11g Wireless Multi-Client Bridge/Bridge Router/AP/WDS

User's Manual

Version: 1.36

Table of Contents

1 INTRODUCTION 5

1.1 FEATURES & BENEFITS 5
1.2 PACKAGE CONTENTS 6
1.3 UNIT DESCRIPTION 6
1.4 SYSTEM REQUIREMENTS 6
1.5 APPLICATIONS 6
1.6 NETWORK CONFIGURATION 7
a) Ad-hoc (peer-to-peer) Mode 7
b) Infrastructure Mode 8

2 UNDERSTANDING THE HARDWARE 9

2.1 HARDWARE INSTALLATION 9
2.2 IP ADDRESS CONFIGURATION 9

3 SWITCH BETWEEN BRIDGE/ BRIDGE ROUTER/ AP 11

3.1 BRIDGE/BRIDGE ROUTER TO ACCESS POINT 11
3.2 ACCESS POINT TO BRIDGE/BRIDGE ROUTER 12

4 BRIDGE MODE – WEB CONFIGURATION 13

4.1 LOGGING IN 13
4.2 MANAGEMENT 14
4.2.1 OPERATION MODE 14
4.2.2 STATUS 16
4.2.3 STATISTICS 17
4.2.4 LOG 17
4.2.5 UPGRADE FIRMWARE 18
4.2.6 SAVE / RELOAD SETTINGS, RESET TO DEFAULT 18
4.2.7 PASSWORD 19
4.3 TCP/IP SETTINGS 20
4.3.1 LAN INTERFACE 20
4.4 WIRELESS 21
4.4.1 BASIC SETTINGS (INFRASTRUCTURE, ADHOC) 21
4.4.2 ADVANCED SETTINGS (INFRASTRUCTURE, ADHOC) 22
4.4.3 SECURITY 24
4.4.3.1 ENCRYPTION DISABLED 24
4.4.3.2 WEP 64-BIT / 128-BIT 24
4.4.3.3 WPA / WPA2 PASSPHRASE 26
4.4.3.4 WPA / WPA2 RADIUS AUTHENTICATION 27
4.4.4 SITE SURVEY 28

5 ACCESS POINT MODE – WEB CONFIGURATION 29

5.1 LOGGING IN 29
5.2 MANAGEMENT 30
5.2.1 OPERATION MODE 30
5.2.2 STATUS 31
5.2.3 STATISTICS 33
5.2.4 LOG 33
5.2.5 UPGRADE FIRMWARE 34
5.2.6 SAVE / RELOAD SETTINGS, RESET TO DEFAULT 34
5.2.7 PASSWORD 35
5.3 TCP/IP SETTINGS 35
5.3.1 LAN INTERFACE 35
5.3.1.1 STATIC IP ADDRESS 36

5.3.1.2 DHCP CLIENT 37
5.3.1.3 DHCP SERVER 38
5.4 WIRELESS 39
5.4.1 BASIC SETTINGS 40
5.4.2 ADVANCED SETTINGS 40
5.4.3 SECURITY 42
5.4.3.1 ENCRYPTION DISABLED 42
5.4.3.2 WEP 64-BIT / 128-BIT 43
5.4.3.3 WPA / WPA2 / WPA2 MIXED PASSPHRASE 44
5.4.3.4 WPA / WPA2 / WPA2 MIXED RADIUS AUTHENTICATION 45
5.4.4 ACCESS CONTROL 46
5.4.5 WDS 47

APPENDIX A – SPECIFICATIONS 49

APPENDIX B – FCC INTERFERENCE STATEMENT 50

Revision History

Version	Date	Notes
1.36	April 26, 2006	

1 Introduction

The Wireless Client Bridge/Bridge Router/Access Point/WDS (wireless distribution system) operates seamlessly in the 2.4 GHz frequency spectrum supporting the 802.11b (2.4GHz, 11Mbps) and faster 802.11g (2.4GHz, 54Mbps) wireless standards. It's the best way to add wireless capability to your existing wired network, or to add bandwidth to your wireless installation.

NCB-3220 has high transmitted output power and high receivable sensitivity. High output power and high sensitivity can extend range and coverage to reduce the roaming between APs to get more stability wireless connection. It also can reduce the expense of equipment in the same environment.

To protect your wireless connectivity, it can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA/WPA2. The MAC address filter lets you select exactly which stations should have access to your network.

This chapter describes the features & benefits, package contents, applications, and network configuration.

1.1 Features & Benefits

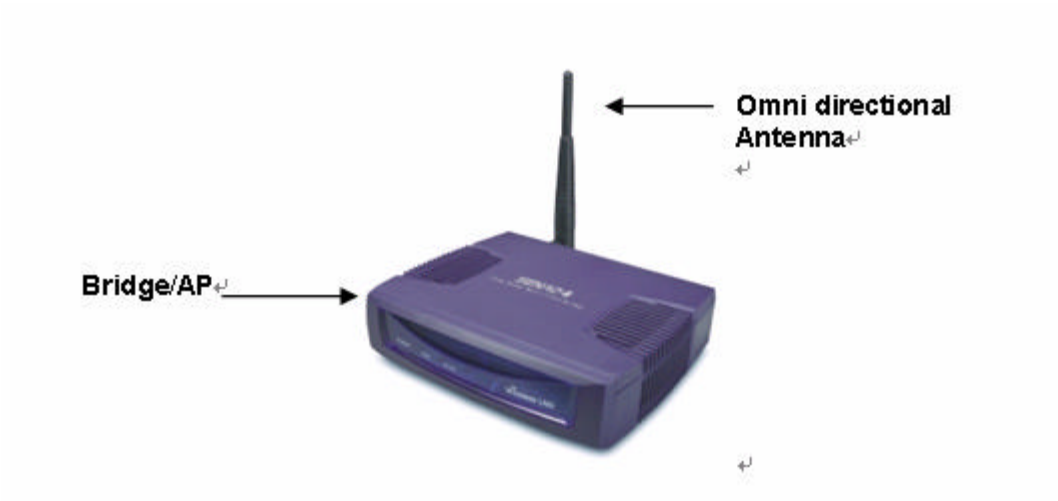
Features	Benefits
High Speed Data Rate Up to 54Mbps	Capable of handling heavy data payloads such as MPEG video streaming
High Output Power and High Sensitivity	Spreads the operation distance and reduce the roaming between APs to get more stability wireless connection
Point-to-point, Point-to-multipoint Wireless Connectivity	Let users transfer data between two buildings or multiple buildings
WPA2/WPA/ IEEE 802.1x Authenticator support	More Powerful data security
WDS (Wireless Distribution System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater
Watertight and Weatherproof	Avoid water invaded and weather corroded
Wide temperature range and robust mechanical design	Delivers reliable, top performance in the most demanding environments
MAC address filtering (AP Mode)	Ensures secure network connection
Power-over-Ethernet (IEEE802.3af Compliant)	Flexible Access Point locations and cost savings

1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- One Wireless Client Bridge Unit
- One Power Adapter (12V/ 1A)
- One CAT5 UTP Cable
- One CD-ROM with User's Manual

1.3 Unit Description



1.4 System Requirements

The following are the minimum system requirements in order configure the device.

- PC/AT compatible computer with a Ethernet interface.
- Operating system that supports HTTP web-browser

1.5 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) **The ability to access real-time information**
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) **Frequently changed environments**
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) **Small Office and Home Office (SOHO) networks**
SOHO users need a cost-effective, easy and quick installation of a small network.

f) **Wireless extensions to Ethernet networks**
Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) **Wired LAN backup**
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) **Training/Educational facilities**
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

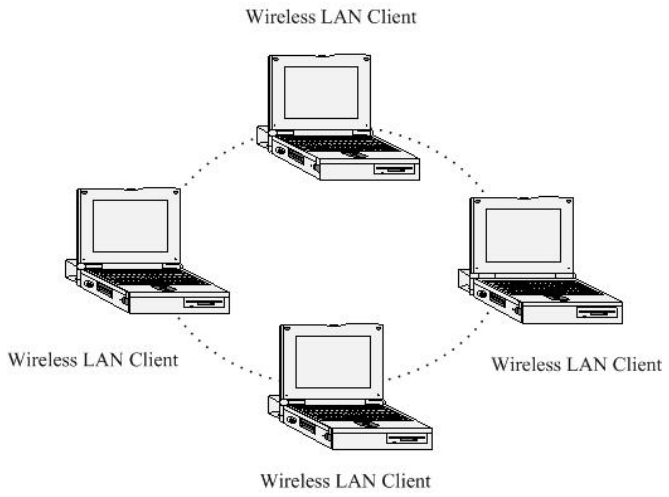
1.6 Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
b) Infrastructure for enterprise LANs.

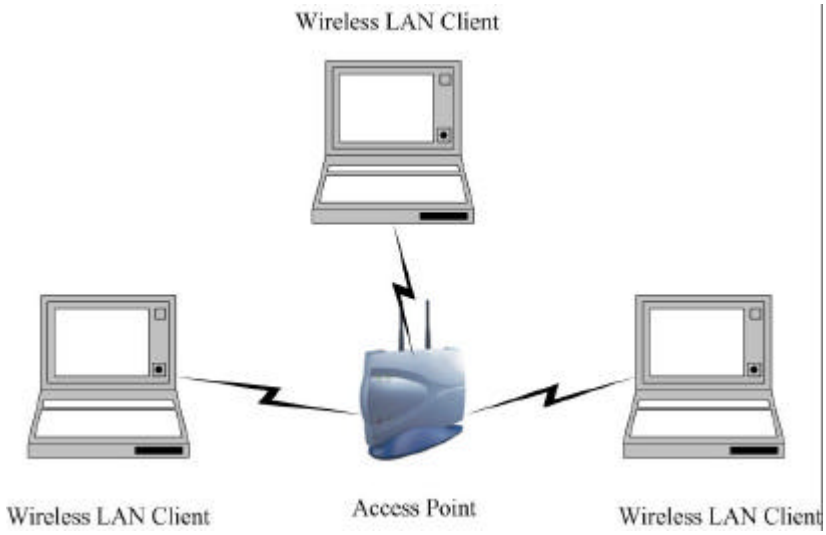
a) Ad-hoc (peer-to-peer) Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.

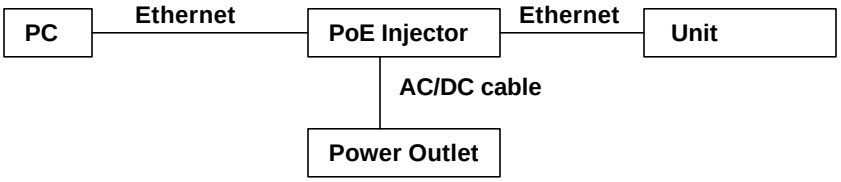


2 Understanding the Hardware

2.1 Hardware Installation

1. Place the unit in an appropriate pace using the mounting kit.
2. Run the Ethernet cable indoors and plug it into the PoE injector port labeled "AP/Router".
3. Plug one end of another Ethernet cable into your PC/Notebook and the other end into the PoE injector port labeled "Network".
4. Insert the DC-inlet of the power adapter into the PoE injector port labeled "DC240V" and the other end into the power socket on the wall.

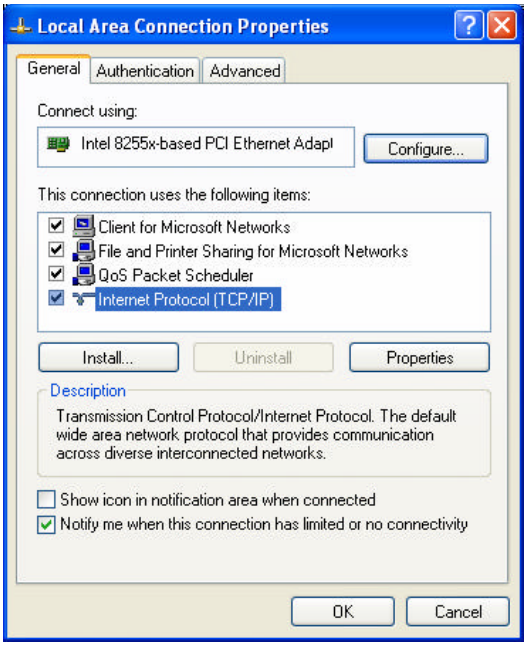
This diagram depicts the hardware configuration



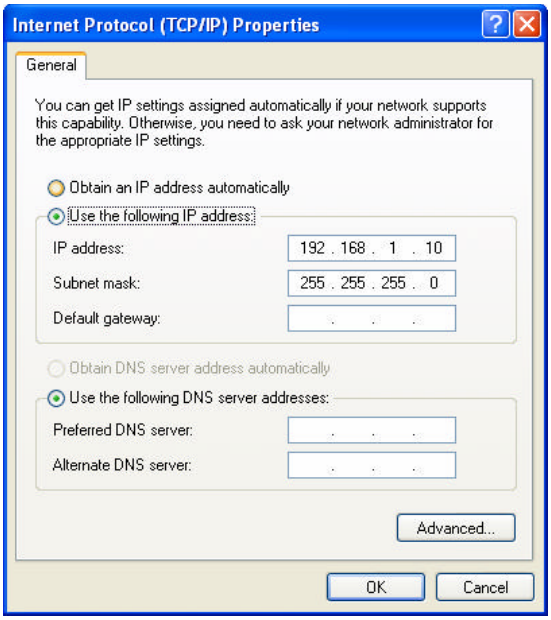
2.2 IP Address Configuration

This device can be configured as a Bridge or Access Point. The default IP address of the device is **192.168.1.1**. In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook.



3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.
   For Example: Device IP address: 192.168.1.1
   PC IP address: 192.168.1.10
   PC subnet mask: 255.255.255.0

4. Click on the **OK** button to close this window, and once again to close LAN properties window.

3 Switch between Bridge/ Bridge Router/ AP

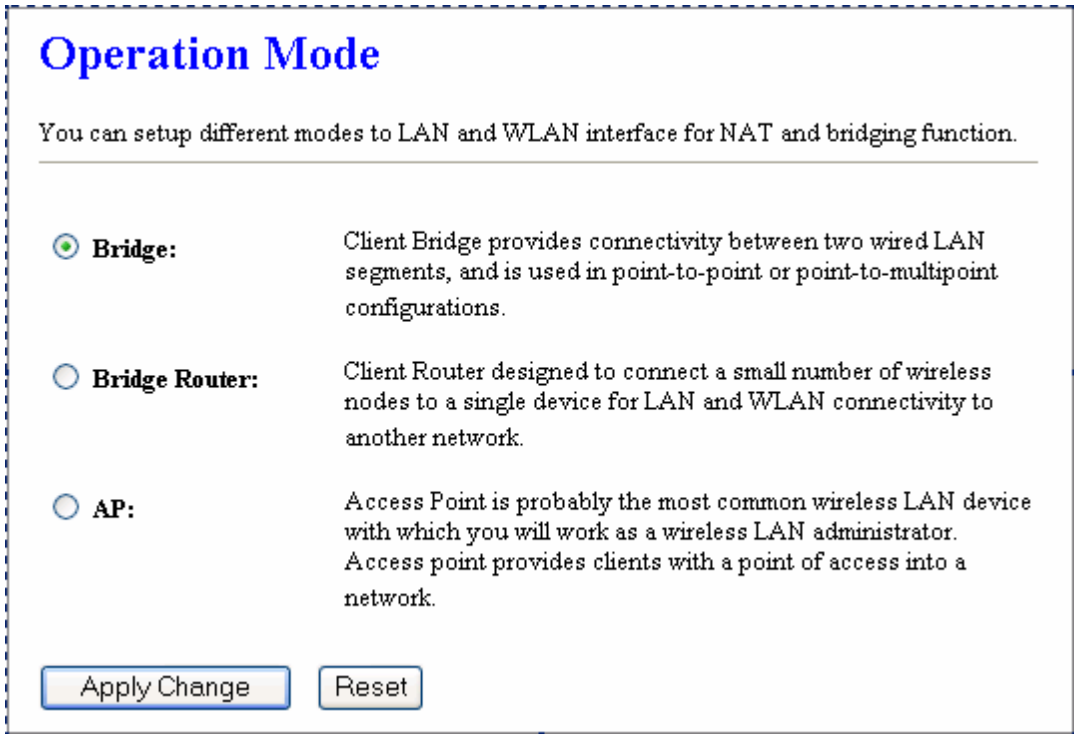
This device can be configured as a Bridge or Access Point. The default IP address of the device is **192.168.1.1** in Bridge mode. This chapter will describe the steps to switch from Bridge to Access Point and Access Point to Bridge.

3.1 Bridge/Bridge Router to Access Point

1 Enter the default IP address (192.168.1.1) of the bridge into the address bar of the web-browser.

2 By default, a user name and password has not been configured. If you have configured a user name and password, please enter them into the field to continue

3 Once you have logged in, click on the **Operation Mode** link under the **Management** menu.



4 Since this device is currently in Bridge mode, the **Bridge** radio button will be selected by default.

5 Select the **AP** radio button to and then click on the **Apply Change** to switch the operation mode to Access Point.

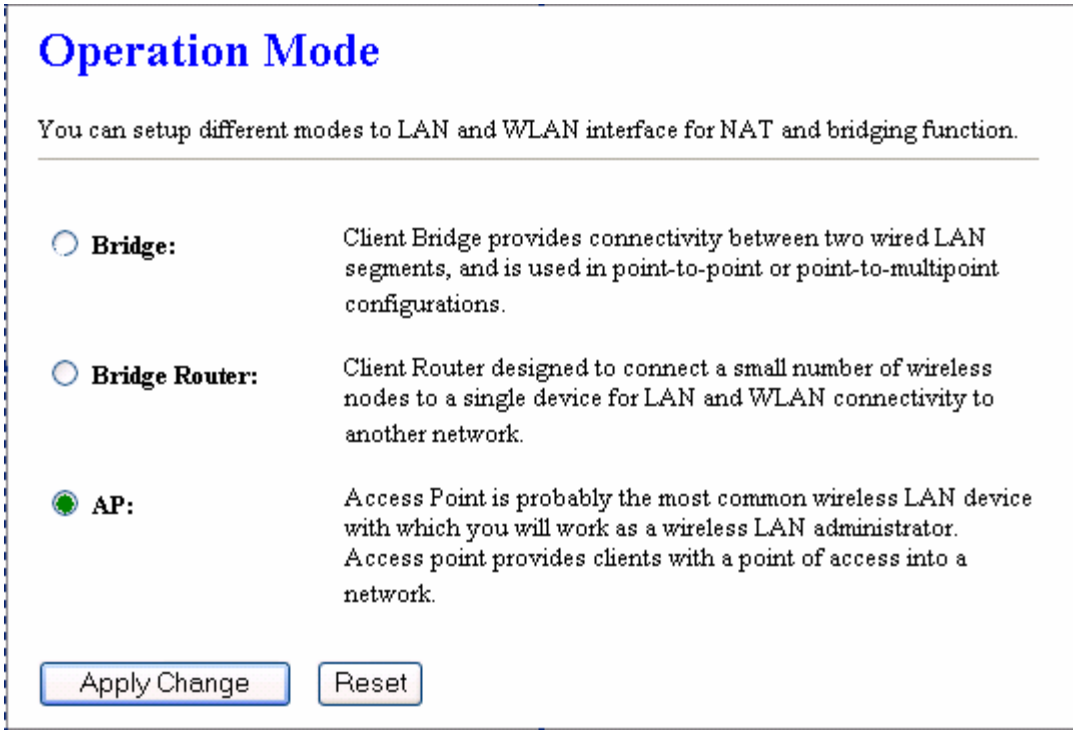
6 Wait for about 1 minute and the device will automatically restart into Access Point mode.

3.2 Access Point to Bridge/Bridge Router

1 Enter the default IP address (192.168.1.2) of the bridge into the address bar of the web-browser.

2 By default, a user name and password has not been configured. If you have configured a user name and password, please enter them into the field to continue

3 Once you have logged in, click on the **Operation Mode** link under the **Management** menu.



4 Since this device is currently in Access Point mode, the **AP** radio button will be selected by default.

5 Select the **Bridge or Bridge Router** radio button to and then click on the **Apply Change** to switch the operation mode to Bridge.

6 Wait for about 1 minute and the device will automatically restart into Bridge mode.

4 Bridge Mode – Web Configuration

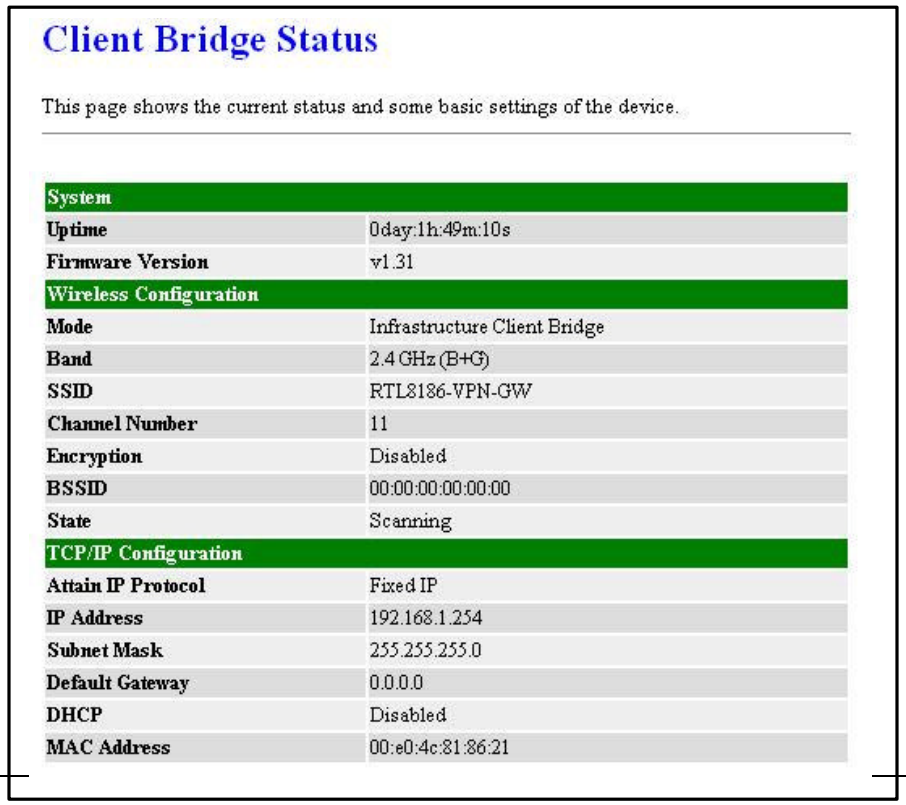
4.1 Logging In

- To configure the Bridge through the web-browser, enter the IP address of the Bridge (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.

- Make sure that the Bridge and your computers are on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- Username：**admin**; Password：**admin**
- After logging in you will graphical user interface (GUI) of the bridge. The navigation drop-down menu on left is divided into three main sections:

1. **Management**: This includes operation mode, status, statistics, logs, upgrade firmware, save/reload settings, and password.
2. **TCP/IP Settings**: This includes the configuration of the LAN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
3. **Wireless**: This includes the basic, advanced, security and site-survey settings for the wireless interface.

- The Bridge status page is also displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.



Client Bridge Status

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

System	
Uptime	0day:1h:49m:10s
Firmware Version	v1.31
Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	RTL8186-VPN-GW
Channel Number	11
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:e0:4c:81:86:21

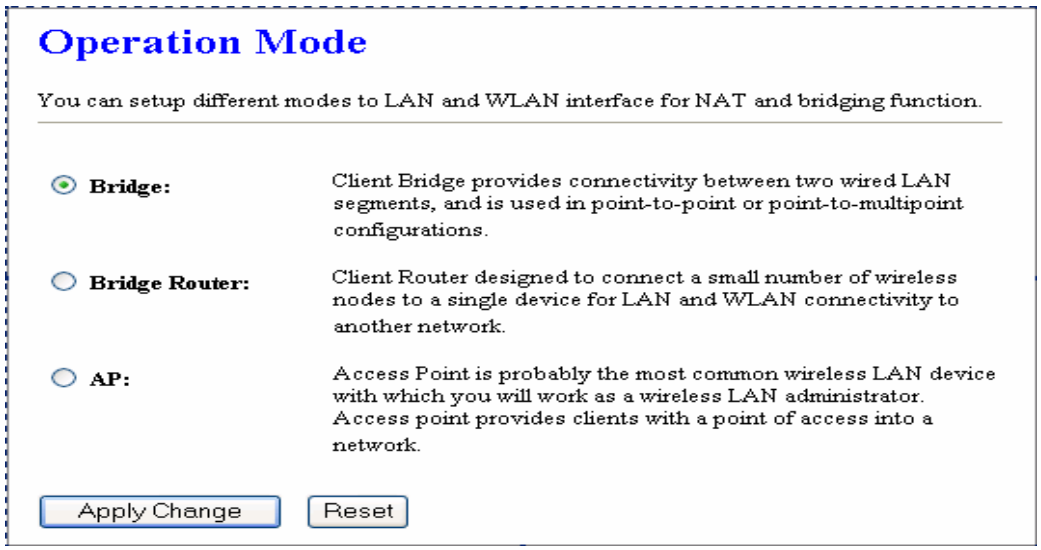
- **System**
  - **Uptime:** Duration of time since the device was last reset.
  - **Firmware version**: Version of the firmware that is currently loaded on the device.
- **Wireless Configuration**:
  - **Mode**: Wireless configuration mode such as client bridge, AP, or WDS.
  - **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
  - **SSID**: The name used to identify the wireless network.
  - **Channel Number**: The channel used to communicate on the wireless network.
  - **Encryption**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
  - **BSSID**: The MAC address of the SSID.
  - **State**: The current state of the bridge. It may be scanning or associated or disabled.
- **TCP/IP Configuration:**
  - **Attain IP Protocol**: The IP address setting may be fixed or static.
  - **IP Address**: Displays the current IP address of the LAN port.
  - **Subnet Mask**: Displays the current subnet mask for the IP address.
  - **Default Gateway**: Displays the default gateway for the device.
  - **DHCP**: Displays the DHCP setting.
  - **MAC Address**: Displays the MAC address of the device.

4.2 Management

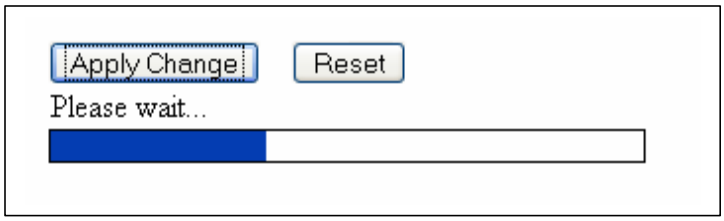
- Click on the **Management** link on the navigation drop-down menu. You will then see five options: operation mode, status, statistics, log, upgrade firmware, save/reload settings, and password. Each option is described below.

4.2.1 Operation Mode

- Click on the **Operation Mode** link under the **Management** menu. The **Operation Mode** allows you to switch from Client Bridge to Access Point mode.



- Select the **AP**, **Bridge** or **Bridge Router** and then click on the **Apply Change** button.



- Wait for about a minute until you see the following Pop-Up message.

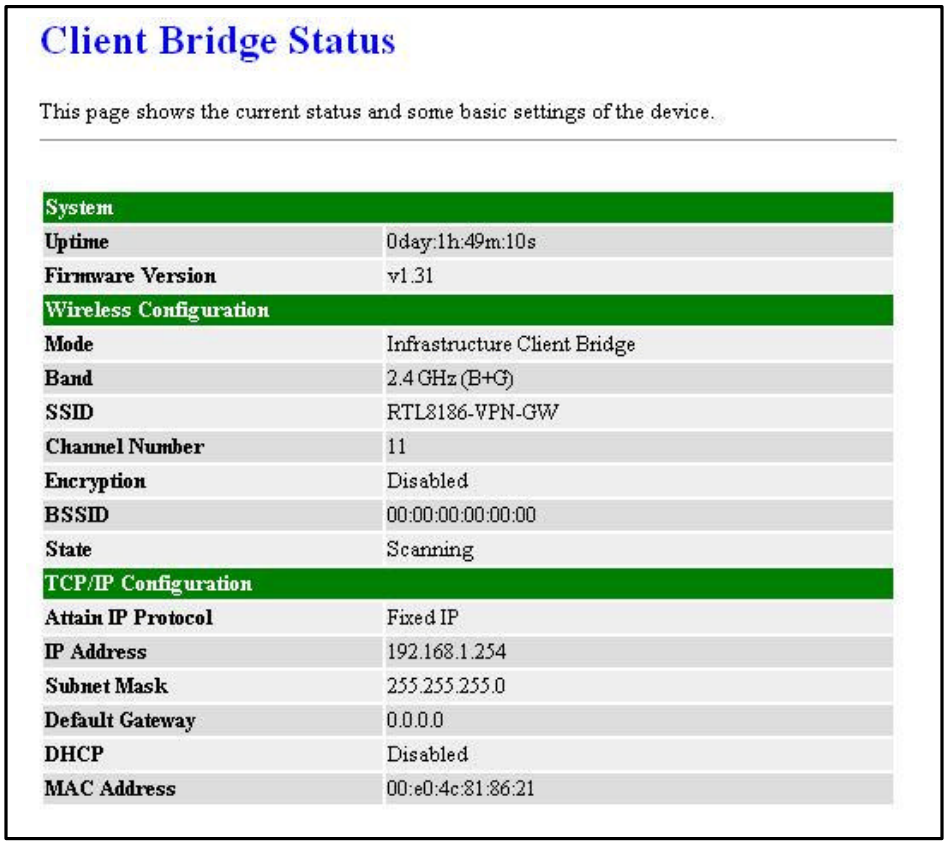
- Click on the **OK** button and then enter the specified IP address into the web-browser.

Switch to other mode, the configuration settings will continue using.

- Refer to **Chapter 5** to learn how to configure this device in Access Point mode.

4.2.2 Status

- Click on the **Status** link under the **Management** menu. The **Status** page is the first page that is displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.



Client Bridge Status

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

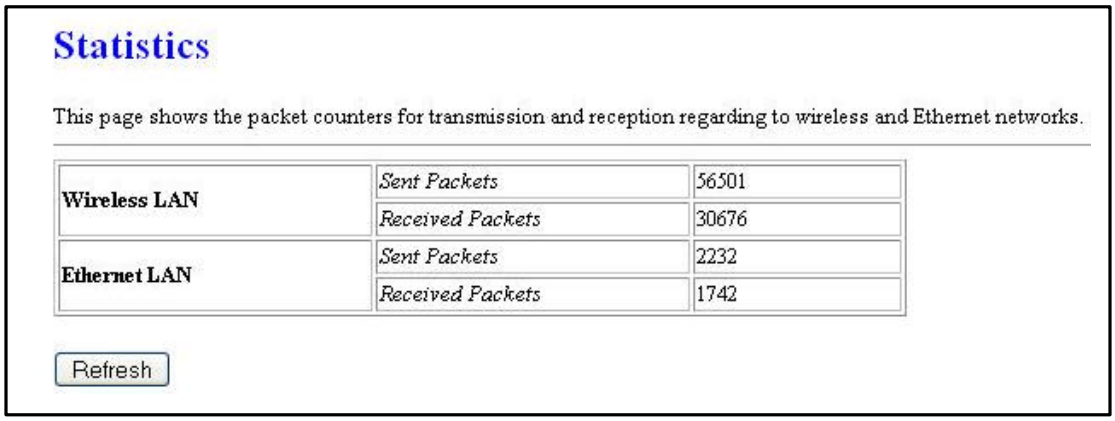
System	
Uptime	0day:1h:49m:10s
Firmware Version	v1.31
Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	RTL8186-VPN-GW
Channel Number	11
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:e0:4c:81:86:21

- **System**
  - **Uptime:** Duration of time since the device was last reset.
  - **Firmware version**: Version of the firmware that is currently loaded on the device.
- **Wireless Configuration**:
  - **Mode**: Wireless configuration mode such as client bridge, AP, or WDS.
  - **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
  - **SSID**: The name used to identify the wireless network.
  - **Channel Number**: The channel used to communicate on the wireless network.
  - **Encryption**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
  - **BSSID**: The MAC address of the SSID.
  - **State**: The current state of the bridge. It may be scanning or associated or disabled.
- **TCP/IP Configuration:**
  - **Attain IP Protocol**: The IP address setting may be fixed or static.
  - **IP Address**: Displays the current IP address of the LAN port.
  - **Subnet Mask**: Displays the current subnet mask for the IP address.
  - **Default Gateway**: Displays the default gateway for the device.

- **DHCP**: Displays the DHCP setting.
- **MAC Address**: Displays the MAC address of the device.

4.2.3 Statistics

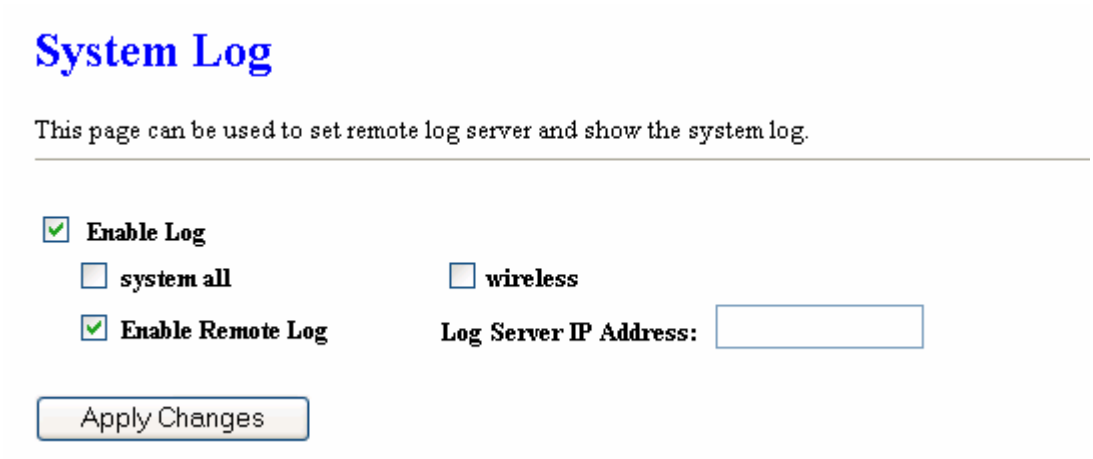
- Click on the **Statistics** link under the **Management** menu. This page displays the number of sent and received packets on the Ethernet and Wireless interface.



- Since the packet counter is not dynamic, you must click on the **Refresh** button for the most recent statistics.

4.2.4 Log

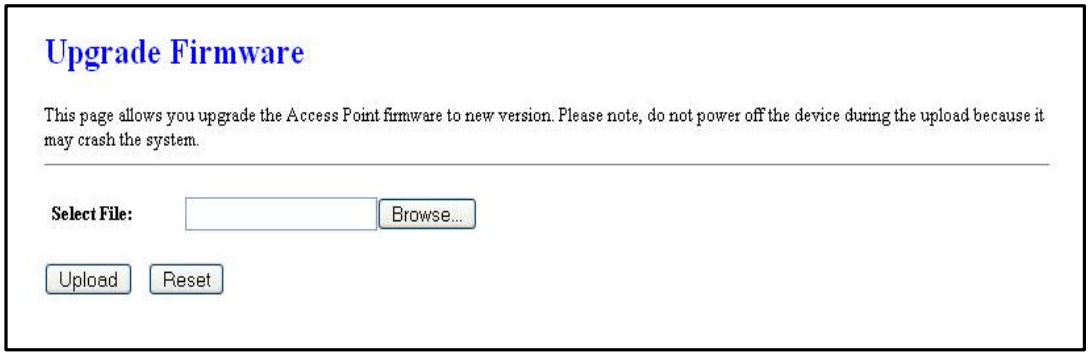
- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.



- In order for the log to record all the events, you must first place a check in the **Enable Log** or **Enable Remote Log (Log Server required)** check box.
- Select **system all** or **wireless** depending on the type of events you want recorded.
- Since the log is not dynamic, you must click on the **Refresh** button for the most recent events, or click on the **Clear** button to clear the log.

4.2.5 Upgrade Firmware

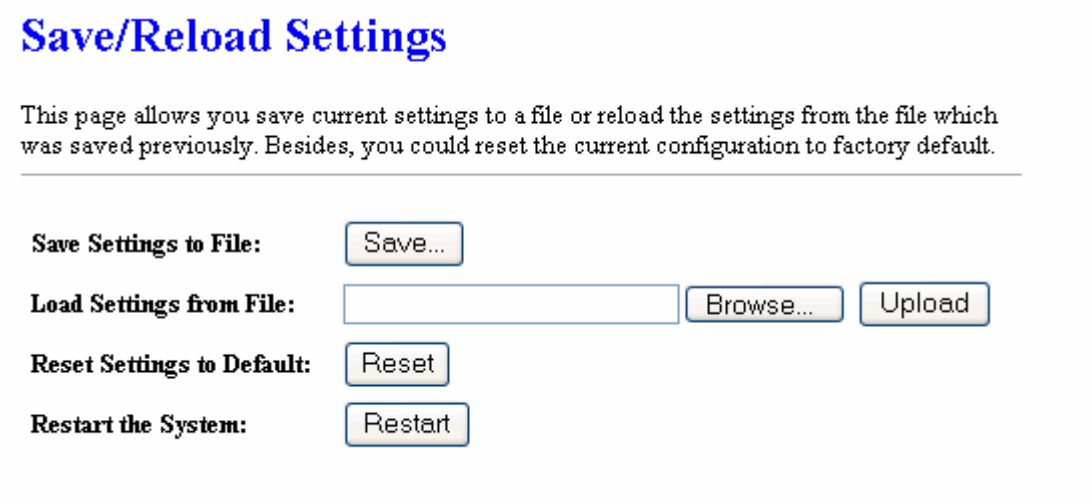
- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



- Click on the Browse button and then select the appropriate firmware and then click on the **Upload** button.
  Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

4.2.6 Save / Reload Settings, Reset to Default

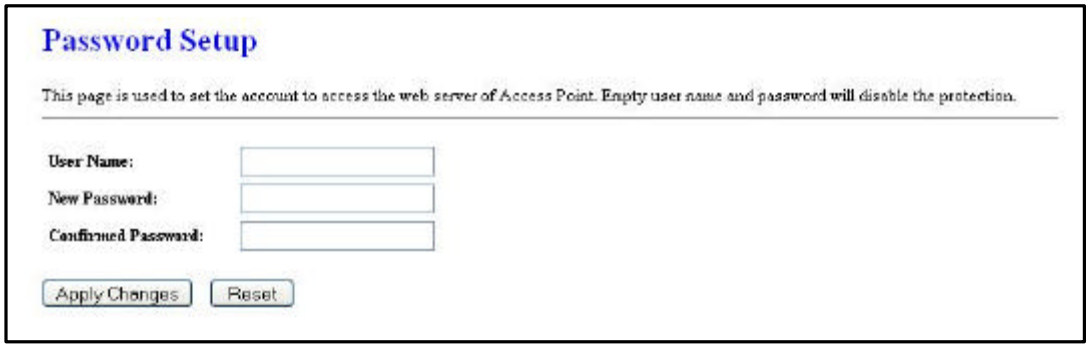
- Click on the **Save / Reload Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.
- This page also allows you to reset the device to its factory default settings.



- Click on the **Save** button to save the current settings to a file on the local disk.
- Click on the **Browse** button to select the settings file and then click on the Upload button to load the previously saved settings.
- Click on the **Reset** button to reset the device to its factory default settings. Click **Restart** to reboot the device.

4.2.7 Password

- Click on the **Password** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password. For security reasons it is highly recommended that you create a user name and password.



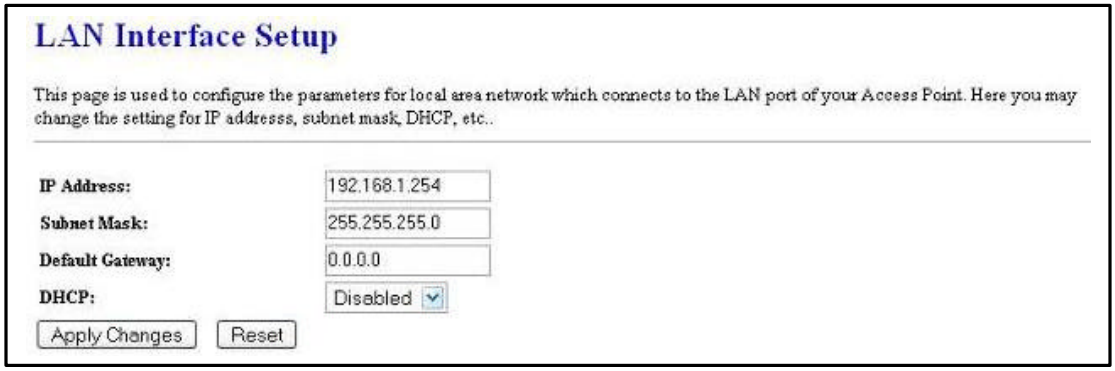
- Enter a **user name** into the first field.
- Enter a password into the **New Password** field and then re-type the password into the **Confirmed Password** field. Then click on the **Apply Changes** button.
- By clicking on the **Reset** button, the user name and password fields will become blank indicating that the username and password has been disabled.

4.3 TCP/IP Settings

- Click on the **TCP/IP Settings** link on the navigation drop-down menu. You will then see the LAN Interface option. This option is described in detail below.

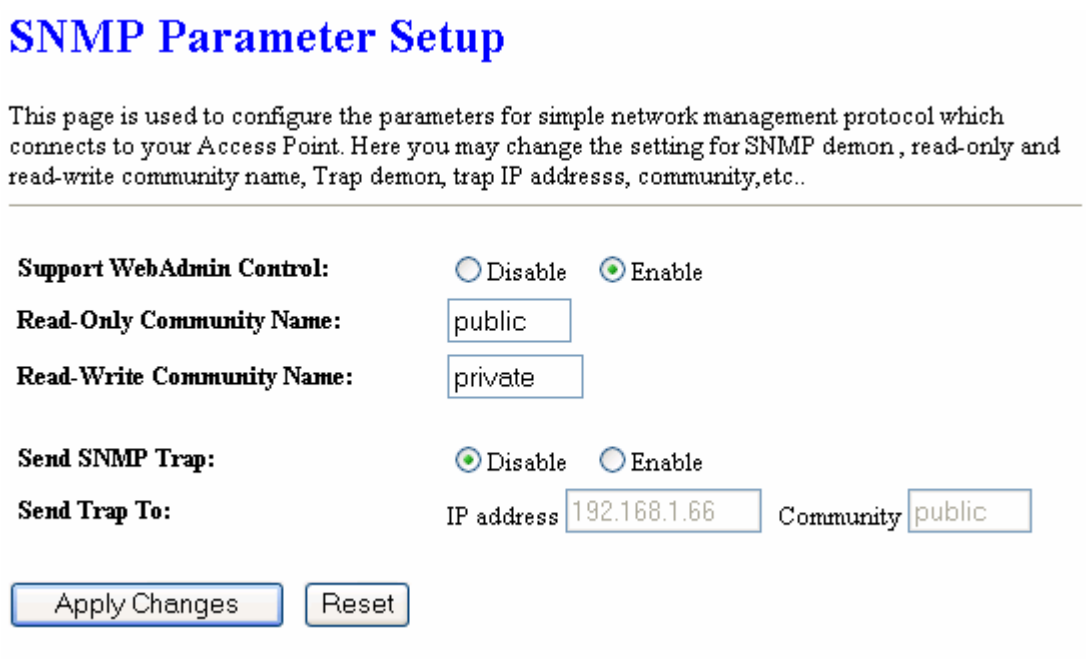
4.3.1 LAN Interface

- Click on the **LAN Interface** link under the **TCP/IP Settings** menu. Using this option you may change the IP address of the device as well as toggle the DHCP and 802.1d spanning tree feature.



- **IP Address**: Enter the IP address.
- **Subnet Mask**: Enter the subnet mask for the IP address.
- **Default Gateway**: Enter the IP address for the default gateway.
- **DHCP**: If this device is a DHCP client and will receive its IP settings from a DHCP server, then select **Enabled** from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is **Disabled**, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.3.2 SNMP Settings



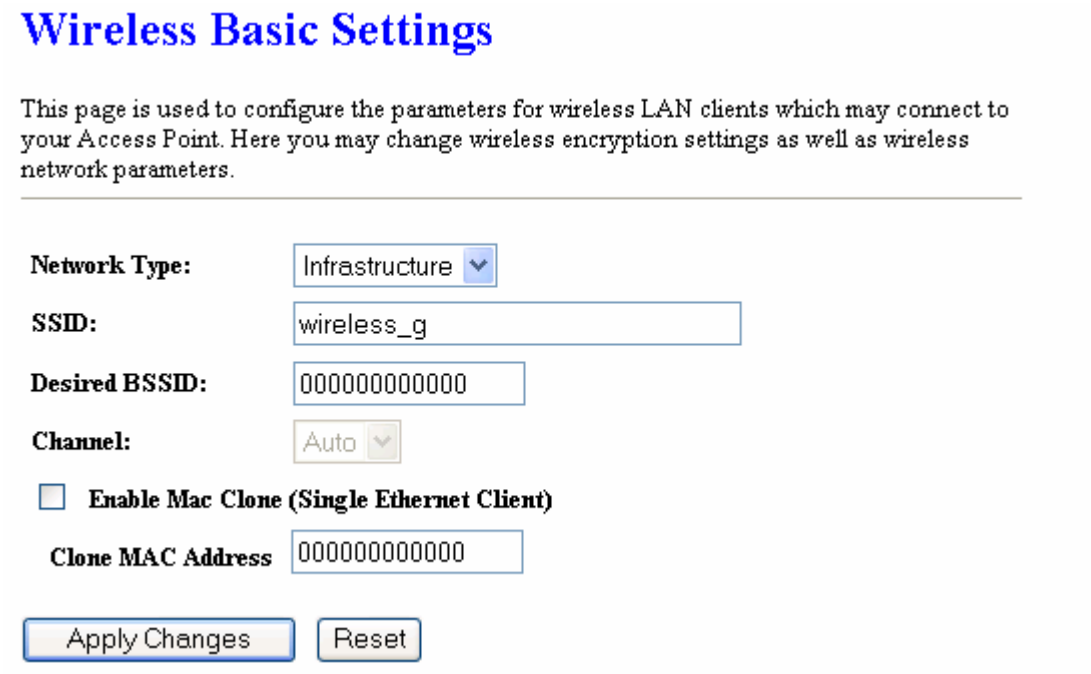
- Check **Enable** to activate the SNMP and then configure the **Read/Write Community** Strings.
- Enable **Send SNMP Trap** to activate the SNMP Trap Agent and input the IP address of SNMP Trap Host.

4.4 Wireless

- Click on the **Wireless** link on the navigation drop-down menu. You will then see four options: basic settings, advanced settings security and site survey. Each option is described below.

4.4.1 Basic Settings (Infrastructure, Adhoc)

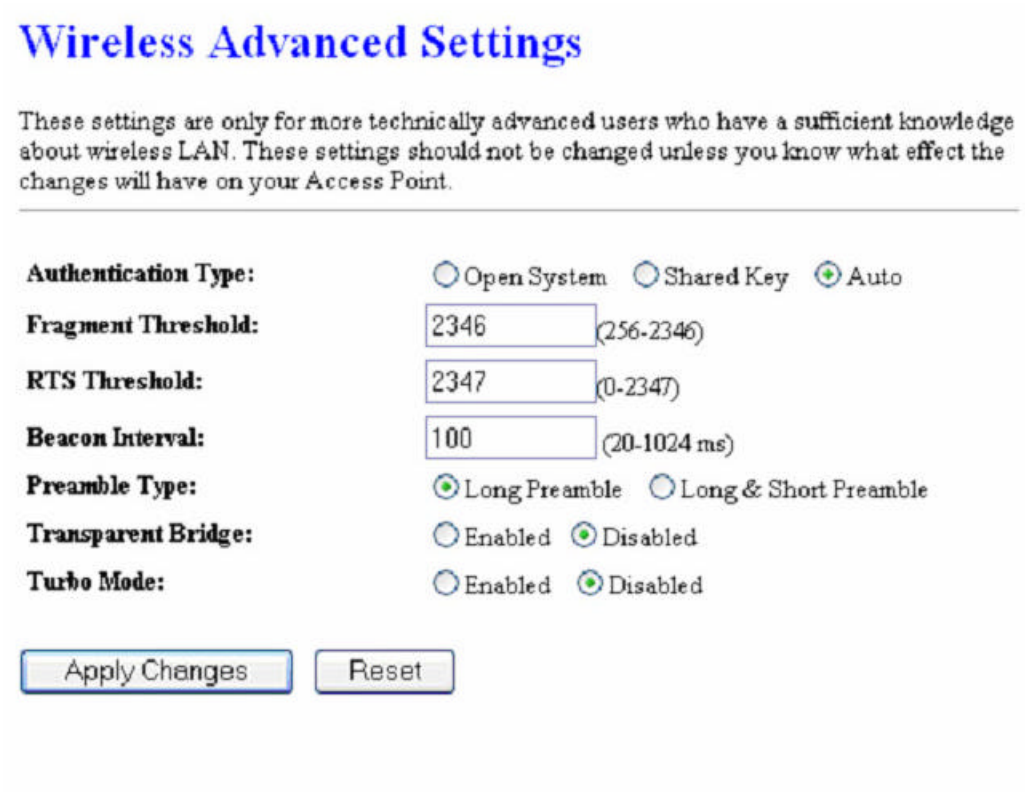
- Click on the **Basic Settings** link under the **Wireless** menu. Using this option you may configure the 802.11b/g settings as well as the frequency, channel, and SSID.



- **Network Type:** Select **Infrastructure** or **Adhoc** from the drop-down list. Infrastructure is a point-to-multipoint (PtMp) topology where as Adhoc is a point-to-point topology (PtP).
- **SSID**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. Enter the MAC address of AP Radio IF for **Desired BSSID**.
- **Channel**: Select a channel from the drop-down list. The channels available are based on the country's regulation. When selecting Infrastructure mode, a channel is not required, however, when selecting Adhoc mode, you must select the same channel on all points.
- **Enable MAC cloning**: Change the Bridge's MAC to the connected Client's MAC which is the first client connects with Bridge. This function only allow one Client connect to network.
- **Clone MAC Address**: Bridge's MAC will be defined by the value in blank space.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.2 Advanced Settings (Infrastructure, Adhoc)

- Click on the **Advanced Settings** link under the **Wireless** menu. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: fragmentation threshold, RTS threshold, beacon interval, output power, preamble type, and 802.11g protection.



- **Authentication Type:** select an authentication method. Options available are **Open System**, **Shared Key** or **Auto**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- **Fragment Threshold**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Beacon Interval**: Beacons will be sent out to devices at the specified intervals. This value is measured in milliseconds (ms).
- **Preamble Type**: For best performance, all devices on the wireless network should use the same preamble type. However, the wireless network will still function even though the wrong preamble type is used.

- **Transparent Bridge:** check **Enable** to activate the Transparent Bridging Function.

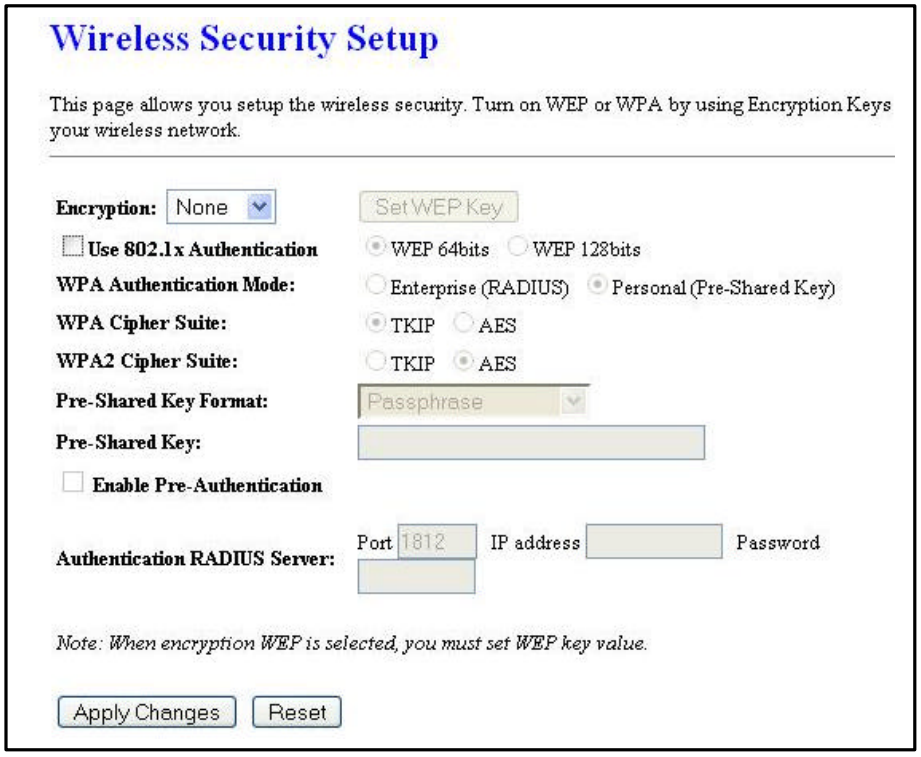
- **Turbo Mode:** Select "**Enable**" to activate the Turbo mode for better performance. The Default is disabled.

- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.3 Security

- Click on the **Security** link under the **Wireless** menu. On this page you can configure the authentication and encryption settings such as WEP, WPA, and 80.1x.

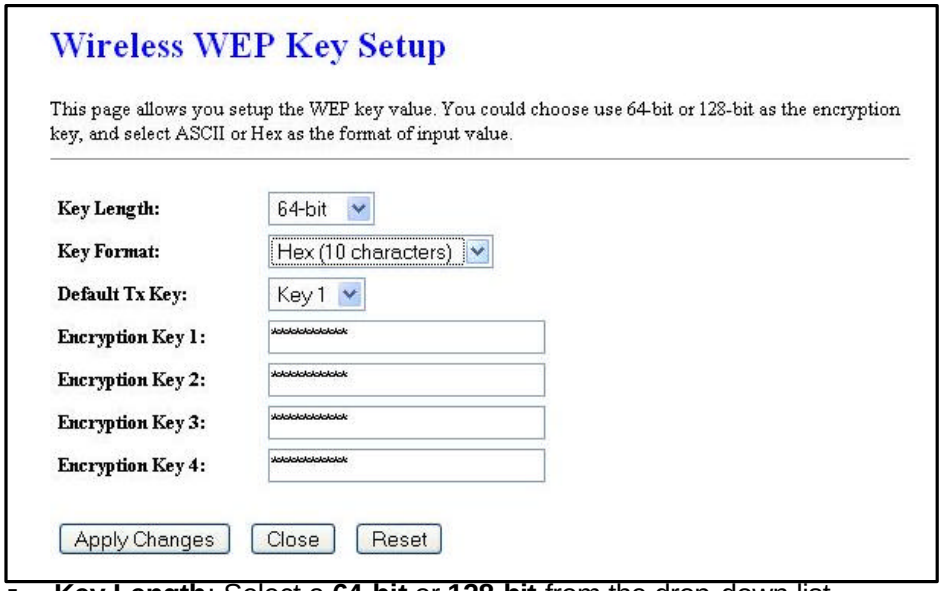
4.4.3.1 Encryption Disabled



- **Encryption**: Select **None** from the drop-down list if your wireless network does not use any type of encryption.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.3.2 WEP 64-bit / 128-bit

- **Encryption**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- **Set WEP Key**: Click on this button to configure the WEP Key.

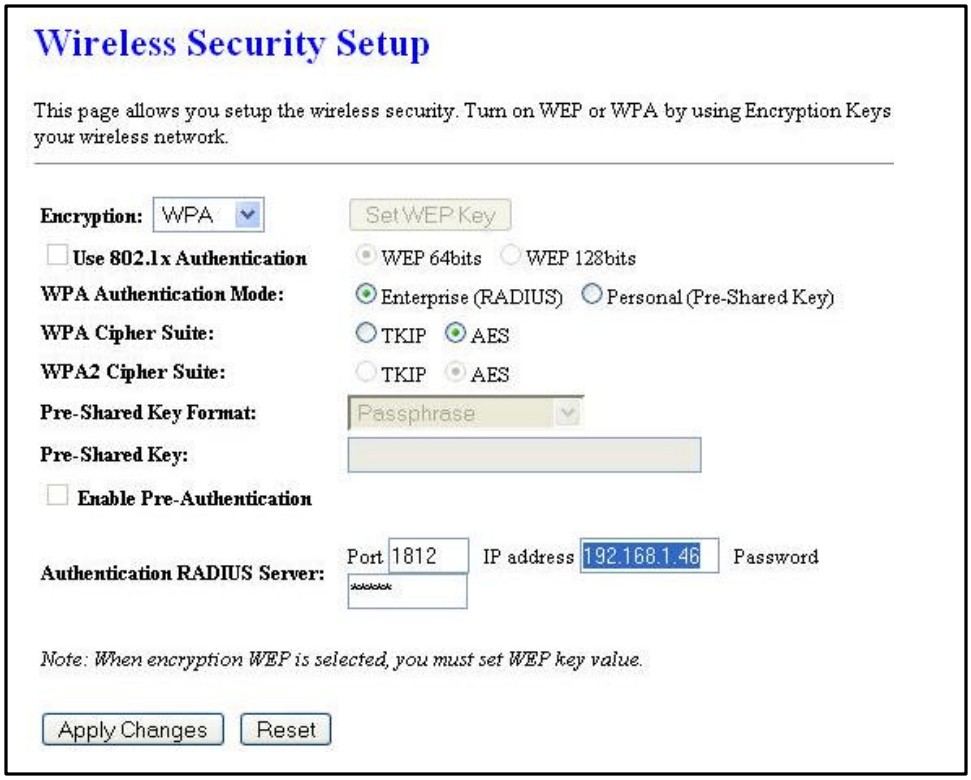


- **Key Length**: Select a **64-bit** or **128-bit** from the drop-down list.
- **Key Format:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Default Tx Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Encryption Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply Changes** button to confirm the changes and then click on the **Close** button to return to the pervious window.

4.4.3.3 WPA / WPA2 Passphrase

- **Encryption**: Select **WPA** or **WPA2** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **WPA Authentication Mode**: Select the **Personal (Pre-Shared Key)** radio button.
- **WPA/WPA2**: Select **TKIP** or **AES** as the cipher suite.
- **Pre-Shared Key Format**: Select **Passphrase** from the drop-down list.
- **Pre-Shared Key**: Enter the pass phrase here, this should be between 8 and 63 characters.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

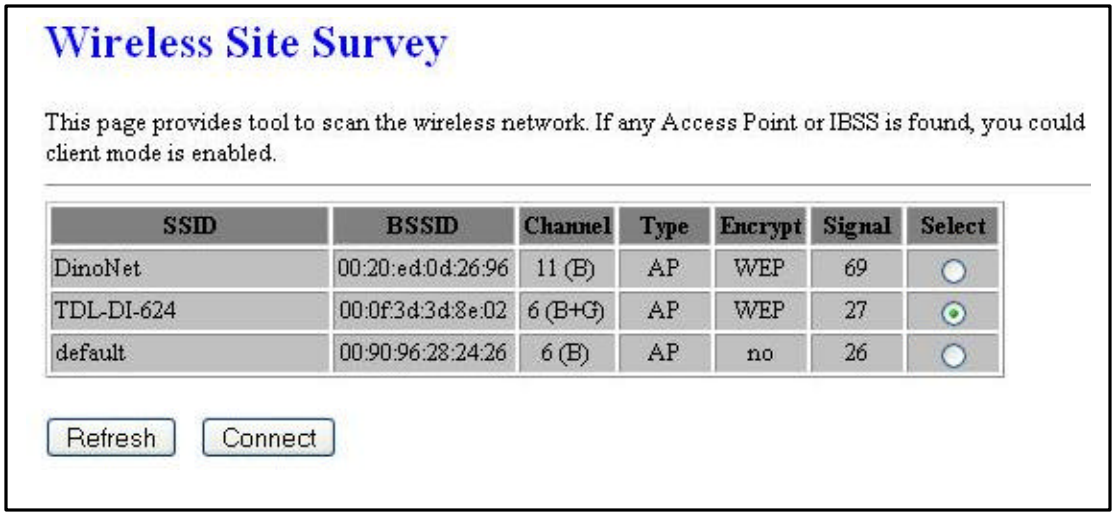
4.4.3.4 WPA / WPA2 RADIUS Authentication



- **Encryption**: Select **WPA** or **WPA2** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **WPA Authentication Mode**: Select the **Enterprise (RADIUS)** radio button.
- **WPA/WPA2**: Select **TKIP** or **AES** as the cipher suite.
- **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.
- **RADIUS IP Address:** Enter the IP address of the RADIUS server.
- **RADIUS Password:** Enter the shared password of the RADIUS server.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.4 Site Survey

- Click on the **Site Survey** link under the **Wireless** menu. This page displays the list of Access Points in the coverage area and allows you to connect to them if you have the required credentials.



- The site survey table lists the following:
  - SSID: This is the unique name of the wireless network.
  - BSSID: This is the MAC address of the Access Point.
  - Channel: This indicates the current channel that the Access Point is operating on, along with the 802.11 network type (B, G, or B+G).
  - Encrypt: This indicates the encryption type.
  - Signal: This indicates the signal strength of the Access Point.
- You may select the radio button of a specific Access Point and then click on the **Conenct** button. If the credentials of this device match that of the Access Point that you will be connected immediately, if not, you must specify the appropriate credentials.
- You may click on the Refresh button at any time to re-scan the area.

5 Access Point Mode – Web Configuration

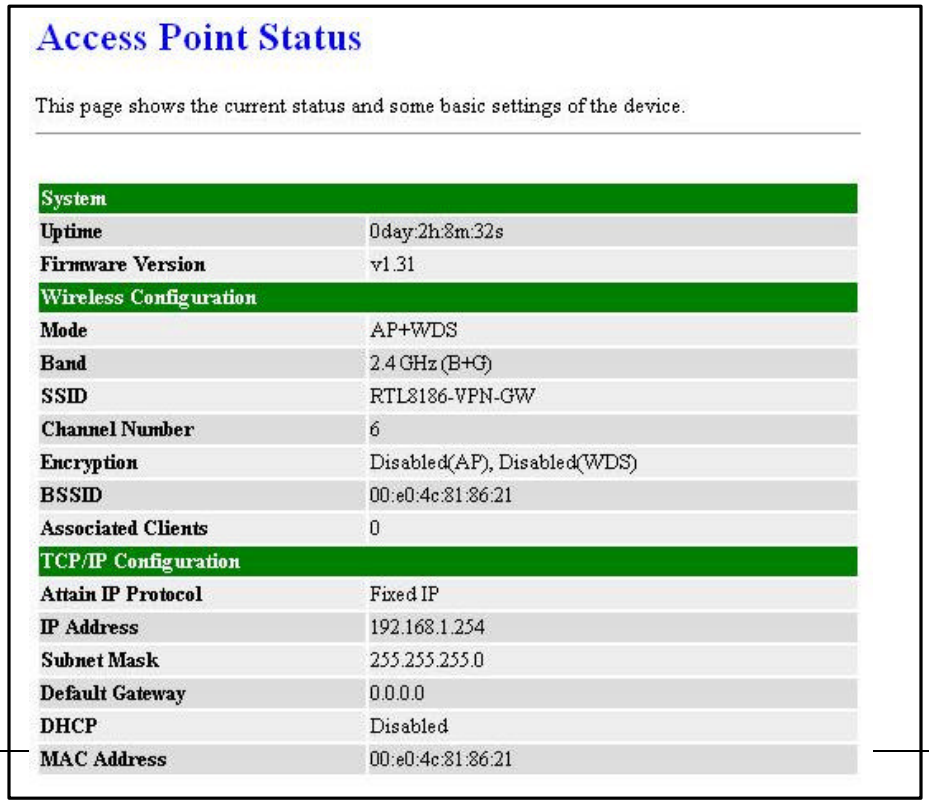
5.1 Logging In

- To configure the Access Point through the web-browser, enter the IP address of the Bridge (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.

- Make sure that the Access Point and your computers are on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- Log in User name：**admin**; Password：**admin**
- After logging in you will graphical user interface (GUI) of the Access Point. The navigation drop-down menu on left is divided into three main sections:

4. **Management**: This includes operation mode, status, statistics, logs, upgrade firmware, save/reload settings, and password.
5. **TCP/IP Settings**: This includes the configuration of the LAN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
6. **Wireless**: This includes the basic, advanced, security and site-survey settings for the wireless interface.

- The Access Point status page is also displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.



Access Point Status

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

System	
Uptime	0day:2h:8m:32s
Firmware Version	v1.31
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	RTL8186-VPN-GW
Channel Number	6
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:e0:4c:81:86:21
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:e0:4c:81:86:21

- **System**
  - **Uptime:** Duration of time since the device was last reset.
  - **Firmware version**: Version of the firmware that is currently loaded on the device.
- **Wireless Configuration**:
  - **Mode**: Wireless configuration mode such as client bridge, AP, or WDS.
  - **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
  - **SSID**: The name used to identify the wireless network.
  - **Channel Number**: The channel used to communicate on the wireless network.
  - **Encryption**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
  - **BSSID**: The MAC address of the SSID.
  - **Associated Clients**: Displays the number of clients currently associated to the Access Point.
- **TCP/IP Configuration:**
  - **Attain IP Protocol**: The IP address setting may be fixed or static.
  - **IP Address**: Displays the current IP address of the LAN port.
  - **Subnet Mask**: Displays the current subnet mask for the IP address.
  - **Default Gateway**: Displays the default gateway for the device.
  - **DHCP**: Displays the DHCP setting.
  - **MAC Address**: Displays the MAC address of the device.

5.2 Management

- Click on the **Management** link on the navigation drop-down menu. You will then see five options: operation mode, status, statistics, log, upgrade firmware, save/reload settings, and password. Each option is described below.

5.2.1 Operation Mode

- Click on the **Operation Mode** link under the **Management** menu. The **Operation Mode** allows you to switch from Access Point to Client Bridge mode.