# Wireless LAN Device Series

## WLAN Outdoor Bridge

# DLB2300/DLB2310/DLB2319
# User Manual

**Version. 1.0.0 (06.01.2006)**

## TABLE OF CONTENTS

# Preface

## FCC Information

### *Electronic Emission Notices*

This device complies with CFR 47 Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

### *FCC Frequency Interference Statement*

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to CFR47 Part 15. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment, not withstanding use in commercial, business and industrial environment,. 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 relocated the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technical for help.

Changes or modifications to this equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

### *FCC Radiation Exposure Statement*

To comply with FCC RF exposure requirements in section 1.1307, a minimum separation distance of 0.4-meters (15.75-inches) is required between the antenna and all persons.

### *Antenna Installation*

**WARNING:** It is installer's responsibility to ensure that when using the outdoor antenna in the United States (or where FCC apply), only those antennas certified with the product are used. The use of any antenna other than those certified with the product is expressly forbidden in accordance to FCC rules CFR47 part 15.204.

The installer should configure the output power level of antennas, according to country regulations and per antenna type. Professional installation is required of equipment with connectors to ensure compliance with health and safety issues.

## Installation Requirements

This guide is for the networking professional who installs and manages the Deliberant DLB-2300/DLB2310/DLB2319 outdoor product hereafter referred to as the “device”. To use this guide, you should have experience working with the TCP/IP configuration and be familiar with the concepts and terminology of wireless local area networks.

**Note: Only those antennas that are of the same type with lesser gain than those that are certified with these devices may be used legally by the installer!**

**The following antennas have been tested with the DLB23xx:**

Microcom Technologies 19dbi Panel Antenna (Model: 24EI19-SAF)
Superpass 14dbi Panel Antenna (Model: SPLG22)
Hyperlink Technology 12dbi Omni Antenna (Model: HG2412U)

# Ch 1. Device Installation

## Packing List

Before you start to install the ODU, make sure the package contains the following items□

- Wireless Outdoor Bridge unit * 1
- Mounting Kit * 1
- Power Over Ethernet Kit * 1

# Ch 2. First Time Configuration

## Before Start to Configure

There are two ways to configure the device, one is through web-browser, and the other is through Secure Shell CLI interface. To access the configuration interfaces, make sure you are using a computer connected to the same network as the device. The default IP address of the device is 192.168.2.254, and the subnet-mask is 255.255.255.0.

The device has three operation modes (Router/Bridge/WISP). In bridge mode, also known as AP Client, you can access the device by both WLAN (Wireless Local Area Network) and wired LAN. And in router/WISP modes, the device can be accessed by both WLAN and WAN. The default IP addresses for the device are 192.168.2.254(for LAN), 172.1.1.1(for WAN), so you need to make sure the IP address of your PC is in the same subnet as the device, such as 192.168.2.X (for LAN), 172.1.1.X (for WAN).

Please note that the DHCP server inside the device is default to up and running. Do not have multiple DHCP servers in your network environment, otherwise it will cause abnormal situation.

We also provide an auto-discovery tool which is for finding out the IP of the device. In case, you've forgot the IP of the device or the IP of the device has been changed, you can use the tool to find out the IP of the device even your

PC is not in the same subnet as the device is.

# Knowing the Network Application

DLB2300/DLB2310/DLB2319 can act as the following roles, and it supports WDS (Wireless Distribution System) function.

- Access Point
- WDS (Wireless Repeater)
- Bridge/Router
- WISP
- AP Client

The device provides 3 different operation modes and the wireless radio of device can act as AP/Client/WDS. The operation mode is about the communication mechanism between the wired Ethernet NIC and wireless NIC, the following is the types of operation mode.

**Router**
The wired Ethernet (WAN) port is used to connect with ADSL/Cable modem and the wireless NIC is used for your private WLAN. The NAT is existed between the 2 NIC and all the wireless clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is static IP. You can access the web server of device through the default WAN IP address 172.1.1.1 and modify the setting base on your ISP requirement.

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

**WISP (Wireless ISP)**
This mode can let you access the AP of your wireless ISP and share the same public IP address form your ISP to the PCs connecting with the wired Ethernet port of the device. To use this mode, first you must set the wireless radio to be client mode and connect to the AP of your ISP then you can configure the WAN IP configuration to meet your ISP requirement.

The wireless radio of the device acts as the following roles.

**AP (Access Point)**
The wireless radio of device serves as communications “hub” for wireless clients and provides a connection to a wired LAN.

**AP Client**

This mode provides the capability to connect with the other AP using infrastructure/Ad-hoc networking types. With bridge operation mode, you can directly connect the wired Ethernet port to your PC and the device becomes a wireless adapter. And with WISP operation mode, you can connect the wired Ethernet port to a hub/switch and all the PCs connecting with hub/switch can share the same public IP address from your ISP.

**WDS (Wireless Distribution System)**

This mode serves as a wireless repeater; the device forwards the packets to another AP with WDS function. When this mode is selected, all the wireless clients can't survey and connect to the device. The device only allows the WDS connection.

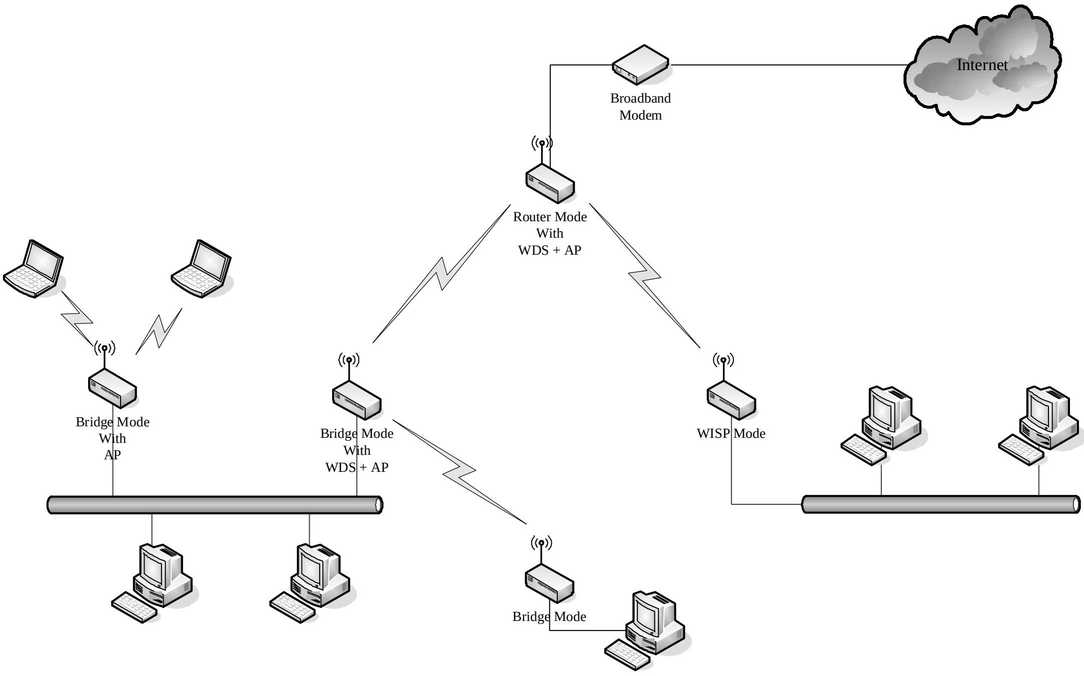
**WDS+AP**

This mode combines WDS plus AP modes, it not only allows WDS connections but also the wireless clients can survey and connect to the device.

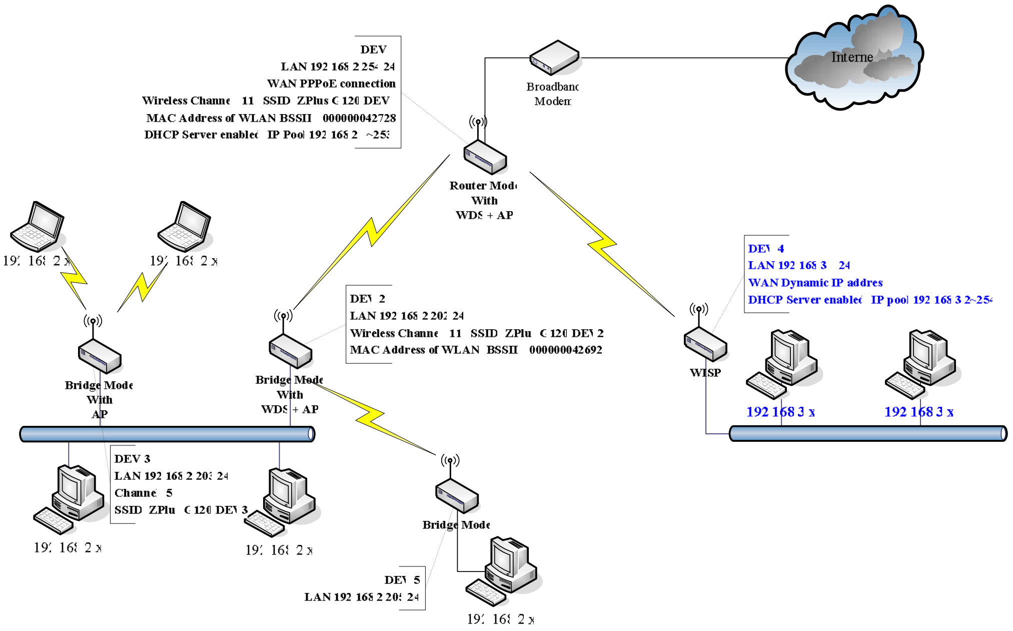
The following table shows the supporting combination of operation and wireless radio modes.

| | *Bridge* | *Router* | *WISP* |
|---|---|---|---|
| ***AP*** | V | V | X |
| ***WDS*** | V | V | X |
| ***Client*** | V | X | V |
| ***AP+WDS*** | V | V | X |

Hereafter are some topologies of network application for your reference.


Internet
Broadband Modem
Router Mode With WDS + AP
Bridge Mode With AP
Bridge Mode With WDS + AP
WISP Mode
Bridge Mode

## Examples of Configuration



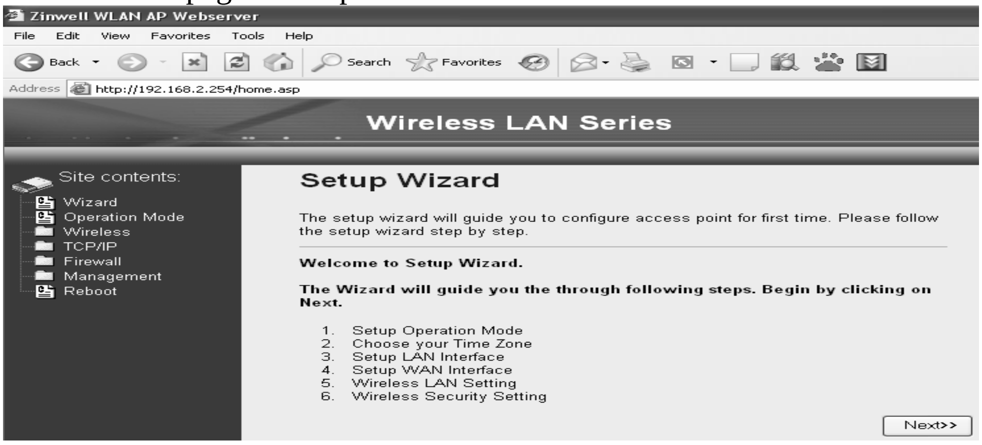
This example demonstrates how to set up a network with different device configurations. There are 2 DHCP servers (DEV1/DEV4) in the network to control the IP configuration of 2 domains (192.168.2.x/192.168.3.x). Once the setting is done, all the PCs can visit Internet through DEV1.

We assume all the devices keep the factory default setting. To make sure that user can continuing press the rest button for more than 5 seconds to restore the factory default setting.

The following descriptions show the steps to configure DEV1 to DEV5.

Configure DEV1:

1. Connect the ADSL modem to Ethernet port of device using Ethernet cable.
2. Access the web server (http://192.168.2.254) of device from the wireless station.
3. Use Wizard page to setup device.



Setup Wizard

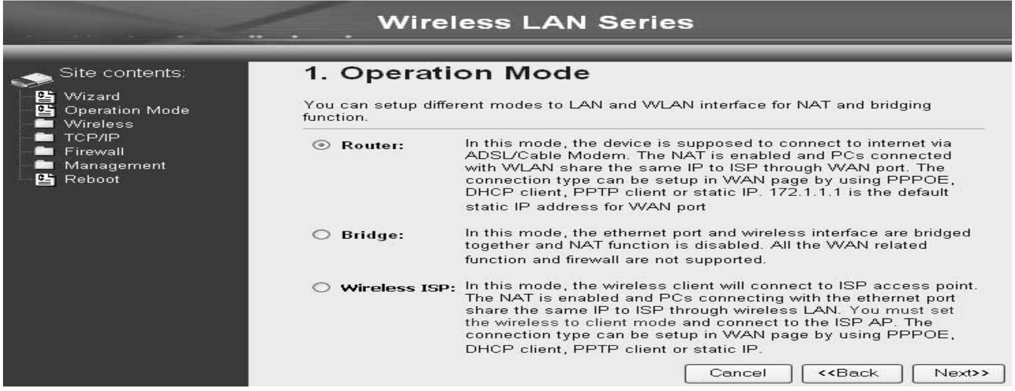
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

**Welcome to Setup Wizard.**

**The Wizard will guide you the through following steps. Begin by clicking on Next.**

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

4. Press “Next>>” button then set the “Operation Mode” to “Router” mode.



1. Operation Mode

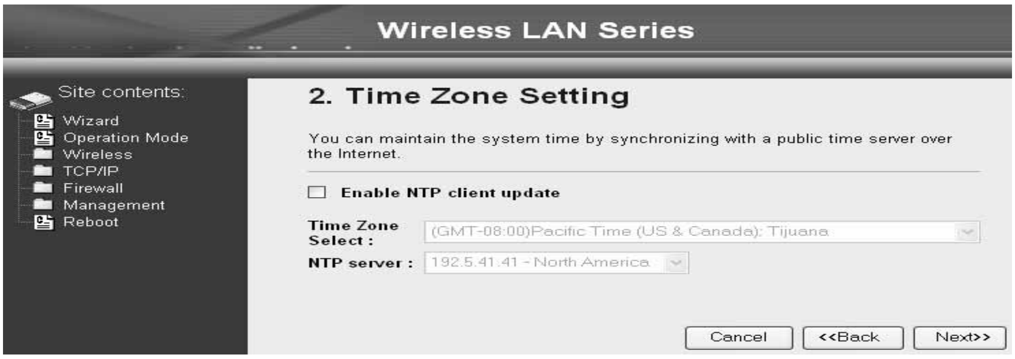
You can setup different modes to LAN and WLAN interface for NAT and bridging function.

● Router: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN 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 or static IP. 172.1.1.1 is the default static IP address for WAN port

○ Bridge: In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ Wireless ISP: In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

5. Press “Next>>” button then disable “Time Zone” function.



2. Time Zone Setting

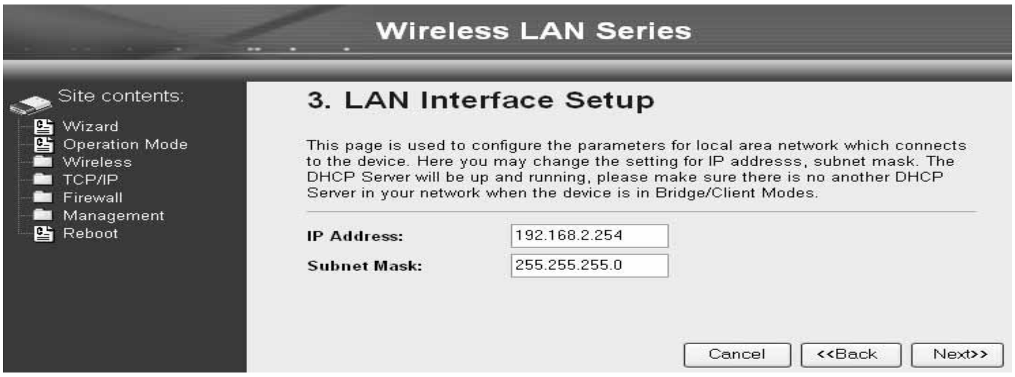
You can maintain the system time by synchronizing with a public time server over the Internet.

□ Enable NTP client update

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

NTP server : 192.5.41.41 - North America

6. Press “Next>>” button then set the IP address of LAN interface.



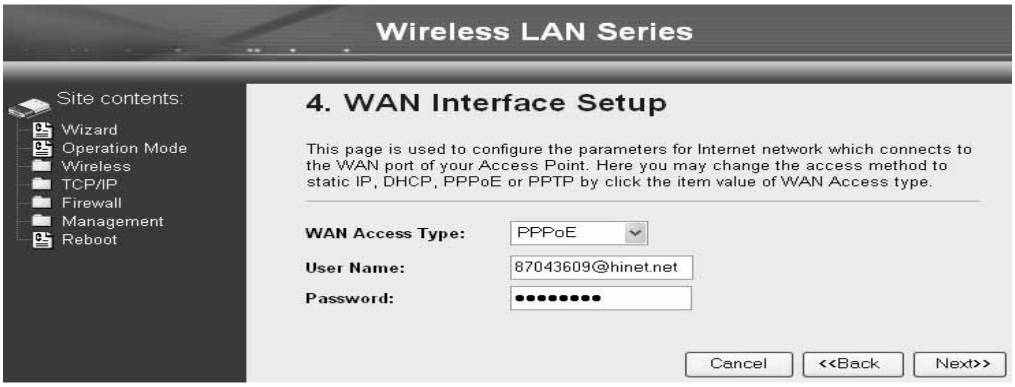
3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.

IP Address: 192.168.2.254

Subnet Mask: 255.255.255.0

7. Press “Next>>” button then select the “PPPoE” for “WAN Access Type” and fill in the “User Name” and “Password” fields.



4. WAN Interface Setup

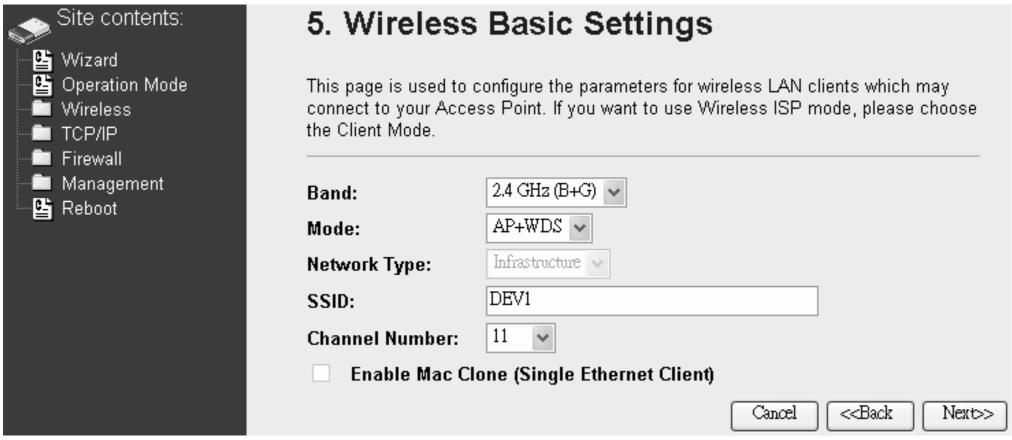
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: PPPoE

User Name: 87043609@hinet.net

Password: ●●●●●●●●●

8. Press “Next>>” button then select the “AP+WDS” for “mode” and change the SSID to “DEV1”.



5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. If you want to use Wireless ISP mode, please choose the Client Mode.

Band: 2.4 GHz (B+G)

Mode: AP+WDS

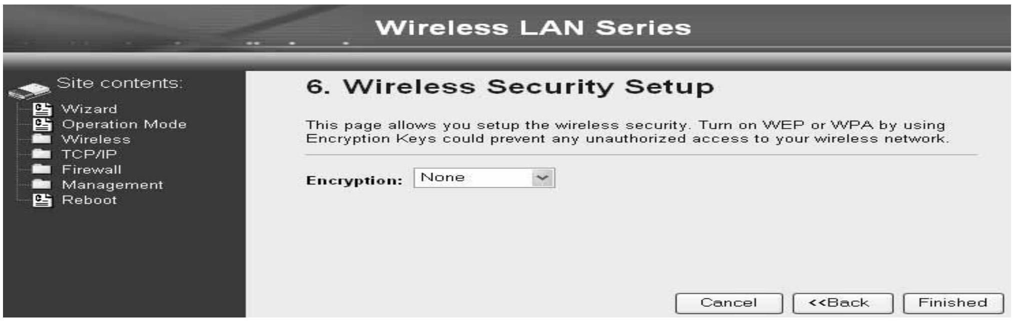
Network Type: Infrastructure

SSID: DEV1

Channel Number: 11

□ Enable Mac Clone (Single Ethernet Client)

9. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

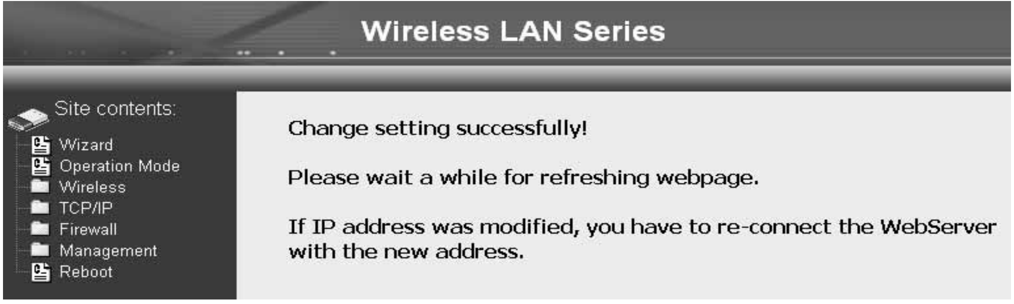


6. Wireless Security Setup

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.

Encryption: None

10. Wait for refreshing web page.

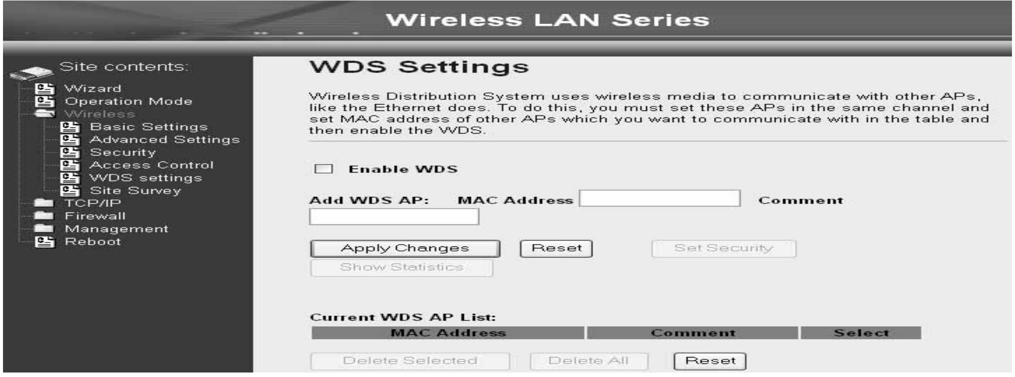


Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

11. Use “WDS Settings” page to configure 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.

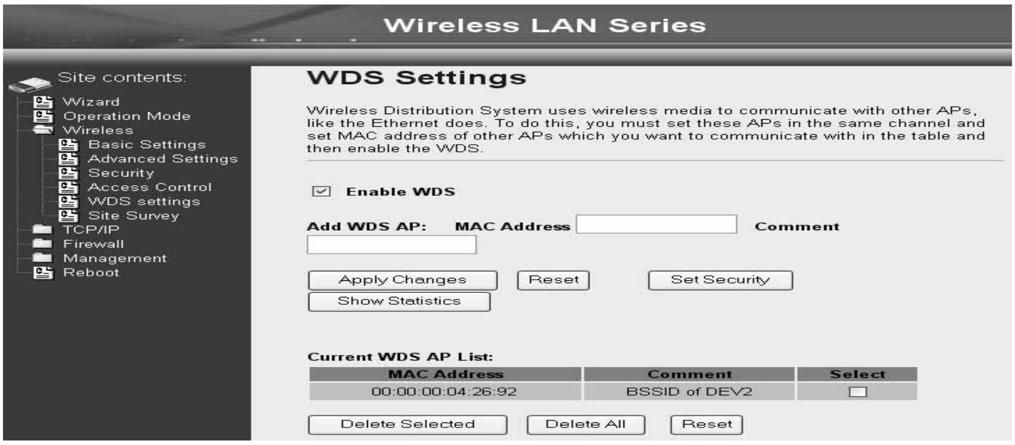
□ Enable WDS

Add WDS AP: MAC Address Comment

Current WDS AP List:

| MAC Address | Comment | Select |
|---|---|---|

12. Enable WDS function and add the BSSID of DEV2 to “Current WDS AP List”.



## 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.

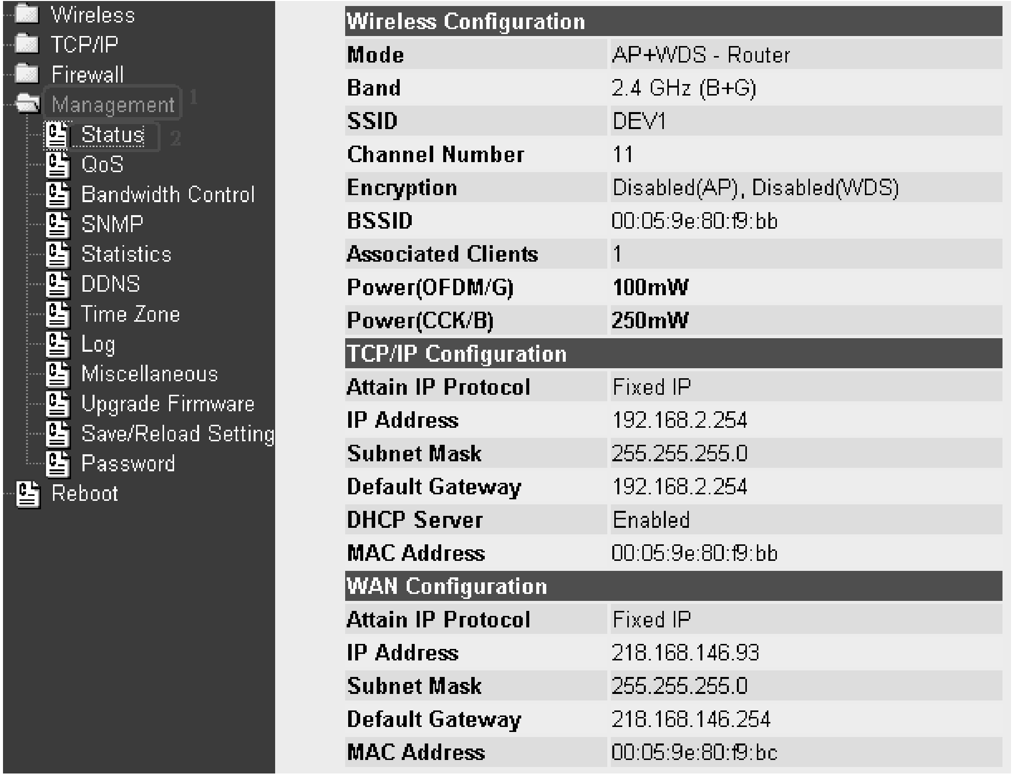
☑ Enable WDS

Add WDS AP: MAC Address ______ Comment ______

Current WDS AP List:

| MAC Address | Comment | Select |
|---|---|---|
| 00:00:00:04:26:92 | BSSID of DEV2 | □ |

13. Since we access the device by wireless connection, it may temporarily disconnect when applying the WDS setting. After re-connecting to the device, use the “Status” page to check the settings.



| Wireless Configuration | |
|---|---|
| Mode | AP+WDS - Router |
| Band | 2.4 GHz (B+G) |
| SSID | DEV1 |
| Channel Number | 11 |
| Encryption | Disabled(AP), Disabled(WDS) |
| BSSID | 00:05:9e:80:f9:bb |
| Associated Clients | 1 |
| Power(OFDM/G) | 100mW |
| Power(CCK/B) | 250mW |
| **TCP/IP Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.2.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.254 |
| DHCP Server | Enabled |
| MAC Address | 00:05:9e:80:f9:bb |
| **WAN Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 218.168.146.93 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 218.168.146.254 |
| MAC Address | 00:05:9e:80:f9:bc |

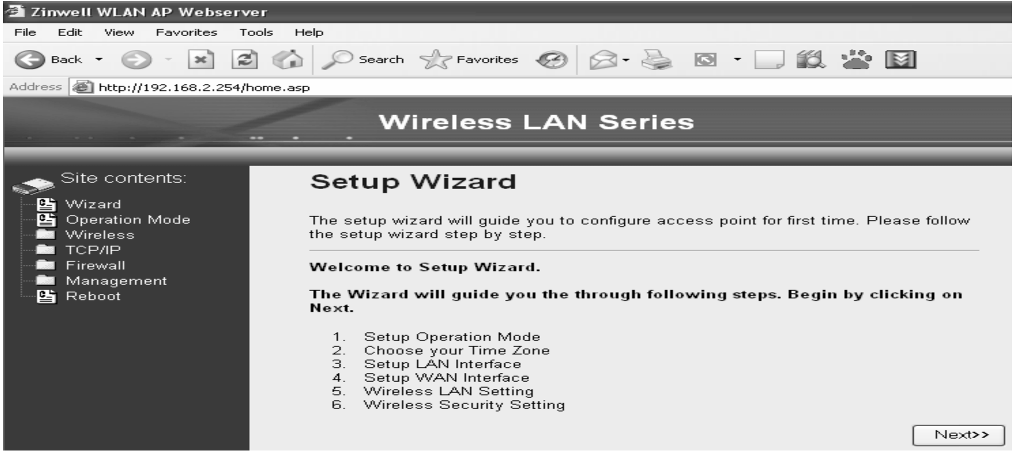
Configure DEV2:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

   **Caution**

   **If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you not able to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.**

2. Use Wizard page to setup device.



Setup Wizard

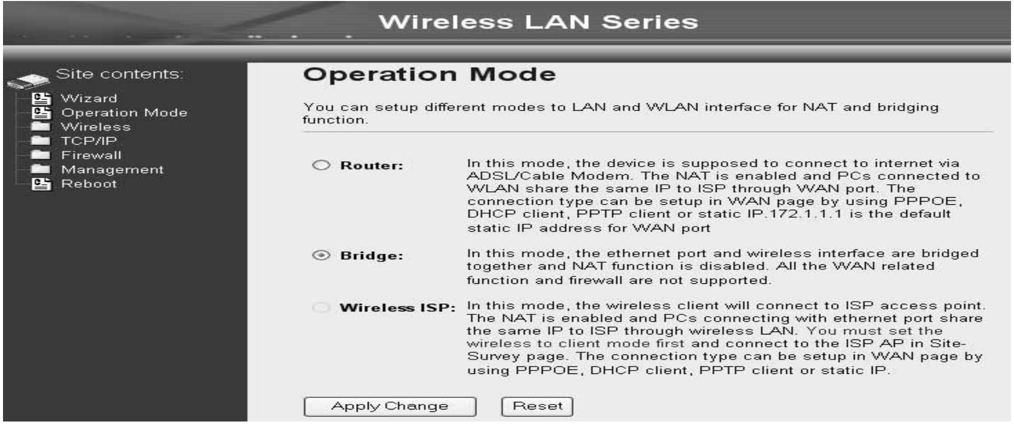
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

**Welcome to Setup Wizard.**

**The Wizard will guide you the through following steps. Begin by clicking on Next.**

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

3. Press "Next>>" button then set the "Operation Mode" to "Bridge" mode.



Operation Mode

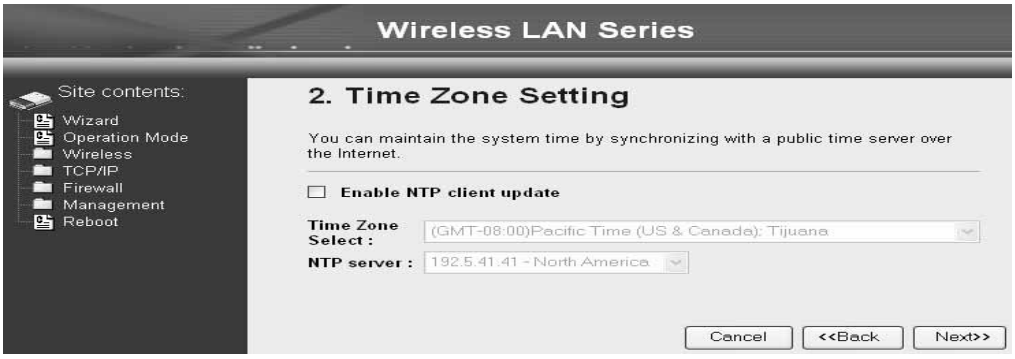
You can setup different modes to LAN and WLAN interface for NAT and bridging function.

○ **Router:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected to WLAN 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 or static IP.172.1.1.1 is the default static IP address for WAN port

● **Bridge:** In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with ethernet port 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 or static IP.

4. Press "Next>>" button then disable "Time Zone" function.



2. Time Zone Setting

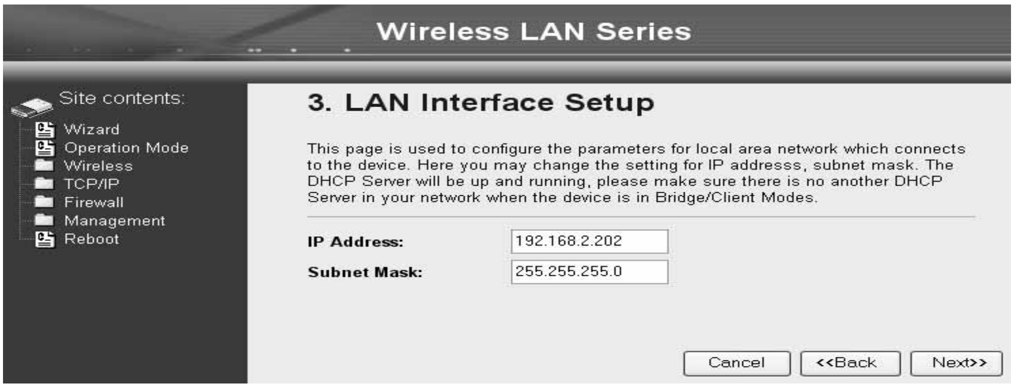
You can maintain the system time by synchronizing with a public time server over the Internet.

□ **Enable NTP client update**

**Time Zone Select :** (GMT-08:00)Pacific Time (US & Canada); Tijuana

**NTP server :** 192.5.41.41 - North America

5. Press “Next>>” button then set the IP address of LAN interface.



Wireless LAN Series

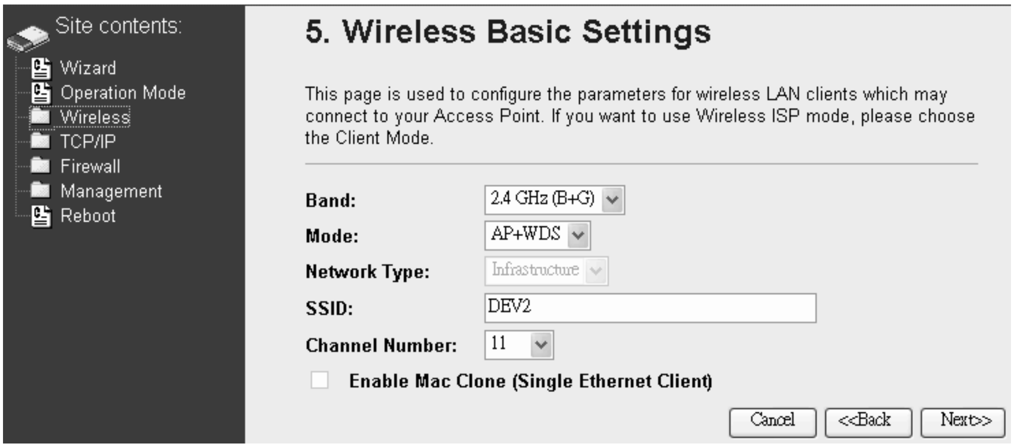
3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.

IP Address: 192.168.2.202

Subnet Mask: 255.255.255.0

6. Press “Next>>” button then select the “AP+WDS” for “mode” and change the SSID to “DEV2”.



5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. If you want to use Wireless ISP mode, please choose the Client Mode.

Band: 2.4 GHz (B+G)

Mode: AP+WDS

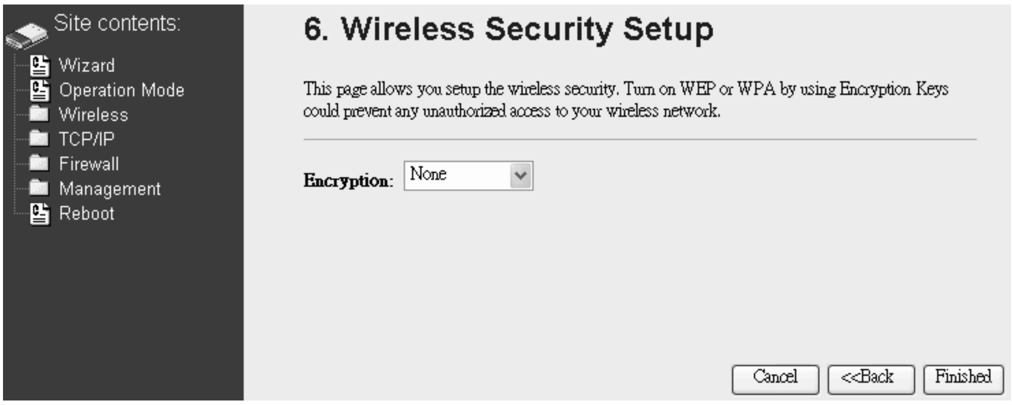
Network Type: Infrastructure

SSID: DEV2

Channel Number: 11

□ Enable Mac Clone (Single Ethernet Client)

7. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

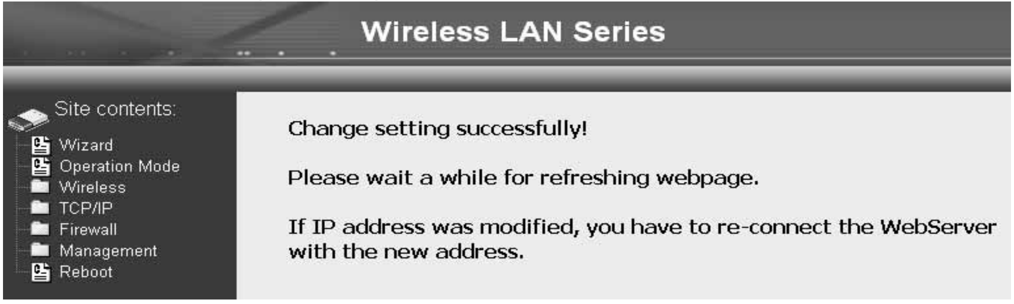


6. Wireless Security Setup

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.

Encryption: None

8. Wait for refreshing web page.



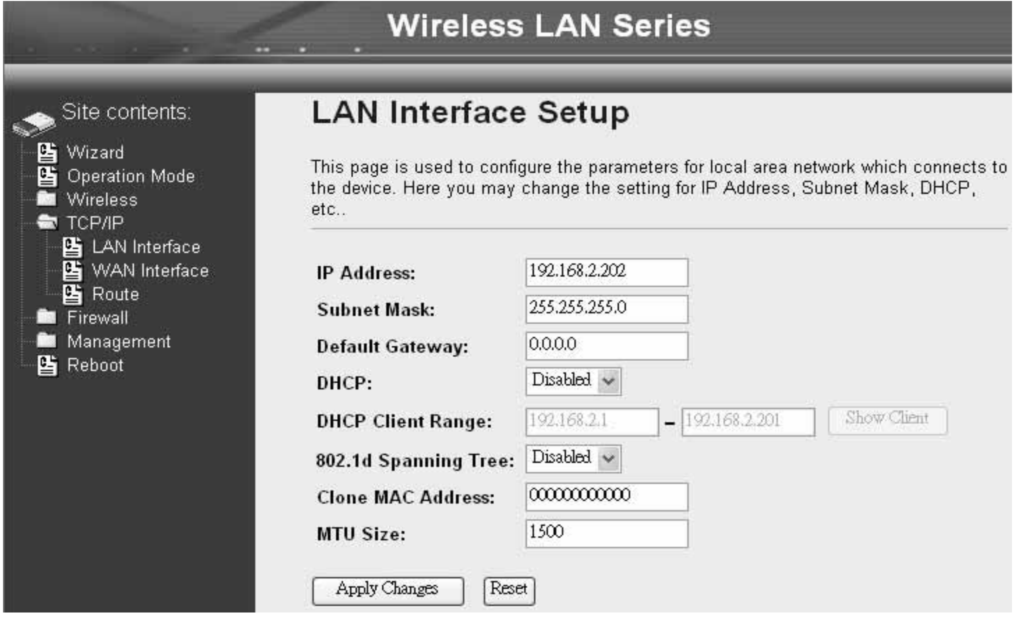
Wireless LAN Series

Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

9. Access the web server by new IP address “192.168.2.202” then use “LAN Interface” page to disable DHCP Server.



## LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

IP Address: 192.168.2.202

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Disabled

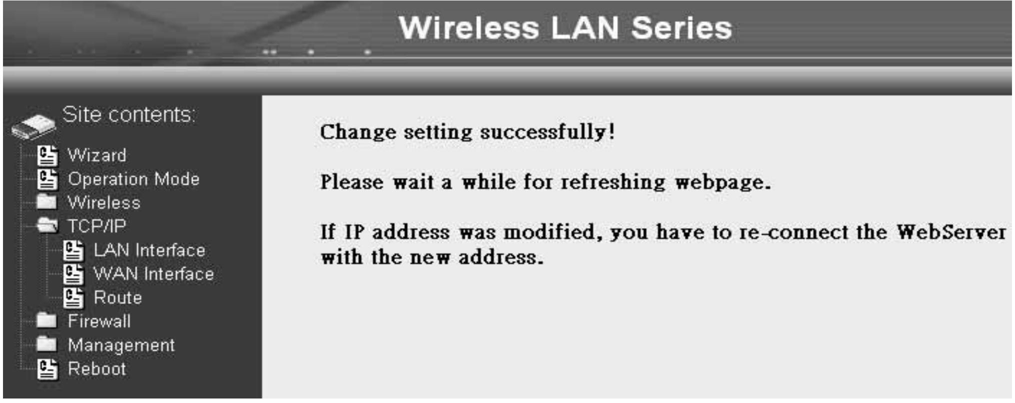
DHCP Client Range: 192.168.2.1 – 192.168.2.201 Show Client

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

MTU Size: 1500

10. Wait for refreshing web page.

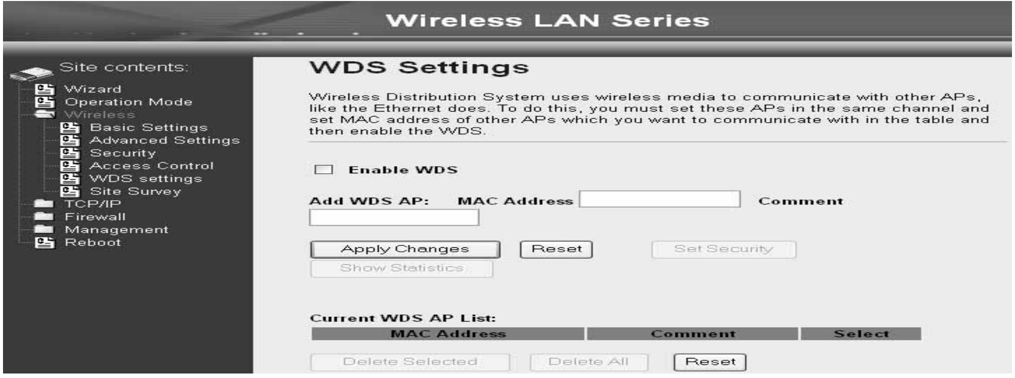


Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

11. Use “WDS Settings” page to configure 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.

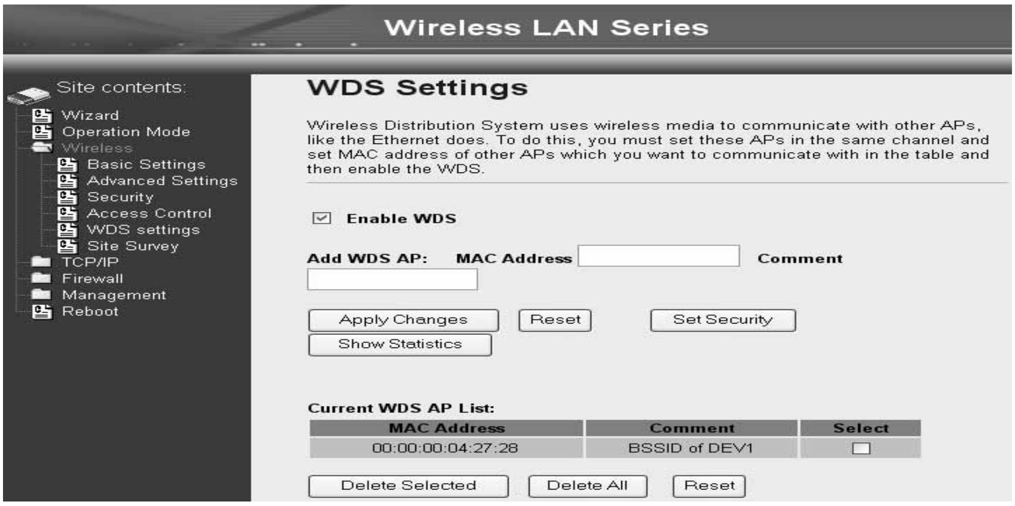
□ Enable WDS

Add WDS AP: MAC Address Comment

Current WDS AP List:

| MAC Address | Comment | Select |
|---|---|---|

12. Enable WDS function and add the BSSID of DEV1 to “Current WDS AP List”.



## 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.

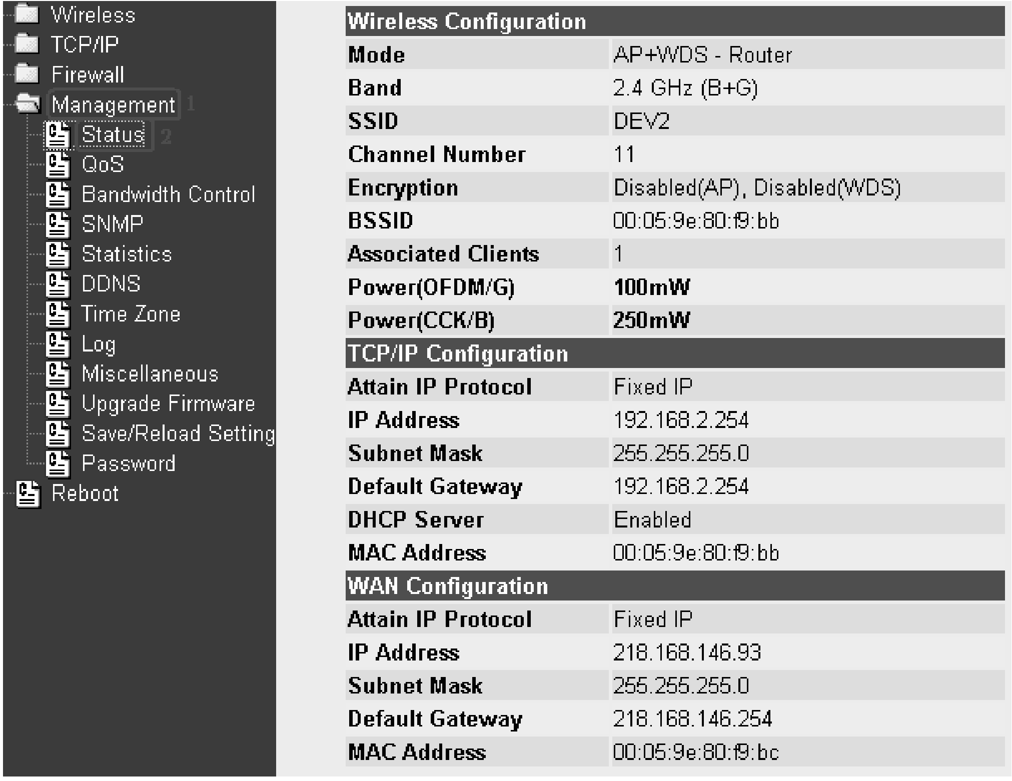
☑ **Enable WDS**

**Add WDS AP:** **MAC Address** ______ **Comment** ______

**Current WDS AP List:**

| MAC Address | Comment | Select |
|---|---|---|
| 00:00:00:04:27:28 | BSSID of DEV1 | □ |

13. Use the “Status” page to check the settings.



| Wireless Configuration | |
|---|---|
| Mode | AP+WDS - Router |
| Band | 2.4 GHz (B+G) |
| SSID | DEV2 |
| Channel Number | 11 |
| Encryption | Disabled(AP), Disabled(WDS) |
| BSSID | 00:05:9e:80:f9:bb |
| Associated Clients | 1 |
| Power(OFDM/G) | **100mW** |
| Power(CCK/B) | **250mW** |
| **TCP/IP Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.2.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.254 |
| DHCP Server | Enabled |
| MAC Address | 00:05:9e:80:f9:bb |
| **WAN Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 218.168.146.93 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 218.168.146.254 |
| MAC Address | 00:05:9e:80:f9:bc |

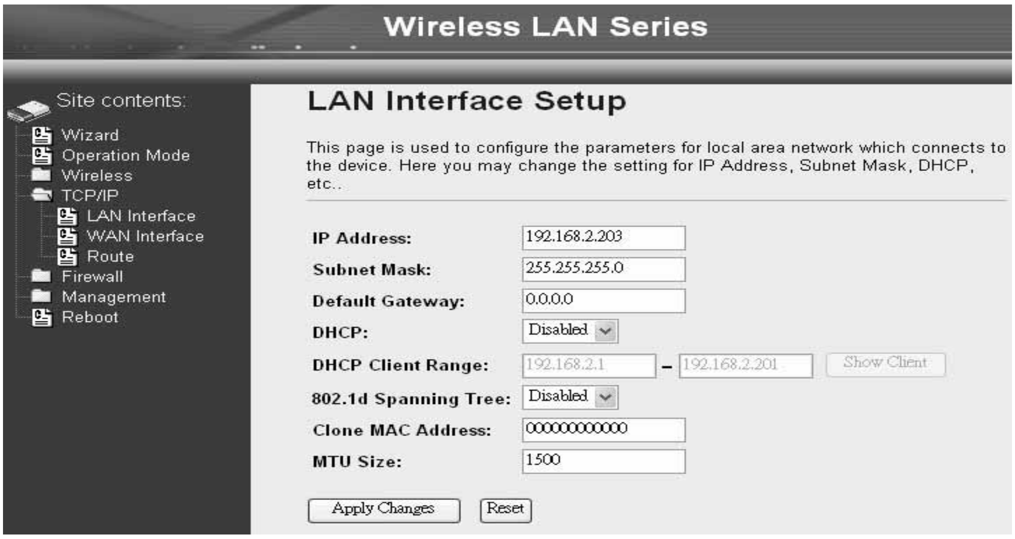
Configure DEV3:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

**Caution**

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you not able to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command “arp –d” then you can access the web server of device using the default IP address.

2. Use “LAN Interface” page to set the IP address of LAN interface and disable DHCP server.

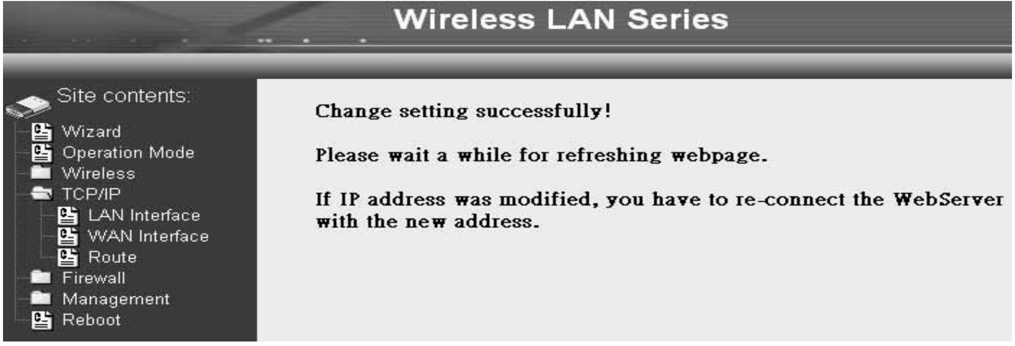


LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

IP Address: 192.168.2.203
Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0
DHCP: Disabled
DHCP Client Range: 192.168.2.1 – 192.168.2.201
802.1d Spanning Tree: Disabled
Clone MAC Address: 000000000000
MTU Size: 1500

3. Wait for refreshing web page.

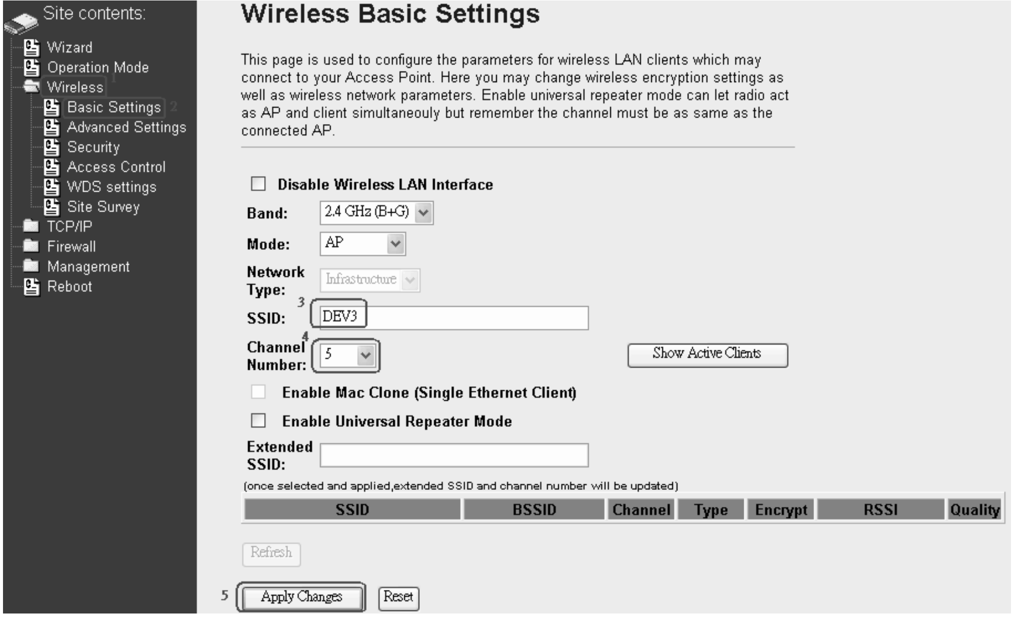


Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

4. Access the web server by new IP address “192.168.2.203” then use “Basic Settings” page to change SSID and CHANNEL.



## 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. Enable universal repeater mode can let radio act as AP and client simultaneously but remember the channel must be as same as the connected AP.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: DEV3

Channel Number: 5

☐ Enable Mac Clone (Single Ethernet Client)

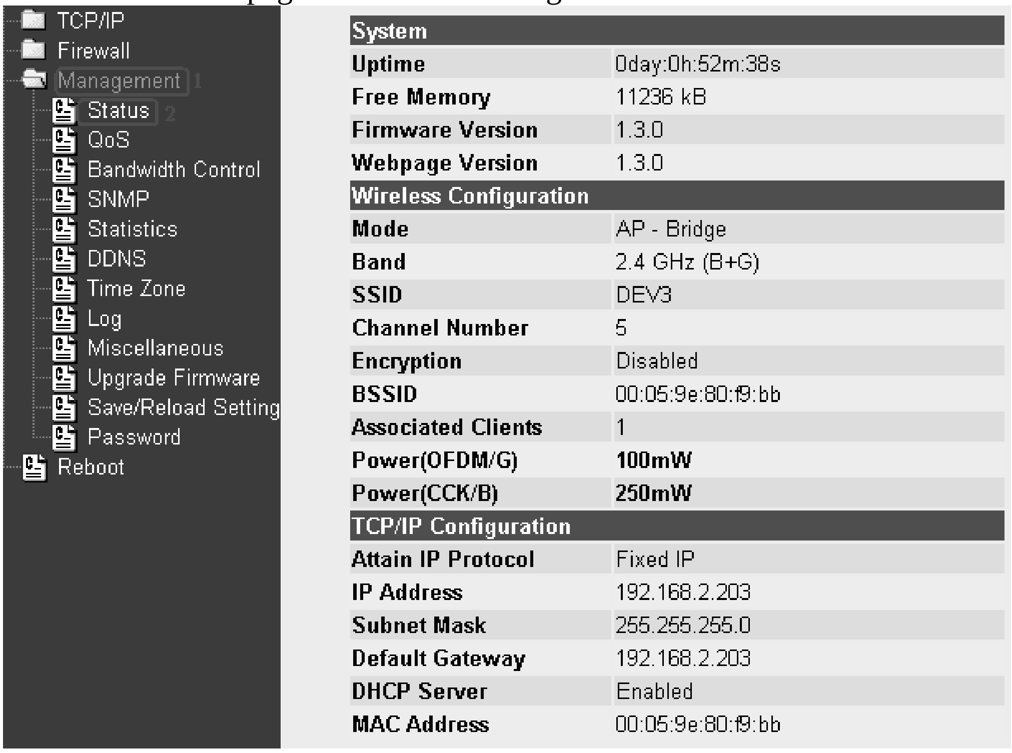
☐ Enable Universal Repeater Mode

Extended SSID:

(once selected and applied,extended SSID and channel number will be updated)

| SSID | BSSID | Channel | Type | Encrypt | RSSI | Quality |
|---|---|---|---|---|---|---|

5. Use the “Status” page to check the settings.



| System | |
|---|---|
| Uptime | 0day:0h:52m:38s |
| Free Memory | 11236 kB |
| Firmware Version | 1.3.0 |
| Webpage Version | 1.3.0 |
| **Wireless Configuration** | |
| Mode | AP - Bridge |
| Band | 2.4 GHz (B+G) |
| SSID | DEV3 |
| Channel Number | 5 |
| Encryption | Disabled |
| BSSID | 00:05:9e:80:f9:bb |
| Associated Clients | 1 |
| Power(OFDM/G) | 100mW |
| Power(CCK/B) | 250mW |
| **TCP/IP Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.2.203 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.203 |
| DHCP Server | Enabled |
| MAC Address | 00:05:9e:80:f9:bb |

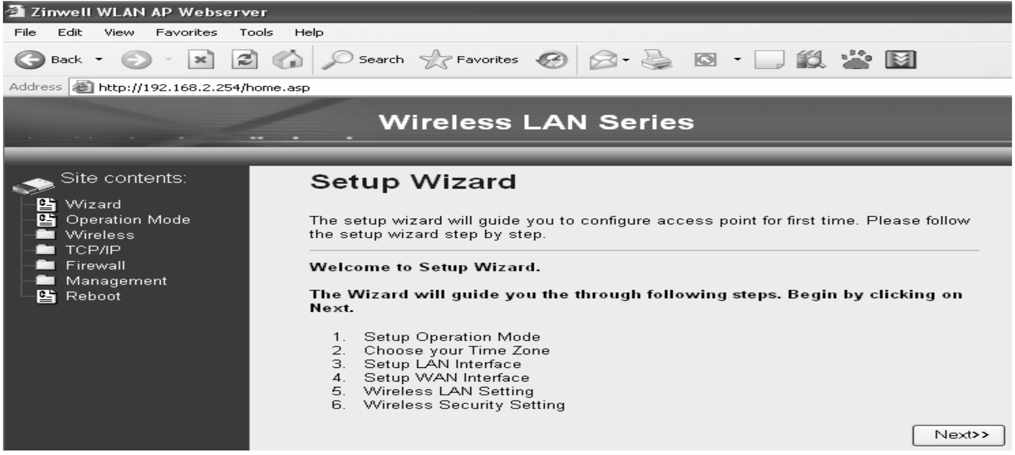
Configure DEV4:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

   **Caution**

   If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you unable to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command “arp –d” then you can access the web server of device using the default IP address.

2. Use Wizard page to setup device.



Setup Wizard

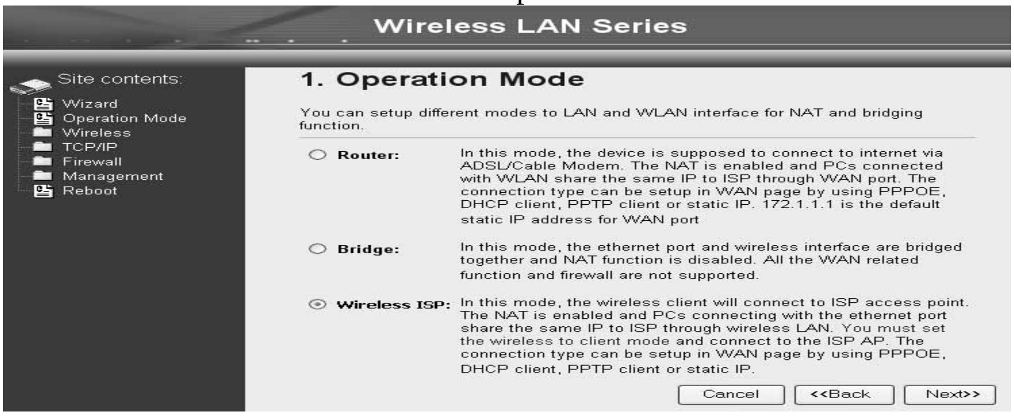
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

**Welcome to Setup Wizard.**

**The Wizard will guide you the through following steps. Begin by clicking on Next.**

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

3. Press “Next>>” button then set the “Operation Mode” to “Wireless ISP” mode.



1. Operation Mode

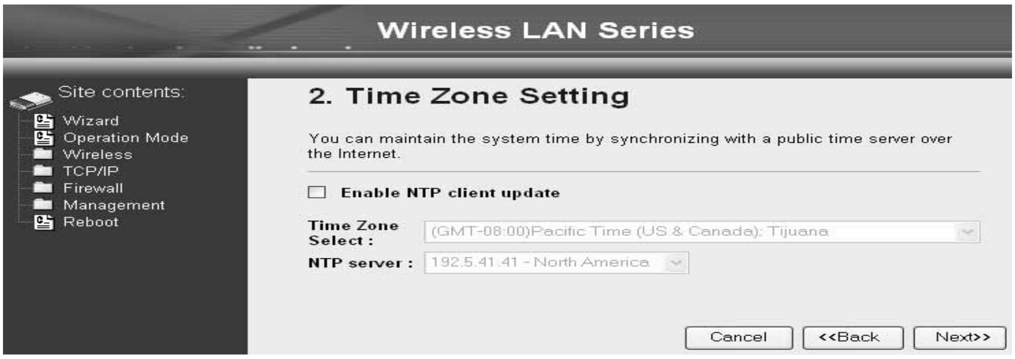
You can setup different modes to LAN and WLAN interface for NAT and bridging function.

○ **Router:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN 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 or static IP. 172.1.1.1 is the default static IP address for WAN port

○ **Bridge:** In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

● **Wireless ISP:** In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

4. Press “Next>>” button then disable “Time Zone” function.



2. Time Zone Setting

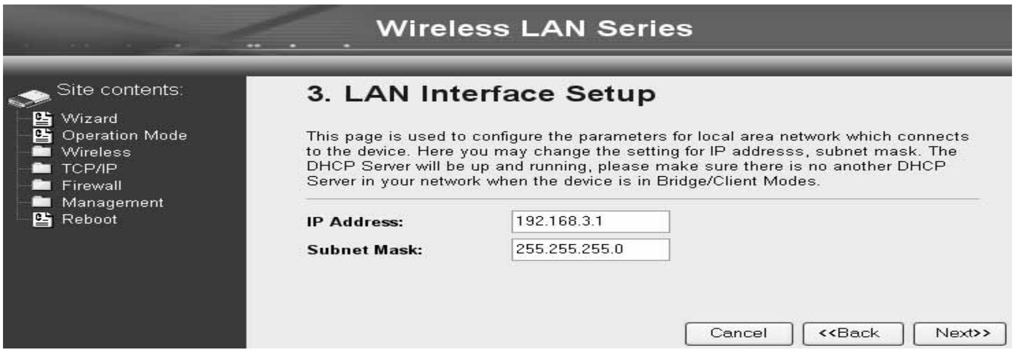
You can maintain the system time by synchronizing with a public time server over the Internet.

□ **Enable NTP client update**

**Time Zone Select :** (GMT-08:00)Pacific Time (US & Canada); Tijuana

**NTP server :** 192.5.41.41 - North America

5. Press “Next>>” button then set the IP address of LAN interface.



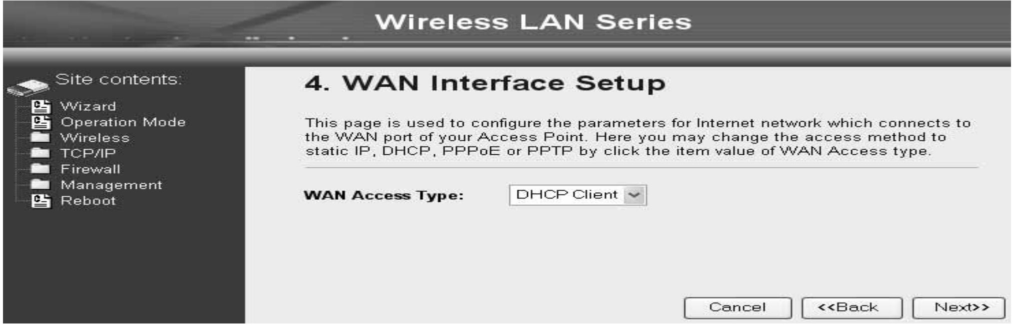
3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

6. Press "Next>>" button then select the "DHCP Client" for "WAN Access Type".

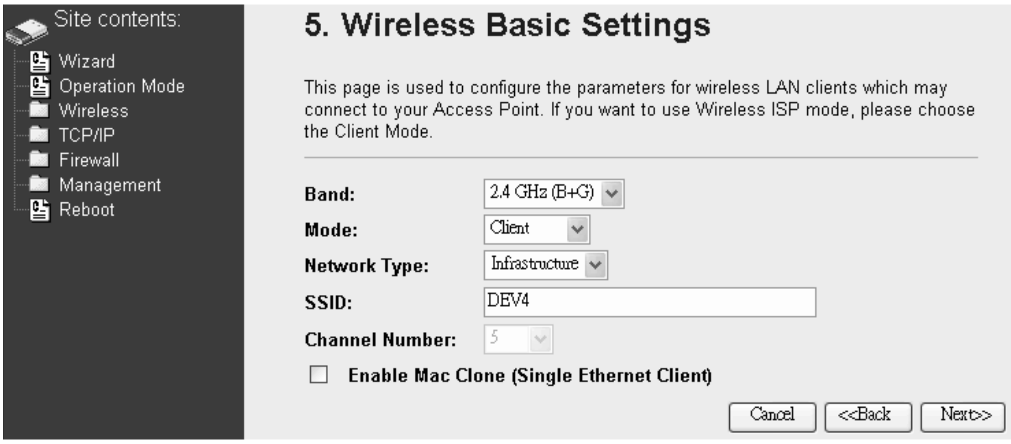


4. WAN Interface Setup

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 or PPTP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

7. Press "Next>>" button then select the "Client" for "mode" and change the SSID to "DEV4".



5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. If you want to use Wireless ISP mode, please choose the Client Mode.

Band: 2.4 GHz (B+G)

Mode: Client

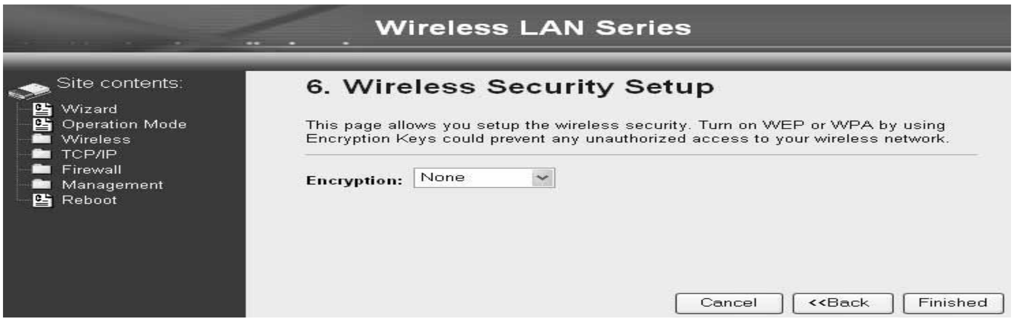
Network Type: Infrastructure

SSID: DEV4

Channel Number: 5

□ Enable Mac Clone (Single Ethernet Client)

8. Press "Next>>" button then select "None" for "Encryption" then press "Finished" button.

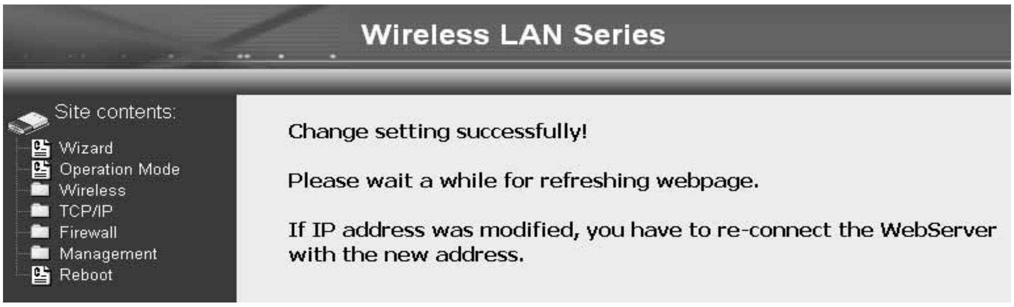


6. Wireless Security Setup

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.

Encryption: None

9. Wait for refreshing web page.

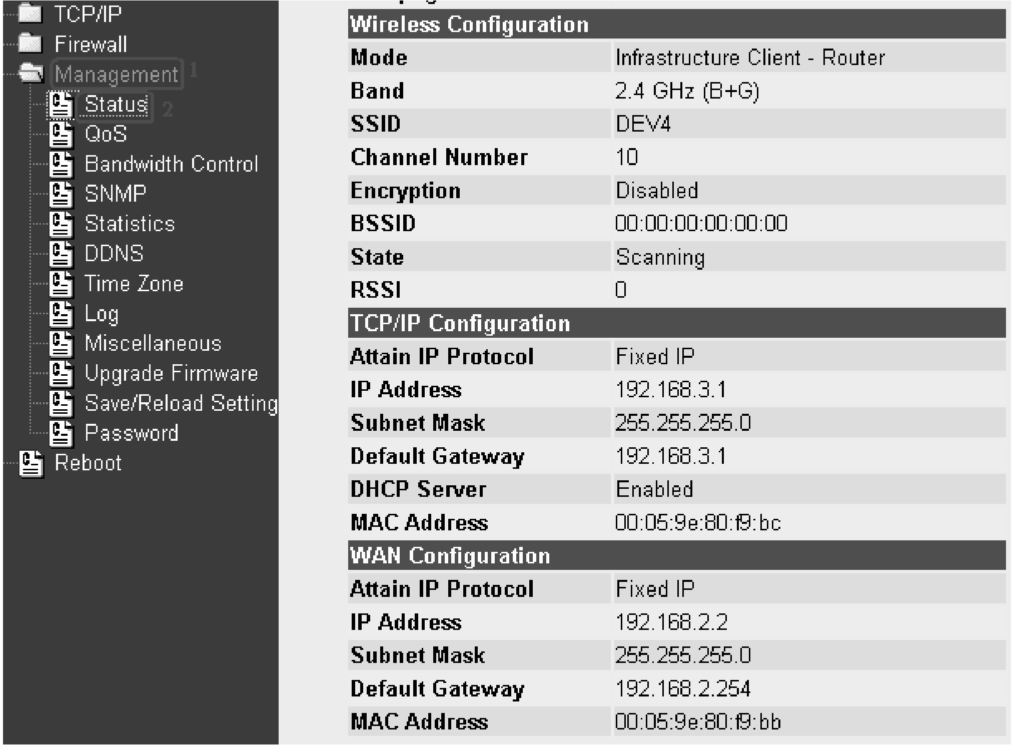


Change setting successfully!

Please wait a while for refreshing webpage.

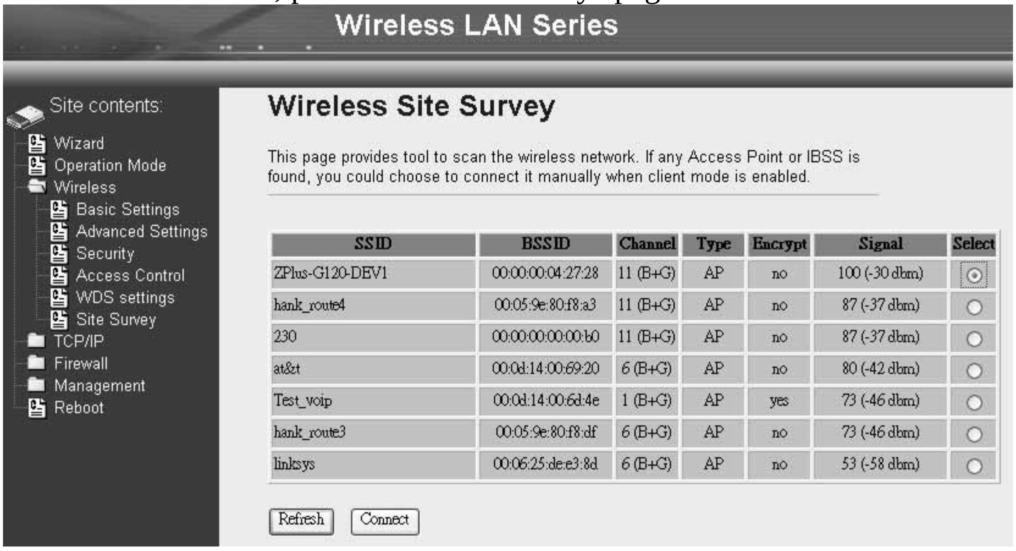
If IP address was modified, you have to re-connect the WebServer with the new address.

10. Change the IP address of your PC to 192.168.3.x then access the web server by the new IP address "192.168.3.1" and use "Status" page check the setting.



| Wireless Configuration | |
|---|---|
| Mode | Infrastructure Client - Router |
| Band | 2.4 GHz (B+G) |
| SSID | DEV4 |
| Channel Number | 10 |
| Encryption | Disabled |
| BSSID | 00:00:00:00:00:00 |
| State | Scanning |
| RSSI | 0 |
| **TCP/IP Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.3.1 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.3.1 |
| DHCP Server | Enabled |
| MAC Address | 00:05:9e:80:f9:bc |
| **WAN Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.2.2 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.254 |
| MAC Address | 00:05:9e:80:f9:bb |

11. If the "State" of "Wireless Configuration" is not "Connected" or you want to refresh the "RSSI ", please use "Site Survey" page to re-connect a AP.



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 |
|---|---|---|---|---|---|---|
| ZPlus-G120-DEV1 | 00:00:00:04:27:28 | 11 (B+G) | AP | no | 100 (-30 dbm) | ● |
| hank_route4 | 00:05:9e:80:f8:a3 | 11 (B+G) | AP | no | 87 (-37 dbm) | ○ |
| 230 | 00:00:00:00:00:b0 | 11 (B+G) | AP | no | 87 (-37 dbm) | ○ |
| at&t | 00:0d:14:00:69:20 | 6 (B+G) | AP | no | 80 (-42 dbm) | ○ |
| Test_voip | 00:0d:14:00:6d:4e | 1 (B+G) | AP | yes | 73 (-46 dbm) | ○ |
| hank_route3 | 00:05:9e:80:f8:df | 6 (B+G) | AP | no | 73 (-46 dbm) | ○ |
| linksys | 00:06:25:de:e3:8d | 6 (B+G) | AP | no | 53 (-58 dbm) | ○ |

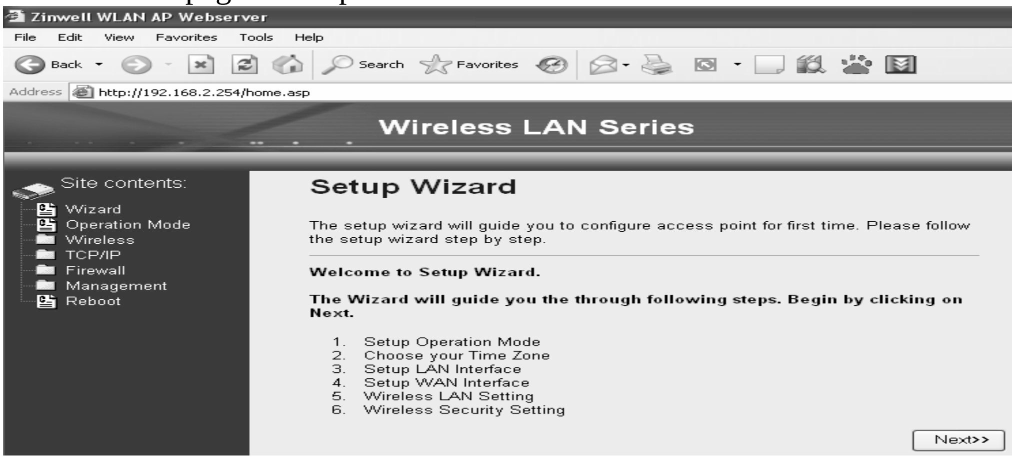
Configure DEV5:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

   **Caution**

   If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you unable to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

2. Use Wizard page to setup device.



## Setup Wizard

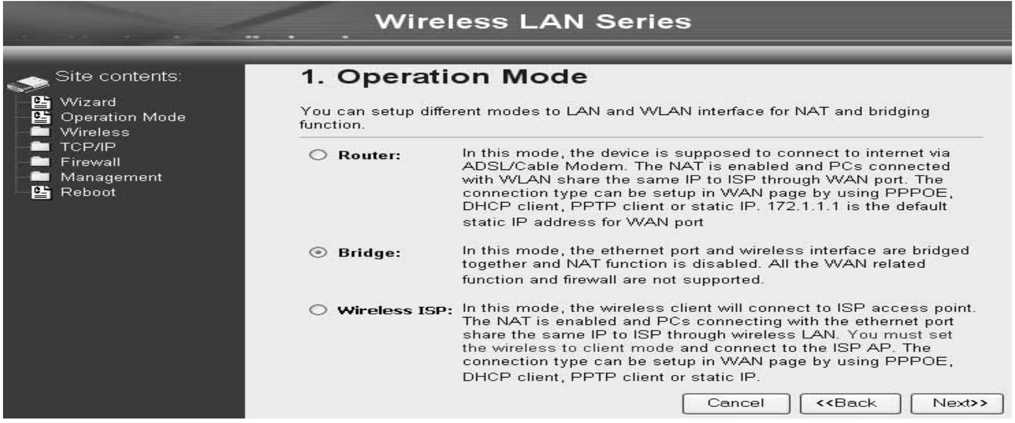
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

**Welcome to Setup Wizard.**

**The Wizard will guide you the through following steps. Begin by clicking on Next.**

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

3. Press "Next>>" button then set the "Operation Mode" to "Wireless ISP" mode.



## 1. Operation Mode

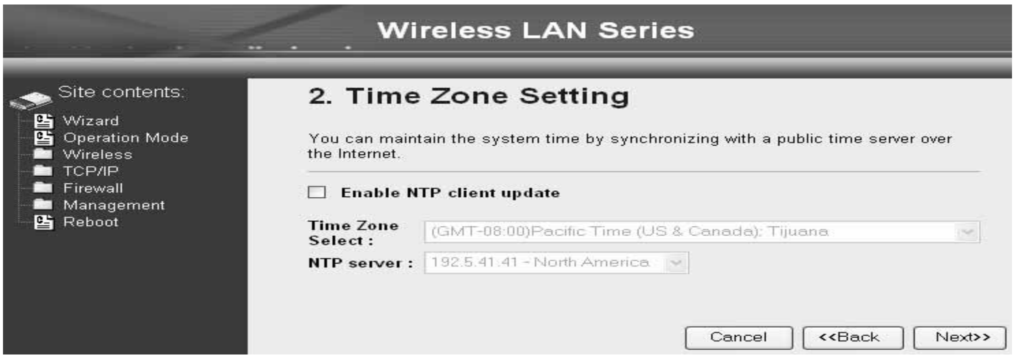
You can setup different modes to LAN and WLAN interface for NAT and bridging function.

○ **Router:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN 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 or static IP. 172.1.1.1 is the default static IP address for WAN port

◉ **Bridge:** In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

4. Press "Next>>" button then disable "Time Zone" function.



## 2. Time Zone Setting

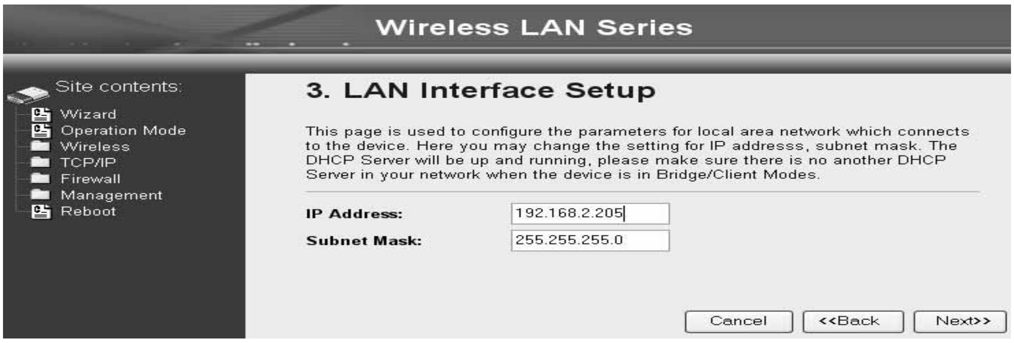
You can maintain the system time by synchronizing with a public time server over the Internet.

☐ **Enable NTP client update**

**Time Zone Select :** (GMT-08:00)Pacific Time (US & Canada); Tijuana

**NTP server :** 192.5.41.41 - North America

5. Press "Next>>" button then set the IP address of LAN interface.



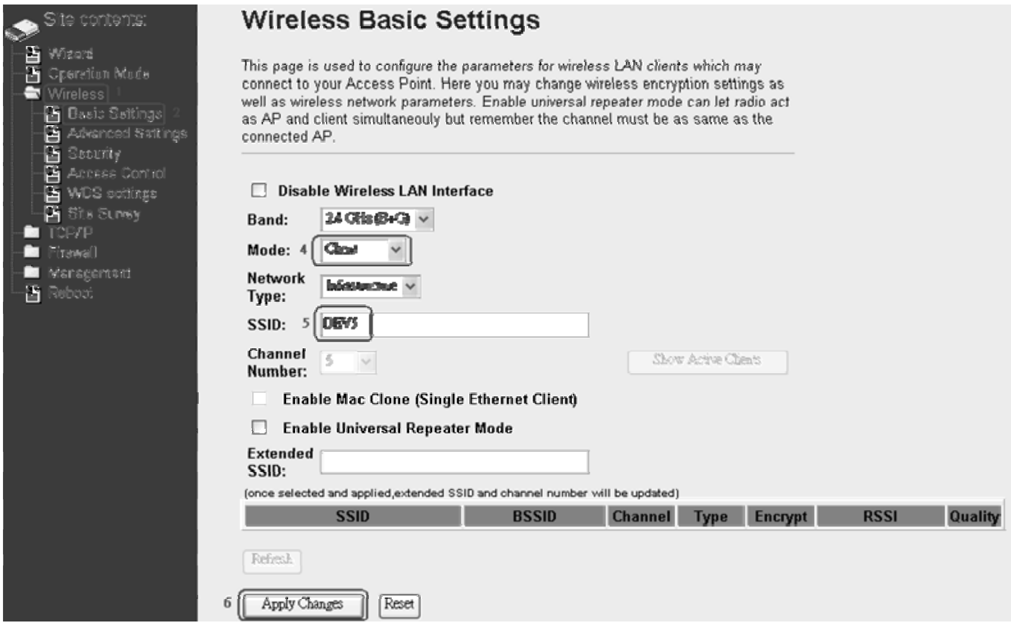
3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.

IP Address: 192.168.2.205

Subnet Mask: 255.255.255.0

6. Press “Next>>” button then select the “Client” for “mode” and change the SSID to “DEV5”.



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. Enable universal repeater mode can let radio act as AP and client simultaneouly but remember the channel must be as same as the connected AP.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: Client

Network Type: Infrastructure

SSID: DEV5

Channel Number: 5

☐ Enable Mac Clone (Single Ethernet Client)

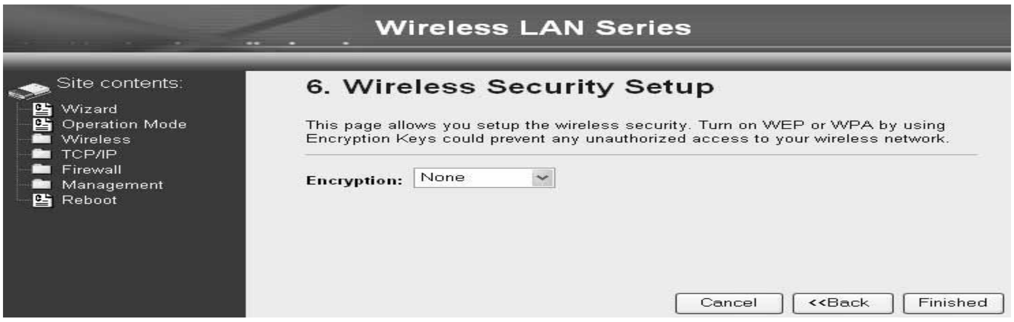
☐ Enable Universal Repeater Mode

Extended SSID:

(once selected and applied,extended SSID and channel number will be updated)

| SSID | BSSID | Channel | Type | Encrypt | RSSI | Quality |
|---|---|---|---|---|---|---|

7. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

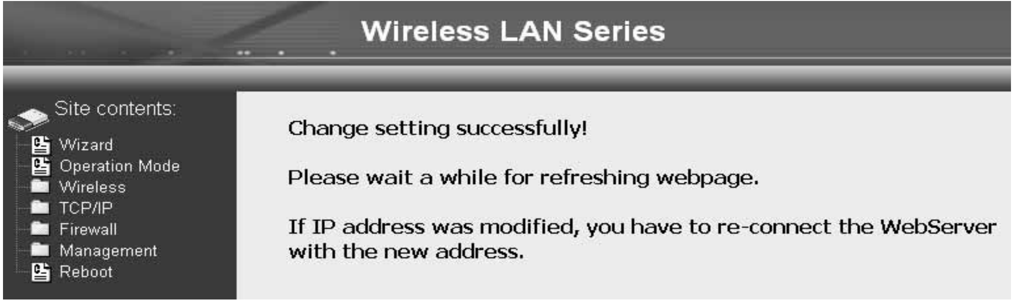


6. Wireless Security Setup

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.

Encryption: None

8. Wait for refreshing web page.

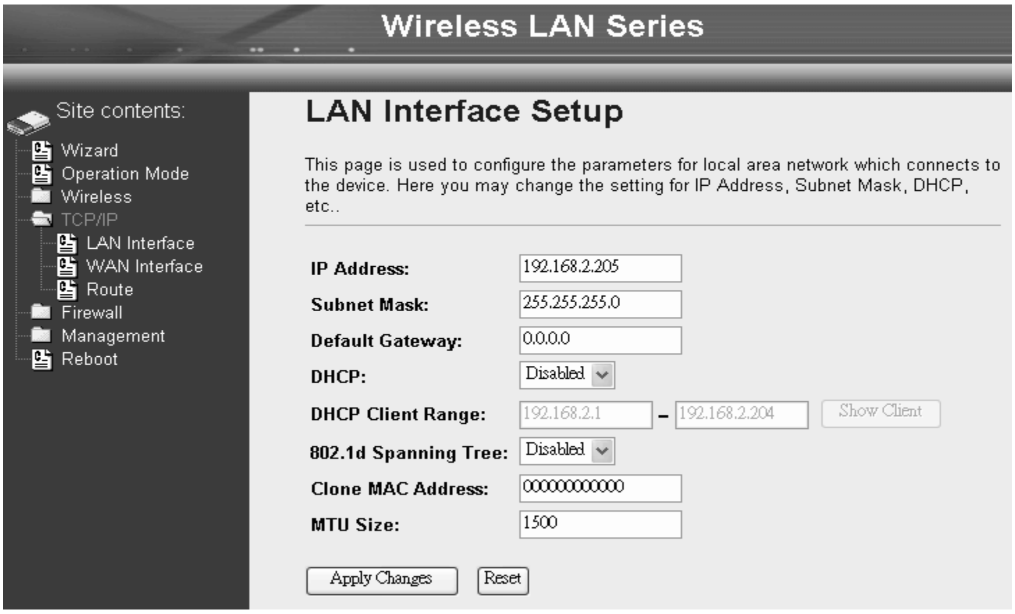


Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

9. Access the web server by the new IP address “192.168.2.205” and use “LAN Interface” page to disable DHCP Server.

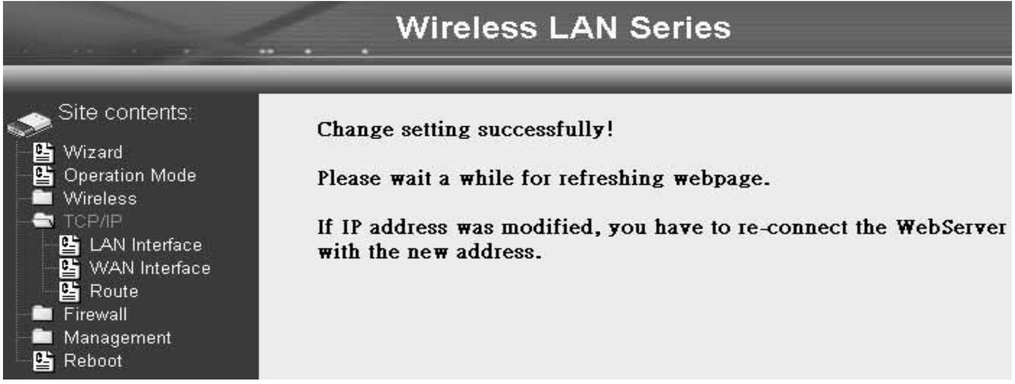


## LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

| | |
|---|---|
| IP Address: | 192.168.2.205 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 0.0.0.0 |
| DHCP: | Disabled |
| DHCP Client Range: | 192.168.2.1 – 192.168.2.204 |
| 802.1d Spanning Tree: | Disabled |
| Clone MAC Address: | 000000000000 |
| MTU Size: | 1500 |

10. Wait for refreshing webpage.

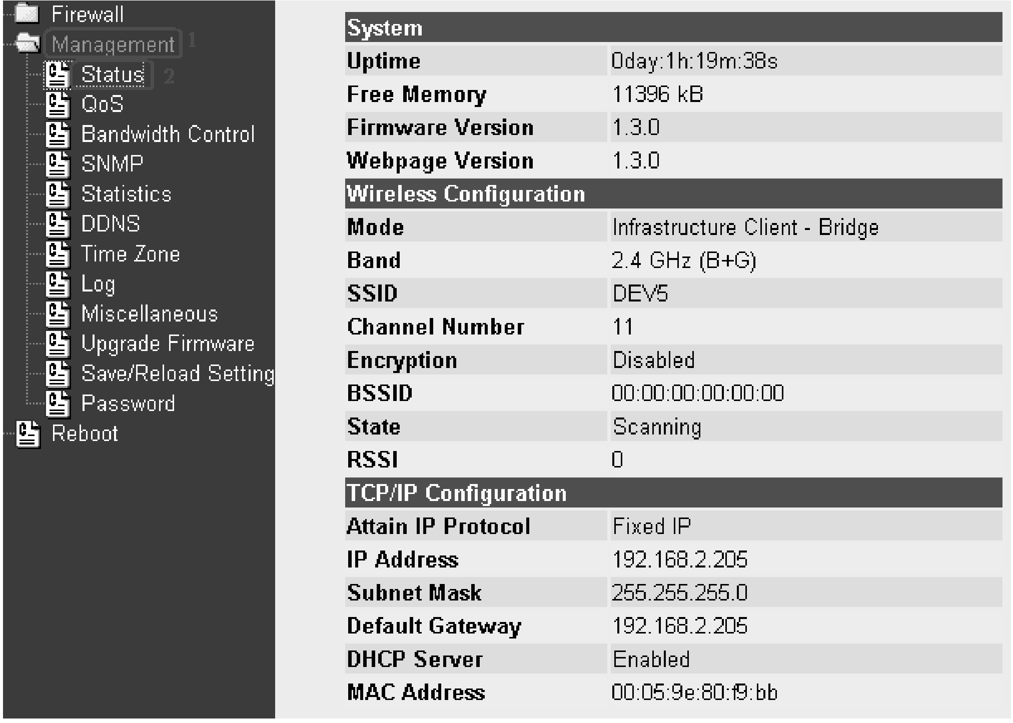


Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

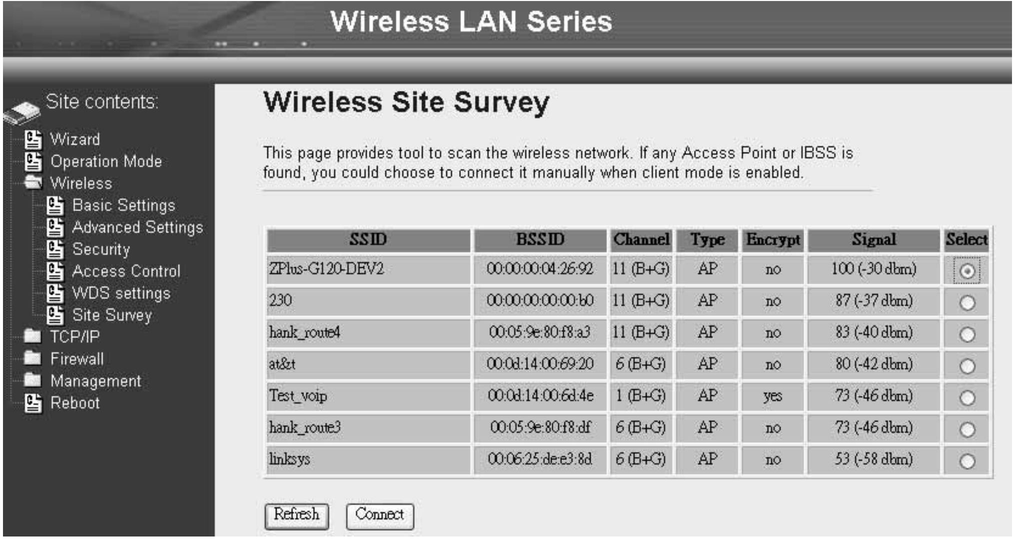
11. Use “State” page to check setting.



| System | |
|---|---|
| Uptime | 0day:1h:19m:38s |
| Free Memory | 11396 kB |
| Firmware Version | 1.3.0 |
| Webpage Version | 1.3.0 |
| **Wireless Configuration** | |
| Mode | Infrastructure Client - Bridge |
| Band | 2.4 GHz (B+G) |
| SSID | DEV5 |
| Channel Number | 11 |
| Encryption | Disabled |
| BSSID | 00:00:00:00:00:00 |
| State | Scanning |
| RSSI | 0 |
| **TCP/IP Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.2.205 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.205 |
| DHCP Server | Enabled |
| MAC Address | 00:05:9e:80:f9:bb |

12. If the “State” of “Wireless Configuration” is not “Connected” or you want to

refresh the “RSSI “, please use “Site Survey” page to re-connect a AP.

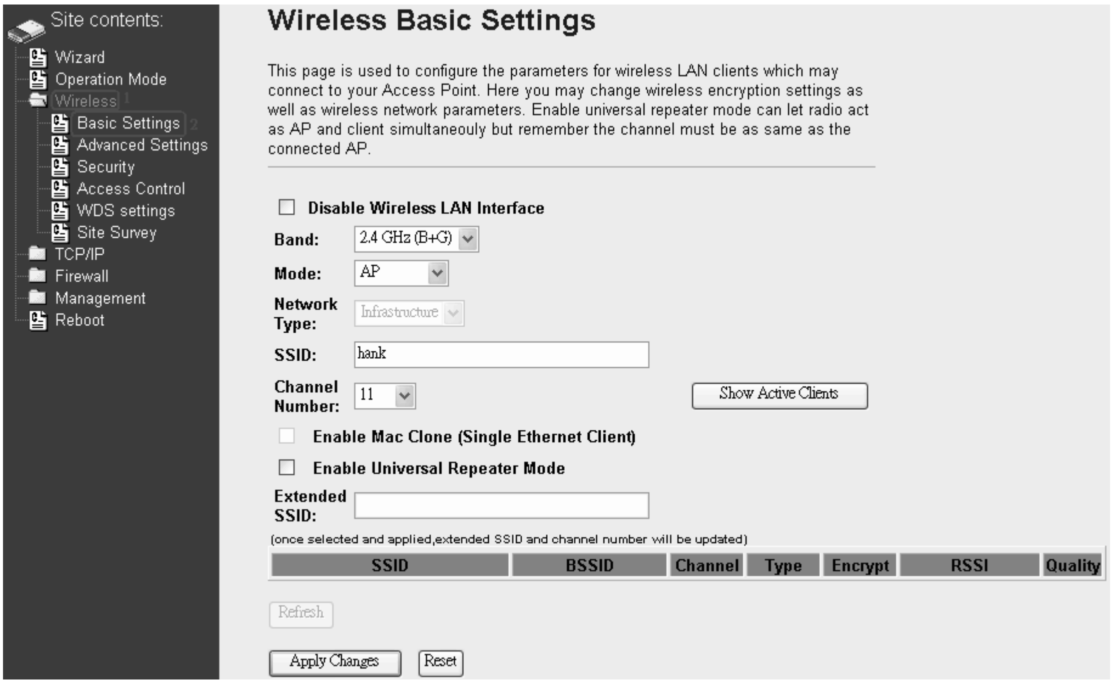


## Wireless Site Survey

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 |
|---|---|---|---|---|---|---|
| ZPlus-G120-DEV2 | 00:00:00:04:26:92 | 11 (B+G) | AP | no | 100 (-30 dbm) | ● |
| 230 | 00:00:00:00:00:b0 | 11 (B+G) | AP | no | 87 (-37 dbm) | ○ |
| hank_route4 | 00:05:9e:80:f8:a3 | 11 (B+G) | AP | no | 83 (-40 dbm) | ○ |
| at&t | 00:0d:14:00:69:20 | 6 (B+G) | AP | no | 80 (-42 dbm) | ○ |
| Test_voip | 00:0d:14:00:6d:4e | 1 (B+G) | AP | yes | 73 (-46 dbm) | ○ |
| hank_route3 | 00:05:9e:80:f8:df | 6 (B+G) | AP | no | 73 (-46 dbm) | ○ |
| linksys | 00:06:25:de:e3:8d | 6 (B+G) | AP | no | 53 (-58 dbm) | ○ |

# Basic Settings



**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. Enable universal repeater mode can let radio act as AP and client simultaneouly but remember the channel must be as same as the connected AP.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: hank

Channel Number: 11

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode

Extended SSID:

(once selected and applied,extended SSID and channel number will be updated)

| SSID | BSSID | Channel | Type | Encrypt | RSSI | Quality |
|---|---|---|---|---|---|---|

**Disable Wireless LAN Interface**

Disable the wireless interface of device

**Band:**

The device supports 2.4GHz(B), 2.4GHz(G) and 2.4GHz(B+G) mixed modes.

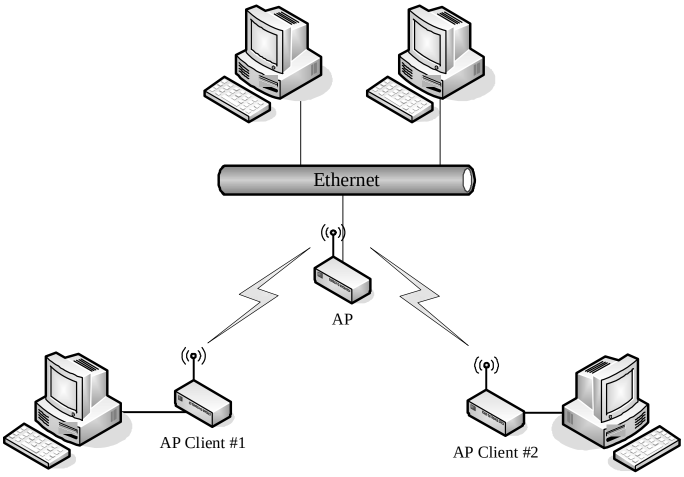
**Mode:**

The radio of device supports different modes as following:

1. AP
   The radio of device acts as an Access Point to serves all wireless clients to join a wireless local network.
2. Client
   Support Infrastructure and Ad-hoc network types to act as a wireless adapter.
3. WDS
   Wireless Distribution System, this mode serves as a wireless repeater, only devices with WDS function supported can connect to it, all the wireless clients can’t survey and connect the device when the mode is selected.
4. AP+WDS
   Support both AP and WDS functions, the wireless clients and devices with WDS function supported can survey and connect to it.

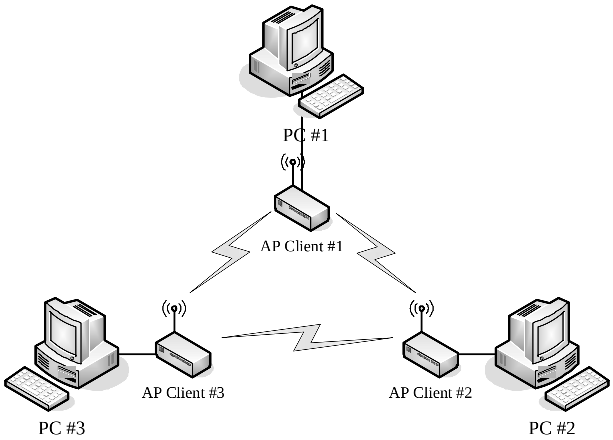
- ***Infrastructure***:

  This type requires the presence of 802.11b/g Access Point. All communication is done via the Access Point.



- ***Ad Hoc***:

  This type provides a peer-to-peer communication between wireless stations. All the communication is done from Client to Client without any Access Point involved. Ad Hoc networking must use the same SSID and channel for establishing the wireless connection.



In client mode, the device can't support the Router mode function including Firewall and WAN settings.

**SSID:**

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID.

**Channel Number**

The following table is the available frequencies (in MHz) for the 2.4-GHz radio:

| Channel No. | Frequency | Country Domain |
|---|---|---|

| | | |
|---|---|---|
| 1 | 2412 | Americas, EMEA, Japan, and China |
| 2 | 2417 | Americas, EMEA, Japan, and China |
| 3 | 2422 | Americas, EMEA, Japan, Israel, and China |
| 4 | 2427 | Americas, EMEA, Japan, Israel, and China |
| 5 | 2432 | Americas, EMEA, Japan, Israel, and China |
| 6 | 2437 | Americas, EMEA, Japan, Israel, and China |
| 7 | 2442 | Americas, EMEA, Japan, Israel, and China |
| 8 | 2447 | Americas, EMEA, Japan, Israel, and China |
| 9 | 2452 | Americas, EMEA, Japan, Israel, and China |
| 10 | 2457 | Americas, EMEA, Japan, and China |
| 11 | 2462 | Americas, EMEA, Japan, and China |
| 12 | 2467 | EMEA and Japan only |
| 13 | 2472 | EMEA and Japan only |
| 14 | 2484 | Japan only |

When set to “Auto”, the device will find the least-congested channel for use.

**Associated Client**

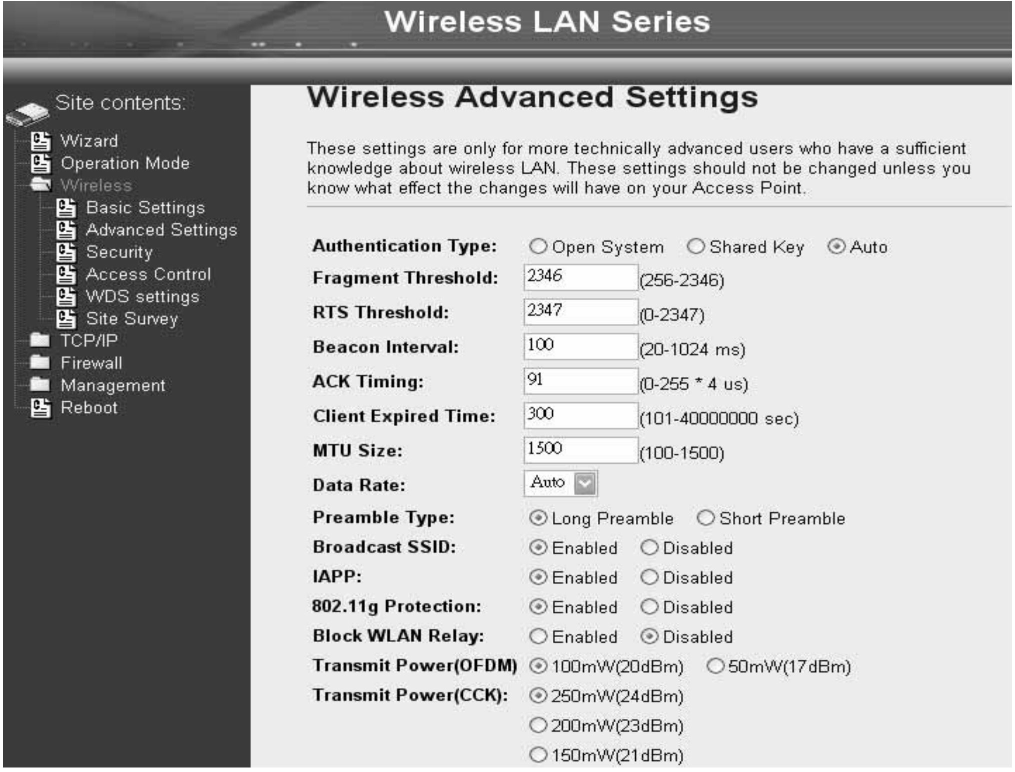
Show the information of active wireless client stations that connected to the device.

# Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your device. The default setting is optimized for the normal operation. For specific application, setting configuration will required highly attention to reach optimistic condition.

**Note**

Any unreasonable value change to default setting will reduce the throughput of the device.



## 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.

| | | |
|---|---|---|
| **Authentication Type:** | ○ Open System ○ Shared Key ● Auto | |
| **Fragment Threshold:** | 2346 | (256-2346) |
| **RTS Threshold:** | 2347 | (0-2347) |
| **Beacon Interval:** | 100 | (20-1024 ms) |
| **ACK Timing:** | 91 | (0-255 * 4 us) |
| **Client Expired Time:** | 300 | (101-40000000 sec) |
| **MTU Size:** | 1500 | (100-1500) |
| **Data Rate:** | Auto | |
| **Preamble Type:** | ● Long Preamble ○ Short Preamble | |
| **Broadcast SSID:** | ● Enabled ○ Disabled | |
| **IAPP:** | ● Enabled ○ Disabled | |
| **802.11g Protection:** | ● Enabled ○ Disabled | |
| **Block WLAN Relay:** | ○ Enabled ● Disabled | |
| **Transmit Power(OFDM)** | ● 100mW(20dBm) ○ 50mW(17dBm) | |
| **Transmit Power(CCK):** | ● 250mW(24dBm)<br>○ 200mW(23dBm)<br>○ 150mW(21dBm) | |

### Authentication Type

The device supports two Authentication Types “Open system” and “Shared Key”. When you select “Share Key”, you need to setup “WEP” key in “Security” page (See the next section). The default setting is “Auto”. The wireless client can associate with the device by using one of the two types.

### Fragment Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help you to improve the network performance.

### RTS Threshold

The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347 bytes.

**Data Rate**

The standard IEEE 802.11b/11g supports 1, 2, 5.5, 11 / 6, 9, 12, 18, 24, 36, 48 and 54 Mbps data rates. You can choose the rate that the device uses for data transmission. The default value is "auto". The device will use the highest possible selected transmission rate.

**Beacon Interval**

The beacon interval is the amount of time between access point beacons in mini-seconds. The default beacon interval is 100.

**Broadcast SSID**

Broadcasting the SSID will let your wireless clients find the device automatically. If you are building a public Wireless Network, disable this function can provide better security. Every wireless stations located within the coverage of the device must connect this device by manually configure the SSID in your client settings.

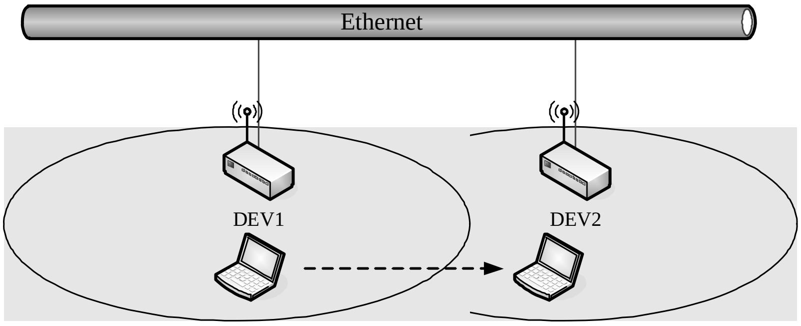
**Int. Roaming**

This function will let Wireless Stations roam among a network environment with multiple devices. Wireless Stations are able to switch from one device to another as they move between the coverage areas. Users can have more wireless working range. An example as the following figure

You should comply with the following instructions to roam among the wireless coverage areas.

<u>Note</u> **For implementing the roaming function, the setting MUST comply the following two items.**

- All the devices must be in the same subnet network and the SSID must be the same.
- If you use the 802.1x authentication, you need to have the user profile in these devices for the roaming station.



Wireless Station moves
between the coverage areas

**Block WLAN Relay (Isolate Client)**

The device supports isolation function. If you are building a public Wireless

Network, enable this function can provide better security. The device will block packets between wireless clients (relay). All the wireless clients connected to the device can’t see each other.

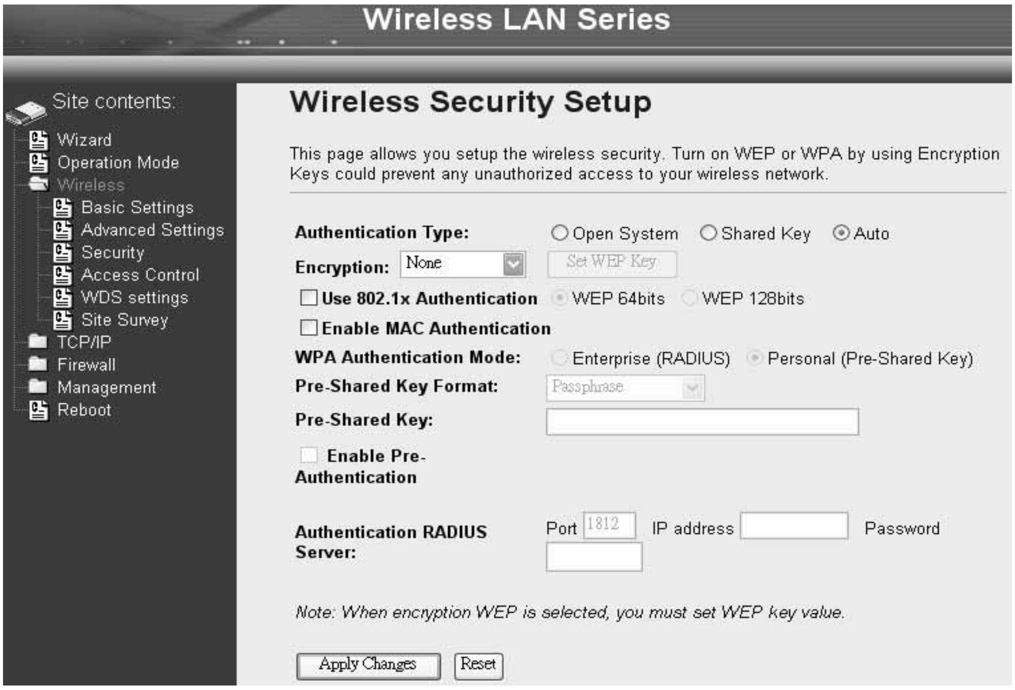
**Transmit Power**

The device supports four transmission output power levels 250, 200, 150 and 100mW for CCK (802.11b) mode and two transmission output power levels 100 and 50mW for OFDM (802.11g) mode. User can adjust the power level to change the coverage of the device. Every wireless stations located within the coverage of the device also needs to have the high power radio. Otherwise the wireless stations only can survey the device, but can’t establish connection with device.

# Configuring Wireless Security

This device provides complete wireless security function include WEP, 802.1x, WPA-TKIP, WPA2-AES and WPA2-Mixed in different mode (see the Security Support Table).

The default security setting of the encryption function is disabled. Choose your preferred security setting depending on what security function you need.



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.

Authentication Type: ○ Open System ○ Shared Key ● Auto

Encryption: None [Set WEP Key]

□ Use 802.1x Authentication ○ WEP 64bits ○ WEP 128bits

□ Enable MAC Authentication

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

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

□ Enable Pre-Authentication

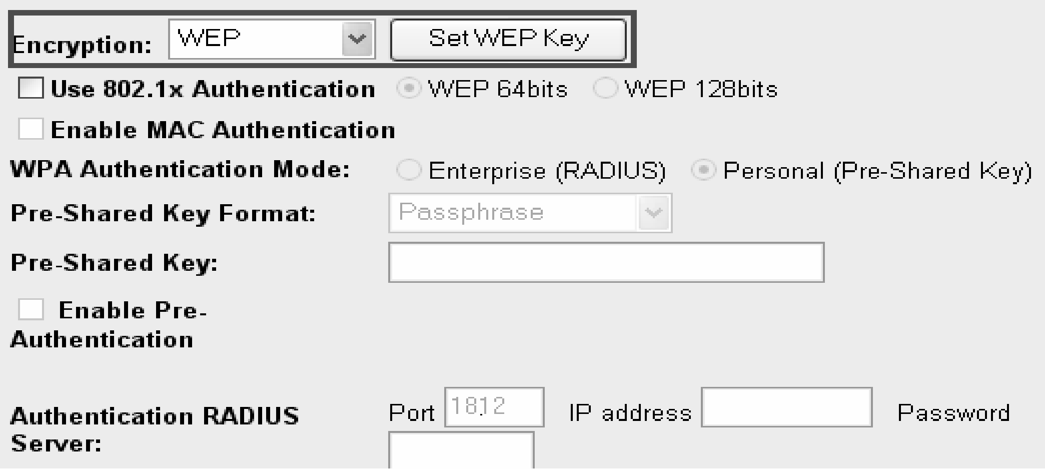
Authentication RADIUS Server: Port 1812 IP address Password

*Note: When encryption WEP is selected, you must set WEP key value.*

[Apply Changes] [Reset]

### WEP Encryption Setting

Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be as same as each client in your wireless network. For more secure data transmission, you can change encryption type to "WEP" and click the "Set WEP Key" button to open the "Wireless WEP Key setup" page.



Encryption: WEP [Set WEP Key]

□ Use 802.1x Authentication ○ WEP 64bits ○ WEP 128bits

□ Enable MAC Authentication

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

Pre-Shared Key Format: Passphrase

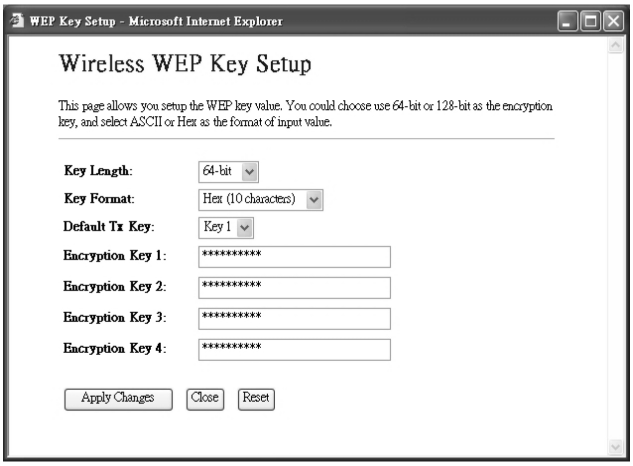
Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

When you decide to use the WEP encryption to secure your WLAN, please refer to the following setting of the WEP encryption:

- 64-bit WEP Encryption□64-bit WEP keys are as same as the encryption method of 40-bit WEP. You can input 10 hexadecimal digits (0~9, a~f or A~F) or 5 ACSII chars.
- 128-bit WEP Encryption□128-bit WEP keys are as same as the encryption method of 104-bit WEP. You can input 26 hexadecimal digits (0~9, a~f or A~F) or 10 ACSII chars.
- The Default Tx Key field decides which of the four keys you want to use in your WLAN environment.



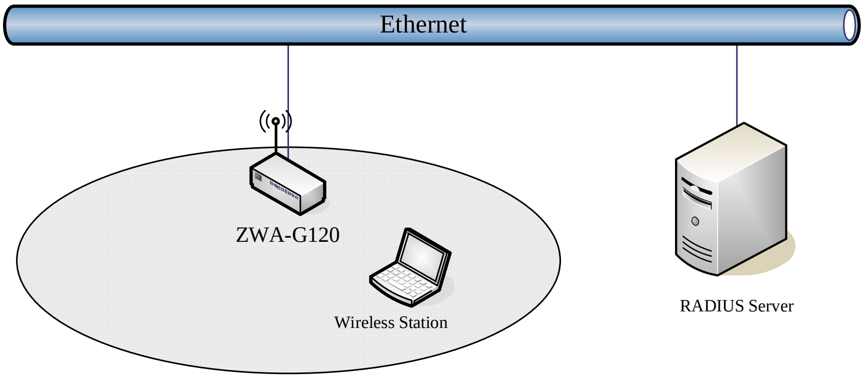
Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

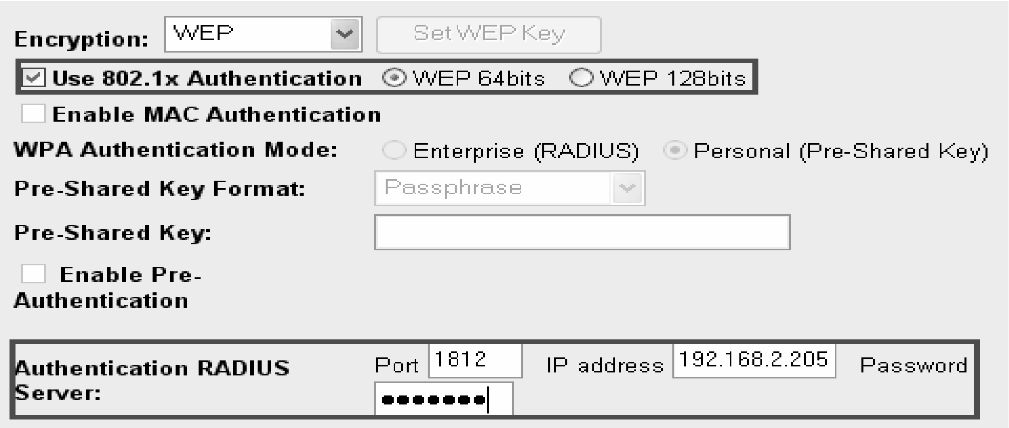
| | |
|---|---|
| Key Length: | 64-bit |
| Key Format: | Hex (10 characters) |
| Default Tx Key: | Key 1 |
| Encryption Key 1: | ********** |
| Encryption Key 2: | ********** |
| Encryption Key 3: | ********** |
| Encryption Key 4: | ********** |

### WEP Encryption with 802.1x Setting

The device supports external RADIUS Server that can secure networks against unauthorized access. If you use the WEP encryption, you can also use the RADIUS server to check the admission of the users. By this way every user must use a valid account before accessing the Wireless LAN and requires a RADIUS or other authentication server on the network. An example is shown as following.



You should choose WEP 64 or 128 bit encryption to fit with your network environment first. Then add user accounts and the target device to the RADIUS server. In the device , you need to specify the IP address□Password (Shared Secret) and Port number of the target RADIUS server.



Encryption: WEP [Set WEP Key]

☑ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

□ Enable MAC Authentication

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

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address 192.168.2.205 Password ●●●●●●●●

**WPA Encryption Setting**

WPA feature provides a high level of assurance for end-users and administrators that their data will remain private and access to their network restricted to authorized users. You can choose the WPA encryption and select the Authentication Mode.

**WPA Authentication Mode**

This device supports two WPA modes. For personal user, you can use the Pre-shared Key to enhance your security setting. This mode requires only an access point and client station that supports WPA-PSK. For Enterprise, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.

- **Enterprise (RADIUS):**

When WPA Authentication mode is Enterprise (RADIUS), you have to add user accounts and the target device to the RADIUS Server. In the device , you need to specify the IP address□Password (Shared Secret) and Port number of the target RADIUS server.

- **Pre-Share Key:**

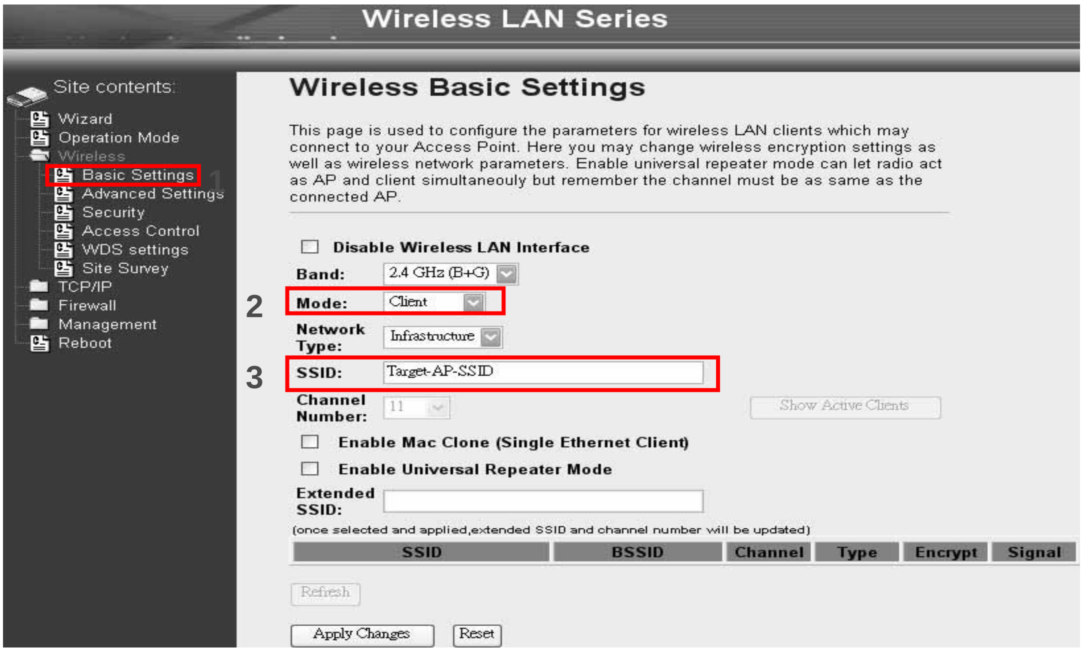
This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8~63 ACSII chars. When Key format is Hex, the key value should have 64 hexadecimal digits (0~9, a~f or A~F).

# Configuring as WLAN Client Adapter

This device can be configured as a wireless Ethernet adapter. In this mode, the device can connect to the other wireless stations (Ad-Hoc network type) or Access Point (Infrastructure network type) and you don't need to install any driver.

# Quick start to configure

***Step 1.*** In "Basic Settings" page, change the Mode to "Client" mode. And key in the SSID of the AP you want to connect then press "Apply Changes" button to apply the change.



## 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. Enable universal repeater mode can let radio act as AP and client simultaneously but remember the channel must be as same as the connected AP.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: Client

Network Type: Infrastructure

SSID: Target-AP-SSID

Channel Number: 11

□ Enable Mac Clone (Single Ethernet Client)

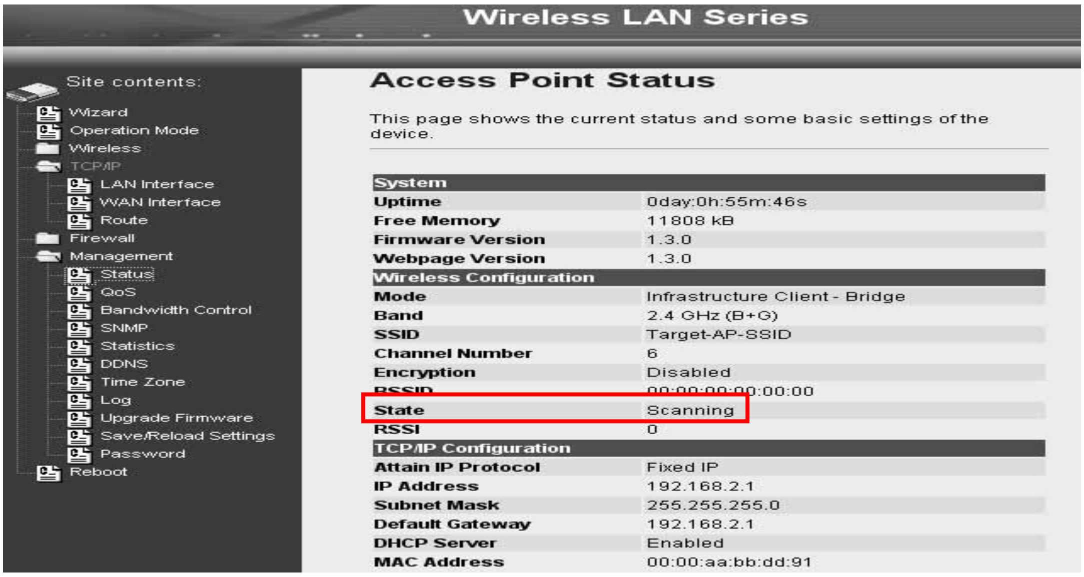
□ Enable Universal Repeater Mode

Extended SSID:

(once selected and applied,extended SSID and channel number will be updated)

| SSID | BSSID | Channel | Type | Encrypt | Signal |
|---|---|---|---|---|---|

***Step 2.*** Check the status of connection in "Status" web page



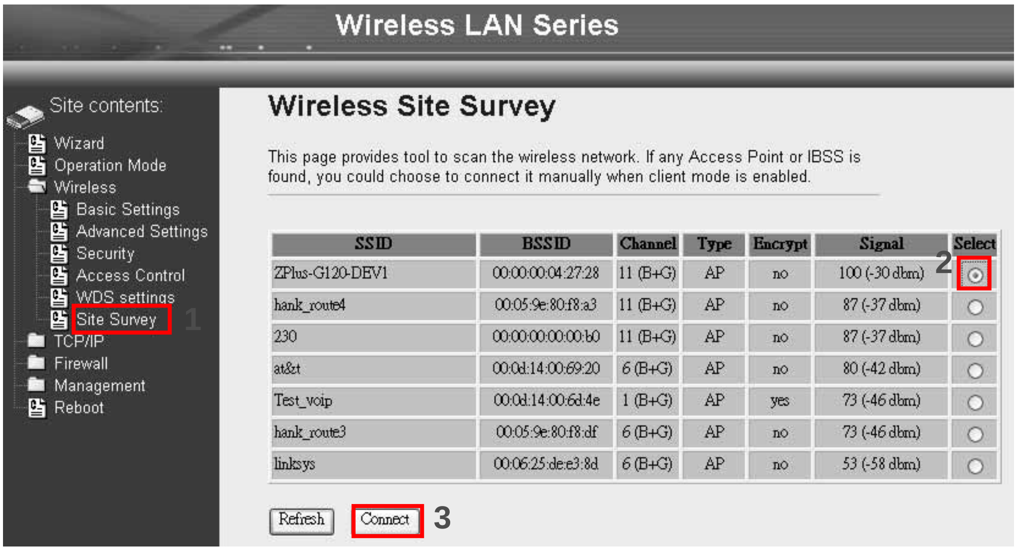
## Access Point Status

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

| System | |
|---|---|
| Uptime | 0day:0h:55m:46s |
| Free Memory | 11808 kB |
| Firmware Version | 1.3.0 |
| Webpage Version | 1.3.0 |
| **Wireless Configuration** | |
| Mode | Infrastructure Client - Bridge |
| Band | 2.4 GHz (B+G) |
| SSID | Target-AP-SSID |
| Channel Number | 6 |
| Encryption | Disabled |
| BSSID | 00:00:00:00:00:00 |
| State | Scanning |
| RSSI | 0 |
| **TCP/IP Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.2.1 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.2.1 |
| DHCP Server | Enabled |
| MAC Address | 00:00:aa:bb:dd:91 |

The alternative way to configure as following:

***Step 1.*** In "Wireless Site Survey" page, select one of the SSIDs you want to connect and then press "Connect" button to establish the link.

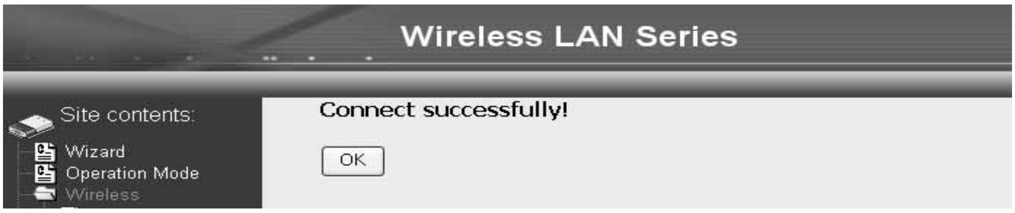


Wireless Site Survey

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.

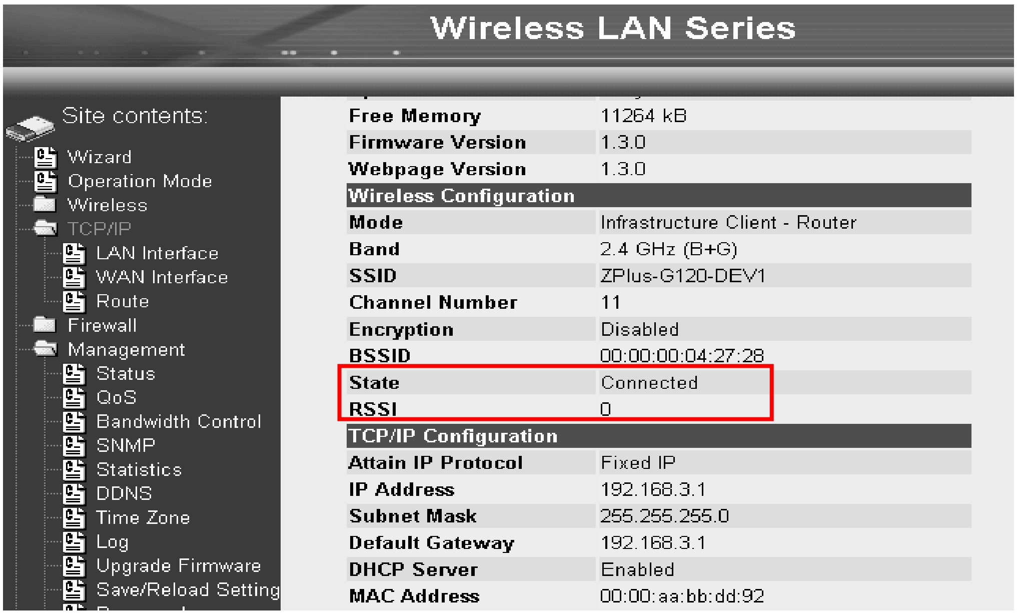
| SSID | BSSID | Channel | Type | Encrypt | Signal | Select |
|---|---|---|---|---|---|---|
| ZPlus-G120-DEV1 | 00:00:00:04:27:28 | 11 (B+G) | AP | no | 100 (-30 dbm) | ● |
| hank_route4 | 00:05:9e:80:f8:a3 | 11 (B+G) | AP | no | 87 (-37 dbm) | ○ |
| 230 | 00:00:00:00:00:b0 | 11 (B+G) | AP | no | 87 (-37 dbm) | ○ |
| at&t | 00:0d:14:00:69:20 | 6 (B+G) | AP | no | 80 (-42 dbm) | ○ |
| Test_voip | 00:0d:14:00:6d:4e | 1 (B+G) | AP | yes | 73 (-46 dbm) | ○ |
| hank_route3 | 00:05:9e:80:f8:df | 6 (B+G) | AP | no | 73 (-46 dbm) | ○ |
| linksys | 00:06:25:de:e3:8d | 6 (B+G) | AP | no | 53 (-58 dbm) | ○ |

***Step 2.*** If the linking is established successfully. It will show the message "Connect successfully". Then press "OK".



Connect successfully!

***Step 3.*** Then you can check the linking information in "Status" page.



| | |
|---|---|
| Free Memory | 11264 kB |
| Firmware Version | 1.3.0 |
| Webpage Version | 1.3.0 |
| **Wireless Configuration** | |
| Mode | Infrastructure Client - Router |
| Band | 2.4 GHz (B+G) |
| SSID | ZPlus-G120-DEV1 |
| Channel Number | 11 |
| Encryption | Disabled |
| BSSID | 00:00:00:04:27:28 |
| State | Connected |
| RSSI | 0 |
| **TCP/IP Configuration** | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.3.1 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.3.1 |
| DHCP Server | Enabled |
| MAC Address | 00:00:aa:bb:dd:92 |

**Note**

If the available network requires authentication and data encryption, you need to setup the authentication and encryption before step1 and all the settings must be as same as the Access Point or Station. About the detail authentication and data encryption settings, please refer the security section.

### Authentication Type

In client mode, the device also supports two Authentication Types “Open system” and “Shared Key”. Although the default setting is “Auto”, not every Access Points can support “Auto” mode. If the authentication type on the Access Point is knew by user, we suggest to set the authentication type as same as the Access Point.

### Data Encryption

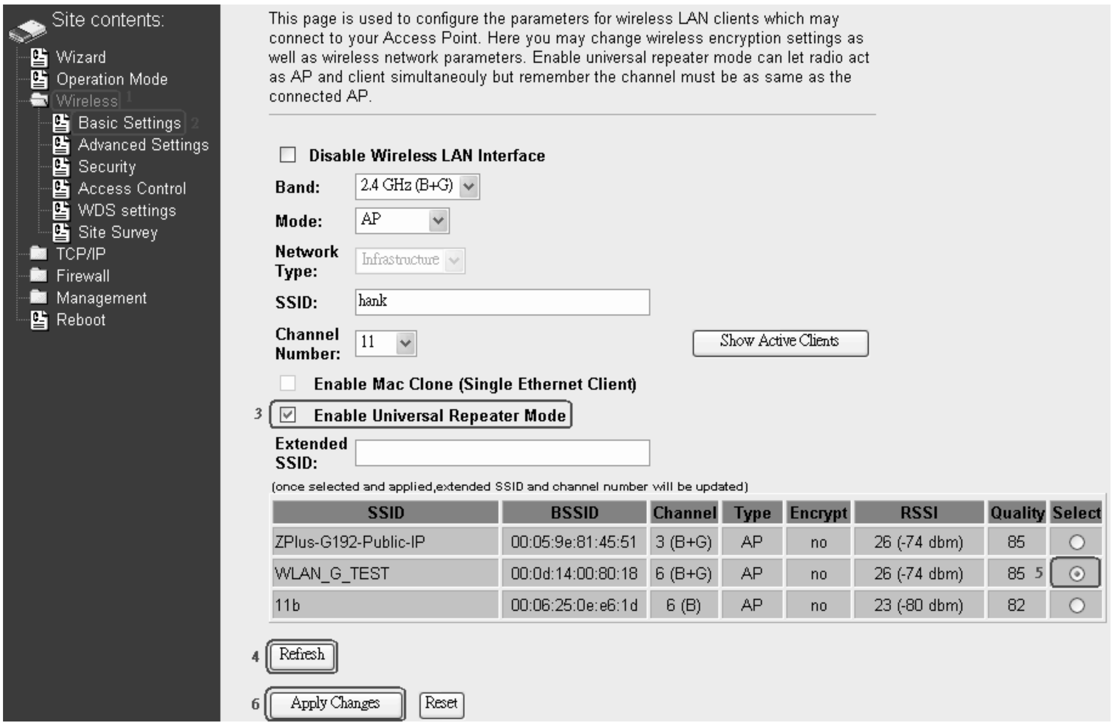
In client mode, the device supports WEP and WPA Personal/Enterprise except WPA2 mixed mode data encryption. About the detail data encryption settings, please refer the security section.

## Configuring Universal Repeater

This device can be configured as a Repeater. In this mode, the device can extend available wireless range of other AP let user can link the network that they want, Also the device working as AP and Repeater same time.

Following two ways describe how to make Universal Repeater effective.

1. Enable Universal Repeater Mode and then select a SSID in the Table that you want. Final click Apply Changes button to take effective. **(Click Refresh button to make table renew)**



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. Enable universal repeater mode can let radio act as AP and client simultaneously but remember the channel must be as same as the connected AP.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: hank

Channel Number: 11

☐ Enable Mac Clone (Single Ethernet Client)

☑ Enable Universal Repeater Mode

Extended SSID:

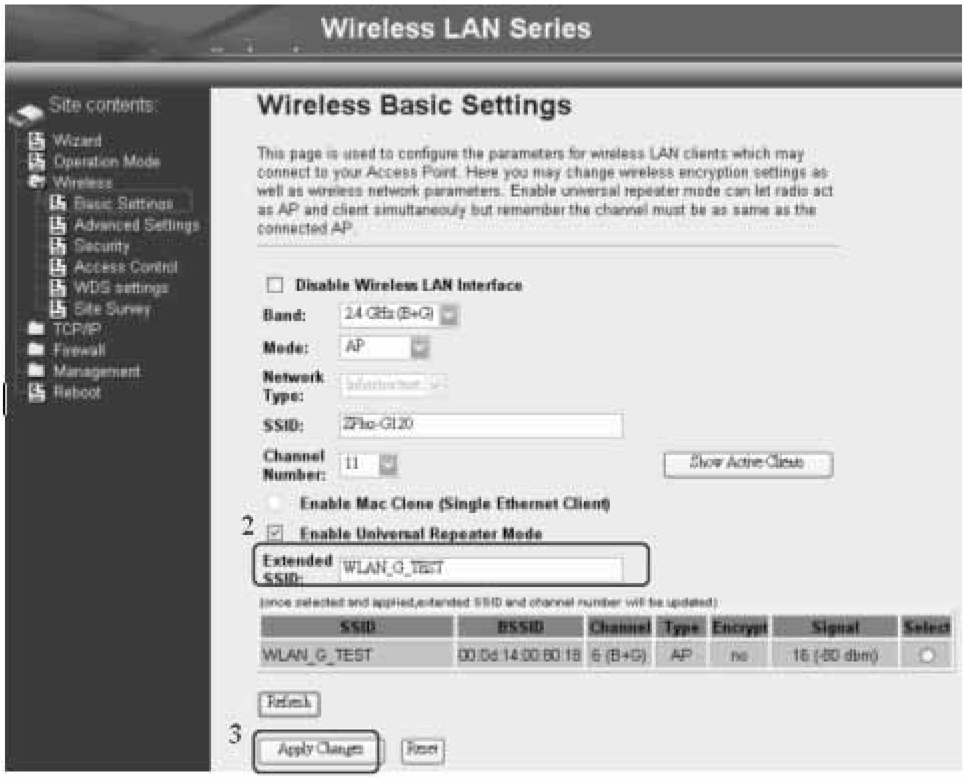
(once selected and applied,extended SSID and channel number will be updated)

| SSID | BSSID | Channel | Type | Encrypt | RSSI | Quality | Select |
|---|---|---|---|---|---|---|---|
| ZPlus-G192-Public-IP | 00:05:9e:81:45:51 | 3 (B+G) | AP | no | 26 (-74 dbm) | 85 | ○ |
| WLAN_G_TEST | 00:0d:14:00:80:18 | 6 (B+G) | AP | no | 26 (-74 dbm) | 85 | ● |
| 11b | 00:06:25:0e:e6:1d | 6 (B) | AP | no | 23 (-80 dbm) | 82 | ○ |

Note: Under **AP  WDS and AP+WDS mode**, The Universal Repeater can take effective.

2. Enter specific SSID in the Extended SSID field and then click Apply

Changes button to take effective.



## 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. Enable universal repeater mode can let radio act as AP and client simultaneouly but remember the channel must be as same as the connected AP.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: ZPlus-G120

Channel Number: 11

○ Enable Mac Clone (Single Ethernet Client)

☑ Enable Universal Repeater Mode

Extended SSID: WLAN_G_TEST

(once selected and applied,extended SSID and channel number will be updated)

| SSID | BSSID | Channel | Type | Encrypt | Signal | Select |
|---|---|---|---|---|---|---|
| WLAN_G_TEST | 00:0d:14:00:80:18 | 6 (B+G) | AP | no | 16 (-80 dbm) | ○ |

# Ch 3. Configuring WDS

Wireless Distribution System (WDS) uses wireless media to communicate with the other devices, like the Ethernet does. This function allows one or more remote LANs connect with the local LAN. To do this, you must set these devices in the same channel and set MAC address of other devices you want to communicate with in the WDS AP List and then enable the WDS.

When you decide to use the WDS to extend your WLAN, please refer the following instructions for configuration.

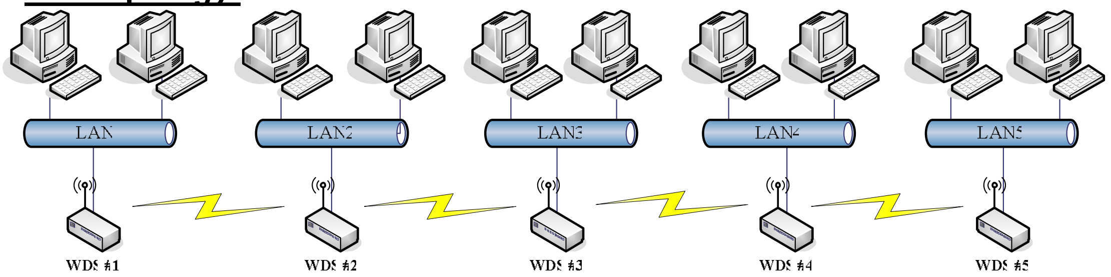
- The bridging devices by WDS must use the same radio channel.
- When the WDS function is enabled, all wireless stations can't connect the device.
- If your network topology has a loop, you need to enable the 802.1d Spanning Tree function.
- You don't need to add all MAC address of devices existed in your network to WDS AP List. WDS AP List only needs to specify the MAC address of devices you need to directly connect to.
- The bandwidth of device is limited, to add more bridging devices will split the more bandwidth to every bridging device.

## WDS network topology

In this section, we will demonstrate the WDS network topologies and WDS AP List configuration. You can setup the four kinds of network topologies: bus, star, ring and mesh.

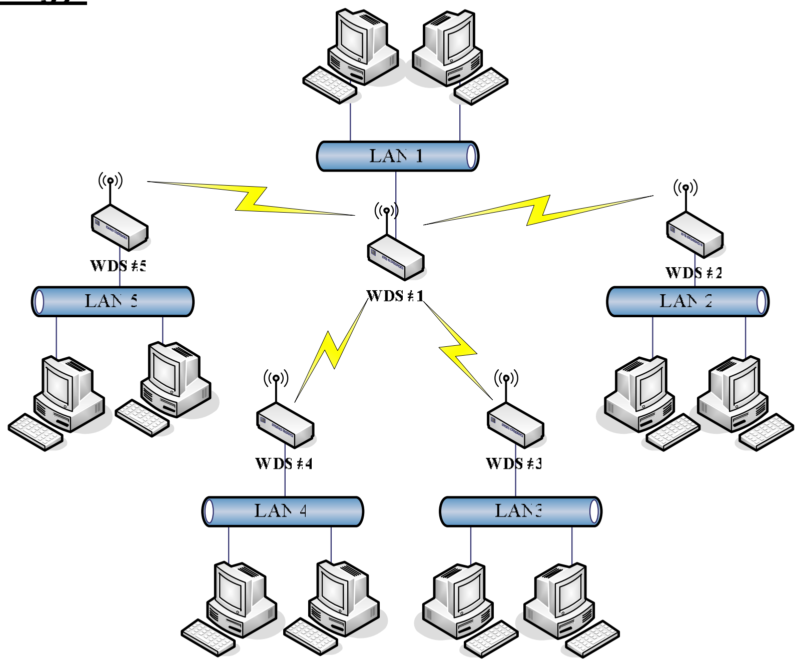
In this case, there are five devices with WDS enabled: WDS1, WDS2, WDS3, WDS4 and WDS5.

**Bus topology:**



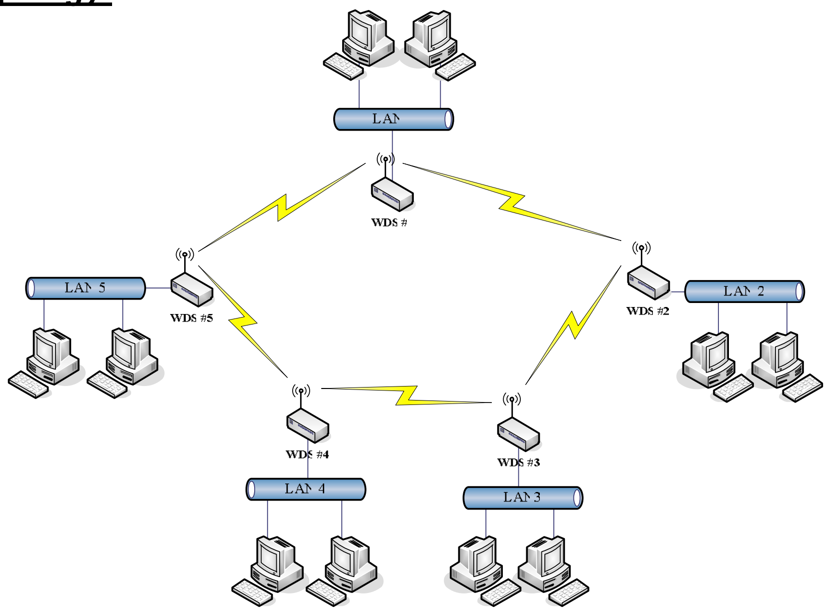
| Device | Entries of WDS AP List | Spanning Tree Protocol Required |
|---|---|---|
| WDS1 | The MAC Address of WDS2 | No |
| WDS2 | The MAC Addresses of WDS1 and WDS3 | No |
| WDS3 | The MAC Addresses of WDS2 and WDS4 | No |
| WDS4 | The MAC Addresses of WDS3 and WDS5 | No |
| WDS5 | The MAC Address of WDS4 | No |

## Star topology:



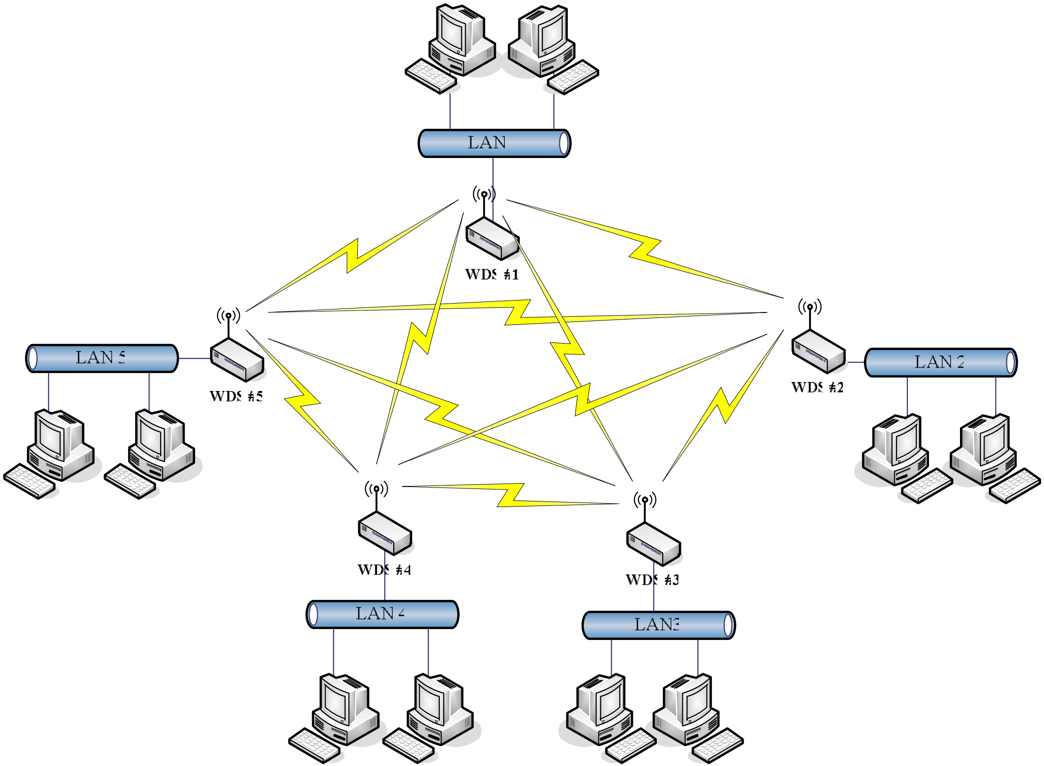
| Device | Entries of WDS AP List | Spanning Tree Protocol Required |
|---|---|---|
| WDS1 | The MAC Addresses of WDS2, WDS3, WDS4 and WDS5 | No |
| WDS2 | The MAC Address of WDS1 | No |
| WDS3 | The MAC Address of WDS1 | No |
| WDS4 | The MAC Address of WDS1 | No |
| WDS5 | The MAC Address of WDS1 | No |

## Ring topology:



| Device | Entries of WDS AP List | Spanning Tree Protocol Required |
|---|---|---|
| WDS1 | The MAC Addresses of WDS2 and WDS5 | Yes |
| WDS2 | The MAC Addresses of WDS1 and WDS3 | Yes |
| WDS3 | The MAC Addresses of WDS2 and WDS4 | Yes |
| WDS4 | The MAC Addresses of WDS3 and WDS5 | Yes |
| WDS5 | The MAC Addresses of WDS4 and WDS1 | Yes |

**Mesh topology**



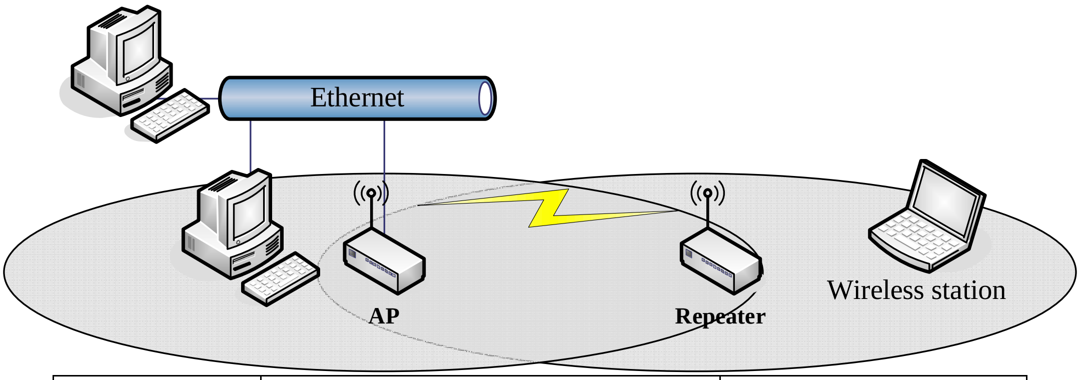
| Device | Entries of WDS AP List | Spanning Tree Protocol Required |
|---|---|---|
| WDS1 | The MAC Addresses of WDS2, WDS3, WDS4 and WDS5 | Yes |
| WDS2 | The MAC Addresses of WDS1, WDS3, WDS4 and WDS5 | Yes |
| WDS3 | The MAC Addresses of WDS1, WDS2, WDS4 and WDS5 | Yes |
| WDS4 | The MAC Addresses of WDS1, WDS2, WDS3 and WDS5 | Yes |
| WDS5 | The MAC Addresses of WDS1, WDS2, WDS3 and WDS4 | Yes |

# WDS Application

### Wireless Repeater

Wireless Repeater can be used to increase the coverage area of another device (Parent AP). Between the Parent AP and the Wireless Repeater, wireless stations can move among the coverage areas of both devices. When you decide to use the WDS as a Repeater, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel and SSID.
- Choose “WDS+AP” mode.
- Using the bus or star network topology.



| Description | Entries of WDS AP List | Spanning Tree Protocol Required |
|---|---|---|
| Access Point | The MAC Address of Repeater | Yes |
| Repeater | The MAC Address of Access Point | Yes |

### Wireless Bridge

Wireless Bridge can establish a wireless connection between two or more Wired LANs. When you decide to use the WDS as a Wireless Bridge, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel, but you may use different SSID.
- Choose “WDS” mode for only wireless backbone extension purpose.
- You can use any network topology, please refer the WDS topology section.

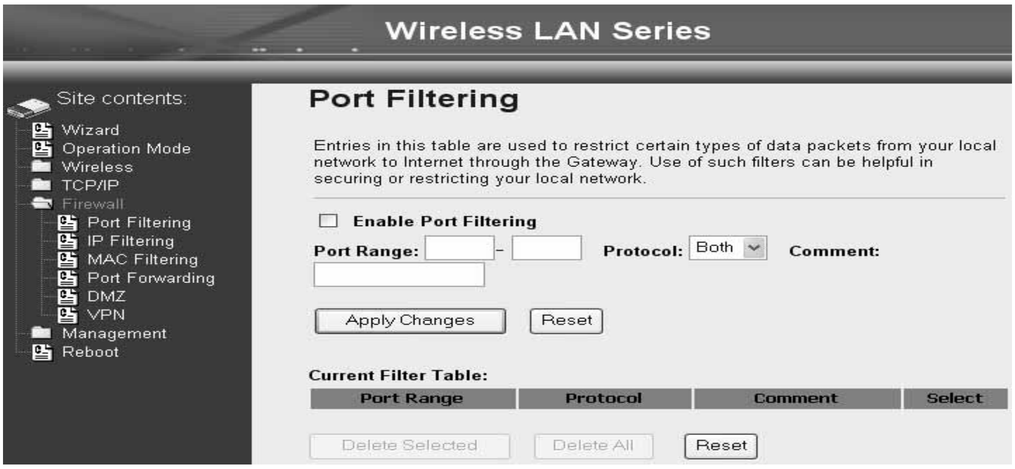
# Ch 4. Advanced Configurations

## Configuring LAN to WAN Firewall

Filtering function is used to block packets from LAN to WAN. The device supports three kinds of filter Port Filtering, IP Filtering and MAC Filtering. All the entries in current filter table are used to restrict certain types of packets from your local network to through the device. Use of such filters can be helpful in securing or restricting your local network.

### Port Filtering

When you enable the Port Filtering function, you can specify a single port or port ranges in current filter table. Once the source port of outgoing packets match the port definition or within the port ranges in the table, the firewall will block those packets from LAN to WAN.



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

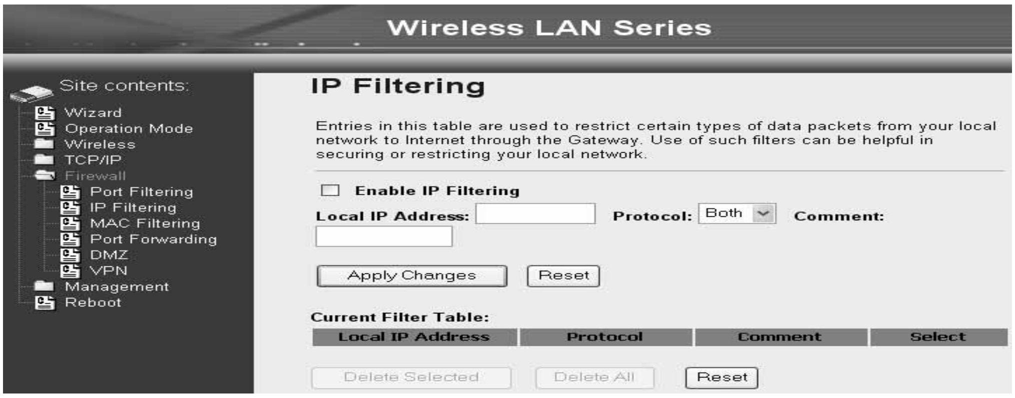
Port Range: - Protocol: Both Comment:

Current Filter Table:

| Port Range | Protocol | Comment | Select |
|---|---|---|---|

### IP Filtering

When you enable the IP Filtering function, you can specify local IP Addresses in current filter table. Once the source IP address of outgoing packets match the IP Addresses in the table, the firewall will block this packet from LAN to WAN.



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

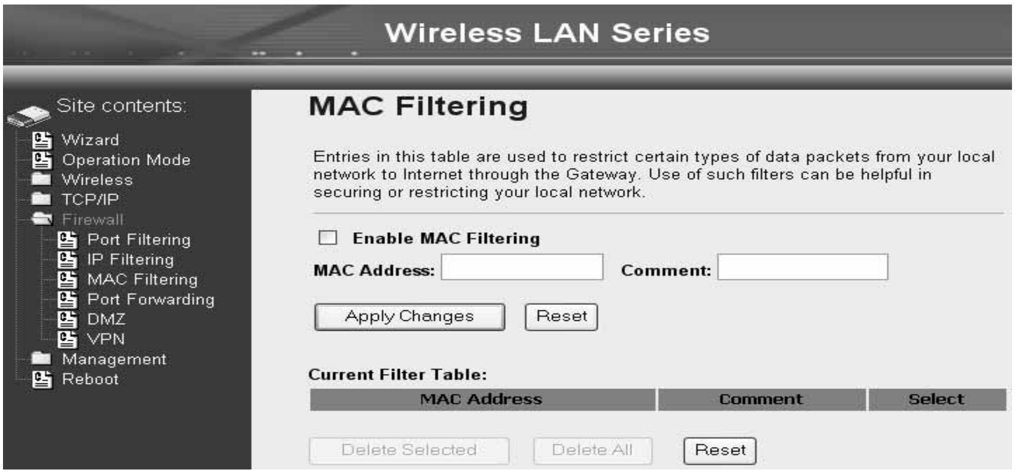
Local IP Address: Protocol: Both Comment:

Current Filter Table:

| Local IP Address | Protocol | Comment | Select |
|---|---|---|---|

### MAC Filtering

When you enable the MAC Filtering function, you can specify the MAC Addresses in current filter table. Once the source MAC Address of outgoing packets match the MAC Addresses in the table, the firewall will block this packet from LAN to WAN.



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

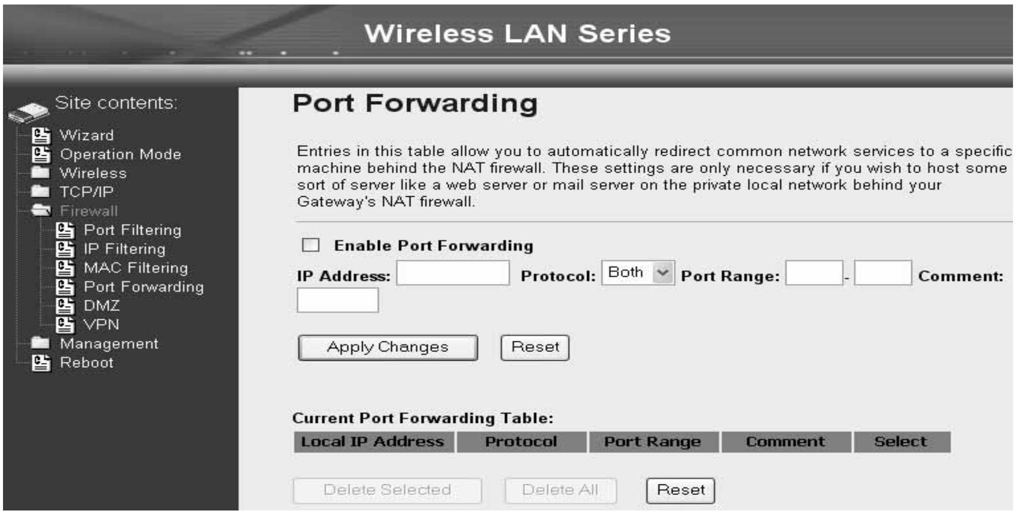
MAC Address: Comment:

Current Filter Table:

| MAC Address | Comment | Select |
|---|---|---|

## Configuring Port Forwarding (Virtual Server)

This function allows 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 the device'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 |
|---|---|---|---|---|

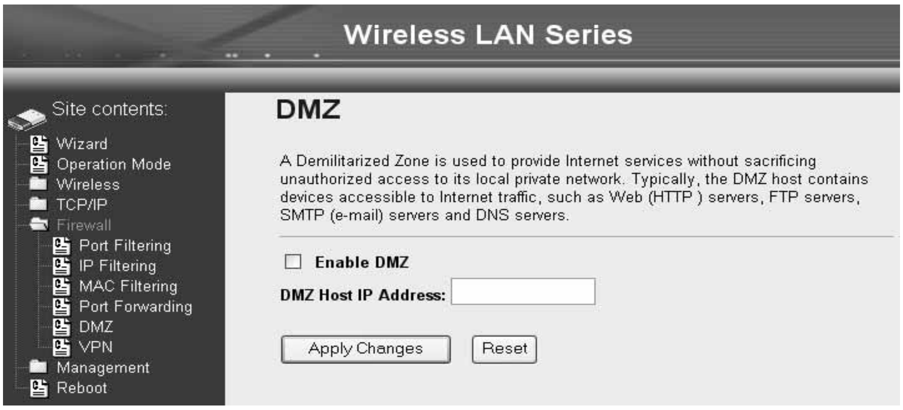
The most often used port numbers are shown in the following table.

| Services | Port Number |
|---|---|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |
| Telnet | 23 |

|  |  |
|---|---|
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer Protocol) | 80 |
| POP3 (Post Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| SNMP (Simple Network Management Protocol) | 161 |
| SNMP trap | 162 |
| SIP (Session Initiation Protocol) | 5060 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

## Configuring 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. So that all inbound packets will be redirected to the computer you set. It also is useful while you run some applications (ex. Internet game) that use uncertain incoming ports.



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.

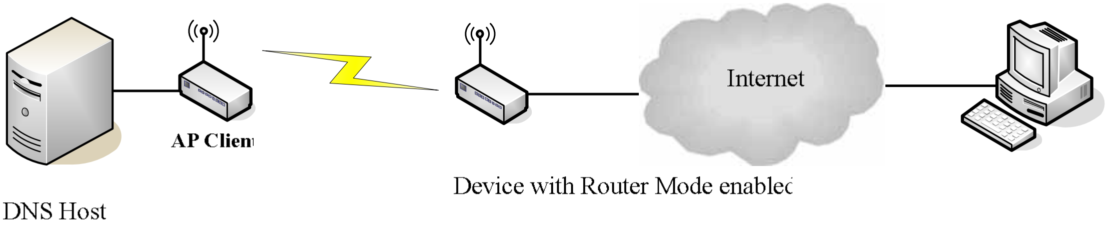
☐ Enable DMZ

DMZ Host IP Address:

[Apply Changes] [Reset]

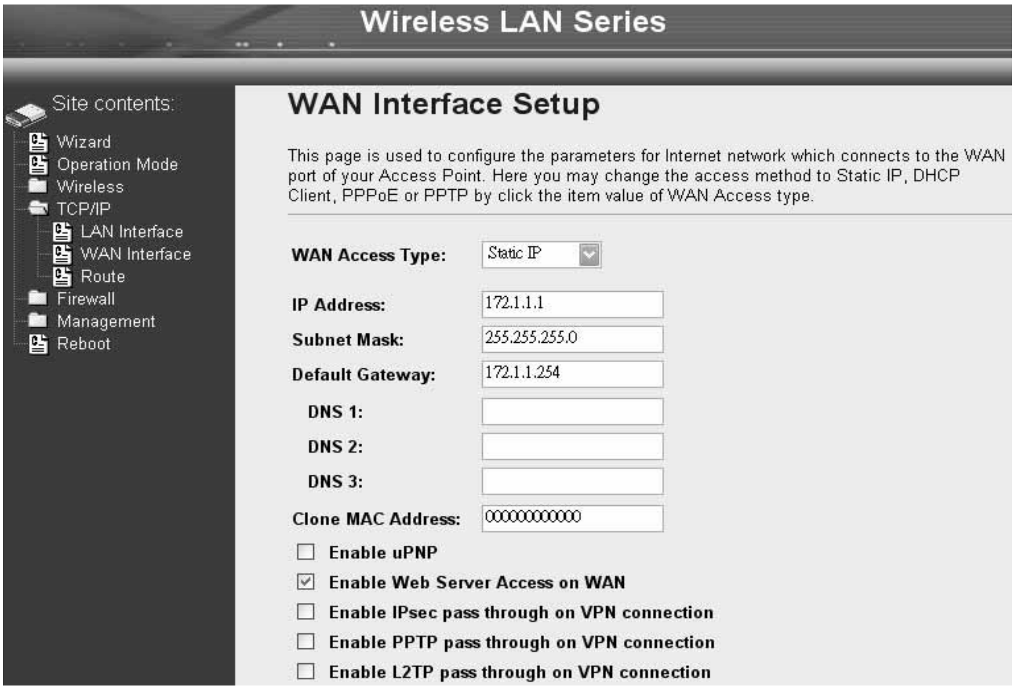
**Enable DMZ:** Enable the “Enable DMZ”, and then click “Apply Changes” button to save the changes.

**DMZ Host IP Address:** Input the IP Address of the computer that you want to expose to Internet.



## Configuring WAN Interface

The device supports four kinds of IP configuration for WAN interface, including Static IP, DHCP Client, PPPoE and PPTP. You can select one of the WAN Access Types depend on your ISP required. The default WAN Access Type is “Static IP”.



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 Client, PPPoE or PPTP by click the item value of WAN Access type.

| | |
|---|---|
| WAN Access Type: | Static IP |
| IP Address: | 172.1.1.1 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 172.1.1.254 |
| DNS 1: | |
| DNS 2: | |
| DNS 3: | |
| Clone MAC Address: | 000000000000 |

□ Enable uPNP

☑ Enable Web Server Access on WAN

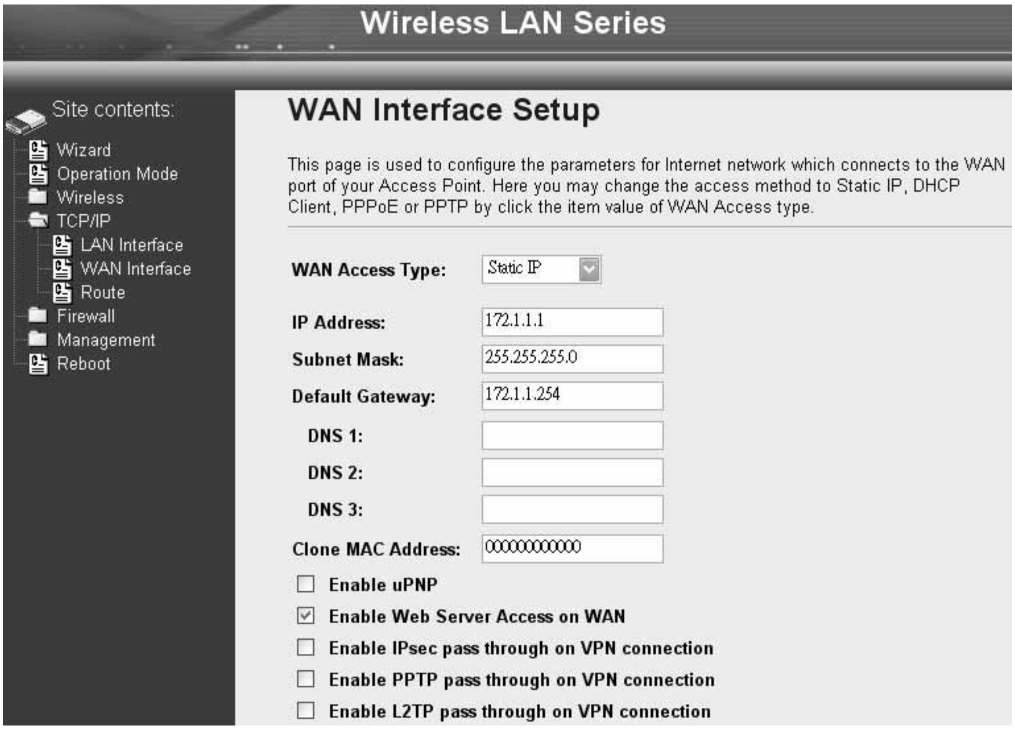
□ Enable IPsec pass through on VPN connection

□ Enable PPTP pass through on VPN connection

□ Enable L2TP pass through on VPN connection

## Static IP

You can get the IP configuration data of Static-IP from your ISP. And you will need to fill the fields of IP address, subnet mask, gateway address, and one of the DNS addresses.



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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

☐ Enable uPNP

☑ 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

**IP Address:** The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.

**Subnet Mask:** The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

**Default Gateway:** The IP address of Default Gateway provided by your ISP or MIS. Default Gateway is the intermediate network device that has knowledge of the network IDs of the other networks in the Wide Area Network, so it can forward the packets to other gateways until they are delivered to the one connected to the specified destination.

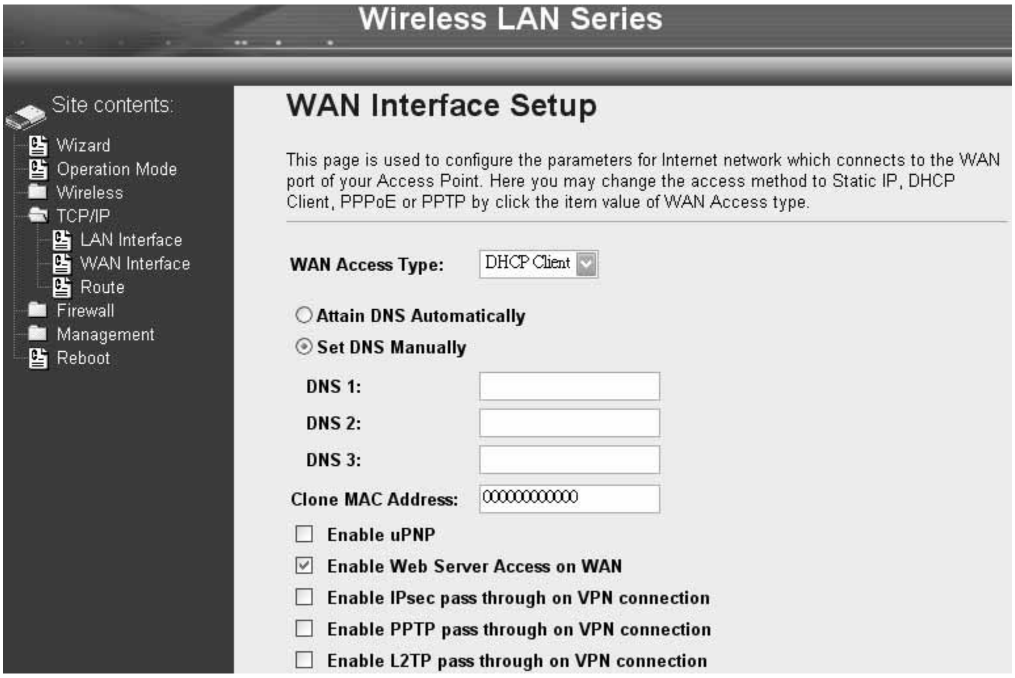
**DNS 1~3:** The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

**Clone MAC Address:** Clone device MAC address to the specify MAC address required by your ISP

**Enable uPnP:** Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

## DHCP Client (Dynamic IP)

All IP configuration data besides DNS will obtain from the DHCP server when DHCP-Client WAN Access Type is selected.



### 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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable Web Server Access on WAN

□ Enable IPsec pass through on VPN connection

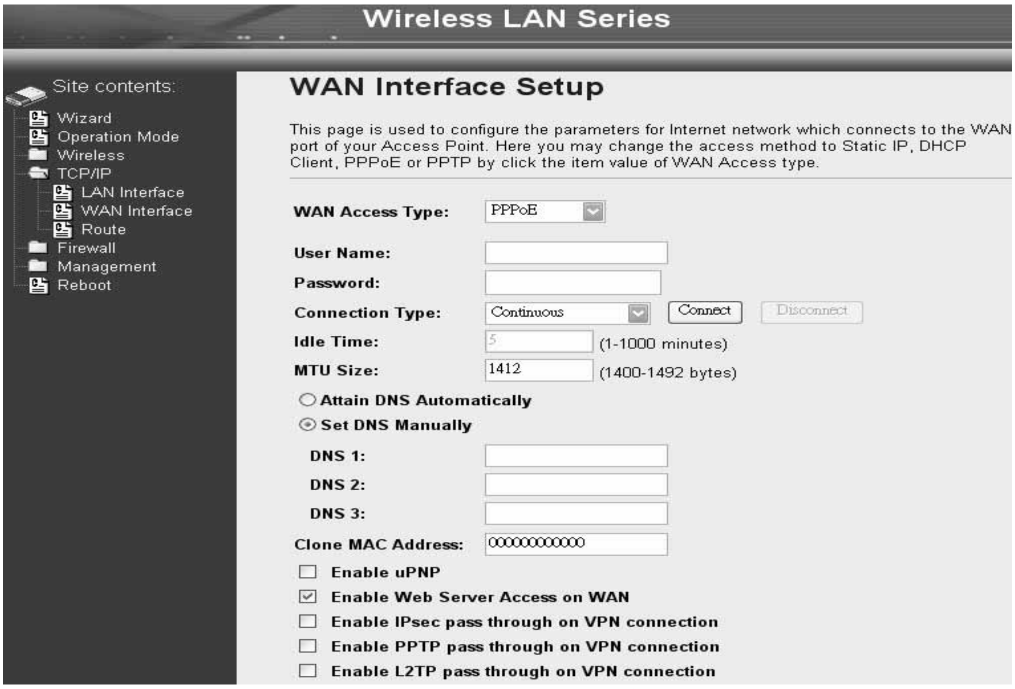
□ Enable PPTP pass through on VPN connection

□ Enable L2TP pass through on VPN connection

| | |
|---|---|
| **DNS1~3:** | The IP addresses of DNS provided by your ISP.<br>DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found. |
| **Clone MAC Address:** | Clone device MAC address to the specify MAC address required by your ISP |
| **Enable uPnP:** | Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP) |

## PPPoE

When the PPPoE (Point to Point Protocol over Ethernet) WAN Access Type is selected, you must fill the fields of User Name, Password provided by your ISP. The IP configuration will be done when the device successfully authenticates with your ISP.



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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: PPPoE

User Name:

Password:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1412 (1400-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ 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

**User Name:** The account provided by your ISP

**Password:** The password for your account.

**Connect Type:** “Continuous “ : connect to ISP permanently

“Manual” : Manual connect/disconnect to ISP

“On-Demand” : Automatically connect to ISP when user need to access the Internet.

**Idle Time:** The number of inactivity minutes to disconnect from ISP. This setting is only available when “Connect on Demand” connection type is selected.

**MTU Size:** Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.

**DNS1~3:** The IP addresses of DNS provided by your ISP.

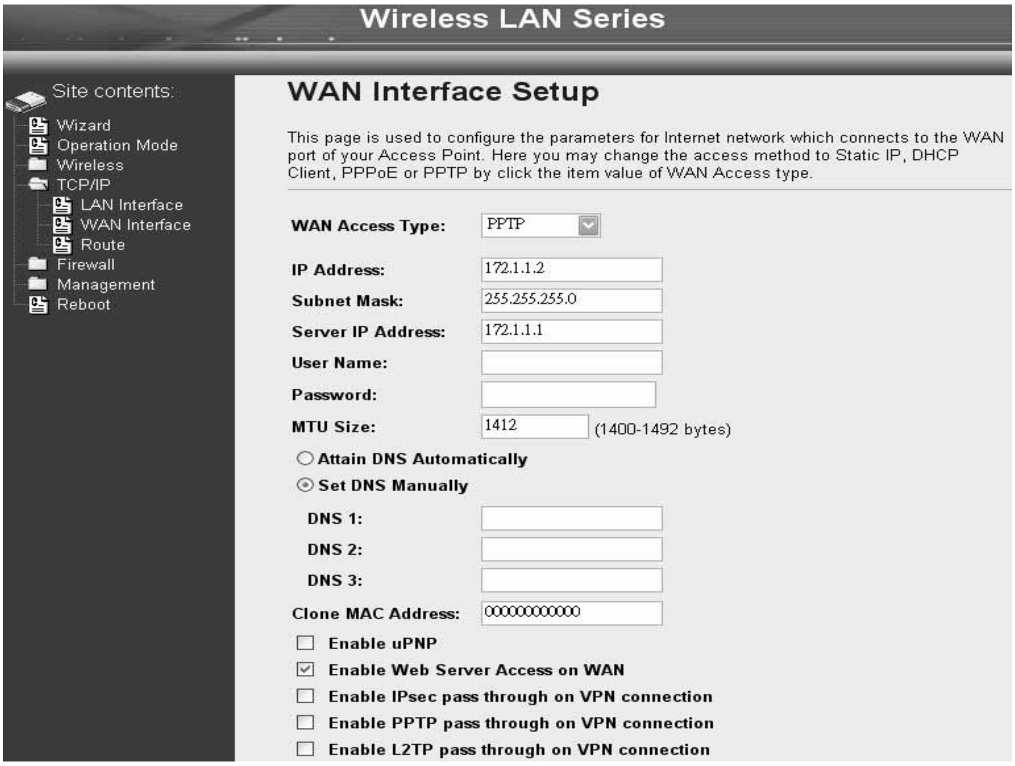
DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

**Clone MAC Address:** Clone device MAC address to the specify MAC address required by your ISP.

**Enable UPnP:** Enable UPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

## PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only



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 Client, PPPoE or PPTP by click the item value of WAN Access type.

| | |
|---|---|
| WAN Access Type: | PPTP |
| IP Address: | 172.1.1.2 |
| Subnet Mask: | 255.255.255.0 |
| Server IP Address: | 172.1.1.1 |
| User Name: | |
| Password: | |
| MTU Size: | 1412 (1400-1492 bytes) |

○ Attain DNS Automatically

● Set DNS Manually

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

□ Enable uPNP

☑ 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

**IP Address:** The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.

**Subnet Mask:** The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

**Server IP Address:** The IP address of PPTP server

**(Default Gateway)**

**User Name:** The account provided by your ISP

**Password:** The password of your account

**MTU Size:** Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.

**DNS1~3:** The IP addresses of DNS provided by your ISP.

DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

**Clone MAC Address:** Clone device MAC address to the specify MAC address required by your ISP.

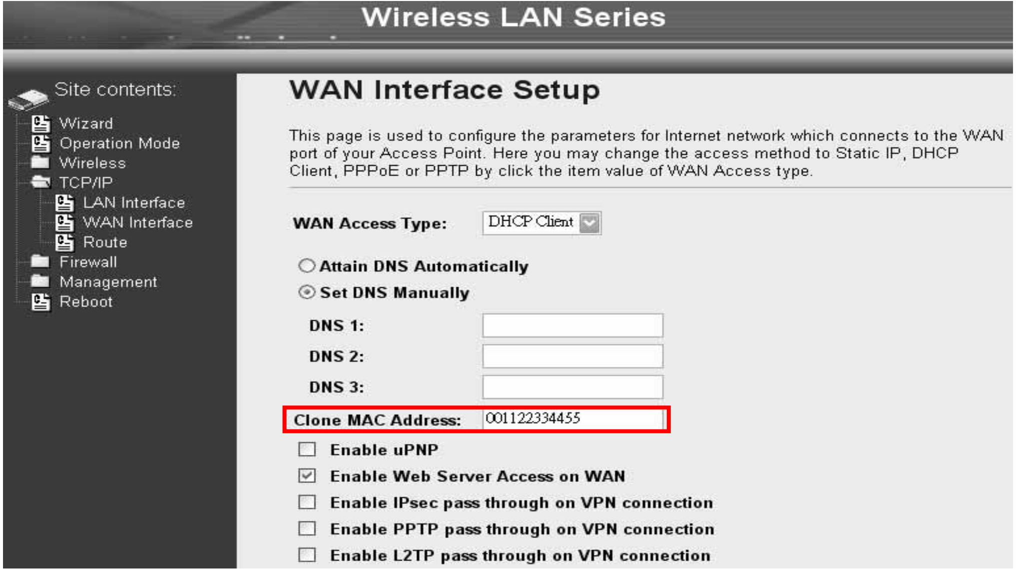
**Enable uPnP:** Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

## Configuring Clone MAC Address

The device provides MAC address clone feature to fit the requirement of some ISP need to specify the client MAC address.

Physical WAN interface MAC Address clone

1. Clone MAC address for DHCP Client 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 Client, PPPoE or PPTP by click the item value of WAN Access type.

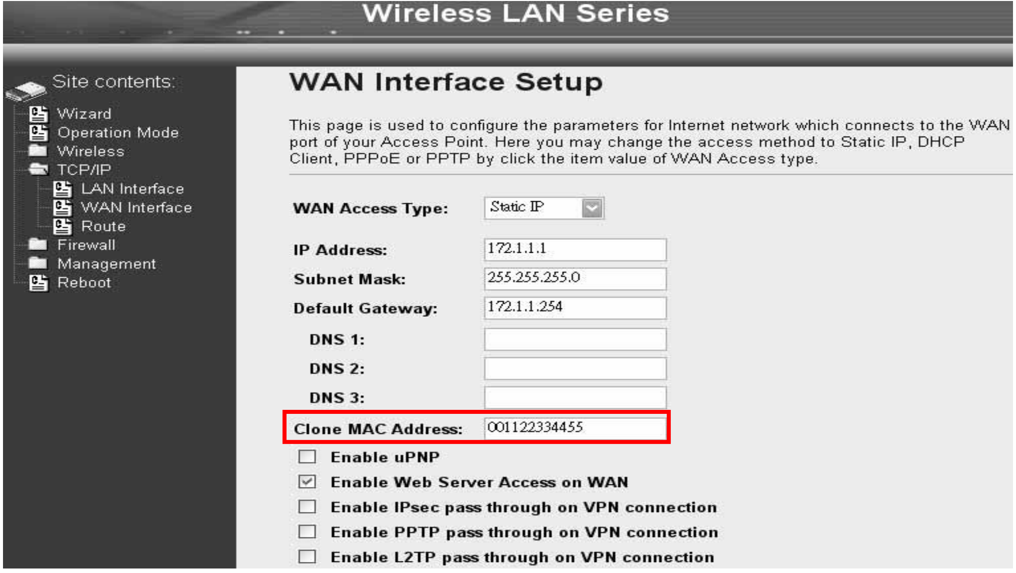
WAN Access Type: DHCP Client

○ Attain DNS Automatically
● Set DNS Manually

DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 001122334455

□ Enable uPNP
☑ 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

2. Clone MAC address for Static IP WAN access type



WAN Interface Setup

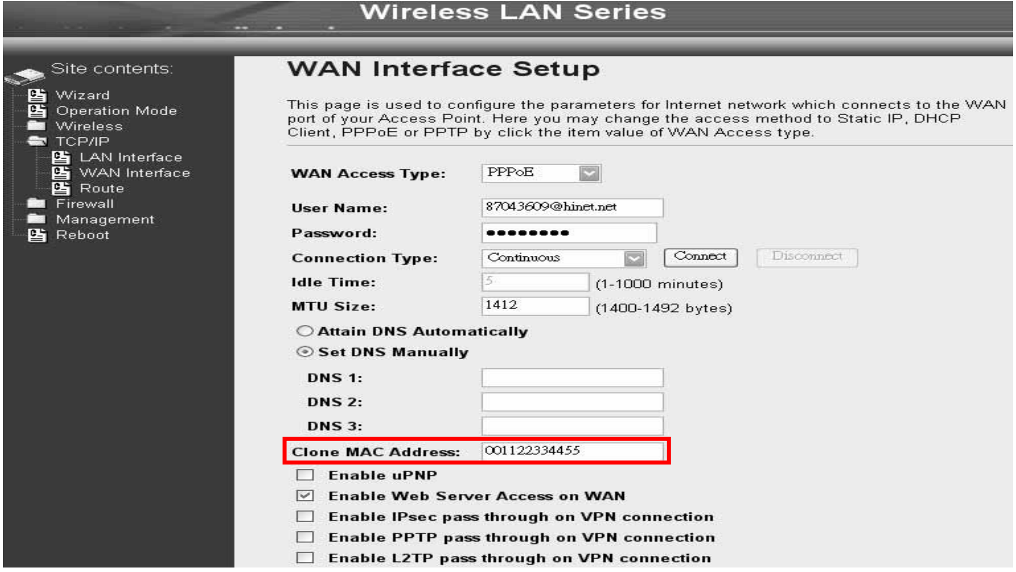
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 172.1.1.254
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 001122334455

□ Enable uPNP
☑ 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

3. Clone MAC address for PPPoE 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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: PPPoE

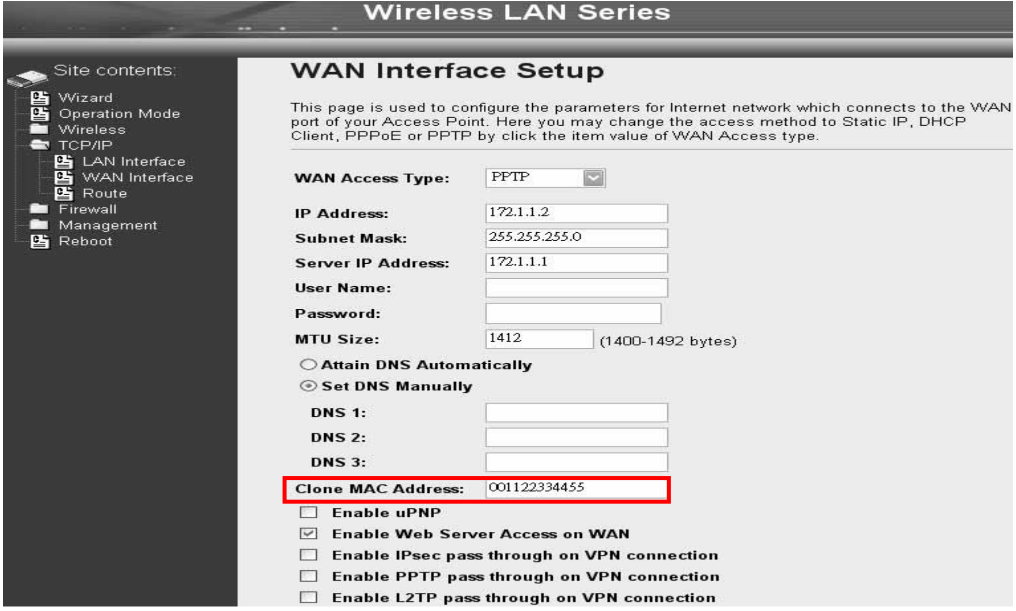
User Name: 87043609@hinet.net
Password: ●●●●●●●●●
Connection Type: Continuous [Connect] [Disconnect]
Idle Time: 5 (1-1000 minutes)
MTU Size: 1412 (1400-1492 bytes)

○ Attain DNS Automatically
● Set DNS Manually

DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 001122334455

□ Enable uPNP
☑ 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

4. Clone MAC address for PPTP 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 Client, PPPoE or PPTP by click the item value of WAN Access type.

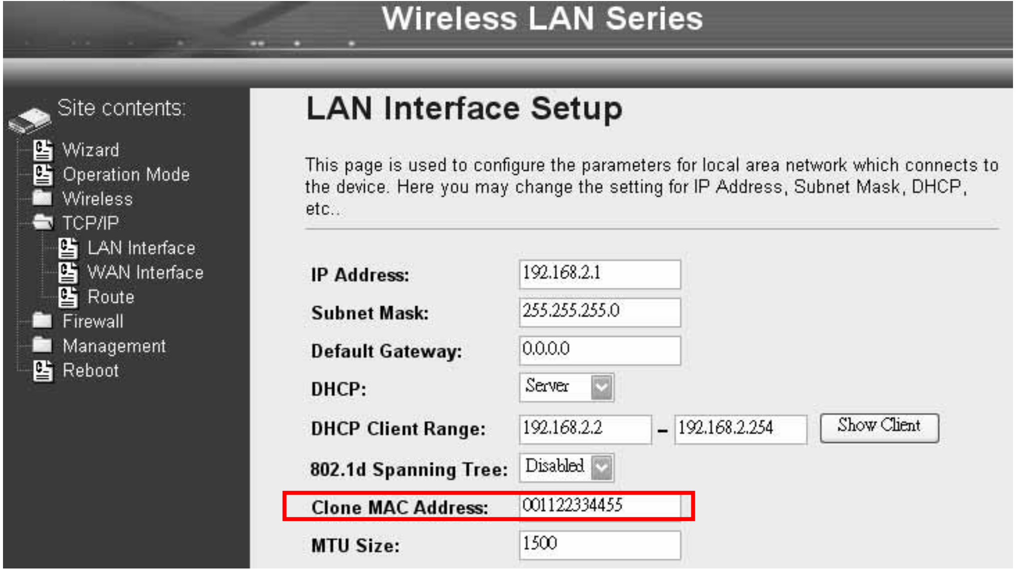
| | |
|---|---|
| WAN Access Type: | PPTP |
| IP Address: | 172.1.1.2 |
| Subnet Mask: | 255.255.255.0 |
| Server IP Address: | 172.1.1.1 |
| User Name: | |
| Password: | |
| MTU Size: | 1412 (1400-1492 bytes) |

○ Attain DNS Automatically
● Set DNS Manually

| | |
|---|---|
| DNS 1: | |
| DNS 2: | |
| DNS 3: | |
| Clone MAC Address: | 001122334455 |

□ Enable uPNP
☑ 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

5. Physical LAN interface MAC address clone



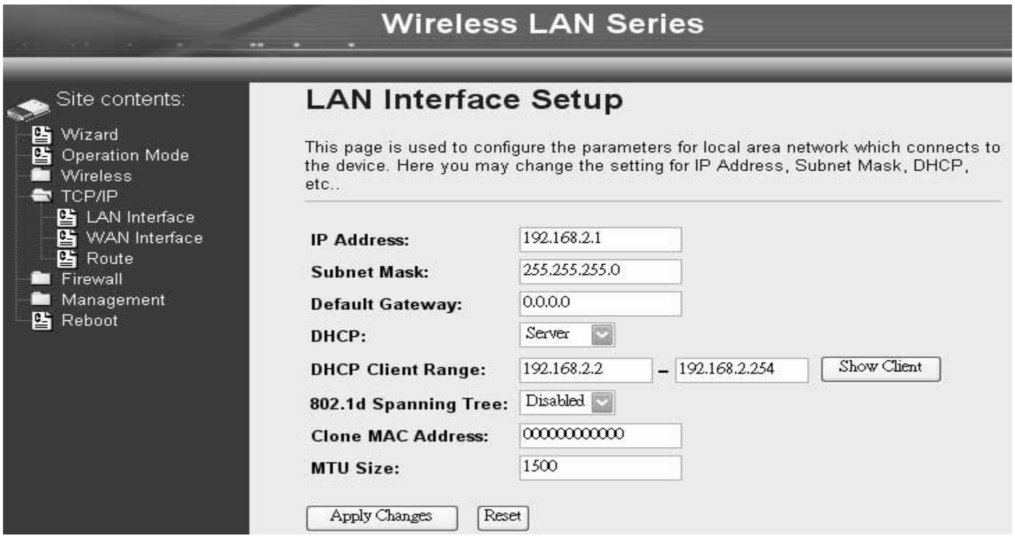
**LAN Interface Setup**

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

| | |
|---|---|
| IP Address: | 192.168.2.1 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 0.0.0.0 |
| DHCP: | Server |
| DHCP Client Range: | 192.168.2.2 – 192.168.2.254 |
| 802.1d Spanning Tree: | Disabled |
| Clone MAC Address: | 001122334455 |
| MTU Size: | 1500 |

## Configuring DHCP Server

1. To use the DHCP server inside the device, please make sure there is no other DHCP server existed in the same network as the device.
2. Enable the DHCP Server option and assign the client range of IP addresses as following page.



LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Server

DHCP Client Range: 192.168.2.2 – 192.168.2.254

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

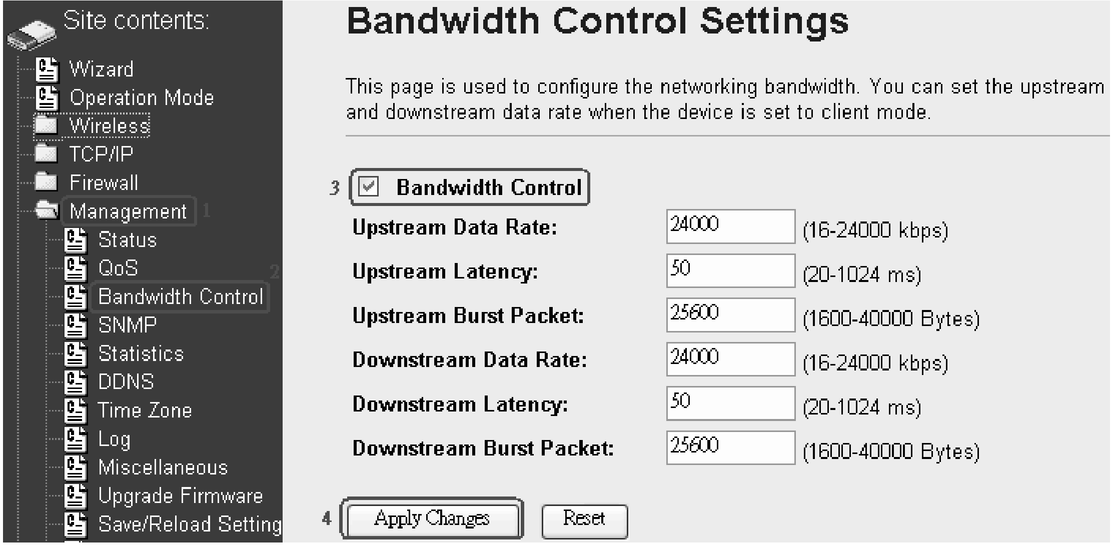
MTU Size: 1500

3. When the DHCP server is enabled and also the device router mode is enabled then the default gateway for all the DHCP client hosts will set to the IP address of device.

## Bandwidth Control

This functionality can control Bandwidth of Up/Downstream

1. Enable Bandwidth Control and then enter Data Rate□Latency and Burst Packet in the specific field.



Bandwidth Control Settings

This page is used to configure the networking bandwidth. You can set the upstream and downstream data rate when the device is set to client mode.

☑ Bandwidth Control

Upstream Data Rate: 24000 (16-24000 kbps)

Upstream Latency: 50 (20-1024 ms)

Upstream Burst Packet: 25600 (1600-40000 Bytes)

Downstream Data Rate: 24000 (16-24000 kbps)

Downstream Latency: 50 (20-1024 ms)

Downstream Burst Packet: 25600 (1600-40000 Bytes)

Note: Only device on **Client** mode or **WISP** mode this functionality can take effective.

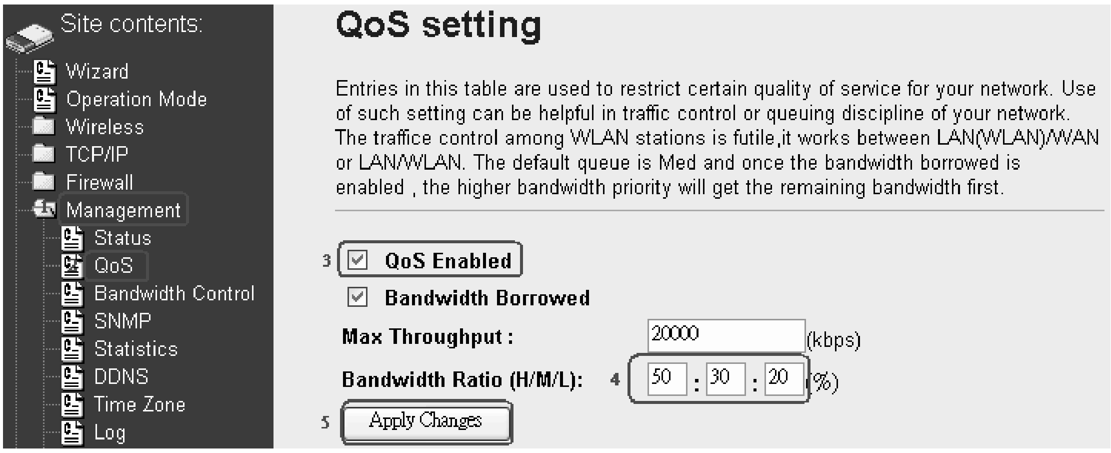
2. Parameter Definition

| Label | Description |
|---|---|
| Upstream Data Rate | Speed of transmit data that from Ethernet interface to Wireless interface. |
| Upstream Latency | Similar a waiting time the data queuing-time. |
| Upstream Burst Packet | Similar a buffer the data will into the buffer while the data is transmit or receive. |
| Downstream Data Rate | Speed of transmit data that from Wireless interface to Ethernet interface. |
| Downstream Latency | Similar a waiting time the data queuing-time. |
| Downstream Burst Packet | Similar a buffer the data will into the buffer while the data is transmit or receive. |

## QoS (Quality of Service)

QoS allows you to specify some rules, to ensure the quality of service in your network. Such as use Bandwidth Priority concept to allocate bandwidth. This function can be helpful in shaping and queuing traffic from LAN (WLAN) to WAN or LAN to WLAN, but not WLAN to WLAN.

Enable the QoS and then fill in Bandwidth Ratio (H/M/L) the device has three Bandwidth Priorities High, Medium and Low user can allocation Bandwidth to these and default is High:50□, Medium:30□ and Low:20□.



QoS setting

Entries in this table are used to restrict certain quality of service for your network. Use of such setting can be helpful in traffic control or queuing discipline of your network. The traffice control among WLAN stations is futile,it works between LAN(WLAN)/WAN or LAN/WLAN. The default queue is Med and once the bandwidth borrowed is enabled , the higher bandwidth priority will get the remaining bandwidth first.

☑ QoS Enabled

☑ Bandwidth Borrowed

Max Throughput : 20000 (kbps)

Bandwidth Ratio (H/M/L): 50 : 30 : 20 (%)

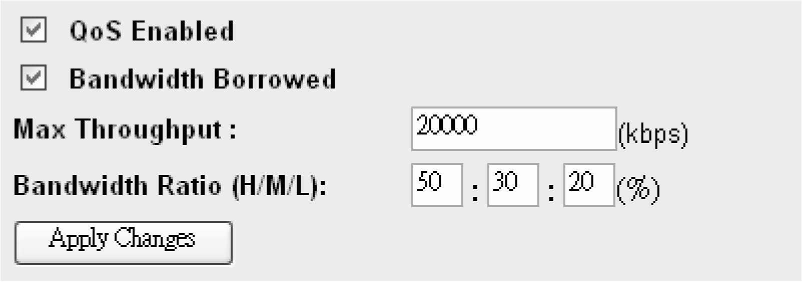
Apply Changes

The following table describes the priorities that you can apply to bandwidth.

| Priority Level | Description |
|---|---|
| High | Typically used for voice or video applications that is especially sensitive to the variations in delay. |
| Medium | Typically used for important traffic that can tolerate some delay. |
| Low | Typically used for non-critical traffic such as a large number of transfers but that should not affect other application. |

Click the **QoS** link under **Management** to open the QoS Setting page. This page is divided into three parts: basic settings, QoS rule settings, and current QoS setting table.

1. Enable QoS and enter Max Throughput (default 20Mbps) □Bandwidth Ratio (default H:50%, M:30%, L:20%)



☑ QoS Enabled

☑ Bandwidth Borrowed

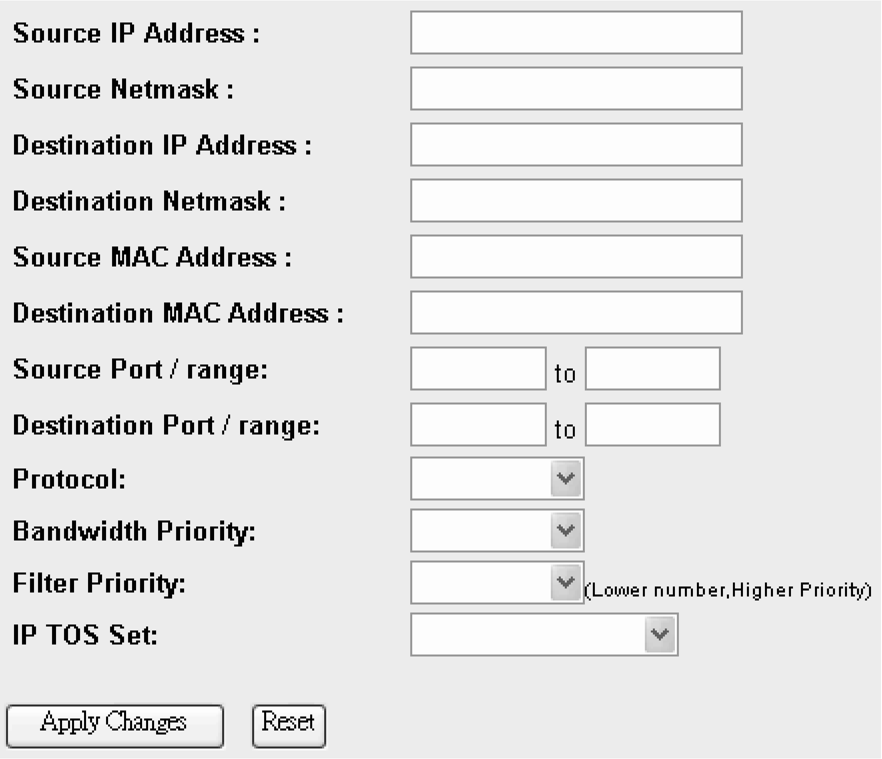
Max Throughput : 20000 (kbps)

Bandwidth Ratio (H/M/L): 50 : 30 : 20 (%)

The following table describes the labels in this part.

| Label | Description |
|---|---|
| QoS Enabled | Select this check box to enable quality of service. |
| Bandwidth Borrowed | Select this check box to allow a rule to borrow unused bandwidth. Bandwidth borrowing is decided by priority of the rules. Higher priority will get the remaining bandwidth first. |
| Max Throughput | Enter the value of max throughput in kbps that you want to allocate for one rule. The value should between 1200 kbps and 24000 kbps. |
| Bandwidth Ratio (H/M/L) | You can specify the ratio of priority in these fields. The range from 1 to 99. The High priority's ratio should higher than Medium priority's ratio and Medium priority's ratio should higher than Low priority's ratio. |
| Apply Changes | Click this button to save and apply your settings. |

2. QoS Rule settings



| | |
|---|---|
| Source IP Address : | |
| Source Netmask : | |
| Destination IP Address : | |
| Destination Netmask : | |
| Source MAC Address : | |
| Destination MAC Address : | |
| Source Port / range: | to |
| Destination Port / range: | to |
| Protocol: | |
| Bandwidth Priority: | |
| Filter Priority: | (Lower number,Higher Priority) |
| IP TOS Set: | |

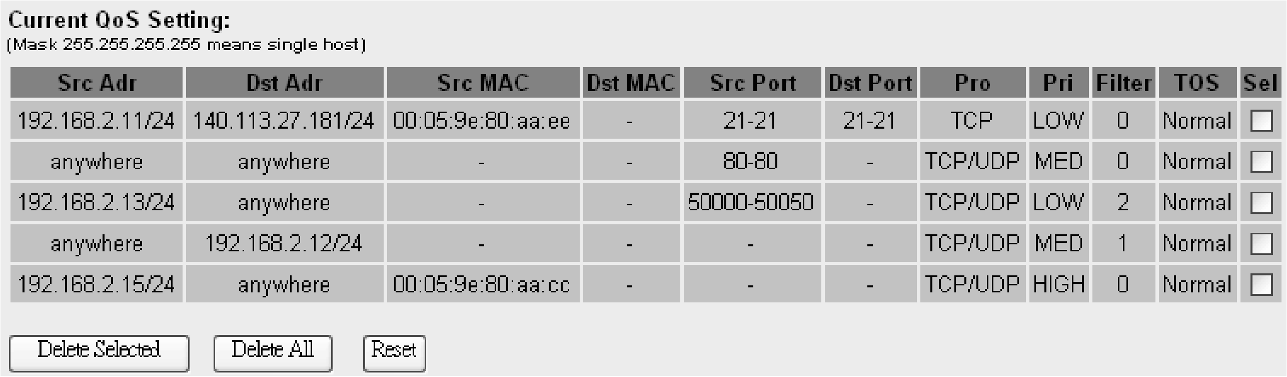
The following table describes the labels in this part.

| **Label** | **Description** |
|---|---|
| IP Address | Enter source/destination IP Address in dotted decimal notation. |
| Netmask | Once the source/destination IP Address is entered, the subnet mask address must be filled in this field. |
| MAC Address | Enter source/destination MAC Address. |
| Port / range | You can enter specific port number or port range of the source/destination |
| Protocol | Select a protocol from the drop down list box. Choose **TCP/UDP**, **TCP** or **UDP**. |
| Bandwidth Priority | Select a bandwidth priority from the drop down list box. Choose **Low**, **Medium** or **High**. |
| Filter Priority | Select a filter priority number from the drop down list box. **Lower number gets higher priority** while two rules have the same bandwidth priority. |
| IP TOS Match | Select an IP **type-of-service** value from the drop down list box. Choose Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, or Minimize Delay. |
| Apply Changes | Click this button to save and apply your settings. |

| | |
|---|---|
| Reset | Click this button to begin re-input the parameters. |

## Current QoS setting table

In this part, you can see how many rules have been specified. And you can see the detail about the rules and manage the rules. This table can input 50 rules at most.

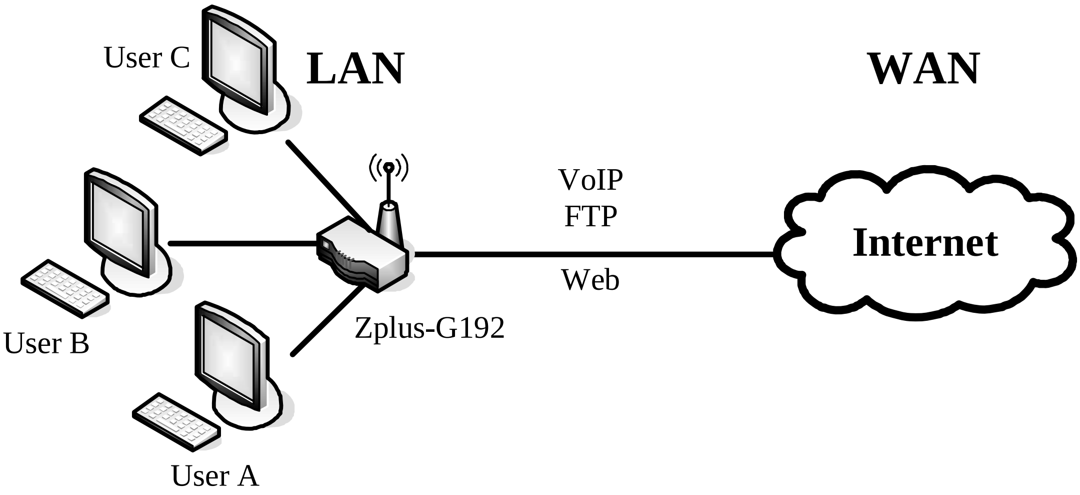


**Current QoS Setting:**

(Mask 255.255.255.255 means single host)

| Src Adr | Dst Adr | Src MAC | Dst MAC | Src Port | Dst Port | Pro | Pri | Filter | TOS | Sel |
|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.2.11/24 | 140.113.27.181/24 | 00:05:9e:80:aa:ee | - | 21-21 | 21-21 | TCP | LOW | 0 | Normal | □ |
| anywhere | anywhere | - | - | 80-80 | - | TCP/UDP | MED | 0 | Normal | □ |
| 192.168.2.13/24 | anywhere | - | - | 50000-50050 | - | TCP/UDP | LOW | 2 | Normal | □ |
| anywhere | 192.168.2.12/24 | - | - | - | - | TCP/UDP | MED | 1 | Normal | □ |
| 192.168.2.15/24 | anywhere | 00:05:9e:80:aa:cc | - | - | - | TCP/UDP | HIGH | 0 | Normal | □ |

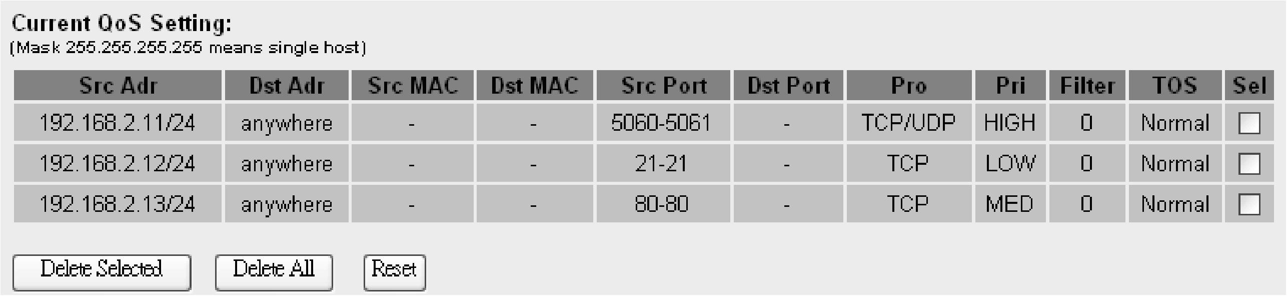
## An example for usage



For example, there are three users in your network.

- User A wants to **browse the websites** to retrieve information.
- User B wants to use **FTP** connection to download a large file.
- User C wants to use **software phone** to connect with customer.

The voice is sensitive to the variations in delay; you can set **High** priority for **User C**. The FTP transmission may take a long time; you can set **Low** priority for **User B**.



**Current QoS Setting:**
(Mask 255.255.255.255 means single host)

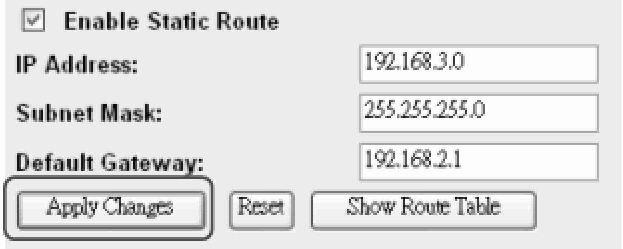
| Src Adr | Dst Adr | Src MAC | Dst MAC | Src Port | Dst Port | Pro | Pri | Filter | TOS | Sel |
|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.2.11/24 | anywhere | - | - | 5060-5061 | - | TCP/UDP | HIGH | 0 | Normal | ☐ |
| 192.168.2.12/24 | anywhere | - | - | 21-21 | - | TCP | LOW | 0 | Normal | ☐ |
| 192.168.2.13/24 | anywhere | - | - | 80-80 | - | TCP | MED | 0 | Normal | ☐ |

## Static Route Setup

User can set the routing information let the Router knows what routing is correct also it can not learn automatically through other means.

For example, if user wants to link the Network 3 and Network 4 separately from Network 1 that Routing Table configuration as below:

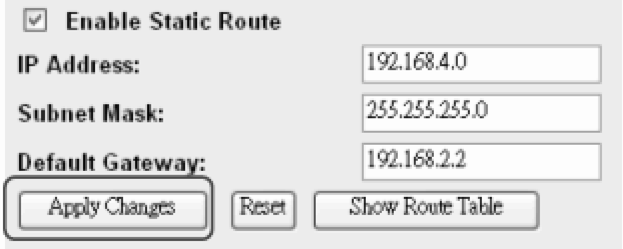
1. Enable Static Route in Route Setup of TCP/IP page and then enter IP Address of Network 3□Subnet Mask and IP Address of Router (R1) in Default Gateway field final click Apply Change button.



☑ Enable Static Route

| | |
|---|---|
| IP Address: | 192.168.3.0 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 192.168.2.1 |

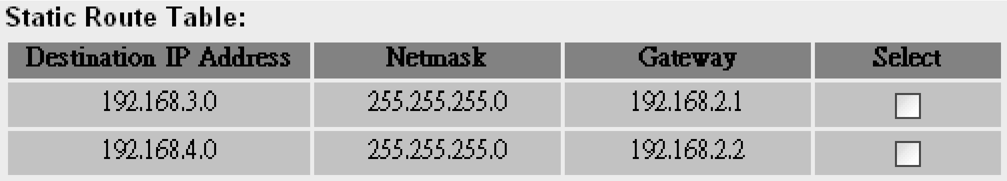
2. Enter IP Address of Network 4□Subnet Mask and IP Address of Router (R2) in Default Gateway field final click Apply Change button.



☑ Enable Static Route

| | |
|---|---|
| IP Address: | 192.168.4.0 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 192.168.2.2 |

3. In Static Route Table there have two routings for Network 3 and Network 4



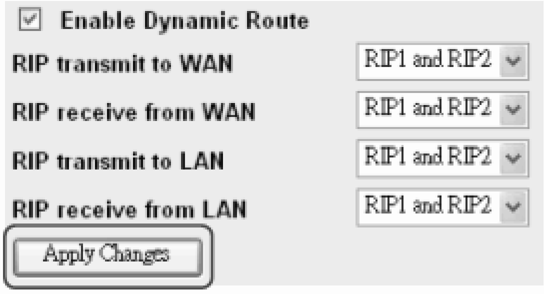
Static Route Table:

| Destination IP Address | Netmask | Gateway | Select |
|---|---|---|---|
| 192.168.3.0 | 255.255.255.0 | 192.168.2.1 | □ |
| 192.168.4.0 | 255.255.255.0 | 192.168.2.2 | □ |

## Dynamic Route Setup

The Dynamic Route utilizes RIP1/2 to transmit and receive the route information with other Routers.

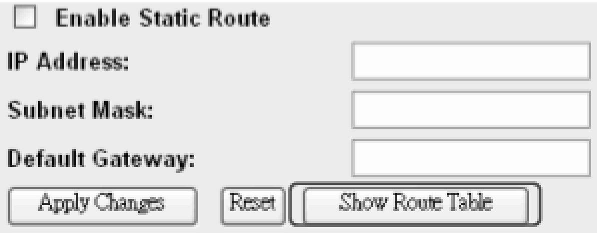
1. Enable Dynamic Route and then select RIP 1□RIP2 or Both to transmit/receive packets final click Apply Change button.



☑ Enable Dynamic Route

| | |
|---|---|
| RIP transmit to WAN | RIP1 and RIP2 |
| RIP receive from WAN | RIP1 and RIP2 |
| RIP transmit to LAN | RIP1 and RIP2 |
| RIP receive from LAN | RIP1 and RIP2 |

2. Click Show Route Table button to show Dynamic Route Table.



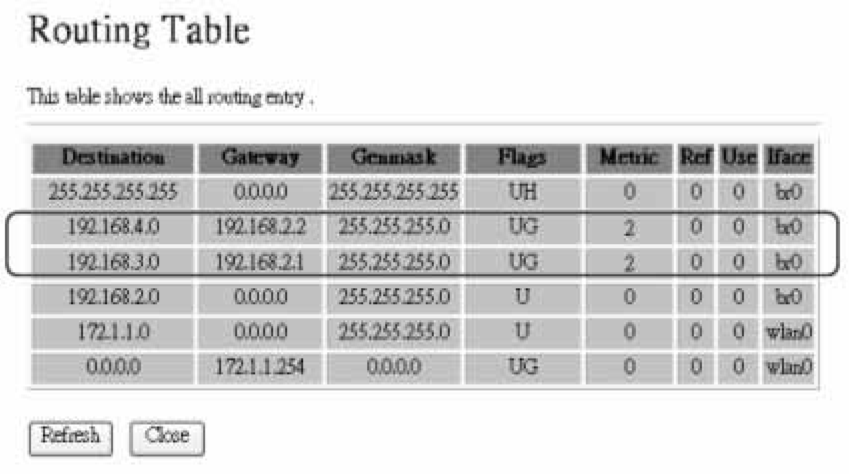
□ Enable Static Route

IP Address:

Subnet Mask:

Default Gateway:

3. In Dynamic Routing Table there have two routings for Network 3 and Network 4



Routing Table

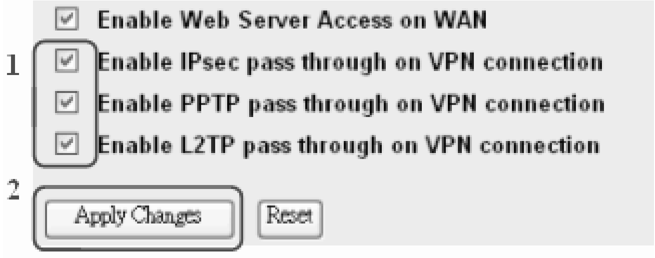
This table shows the all routing entry .

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|---|---|---|---|---|---|---|---|
| 255.255.255.255 | 0.0.0.0 | 255.255.255.255 | UH | 0 | 0 | 0 | br0 |
| 192.168.4.0 | 192.168.2.2 | 255.255.255.0 | UG | 2 | 0 | 0 | br0 |
| 192.168.3.0 | 192.168.2.1 | 255.255.255.0 | UG | 2 | 0 | 0 | br0 |
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | br0 |
| 172.1.1.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | wlan0 |
| 0.0.0.0 | 172.1.1.254 | 0.0.0.0 | UG | 0 | 0 | 0 | wlan0 |

## VPN Pass-through

This functionality let the device can Pass-through the VPN packets including PPTP/ L2TP/IPsec VPN Connection.

1. Check the VPN Pass-through in WAN Interface of TCP/IP Page that you want and then click Apply Changes button.



☑ 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

## Using CLI Menu

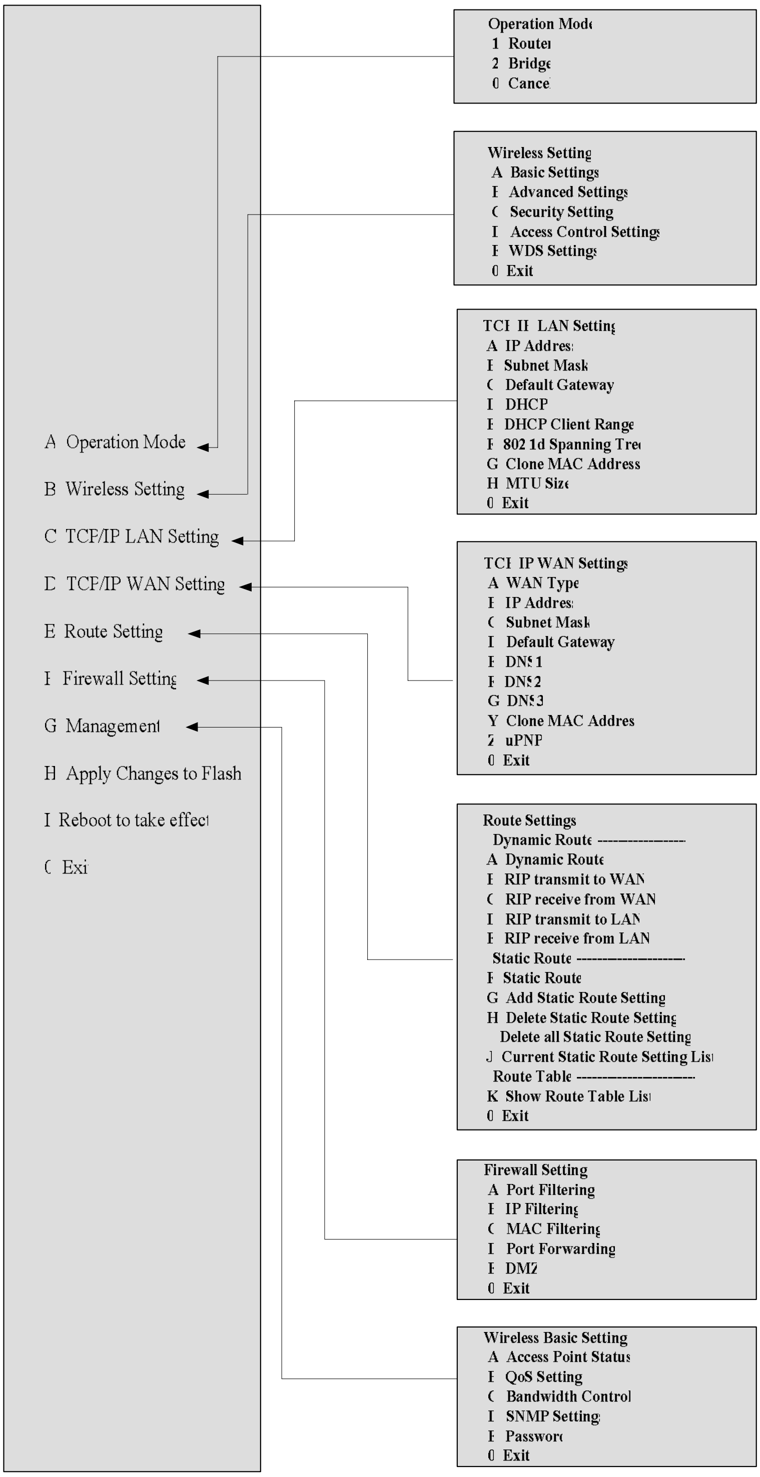
Start a SSH(Secure Shell) client session to login the device

The SSH server daemon inside device uses well-known TCP port 22. User must use SSH client utility such like Putty to login the device. The default password for user “root” is “qwert”, once user login the device then can change the password by CLI command.

Execute CLI program

This program won’t execute automatically when user login the device. User must manually execute it by typing the case-sensitive command “cli”. Please note that any modified settings won’t save permanently until user “Apply Changes to Flash” or reboot it. The new settings modified by CLI will take effect after rebooting the device.

Menu Tree List



A Operation Mode

B Wireless Setting

C TCP/IP LAN Setting

D TCP/IP WAN Setting

E Route Setting

F Firewall Setting

G Management

H Apply Changes to Flash

I Reboot to take effect

0 Exit

Operation Mode
1 Router
2 Bridge
0 Cancel

Wireless Setting
A Basic Settings
B Advanced Settings
C Security Setting
D Access Control Settings
E WDS Settings
0 Exit

TCP IP LAN Setting
A IP Address
B Subnet Mask
C Default Gateway
D DHCP
E DHCP Client Range
F 802 1d Spanning Tree
G Clone MAC Address
H MTU Size
0 Exit

TCP IP WAN Settings
A WAN Type
B IP Address
C Subnet Mask
D Default Gateway
E DNS 1
F DNS 2
G DNS 3
Y Clone MAC Address
Z uPNP
0 Exit

Route Settings
Dynamic Route ------------------
A Dynamic Route
B RIP transmit to WAN
C RIP receive from WAN
D RIP transmit to LAN
E RIP receive from LAN
Static Route ---------------------
F Static Route
G Add Static Route Setting
H Delete Static Route Setting
Delete all Static Route Setting
J Current Static Route Setting List
Route Table -----------------------
K Show Route Table List
0 Exit

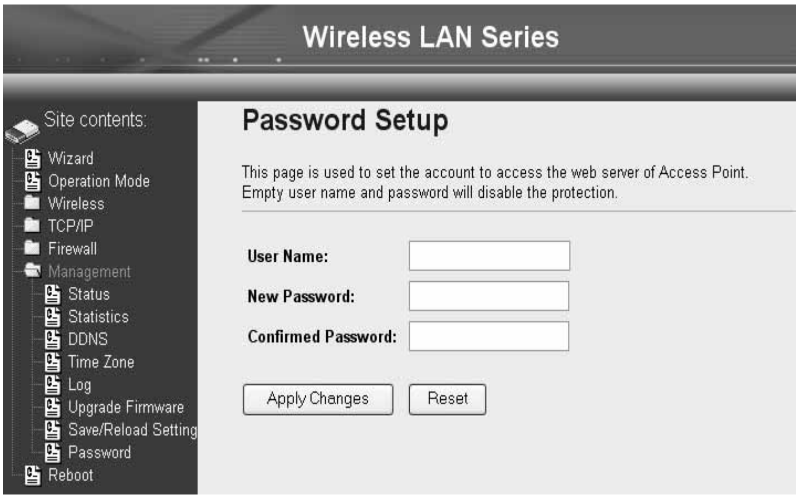
Firewall Setting
A Port Filtering
B IP Filtering
C MAC Filtering
D Port Forwarding
E DMZ
0 Exit

Wireless Basic Setting
A Access Point Status
B QoS Setting
C Bandwidth Control
D SNMP Setting
E Password
0 Exit

## The System Management

### Password Protection

Both Web-Browser and SSH configuration interfaces have password 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:

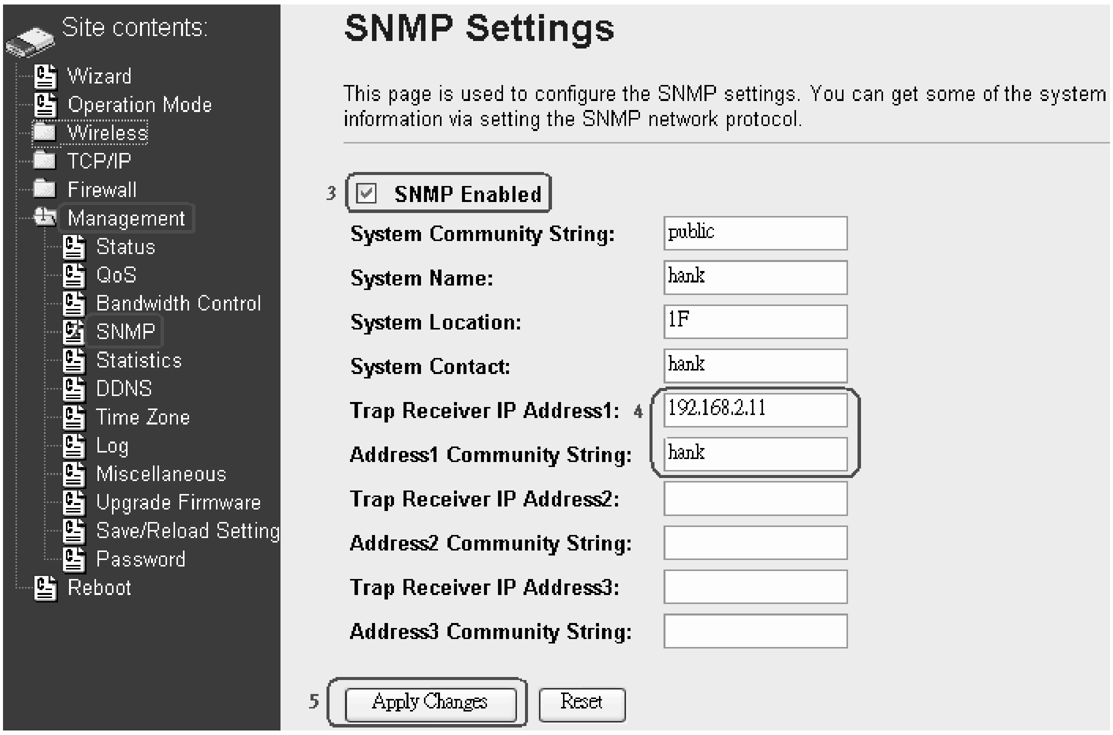
To disable the Web-Browser password protection just leave the “User Name” field to blank then click “Apply Changes” button.

To change the password of user “root” for SSH session, please use the CLI menu item G. System Setting→A. Root Password

## SNMP Agent

This device is compatible with SNMP v1/v2c and provide standard MIB II. Currently only the “public” community string is available and the modified settings by SNMP SET request will be lost after rebooting the device.

1. Enable SNMP and then enter IP Address of SNMP Manager in Trap Receiver IP Address field and Community String in System Community String field. Final click Apply Changes button.



SNMP Settings

This page is used to configure the SNMP settings. You can get some of the system information via setting the SNMP network protocol.

3 ☑ SNMP Enabled

System Community String: public

System Name: hank

System Location: 1F

System Contact: hank

Trap Receiver IP Address1: 4 192.168.2.11

Address1 Community String: hank

Trap Receiver IP Address2:

Address2 Community String:

Trap Receiver IP Address3:

Address3 Community String:

2. Following Table describes the SNMP configuration parameter

| Label | Description |
|---|---|
| System Community String | This is password sent with each trap to the SNMP Manager. |
| System Name | Type the Name which is name of device. |
| System Location | Type the Location which is location of device |
| System Contact | Type the Name which is person or group when the device has problem can find they. |
| Trap Receiver IP Address | Type the IP Address which is address of SNMP Manager. |
| Trap Receiver Community String | This is password receive with trap from the device (SNMP Agent). |

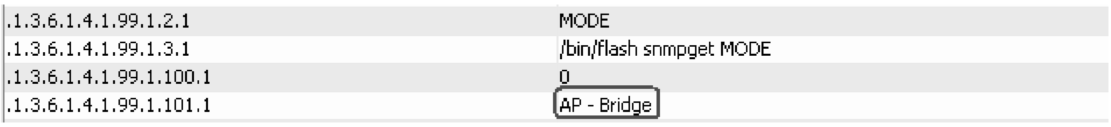
3. SNMP Traps

| Traps | Description |
|---|---|
| coldStart(0) | The trap from device after reboot the device |
| linkDown(2) | The trap is sent when any of the links are down. See the following table. |
| linkup(3) | The trap is sent when any of the links are UP. See the following table. |
| authenticationFailure(4) | The trap is sent when the device receiving gets or sets requirement with wrong community. |

4. Private MIBs

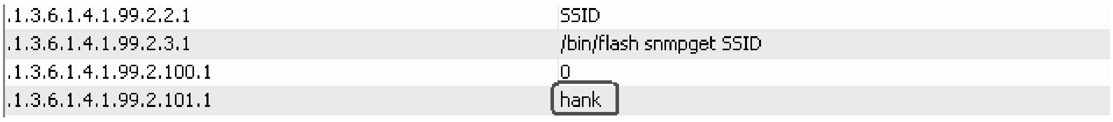
| OID | Description |
|---|---|
| 1.3.6.1.4.1.99.1 | Mode, Operation Mode in device. |
| 1.3.6.1.4.1.99.2 | SSID, SSID of the device |
| 1.3.6.1.4.1.99.3 | Channel, Channel of the device in WLAN |
| 1.3.6.1.4.1.99.4 | Band, 802.11g / 802.11b only |
| 1.3.6.1.4.1.99.5 | RSSI, Receive Signal Strength Index (Support AP and Client RSSI) |
| 1.3.6.1.4.1.99.6 | Active_Clients, The number of associate clients |
| 1.3.6.1.4.1.99.7 | Active_Clients_List, Client's Information (MAC Address, Data Rate, RSSI…etc) |
| 1.3.6.1.4.1.99.8 | Encryption, Encryption type of device in Wireless Network |

1.3.6.1.4.1.99.1 - Mode



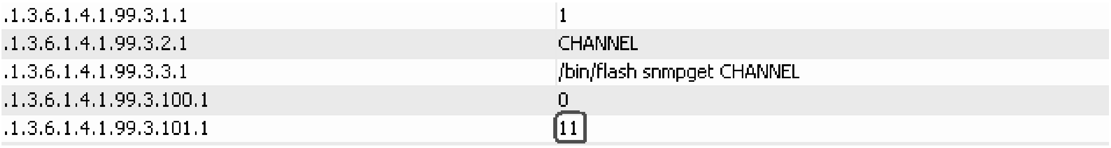
| | |
|---|---|
| .1.3.6.1.4.1.99.1.2.1 | MODE |
| .1.3.6.1.4.1.99.1.3.1 | /bin/flash snmpget MODE |
| .1.3.6.1.4.1.99.1.100.1 | 0 |
| .1.3.6.1.4.1.99.1.101.1 | AP - Bridge |

1.3.6.1.4.1.99.2 - SSID



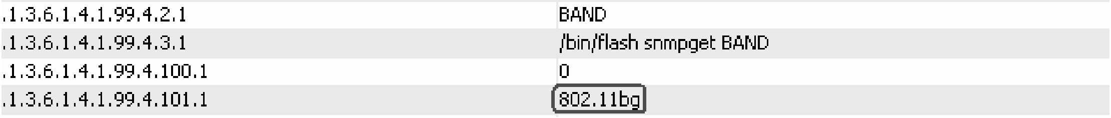
| | |
|---|---|
| .1.3.6.1.4.1.99.2.2.1 | SSID |
| .1.3.6.1.4.1.99.2.3.1 | /bin/flash snmpget SSID |
| .1.3.6.1.4.1.99.2.100.1 | 0 |
| .1.3.6.1.4.1.99.2.101.1 | hank |

## 1.3.6.1.4.1.99.3 - Channel



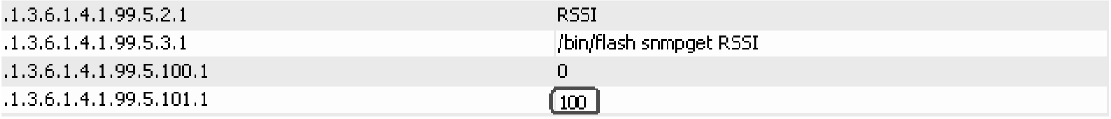
| | |
|---|---|
| .1.3.6.1.4.1.99.3.1.1 | 1 |
| .1.3.6.1.4.1.99.3.2.1 | CHANNEL |
| .1.3.6.1.4.1.99.3.3.1 | /bin/flash snmpget CHANNEL |
| .1.3.6.1.4.1.99.3.100.1 | 0 |
| .1.3.6.1.4.1.99.3.101.1 | 11 |

## 1.3.6.1.4.1.99.4 - Band



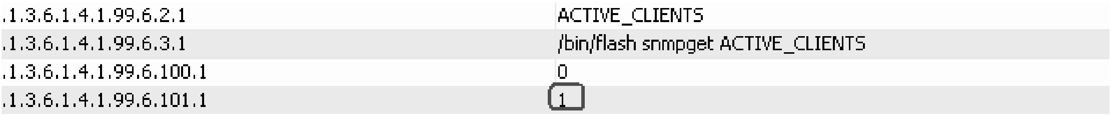
| | |
|---|---|
| .1.3.6.1.4.1.99.4.2.1 | BAND |
| .1.3.6.1.4.1.99.4.3.1 | /bin/flash snmpget BAND |
| .1.3.6.1.4.1.99.4.100.1 | 0 |
| .1.3.6.1.4.1.99.4.101.1 | 802.11bg |

## 1.3.6.1.4.1.99.5 - RSSI



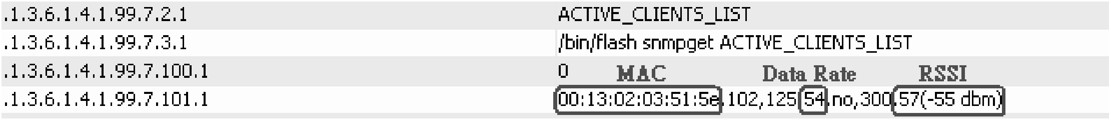
| | |
|---|---|
| .1.3.6.1.4.1.99.5.2.1 | RSSI |
| .1.3.6.1.4.1.99.5.3.1 | /bin/flash snmpget RSSI |
| .1.3.6.1.4.1.99.5.100.1 | 0 |
| .1.3.6.1.4.1.99.5.101.1 | 100 |

## 1.3.6.1.4.1.99.6 - Active_Clients



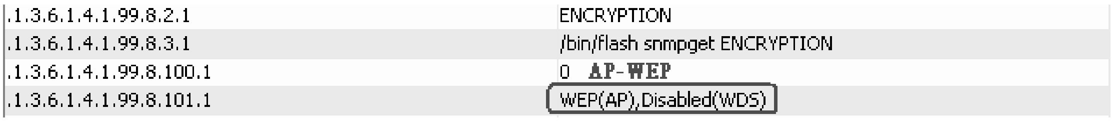
| | |
|---|---|
| .1.3.6.1.4.1.99.6.2.1 | ACTIVE_CLIENTS |
| .1.3.6.1.4.1.99.6.3.1 | /bin/flash snmpget ACTIVE_CLIENTS |
| .1.3.6.1.4.1.99.6.100.1 | 0 |
| .1.3.6.1.4.1.99.6.101.1 | 1 |

## 1.3.6.1.4.1.99.7 - Active_Clients_List



| | |
|---|---|
| .1.3.6.1.4.1.99.7.2.1 | ACTIVE_CLIENTS_LIST |
| .1.3.6.1.4.1.99.7.3.1 | /bin/flash snmpget ACTIVE_CLIENTS_LIST |
| .1.3.6.1.4.1.99.7.100.1 | 0 |
| .1.3.6.1.4.1.99.7.101.1 | 00:13:02:03:51:5e,102,125,54,no,300,57(-55 dbm) |

## 1.3.6.1.4.1.99.8 - Encryption



| | |
|---|---|
| .1.3.6.1.4.1.99.8.2.1 | ENCRYPTION |
| .1.3.6.1.4.1.99.8.3.1 | /bin/flash snmpget ENCRYPTION |
| .1.3.6.1.4.1.99.8.100.1 | 0 |
| .1.3.6.1.4.1.99.8.101.1 | WEP(AP),Disabled(WDS) |

## Firmware Upgrade

### Firmware Types

The firmware for this device is divided into 2 parts, one is web pages firmware the other is application firmware, and the naming usually are **g120webpage.bin** and **g120linux.bin**. To upgrade firmware, we suggest user first upgrade the application firmware then web pages firmware.

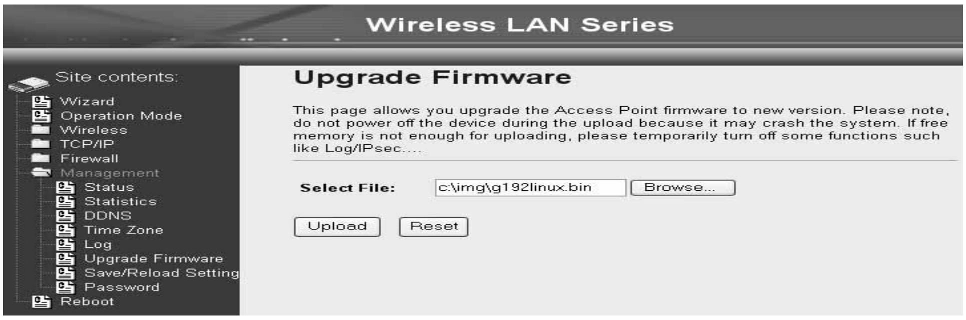
### Upgrading Firmware

The Web-Browser upgrading interface is the simplest and safest way for user, it will check the firmware checksum and signature, and the wrong firmware won’t be accepted. After upgrading, the device will reboot and please note that depends on the version of firmware, the upgrading may cause the device configuration to be restored to the factory default setting, and the original configuration data will be lost!

To upgrade firmware, just assign the file name with full path then click “Upload” button as the following page.

Memory Limitation

To make sure the device have enough memory to upload firmware, the system will check the capacity of free memory, if the device lack of memory to upload firmware, please temporarily turn-off some functions then reboot the device to get enough memory for firmware uploading.



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. If free memory is not enough for uploading, please temporarily turn off some functions such like Log/IPsec....

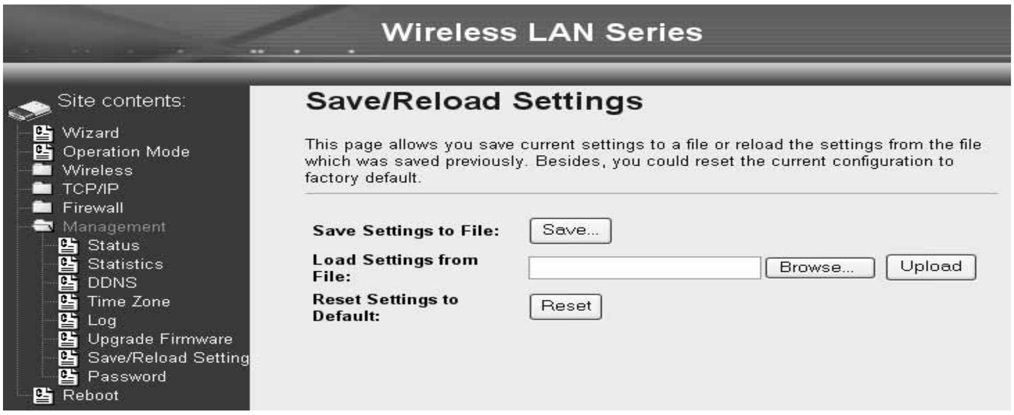
Select File: c:\img\g192linux.bin

## Configuration Data Backup & Restore

Rest Setting to Factory Default Value

Since the device is designed for outdoor used, there is no interface outside the housing to reset the configuration value to the factory default value. The device provides the Web-Browser interface to rest the configuration data. After resetting it, the current configuration data will be lost and restored to factory default value.

Saving & Restoring Configuration Data



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:

To save & restore configuration data of device, just assign the target filename with full path at your local host, then you can backup configuration data to local host or restore configuration data to the device.

## Auto Discovery Tool

User can use this tool to find out how many devices in your local area network
The name of tool is WirelessConf.exe it in the packing CD.

1. **Discover**

   After press this button, you could see there are how many devices in your network. And you would see the basic information about these devices, such as:

   - **SSID**
   - **IP Address**
   - **Subnet Mask**
   - **Channel number**
   - **MAC Address**
   - **Active Client:** this field shows how many clients associated with the device
   - **RSSI:** this field shows Received Signal Strength Indication while device is on AP-Client mode

2. **Setup IP**

   After you press the ***Setup IP*** button, you would see **Setup IP Address** window. You could change device's IP Address, Netmask, and Default Gateway in this window. But if the device's web server needs User Name and Password to login, you should fill in these two fields and then apply changes.

3. **Detail**

   If you want to see more detailed information, you could press the ***Detail*** button, and then you would see the **Detail Information** window.

4. **WDS**

   If the device you selected is on WDS mode or AP+WDS mode, you could press ***WDS*** button, and then you would see the **WDS List** window.

5. **Active Clients**

   After press ***Active Clients*** button, you would see WLAN AP Active Clients window. In this window, you could see client’s information, such as:

6. **Connect to Web Server**
   If you want connect to device’s web server, you could press this button, or double-click on the device.

7. **Close**
   You could press this button to leave this tool.