphrase

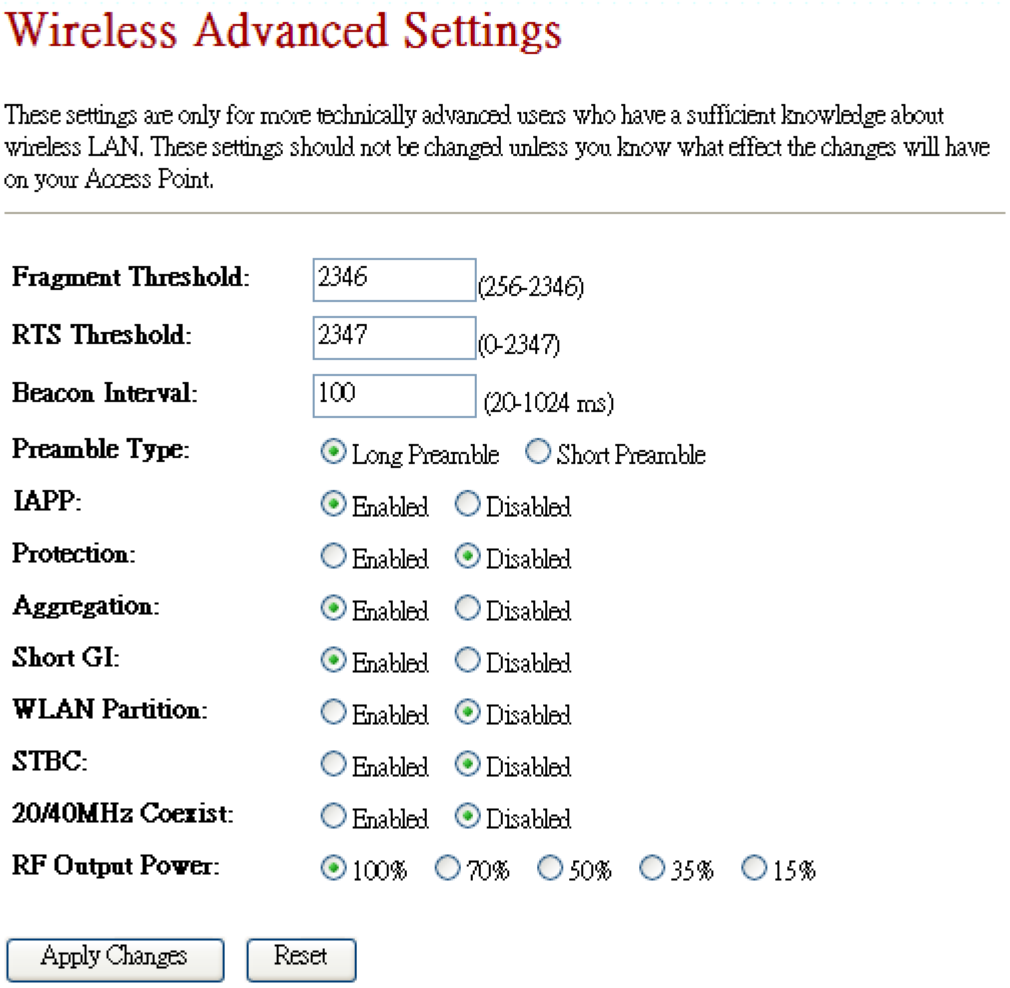
Pre-Shared Key:

3.1.1 Client + Extended AP

If user would like to enable extended AP in Client mode, check “Enable Universal Repeater Mode (Acting as AP and client simultaneously) and assign SSID

3.2 Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Preamble Type: ● Long Preamble ○ Short Preamble

IAPP: ● Enabled ○ Disabled

Protection: ○ Enabled ● Disabled

Aggregation: ● Enabled ○ Disabled

Short GI: ● Enabled ○ Disabled

WLAN Partition: ○ Enabled ● Disabled

STBC: ○ Enabled ● Disabled

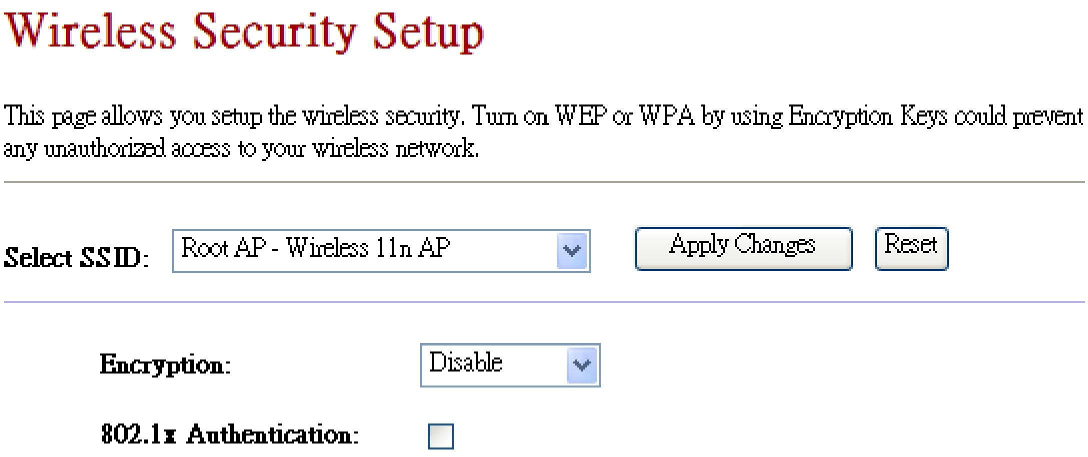
20/40MHz Coexist: ○ Enabled ● Disabled

RF Output Power: ● 100% ○ 70% ○ 50% ○ 35% ○ 15%

3.3 Security

3.3.1 Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.



Wireless Security Setup

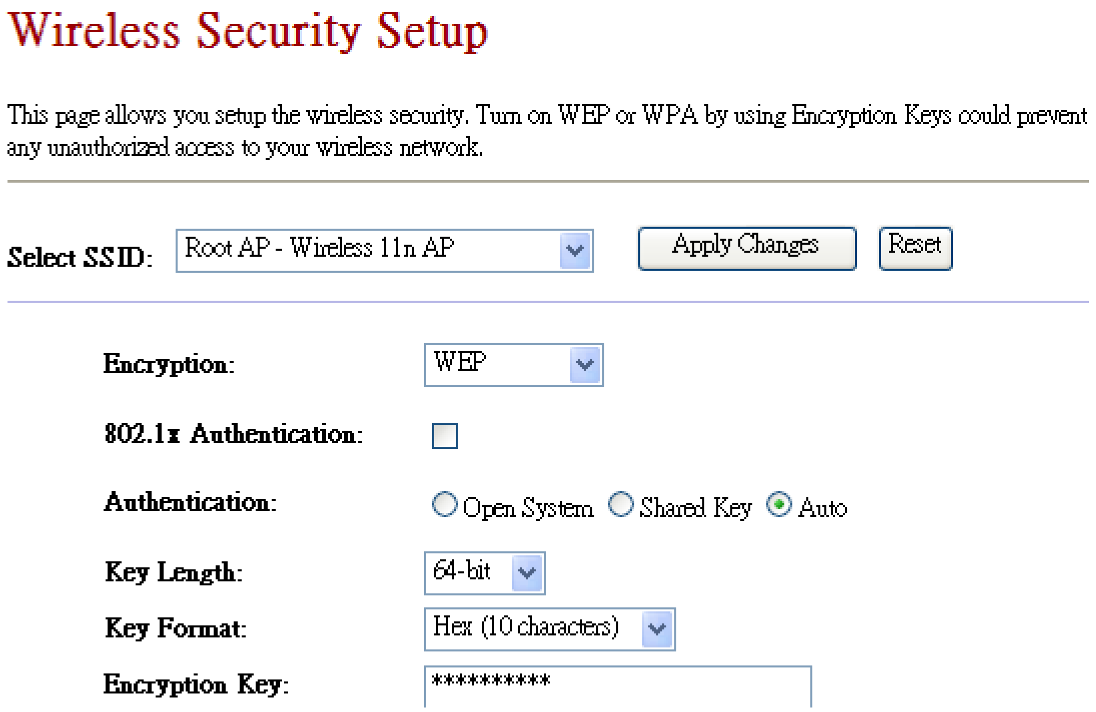
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: Disable

802.1x Authentication: □

3.3.2 WEP



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: WEP

802.1x Authentication: □

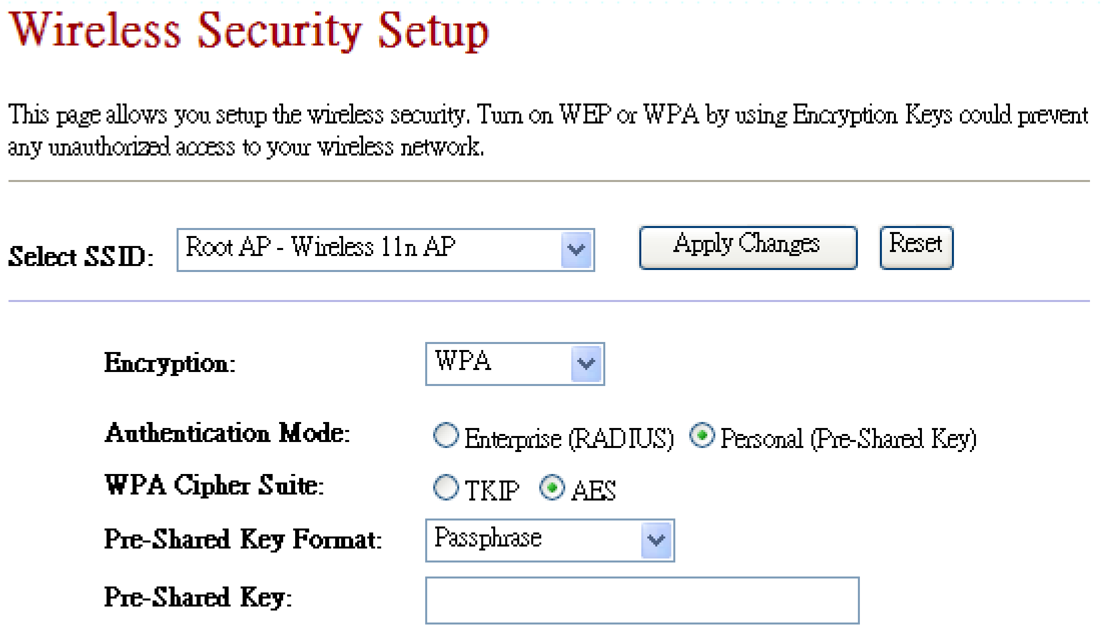
Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

Encryption Key: **********

3.3.3 WPA-PSK



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: WPA

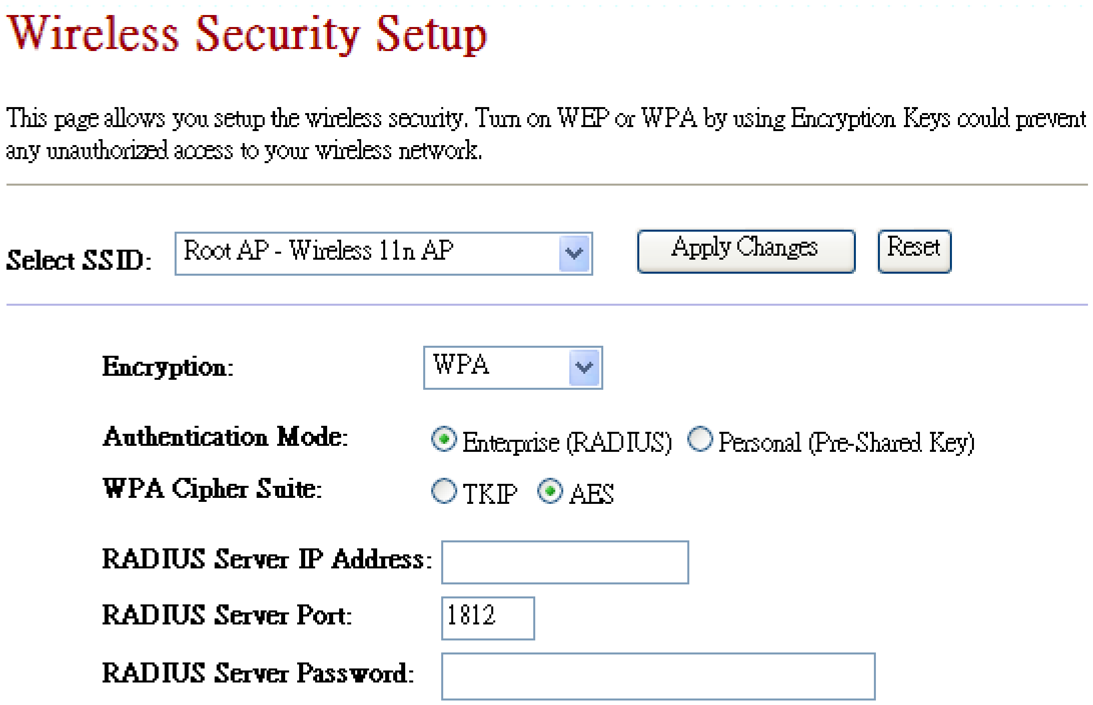
Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ○ TKIP ● AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

3.3.4 WPA + 802.1x



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: WPA

Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

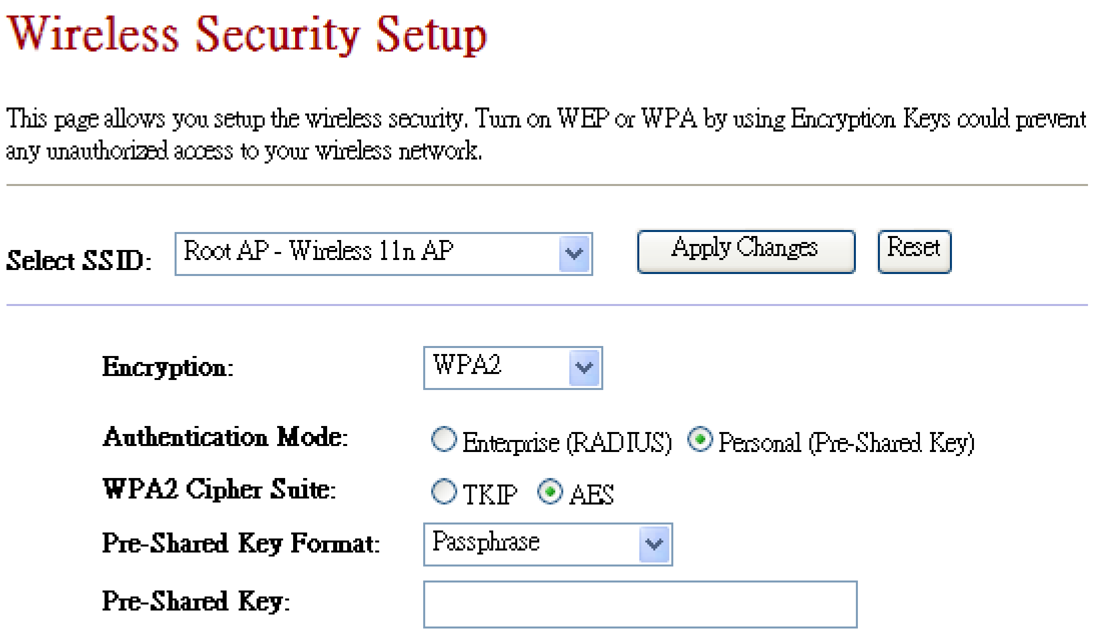
WPA Cipher Suite: ○ TKIP ● AES

RADIUS Server IP Address:

RADIUS Server Port: 1812

RADIUS Server Password:

3.3.5 WPA2-PSK



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: WPA2

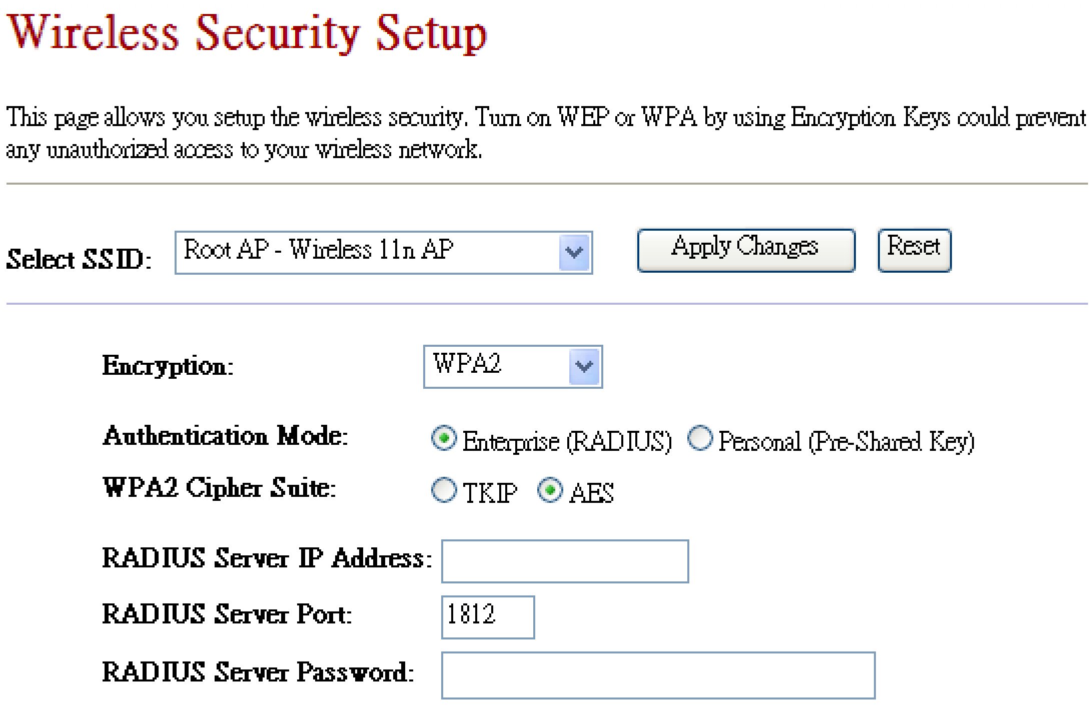
Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA2 Cipher Suite: ○ TKIP ● AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

3.3.6 WPA2 + 802.1x



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: WPA2

Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

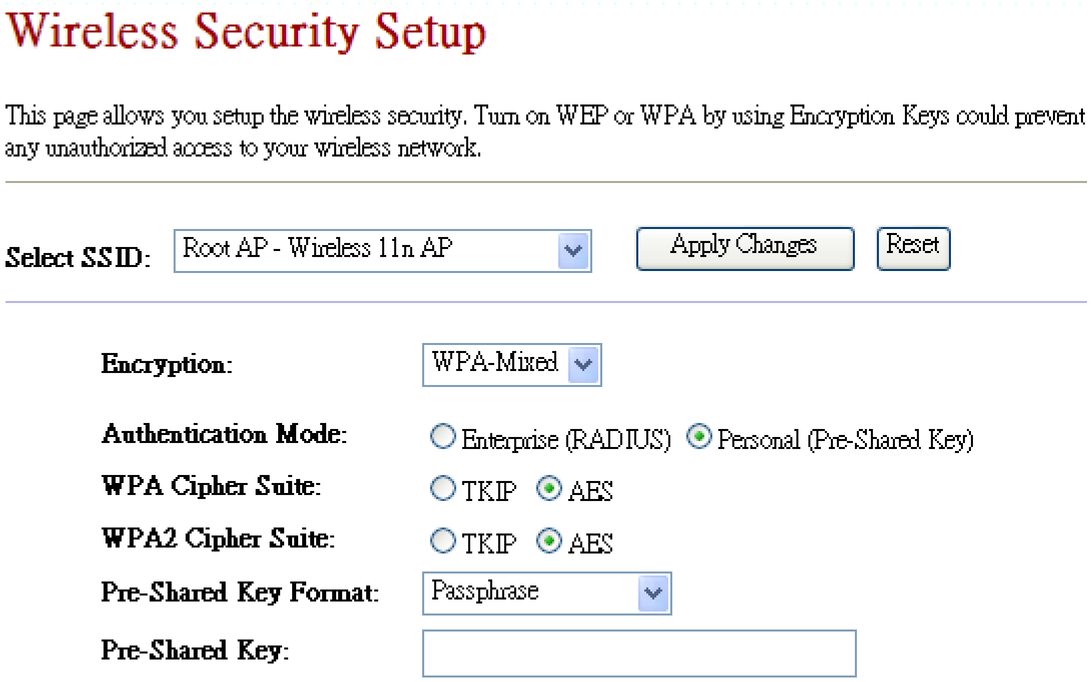
WPA2 Cipher Suite: ○ TKIP ● AES

RADIUS Server IP Address:

RADIUS Server Port: 1812

RADIUS Server Password:

3.3.7 WPA2-Mixed-PSK



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: WPA-Mixed

Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

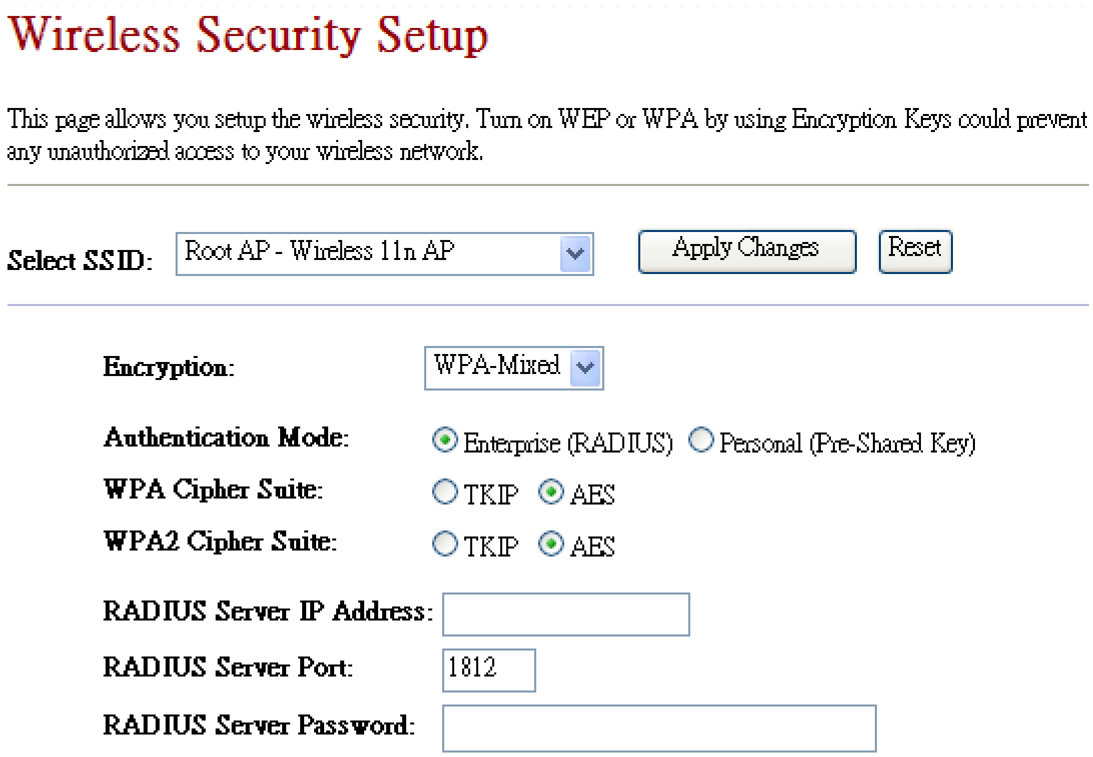
WPA Cipher Suite: ○ TKIP ● AES

WPA2 Cipher Suite: ○ TKIP ● AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

3.3.8 WPA-Mixed + 802.1x



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - Wireless 11n AP

Encryption: WPA-Mixed

Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

WPA Cipher Suite: ○ TKIP ● AES

WPA2 Cipher Suite: ○ TKIP ● AES

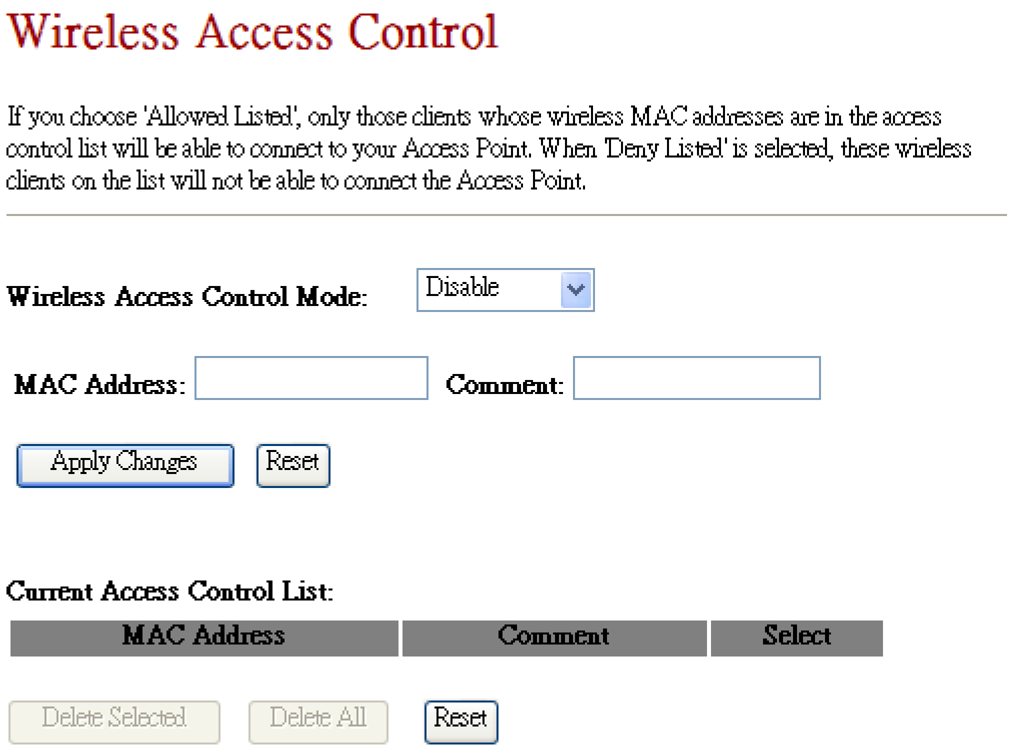
RADIUS Server IP Address:

RADIUS Server Port: 1812

RADIUS Server Password:

3.4 Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

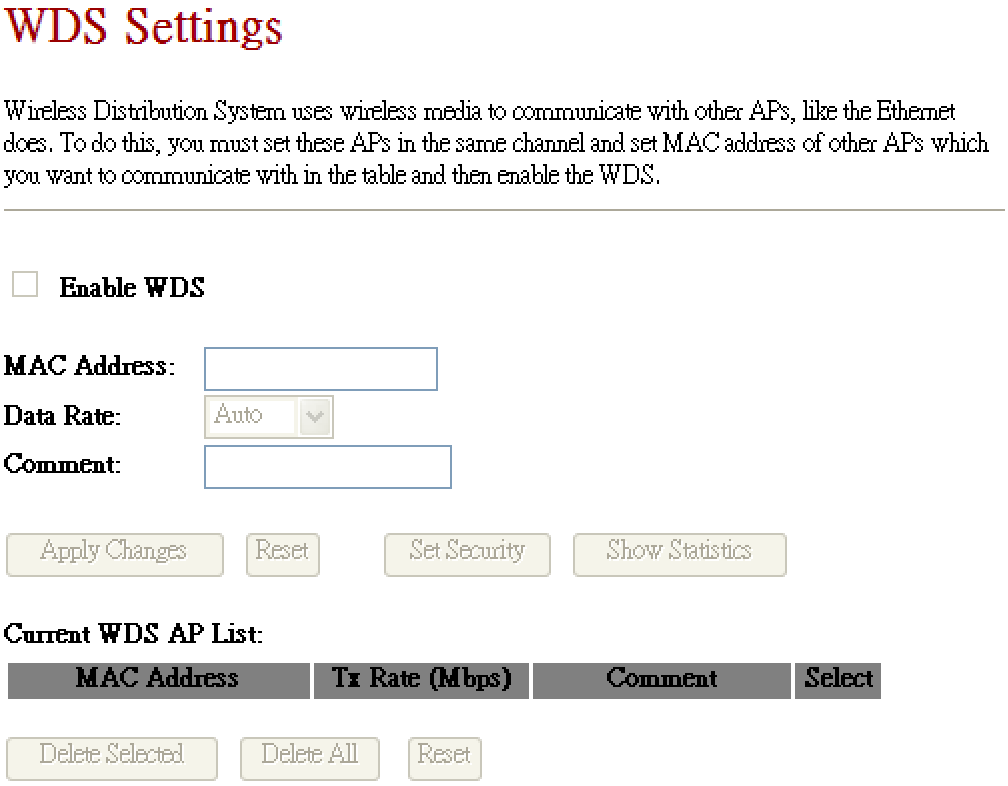
MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select

3.5 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

□ Enable WDS

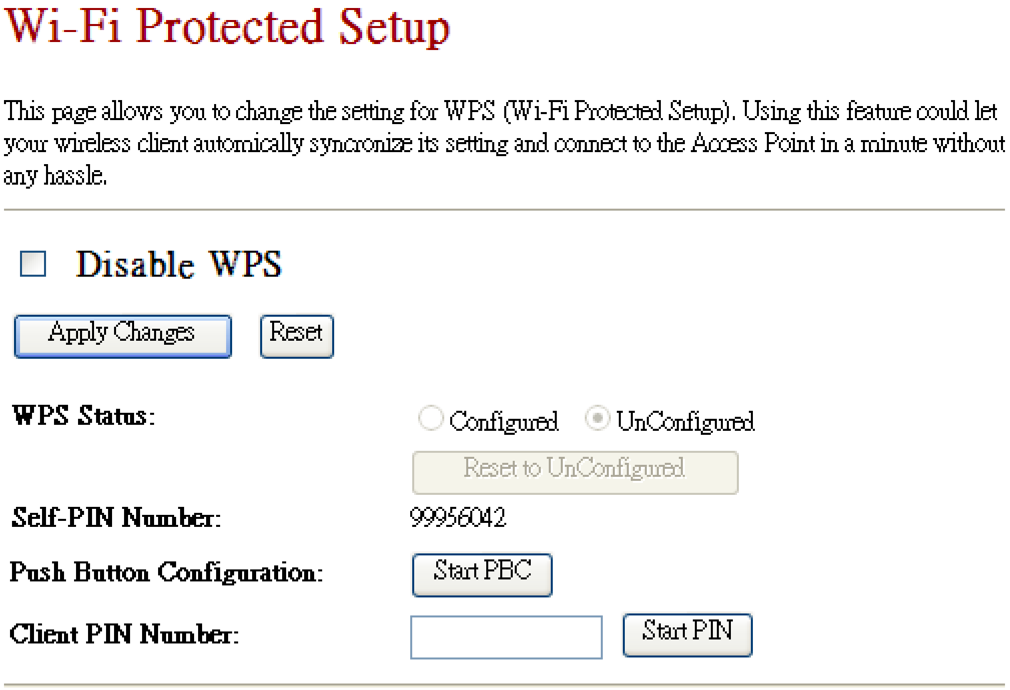
MAC Address:	
Data Rate:	Auto
Comment:	

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

3.6 WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.



Wi-Fi Protected Setup

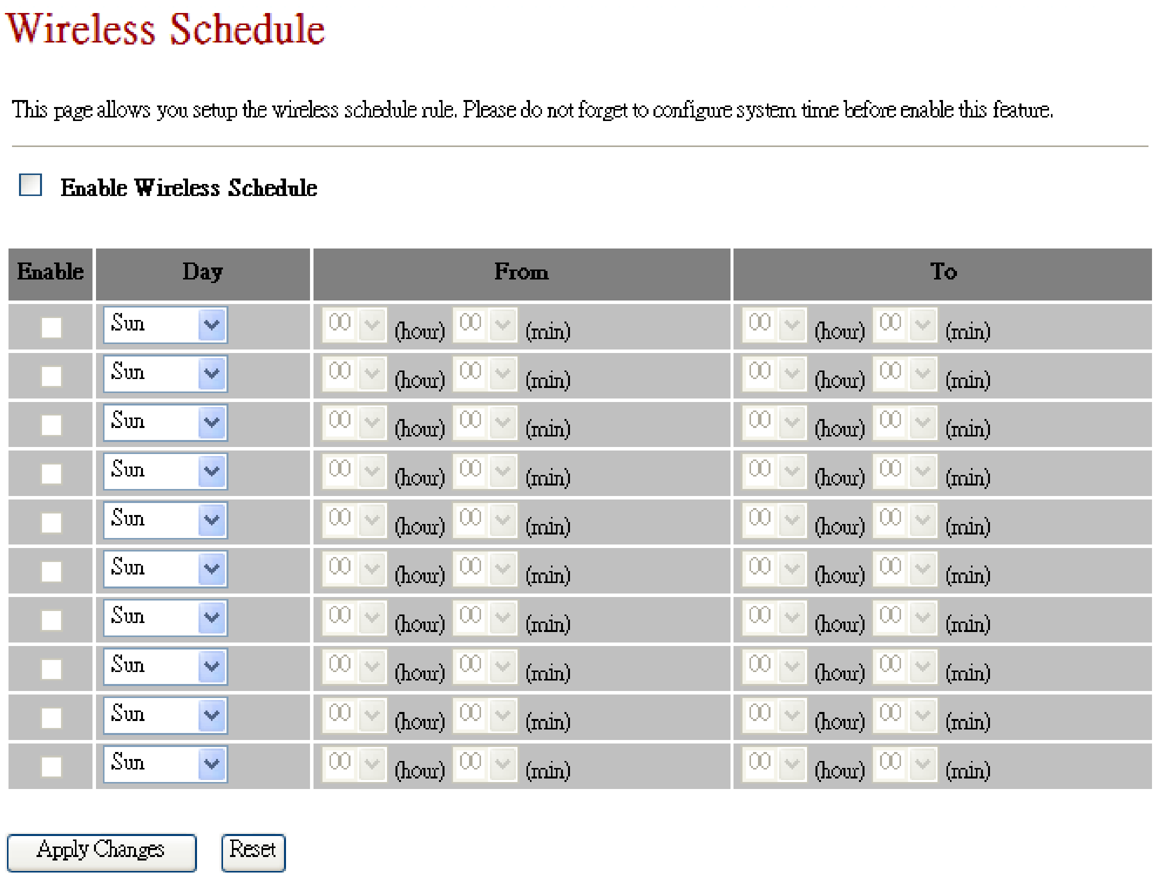
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ Disable WPS

WPS Status:	○ Configured ● UnConfigured Reset to UnConfigured
Self-PIN Number:	99956042
Push Button Configuration:	Start PBC
Client PIN Number:	Start PIN

3.7 Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.



Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

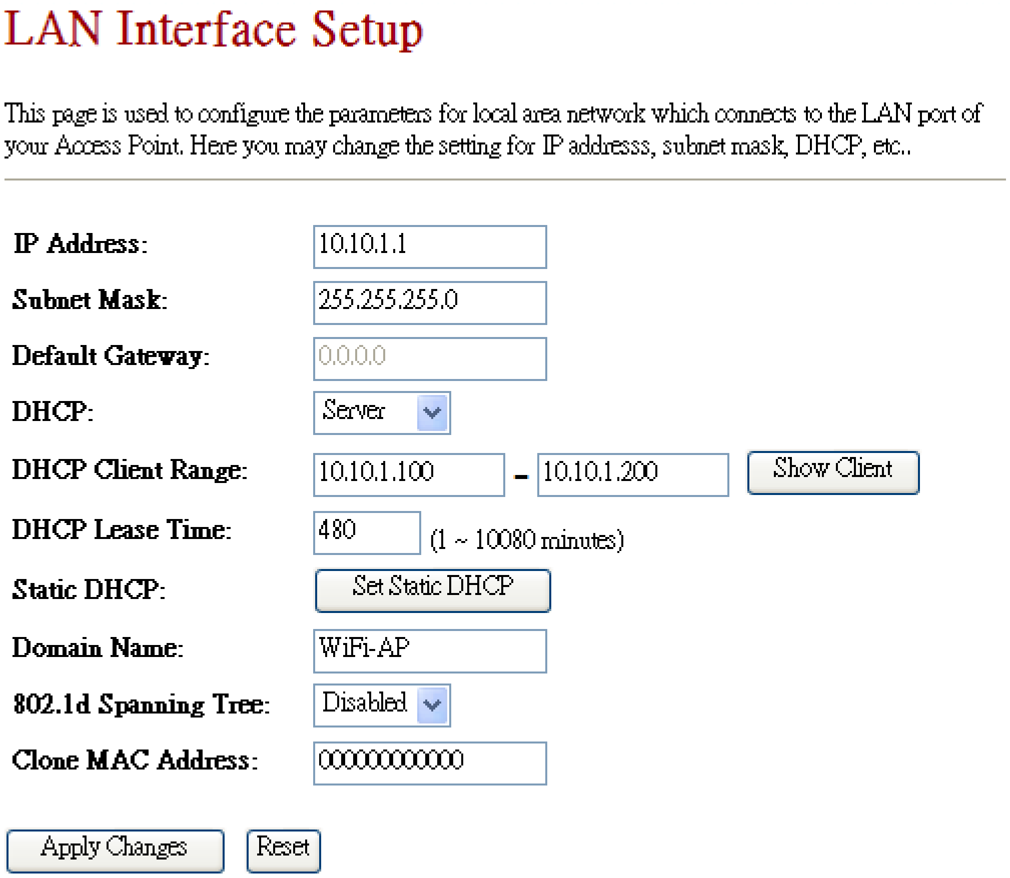
□ **Enable Wireless Schedule**

Enable	Day	From	To
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)

4. TCP/IP SETTINGS

4.1 LAN Interface

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresses, subnet mask, DHCP, etc…



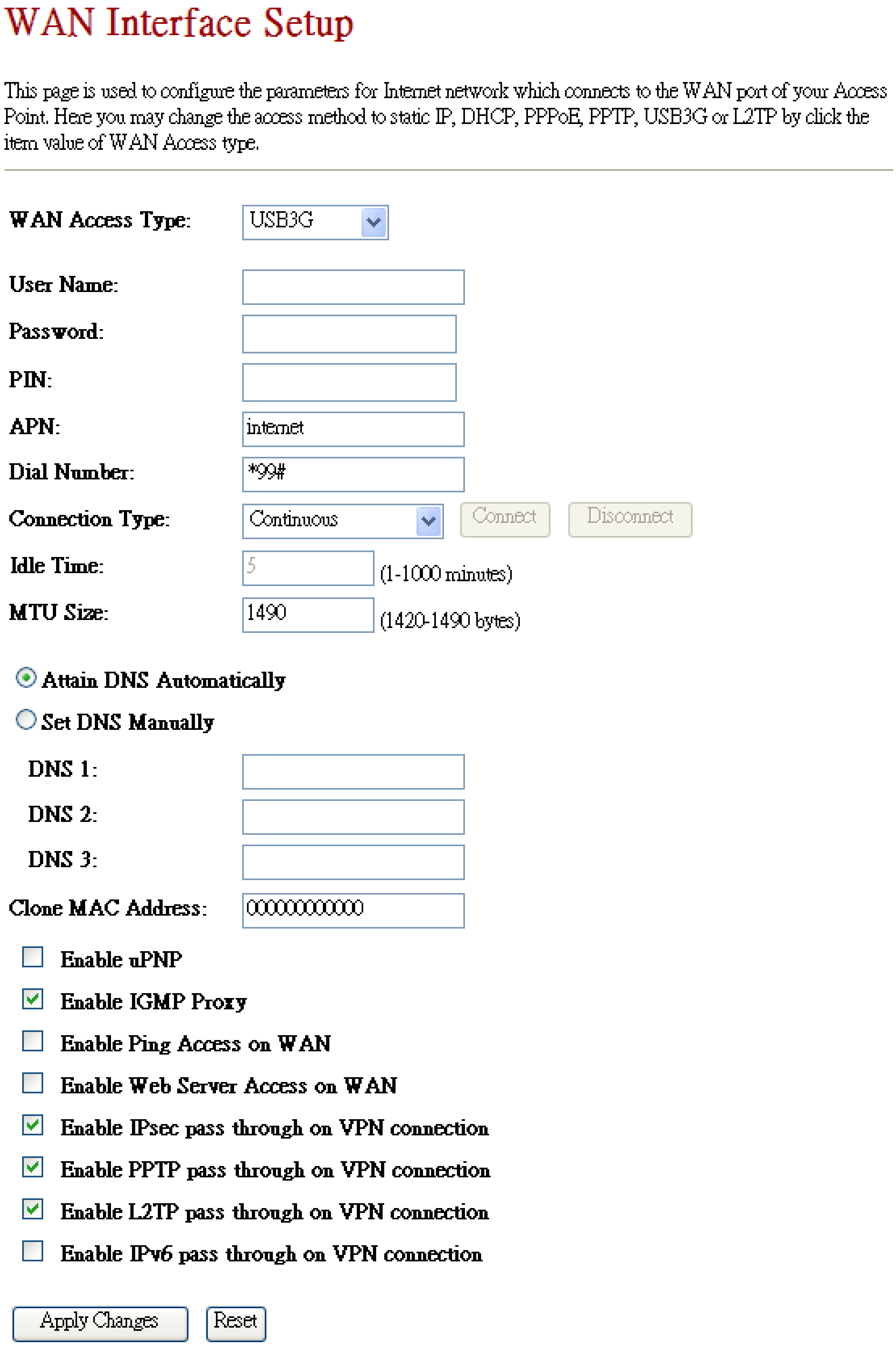
LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	10.10.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	10.10.1.100 - 10.10.1.200 Show Client
DHCP Lease Time:	480 (1 ~ 10080 minutes)
Static DHCP:	Set Static DHCP
Domain Name:	WiFi-AP
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

4.2 WAN Interface

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type:	USB3G
User Name:	
Password:	
PIN:	
APN:	internet
Dial Number:	*99#
Connection Type:	Continuous
Idle Time:	5 (1-1000 minutes)
MTU Size:	1490 (1420-1490 bytes)

● **Attain DNS Automatically**

○ **Set DNS Manually**

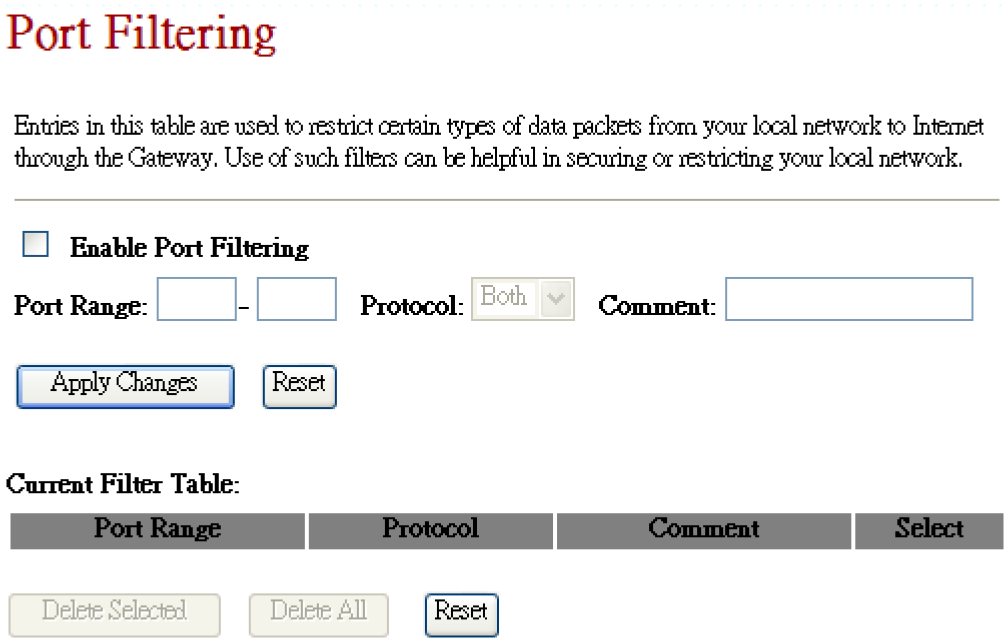
DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

- □ **Enable uPNP**
- ☑ **Enable IGMP Proxy**
- □ **Enable Ping Access on WAN**
- □ **Enable Web Server Access on WAN**
- ☑ **Enable IPsec pass through on VPN connection**
- ☑ **Enable PPTP pass through on VPN connection**
- ☑ **Enable L2TP pass through on VPN connection**
- □ **Enable IPv6 pass through on VPN connection**

5. FIREWALL

5.1 Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

□ Enable Port Filtering

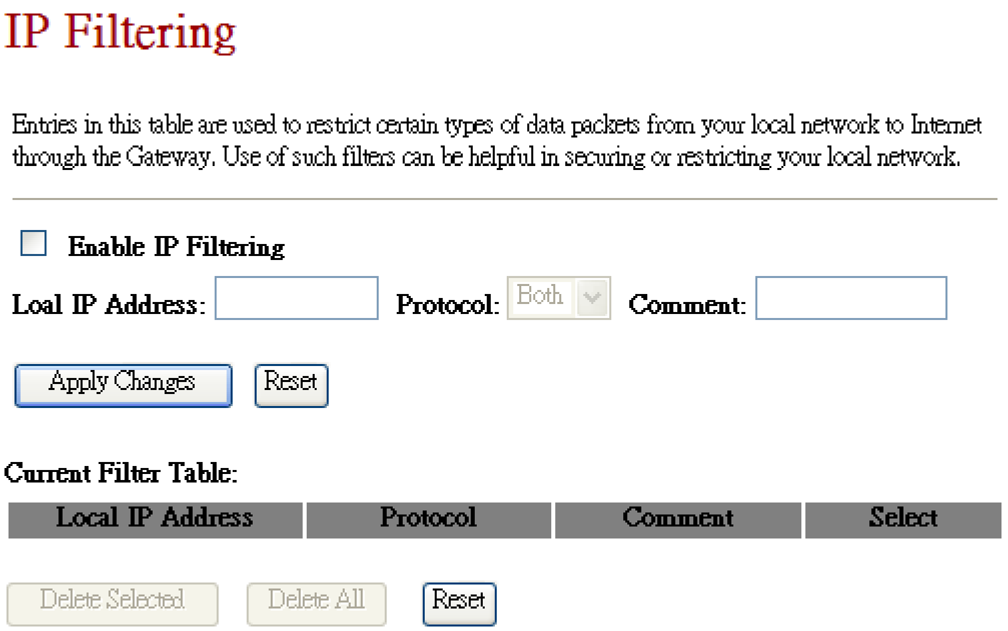
Port Range: ___ - ___ Protocol: Both Comment: ___

Current Filter Table:

Port Range	Protocol	Comment	Select

5.2 IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

□ Enable IP Filtering

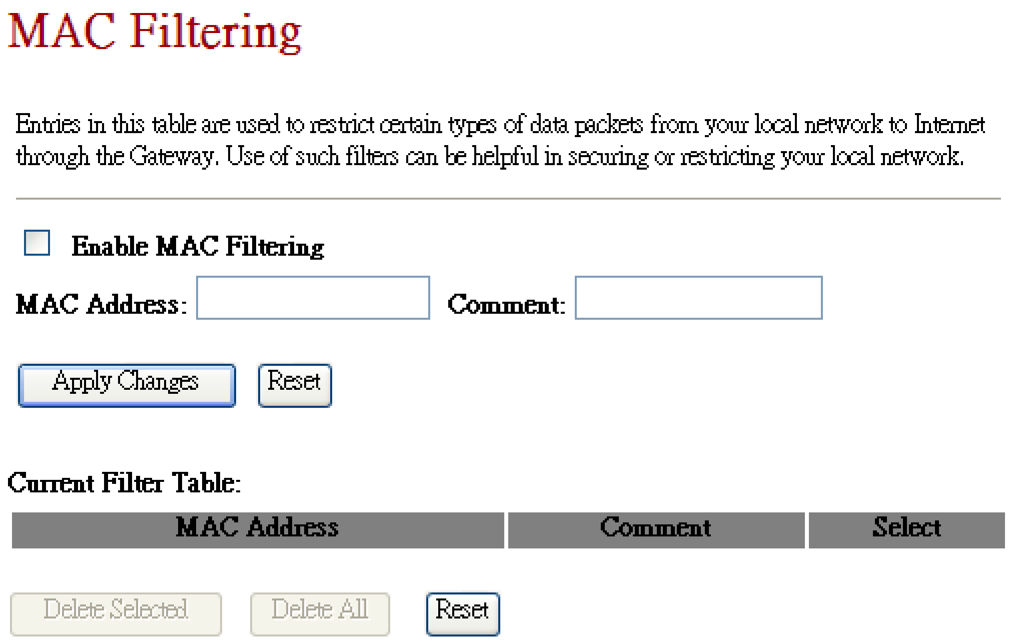
Loal IP Address: ___ Protocol: Both Comment: ___

Current Filter Table:

Local IP Address	Protocol	Comment	Select

5.3 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

□ Enable MAC Filtering

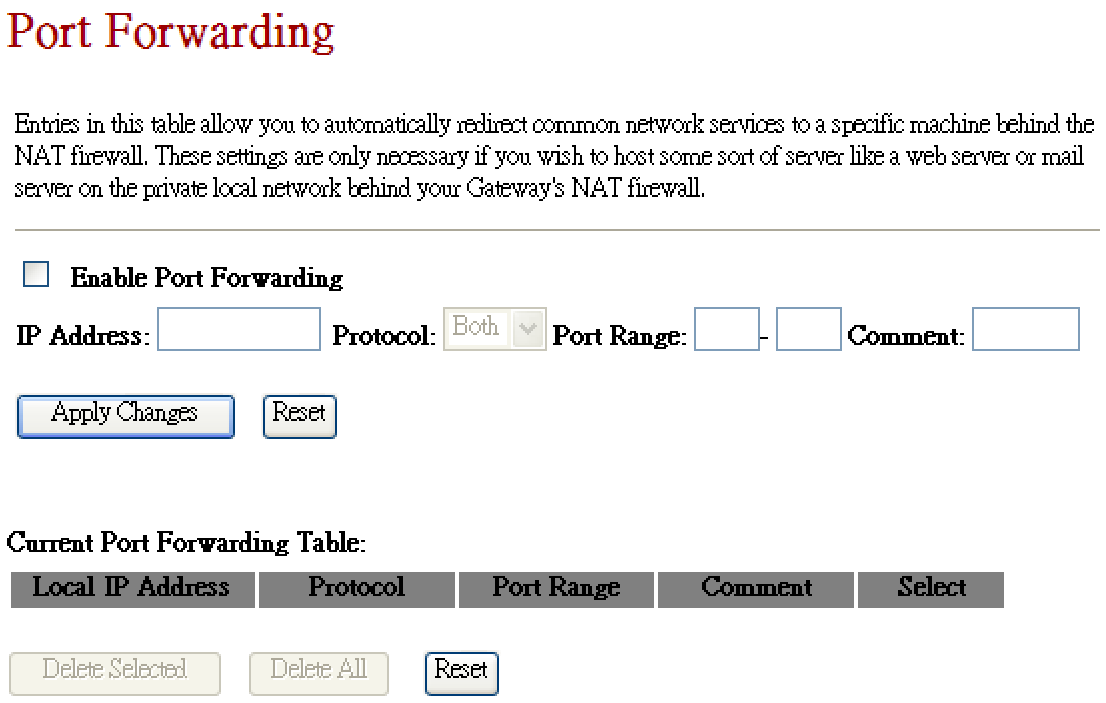
MAC Address: ____ Comment: ____

Current Filter Table:

MAC Address	Comment	Select

5.4 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

□ Enable Port Forwarding

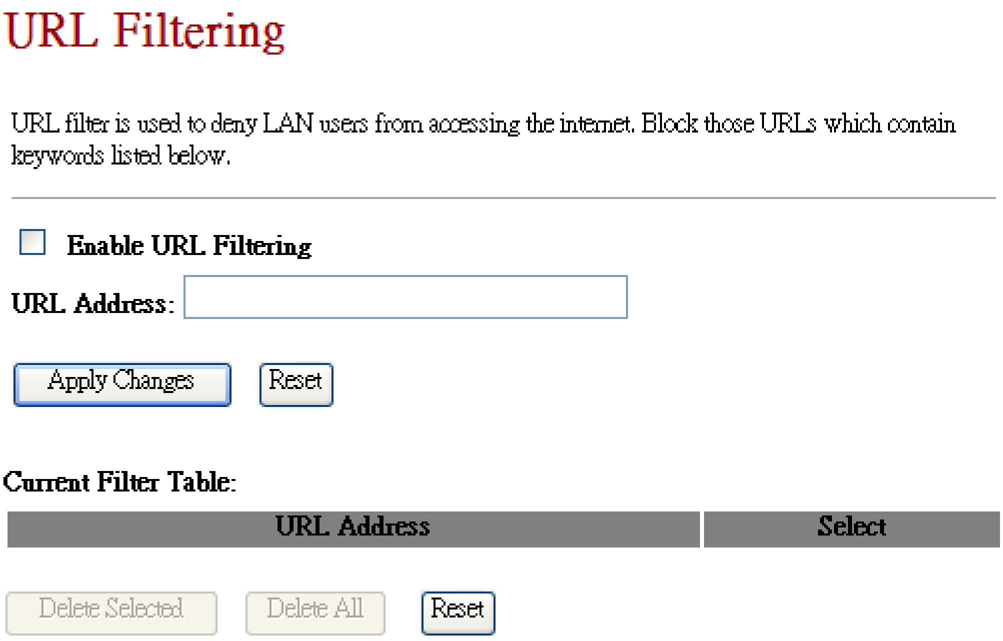
IP Address: ____ Protocol: Both Port Range: ____ - ____ Comment: ____

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

5.4 URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.



URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

□ **Enable URL Filtering**

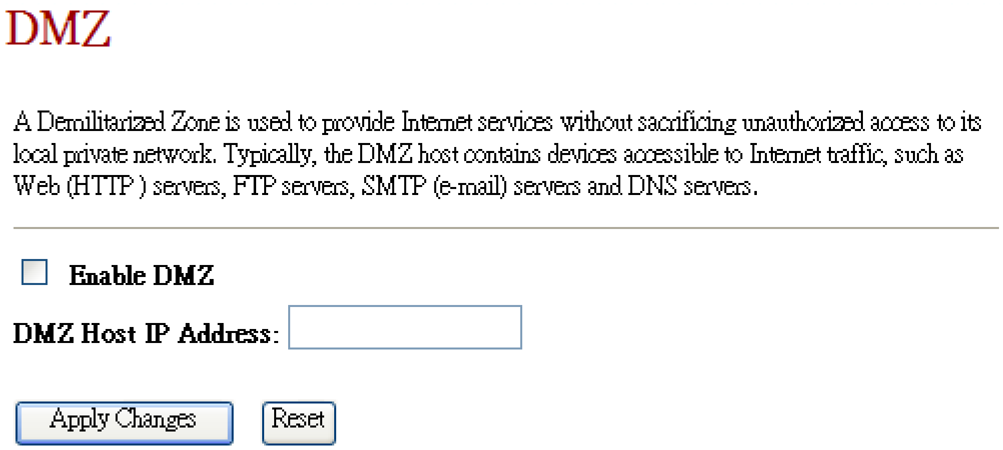
URL Address:

Current Filter Table:

URL Address	Select

5.5 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



DMZ

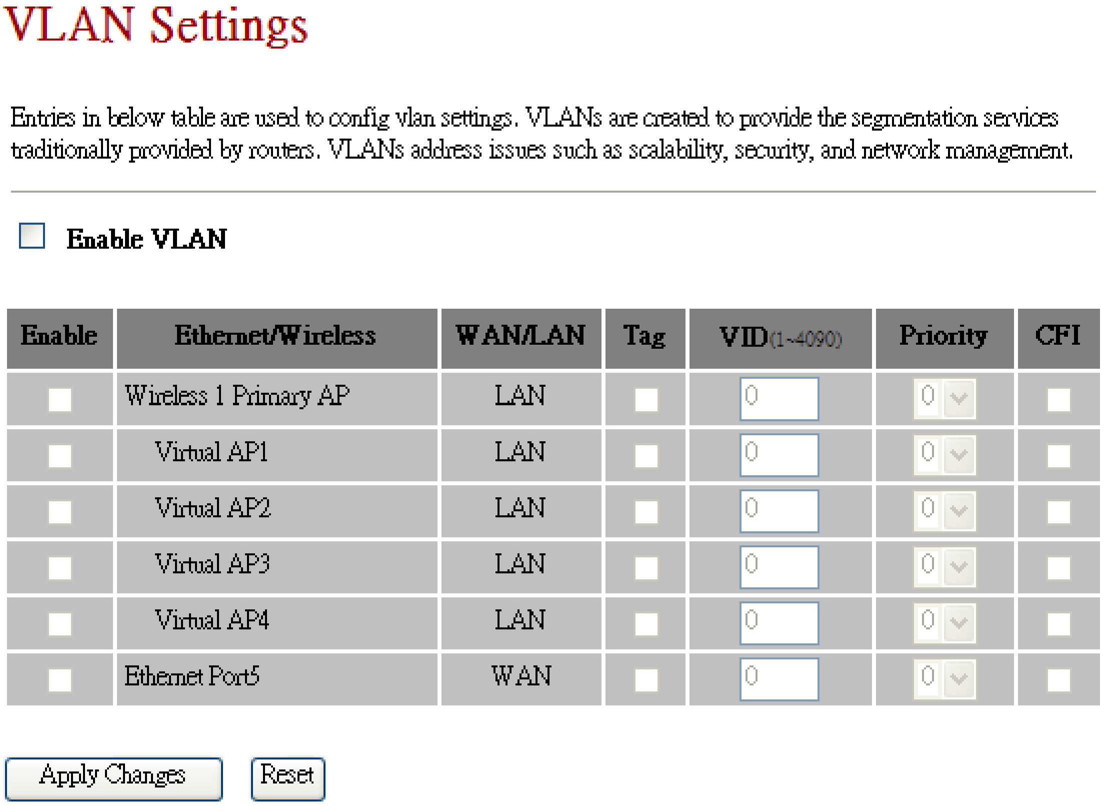
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

□ **Enable DMZ**

DMZ Host IP Address:

5.6 VLAN Settings

Entries in below table are used to configure VLAN settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.



VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

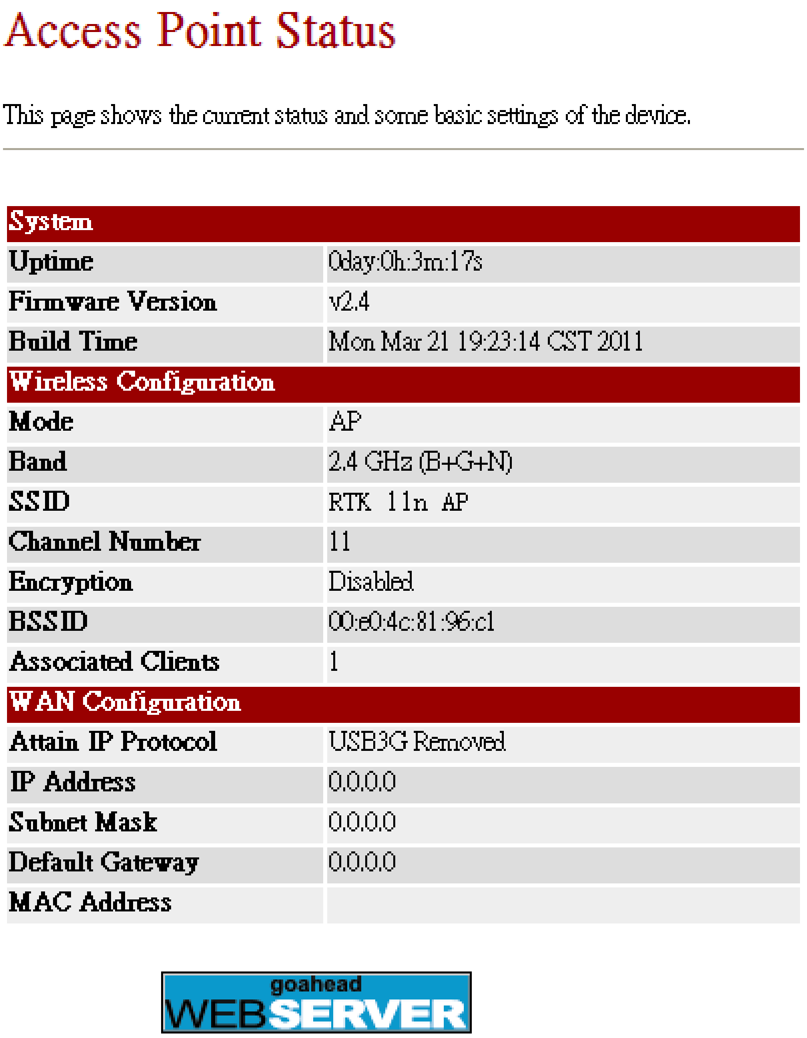
□ Enable VLAN

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1~4090)	Priority	CFI
□	Wireless 1 Primary AP	LAN	□	0	0	□
□	Virtual AP1	LAN	□	0	0	□
□	Virtual AP2	LAN	□	0	0	□
□	Virtual AP3	LAN	□	0	0	□
□	Virtual AP4	LAN	□	0	0	□
□	Ethernet Port5	WAN	□	0	0	□

6. MANAGEMENT

6.1 Status

This page shows the current status and some basic settings of the device.



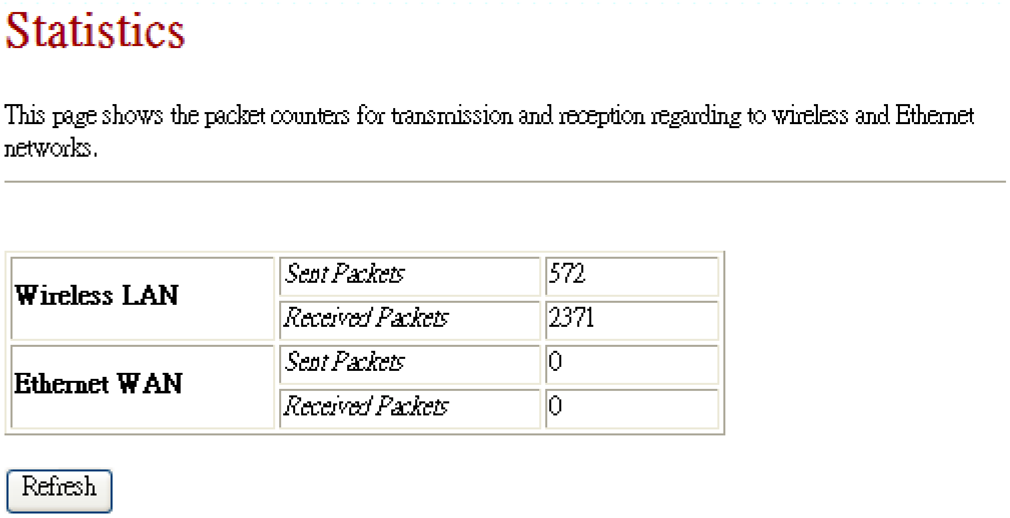
Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:3m:17s
Firmware Version	v2.4
Build Time	Mon Mar 21 19:23:14 CST 2011
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	RTK 11n AP
Channel Number	11
Encryption	Disabled
BSSID	00:e0:4c:81:96:c1
Associated Clients	1
WAN Configuration	
Attain IP Protocol	USB3G Removed
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	

6.2 Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.



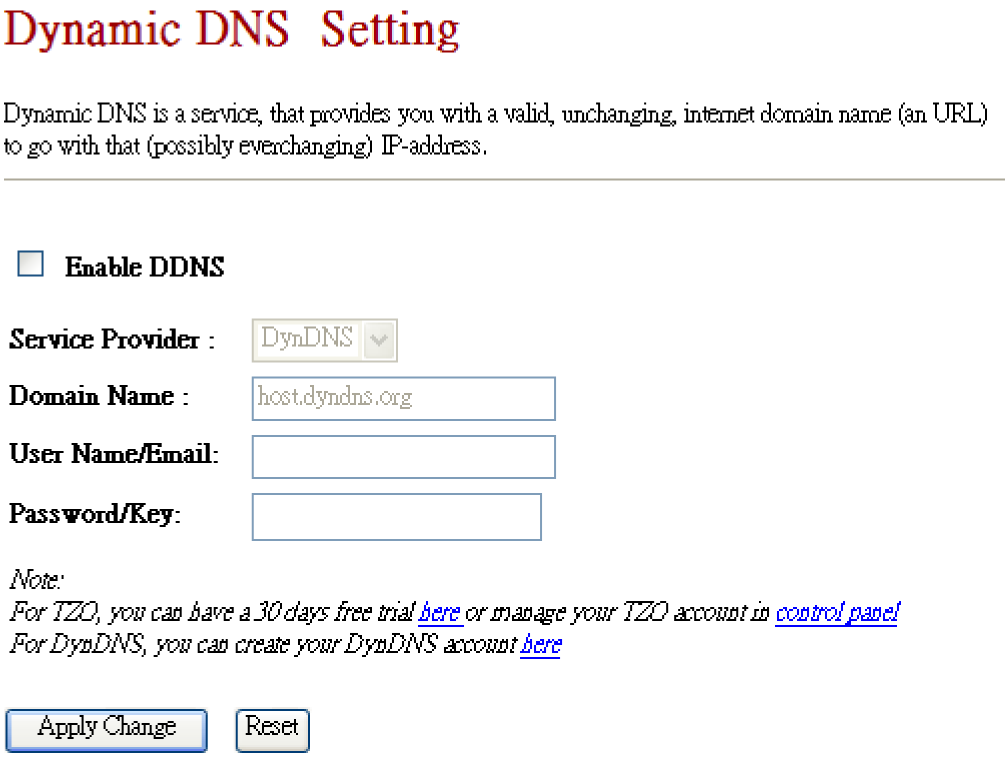
Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	572
	Received Packets	2371
Ethernet WAN	*Sent Packets*	0
	Received Packets	0

6.3 DDNS

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly every changing) IP-address.



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

□ **Enable DDNS**

Service Provider : DynDNS

Domain Name : host.dyndns.org

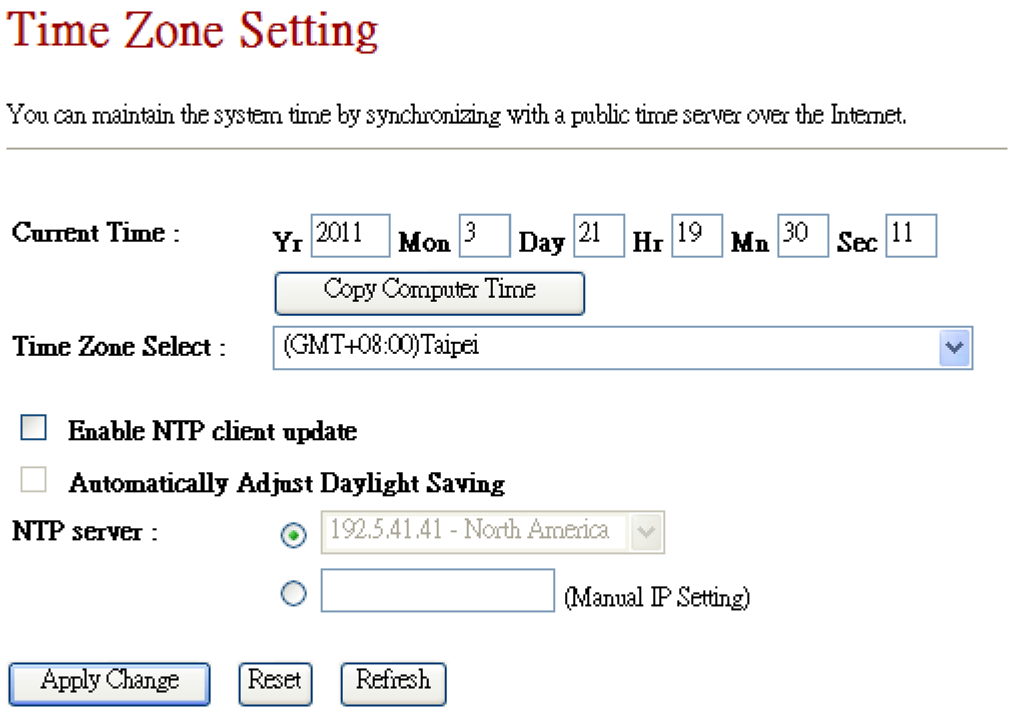
User Name/Email:

Password/Key:

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

6.4 Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : **Yr** 2011 **Mon** 3 **Day** 21 **Hr** 19 **Mn** 30 **Sec** 11

Time Zone Select : (GMT+08:00)Taipei

□ **Enable NTP client update**

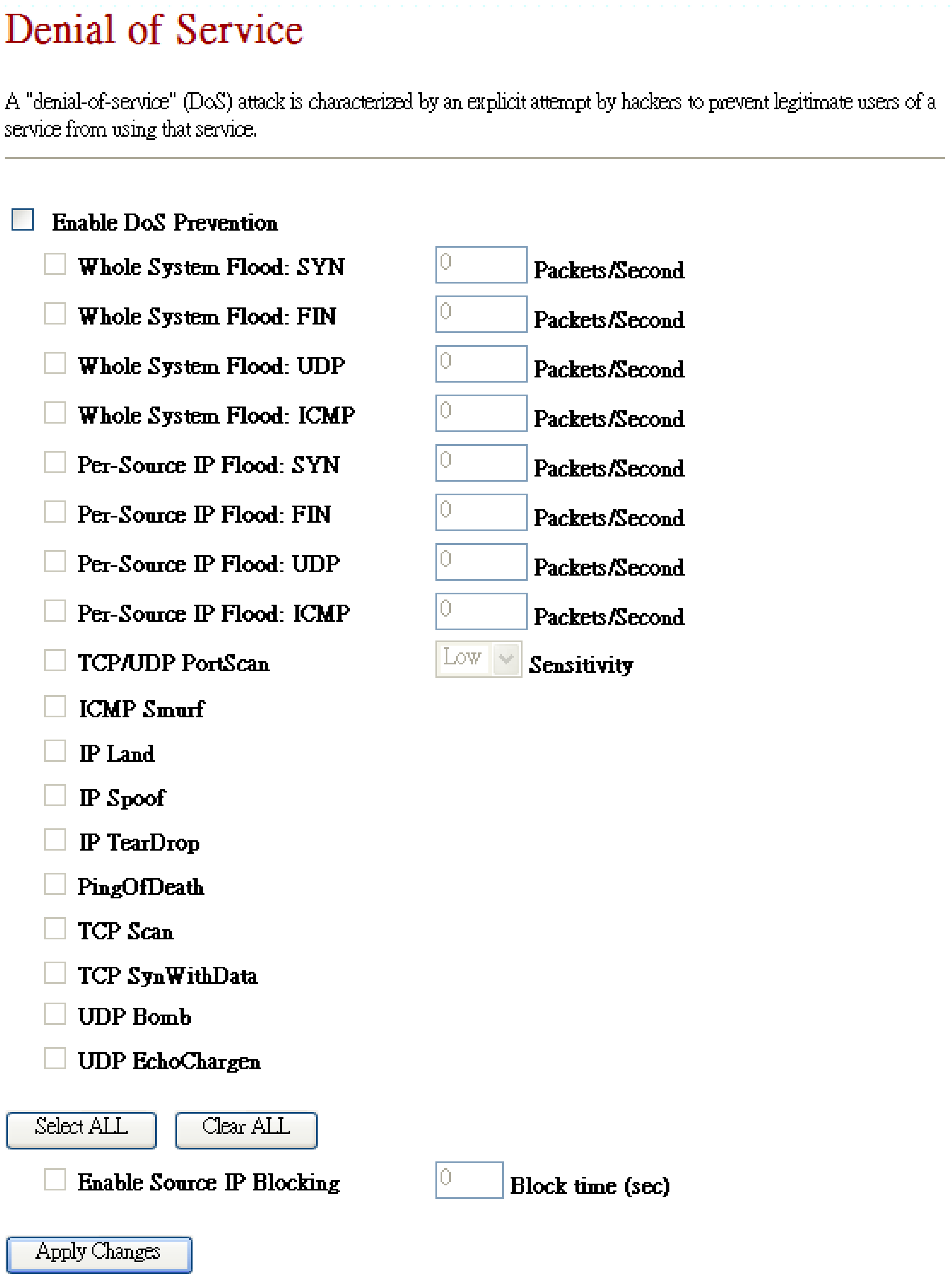
□ **Automatically Adjust Daylight Saving**

NTP server : ● 192.5.41.41 - North America

○ (Manual IP Setting)

6.5 Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.



Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

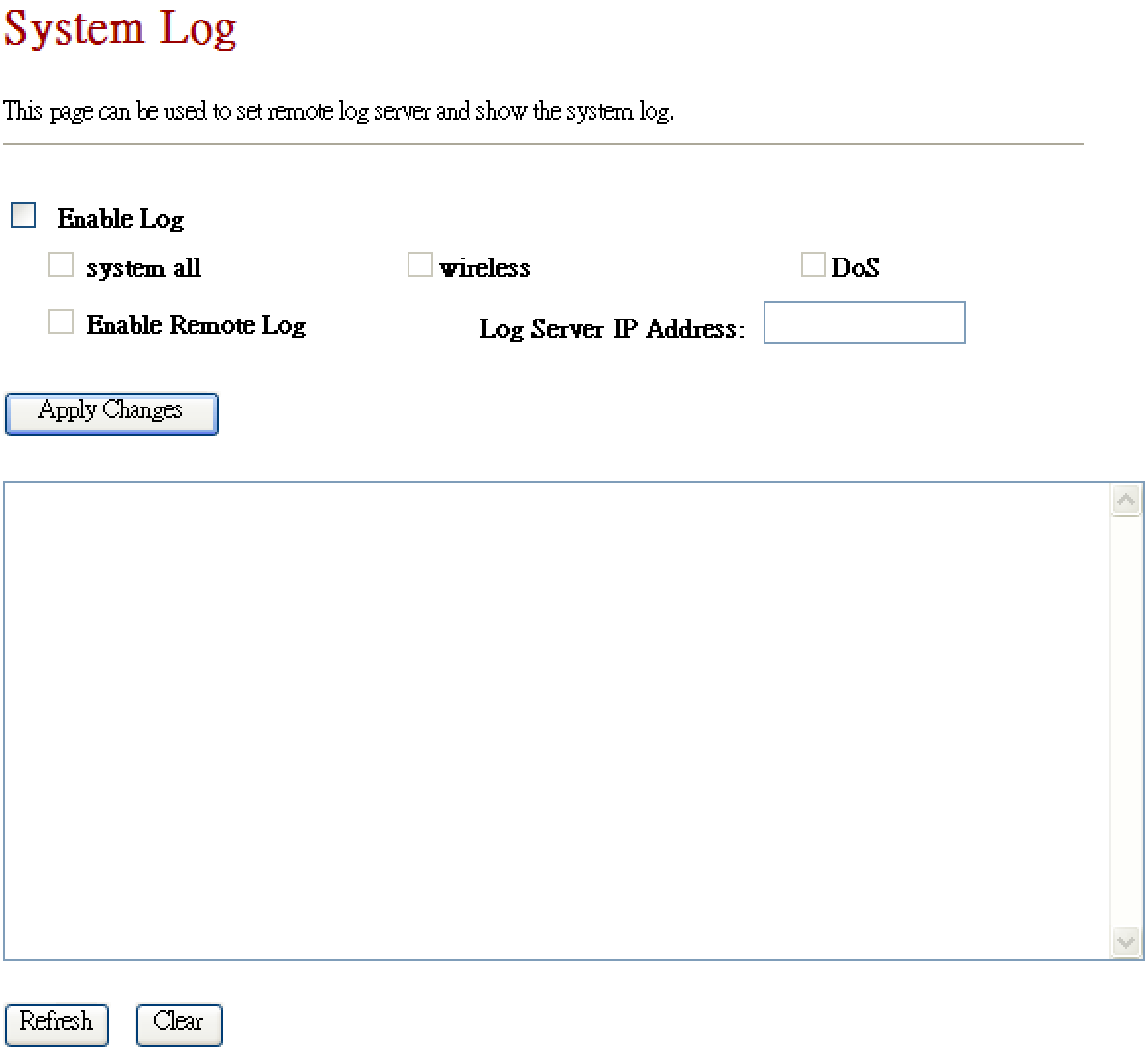
□ Enable DoS Prevention

□ Whole System Flood: SYN	0	Packets/Second
□ Whole System Flood: FIN	0	Packets/Second
□ Whole System Flood: UDP	0	Packets/Second
□ Whole System Flood: ICMP	0	Packets/Second
□ Per-Source IP Flood: SYN	0	Packets/Second
□ Per-Source IP Flood: FIN	0	Packets/Second
□ Per-Source IP Flood: UDP	0	Packets/Second
□ Per-Source IP Flood: ICMP	0	Packets/Second
□ TCP/UDP PortScan	Low	Sensitivity
□ ICMP Smurf		
□ IP Land		
□ IP Spoof		
□ IP TearDrop		
□ PingOfDeath		
□ TCP Scan		
□ TCP SynWithData		
□ UDP Bomb		
□ UDP EchoChargen		

□ Enable Source IP Blocking 0 Block time (sec)

6.5 System Log

This page can be used to set remote log server and show the system log.



System Log

This page can be used to set remote log server and show the system log.

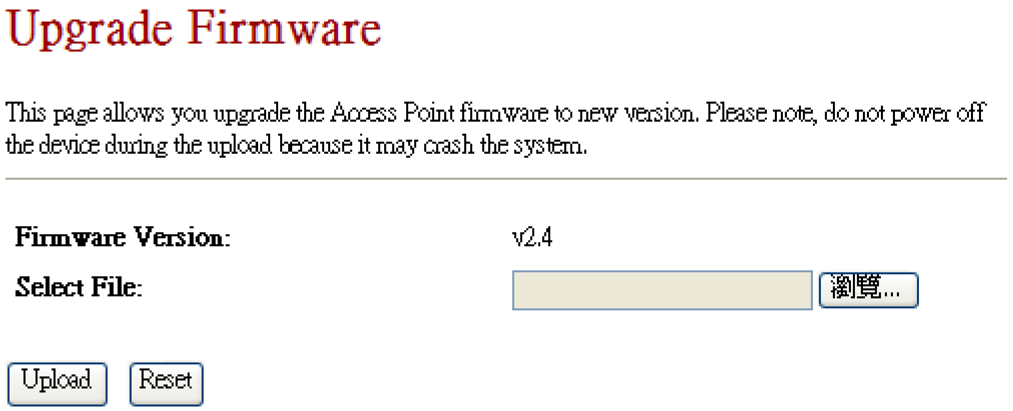
□ Enable Log

□ system all □ wireless □ DoS

□ Enable Remote Log Log Server IP Address:

6.5 Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.



Upgrade Firmware

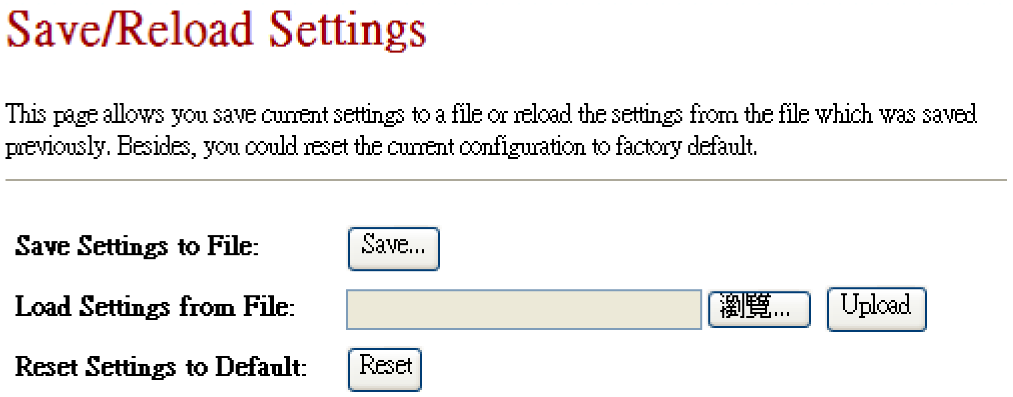
This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Firmware Version: v2.4

Select File:

6.5 Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.



Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

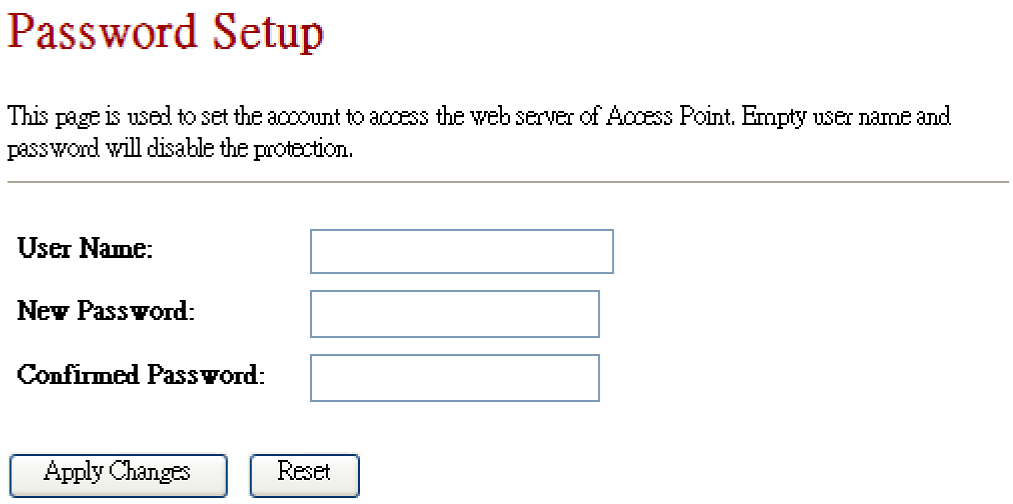
Save Settings to File:

Load Settings from File:

Reset Settings to Default:

6.5 Password

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.



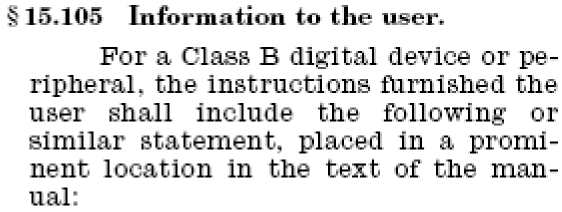
Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

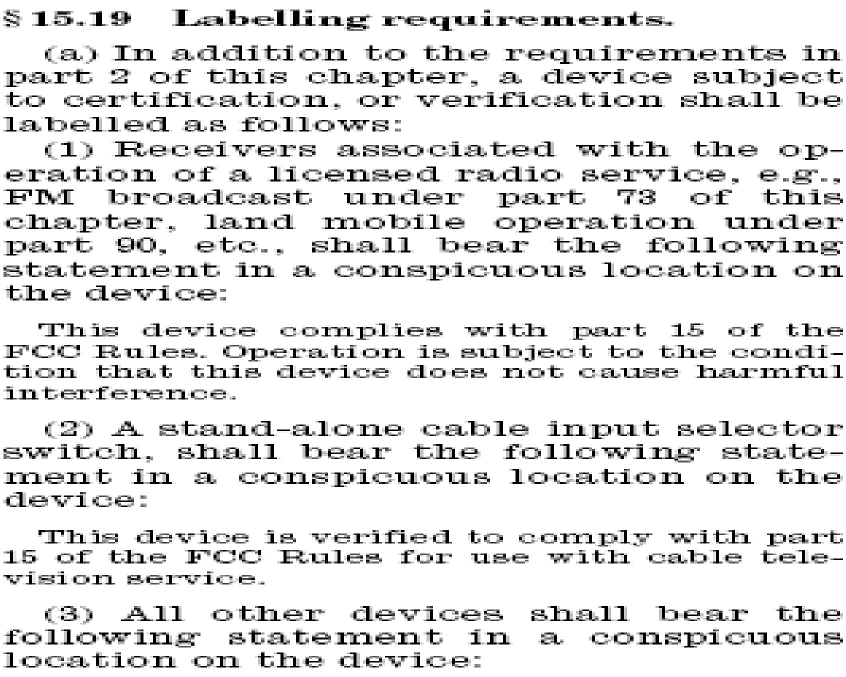


§ 15.105 **Information to the user.**

For a Class B digital device or peripheral, the instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual:

Federal Communication Commission interference statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: -Reorient or relocate the receiving antenna. -Increase the separation between the equipment and receiver. -Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. -Consult the dealer or an experienced radio/TV technician for help.



§ 15.19 **Labelling requirements.**

(a) In addition to the requirements in part 2 of this chapter, a device subject to certification, or verification shall be labelled as follows:

(1) Receivers associated with the operation of a licensed radio service, e.g., FM broadcast under part 73 of this chapter, land mobile operation under part 90, etc., shall bear the following statement in a conspicuous location on the device:

This device complies with part 15 of the FCC Rules. Operation is subject to the condition that this device does not cause harmful interference.

(2) A stand-alone cable input selector switch, shall bear the following statement in a conspicuous location on the device:

This device is verified to comply with part 15 of the FCC Rules for use with cable television service.

(3) All other devices shall bear the following statement in a conspicuous location on the device:

FCC Caution:

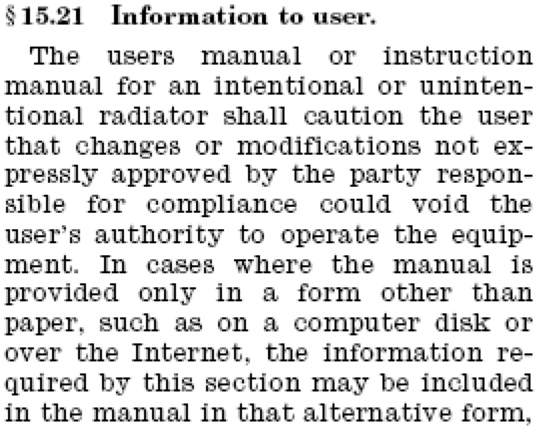
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference and

(2) this device must accept any interference received, including interference that may cause undesired operation

RF Exposure Warning

The equipment complies with RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



§15.21 Information to user.

The users manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form,

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.