11b/g Wireless Outdoor Client Bridge/AP

User’s Manual
Version: 2.2
5.2.6 SAVE / RELOAD SETTINGS, RESET TO DEFAULT .................................................................38
5.2.7 PASSWORD ..........................................................................................................................39
5.3 TCP/IP SETTINGS ....................................................................................................................40
5.3.1 LAN INTERFACE ................................................................................................................40
5.3.1.1 STATIC IP ADDRESS .......................................................................................................40
5.3.1.2 DHCP CLIENT ..................................................................................................................41
5.3.1.3 DHCP SERVER ................................................................................................................42
5.3.2 SNMP SETTINGS ..................................................................................................................43
5.4 WIRELESS .............................................................................................................................43
5.4.1 BASIC SETTINGS ................................................................................................................44
5.4.2 ADVANCED SETTINGS ........................................................................................................45
5.4.3 SECURITY ............................................................................................................................47
5.4.3.1 ENCRYPTION DISABLED .................................................................................................47
5.4.3.2 WEP 64-BIT / 128-BIT .....................................................................................................48
5.4.3.3 WPA / WPA2 / WPA2 MIXED PASSPHRASE ..................................................................49
5.4.3.4 WPA / WPA2 / WPA2 MIXED RADIUS AUTHENTICATION ...........................................50
5.4.4 ACCESS CONTROL .............................................................................................................51
5.4.5 WDS .....................................................................................................................................52

APPENDIX A – SPECIFICATIONS ...............................................................................................54
APPENDIX B – FCC INTERFERENCE STATEMENT ......................................................................55
APPENDIX C – IC STATEMENT ....................................................................................................56
### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.36</td>
<td>April 26, 2006</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>January 24, 2007</td>
<td>Add one option with built-in 16dBi Antenna</td>
</tr>
<tr>
<td>2.1</td>
<td>June 19, 2007</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>September 30, 2007</td>
<td>PM Editing</td>
</tr>
</tbody>
</table>
1 Introduction

The Outdoor Wireless Bridge/Client Router/AP/Repeater 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.

EOC-3220 Series 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

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Speed Data Rate Up to 54Mbps</td>
<td>Capable of handling heavy data payloads such as MPEG video streaming</td>
</tr>
<tr>
<td>High Output Power EIRP up to 35 dBm</td>
<td>Excellent output power spreads the operation distance</td>
</tr>
<tr>
<td>(with 9 dBi Patch Antenna)</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.11b/g Compliant</td>
<td>Fully Interoperable with IEEE 802.11b/802.11g compliant devices</td>
</tr>
<tr>
<td>Watertight and Weatherproof</td>
<td>Avoid water invaded and weather corroded for outdoor environment</td>
</tr>
<tr>
<td>SNMP Remote Configuration Management</td>
<td>Help administrators to remotely configure or manage the Access Point easily.</td>
</tr>
<tr>
<td>Point-to-point, Point-to-multipoint</td>
<td>Let users transfer data between two buildings or multiple buildings</td>
</tr>
<tr>
<td>Wireless Connectivity</td>
<td></td>
</tr>
<tr>
<td>WPA2/WPA/IEEE 802.1x support</td>
<td>Powerful data security</td>
</tr>
<tr>
<td>Hide SSID (AP Mode)</td>
<td>Avoids unallowable users sharing bandwidth, increases efficiency of the network</td>
</tr>
<tr>
<td>DHCP Client/Server</td>
<td>Simplifies network administration</td>
</tr>
<tr>
<td>WDS (Wireless Distributed System)</td>
<td>Make wireless AP and Bridge mode simultaneously as a wireless repeater</td>
</tr>
</tbody>
</table>
11b/g Wireless Outdoor Client Bridge/AP

**Universal Repeater**
- The easiest way to expand your wireless network’s coverage

**MAC address filtering (AP mode)**
- Ensures secure network connection

**User isolation support (AP mode)**
- Protect the private network between client users.

**PPPoE function support (CR mode)**
- Easy to access internet via ISP service authentication

**Power-over-Ethernet (IEEE802.3af)**
- Flexible Access Point locations and cost savings

**Keep personal setting**
- Keep the latest setting when firmware upgrade

### 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 Outdoor Wireless Client Bridge unit
- 48V, 0.375A AC/DC adapter with wall-plug power cable
- Inline Power Injector (PoE)
- 1.8m Grounding Cable
- User’s manual CD-ROM
- Wall mounting kit
- Mast mounting kit
- Waterproof kit

### 1.3 Outdoor Unit Description

![Diagram of Outdoor Unit with built-in antenna and external antenna connector.](image)
C) Outdoor Unit with built-in 16dbi Patch antenna

1.5 Ethernet cable water proof kit Install Guide

Install the Ethernet cable with the waterproof kits shown as below pictures 1~4.

1.6 Mounting Install Guide

a) Pole mounting
1) Lock the bracket on device.
2) Using hoop to fix on pole and bind with U-clamp.
3) Adjust degree of device.
4) Using washer screw to lock with device.

b) Wall mounting
1) Lock the bracket on device.
2) Lock the wall mount bracket on wall.
3) Adjust degree of device.
4) Using washer screw to lock with device.

1.7 System Requirements

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

- PC/AT compatible computer with an Ethernet interface.
- Operating system that supports HTTP web-browser
1.8 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.

1.9 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 outdoor 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

![Diagram of 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.

![Network Connections properties window]
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.

**Operation Mode**

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

- **Bridge:** Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.
- **Bridge Router:** Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.
- **AP:** Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.

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.

**Operation Mode**

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

- **Bridge**: Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.
- **Bridge Router**: Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.
- **AP**: Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.

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/Bridge Router 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**: 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**: Infrastructure Client Bridge
- **Band**: 2.4 GHz (b+g)
- **SSID**: wireless_g
- **Channel Number**: 5
- **Encryption**: Disabled
- **BSSID**: 00:00:00:00:00:00
- **State**: Scanning
- **Signal Strength**: 0.00
- **Noise Level**: 0.00

**TCP/IP Configuration**
- **Attain IP Protocol**: Fixed IP
- **IP Address**: 192.168.1.1
- **Subnet Mask**: 255.255.255.0
- **Default Gateway**: 0.0.0.0
- **DHCP**: Disabled
- **MAC Address**: 00:02:56:46:1b:0f

- **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.
  - **Signal Strength**: The signal strength of the wireless device.
  - **Noise Level**: The level of interference.

- **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.

**Operation Mode**

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

- **Bridge:** Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.

- **Bridge Router:** Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.

- **AP:** Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.

  ![Apply Change]  ![Reset]

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

  ![Apply Change]  ![Reset]

  Please wait...
Please wait and then enter the specified IP address into the web-browser. The previous settings will be retained in AP mode.
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.

<table>
<thead>
<tr>
<th>System</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>0day 0h 17m 37s</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>v1.39.06</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Infrastructure Client Bridge</td>
</tr>
<tr>
<td>Band</td>
<td>2.4GHz (B+C)</td>
</tr>
<tr>
<td>SSID</td>
<td>wireless_g</td>
</tr>
<tr>
<td>Channel Number</td>
<td>5</td>
</tr>
<tr>
<td>Encryption</td>
<td>Disabled</td>
</tr>
<tr>
<td>BSSID</td>
<td>00:00:00:00:00:00</td>
</tr>
<tr>
<td>State</td>
<td>Scanning</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>0.0</td>
</tr>
<tr>
<td>Noise Level</td>
<td>0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP/IP Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto IP Protocol</td>
<td>Fixed IP</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>DHCP</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:02:61:40:3b:66</td>
</tr>
</tbody>
</table>

- **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.
- **Signal Strength**: The signal strength of the wireless device.
- **Noise Level**: The level of interference.

### 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.

#### Statistics

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

<table>
<thead>
<tr>
<th></th>
<th>Sent Packets</th>
<th>Received Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>65301</td>
<td>39575</td>
</tr>
<tr>
<td>Ethernet</td>
<td>2222</td>
<td>1742</td>
</tr>
</tbody>
</table>

- 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.

**System Log**

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

- 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.

**Upgrade Firmware**

This page allows you to 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.
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.

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.

- 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.

**Password Setup**

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

- 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 and SNMP option. The options 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 setting.
LAN Interface Setup

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

- **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

**SNMP Parameter Setup**

This page is used to configure the parameters for the simple network management protocol which connects to your device. Here you may change the setting for SNMP daemon, read-only and read-write community name, Trap daemon, trap IP address.

- **SNMP Daemon**: Select **Enable** if you would like to use the SNMP feature.
- **Read-Only Community Name**: Specify the password for access to the SNMP community for read-only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap**: Select **Enable** if you would like to receive SNMP traps.
- **Send Trap To**: Specify the IP address that would receive the SNMP traps.
- **Trap Community Name**: Specify the password for the SNMP trap community.
- Click on the **Save Settings** button once you have modified the settings.
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.

**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.

- **Band:** Depending on the type of wireless clients that are connected to the network, you may select B, G, or B+G. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select B+G for the best performance.
- **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 (PIP).
- **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.
- **Desired BSSID:** Enter the MAC address of AP Radio.
- **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 Universal Repeater Mode**: Select Enable to activate Universal Repeater Mode and type below SSID for extended wireless interface.

### 4.4.2 Advanced Settings

- 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.

#### Wireless Advanced Settings

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Open System, Shared Key, Auto</td>
</tr>
<tr>
<td><strong>Fragment Threshold</strong></td>
<td>2246 (2-2346)</td>
</tr>
<tr>
<td><strong>RTS Threshold</strong></td>
<td>2347 (0-2347)</td>
</tr>
<tr>
<td><strong>Beacon Interval</strong></td>
<td>100 (20-1024 ms)</td>
</tr>
<tr>
<td><strong>Ack Timeout</strong></td>
<td>0 (0-235 x 4 us)</td>
</tr>
<tr>
<td><strong>Data Rate</strong></td>
<td>Auto</td>
</tr>
<tr>
<td><strong>Output Power Level (OFDM)</strong></td>
<td>High</td>
</tr>
<tr>
<td><strong>Output Power Level (CCK)</strong></td>
<td>High</td>
</tr>
<tr>
<td><strong>Preamble Type</strong></td>
<td>Long Preamble, Long &amp; Short Preamble</td>
</tr>
<tr>
<td><strong>Transparent Bridge</strong></td>
<td>Enabled, Disabled</td>
</tr>
</tbody>
</table>

- **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).
- **ACK Timeout**: You may specify a value for the acknowledge timeout.
- **Data Rate**: Select a data rate from the drop-down list. However, it is recommended to select **auto** for the best performance.
- **Output Power Level (OFDM/CCK)**: You may have different application distances of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **You can arrange the different data rate in distance in Bridge mode. Please refer below table. This table only for 11g and 11b/g mix mode**

<table>
<thead>
<tr>
<th></th>
<th>6M-24M</th>
<th>36M</th>
<th>48M</th>
<th>54M</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ultra High</td>
<td>✓</td>
<td>✓</td>
<td>Great</td>
<td>N/A</td>
</tr>
<tr>
<td>Super</td>
<td>✓</td>
<td>Great</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Extreme</td>
<td>Great</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- **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**: Select **Enable** to activate the Transparent Bridging feature. The MAC address of this device will be transparent, and clients from either side of the network will be able to pick each other. The connected AP shall be 3220 series.
- **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

**Wireless Security Setup**

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

```plaintext
<table>
<thead>
<tr>
<th>Encryption:</th>
<th>None</th>
<th>Set WEP Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use 802.1x Authent.</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>WPA Authentication</td>
<td>Enterprise (RADIUS)</td>
<td>Personal (Pre-Shared Key)</td>
</tr>
<tr>
<td>WPA Cipher Suite:</td>
<td>TKIP</td>
<td>AES</td>
</tr>
<tr>
<td>WPA2 Cipher Suite:</td>
<td>TKIP</td>
<td>AES</td>
</tr>
<tr>
<td>Pre-Shared Key Format:</td>
<td>Passphrase</td>
<td></td>
</tr>
<tr>
<td>Pre-Shared Key:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Pre-Authent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication RADIUS Server:</td>
<td>Port 612</td>
<td>IP Address</td>
</tr>
</tbody>
</table>
```

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

- **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

Wireless Security Setup

This page allows you to set up the wireless security. Turn on WEP or WPA by using Encryption Keys:

- **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.

**Wireless WEP Key Setup**

This page allows you to set up 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:**
- **Key Format:**
- **Default Tx Key:**
- **Encryption Key 1:**
- **Encryption Key 2:**
- **Encryption Key 3:**
- **Encryption Key 4:**
- **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, whereas 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 previous window.

### 4.4.3.3 WPA / WPA2 Passphrase

#### Wireless Security Setup

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

<table>
<thead>
<tr>
<th>Encryption:</th>
<th>WPA2</th>
<th>Set WEP Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use 802.1x Authentication</td>
<td></td>
<td>WEP 64bit ○ WEP 128bit</td>
</tr>
<tr>
<td>WPA Authentication Mode:</td>
<td>○ Enterprise (RADIUS) ○ Personal (Pre-Shared Key)</td>
<td></td>
</tr>
<tr>
<td>WPA Cipher Suite:</td>
<td>○ TKIP ○ AES</td>
<td></td>
</tr>
<tr>
<td>WPA2 Cipher Suite:</td>
<td>○ TKIP ○ AES</td>
<td></td>
</tr>
<tr>
<td>Pre-Shared Key Format:</td>
<td>Passphrase</td>
<td></td>
</tr>
<tr>
<td>Pre-Shared Key:</td>
<td>12345</td>
<td></td>
</tr>
<tr>
<td>Enable Pre-Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication RADIUS Server:</td>
<td>Port 812</td>
<td>IP address 192.168.1.46</td>
</tr>
</tbody>
</table>

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

- **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

### Wireless Security Setup

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

<table>
<thead>
<tr>
<th>Encryption: WPA</th>
<th>WPA Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use 802.1x Authentication</td>
<td>WEP 64bits</td>
</tr>
<tr>
<td>WPA Authentication Mode:</td>
<td>WEP 128bits</td>
</tr>
<tr>
<td>WPA Cipher Suite:</td>
<td>Enterprise (RADIUS)</td>
</tr>
<tr>
<td>WPA2 Cipher Suite:</td>
<td>Personal (Pre-Shared Key)</td>
</tr>
<tr>
<td>Pre-Shared Key Format:</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Pre-Shared Key:</td>
<td></td>
</tr>
<tr>
<td>Enable Pre-Authentication</td>
<td></td>
</tr>
<tr>
<td>Authentication RADIUS Server:</td>
<td>Port 1812 IP address 192.168.0.48 Password</td>
</tr>
</tbody>
</table>

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

- **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.

**Wireless Site Survey**

This page provides tool to scan the wireless network. If any Access Point or BSSID is found, you could client mode is enabled.

<table>
<thead>
<tr>
<th>SSID</th>
<th>BSSID</th>
<th>Channel</th>
<th>Type</th>
<th>Encrypt</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirecNet</td>
<td>00:20:30:36:96</td>
<td>11 (B)</td>
<td>AP</td>
<td>WEP</td>
<td>69</td>
</tr>
<tr>
<td>TDL-DI-624</td>
<td>00:03:43:84:02</td>
<td>6 (B+G)</td>
<td>AP</td>
<td>WEP</td>
<td>27</td>
</tr>
<tr>
<td>default</td>
<td>00:90:96:28:24:26</td>
<td>6 (B)</td>
<td>AP</td>
<td>n/a</td>
<td>26</td>
</tr>
</tbody>
</table>

You may select the radio button of a specific Access Point and then click on the **Connect** 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.

<table>
<thead>
<tr>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
</tr>
<tr>
<td>Firmware Version</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
</tr>
<tr>
<td>Band</td>
</tr>
<tr>
<td>SSID</td>
</tr>
<tr>
<td>Channel Number</td>
</tr>
<tr>
<td>Encryption</td>
</tr>
<tr>
<td>BSSID</td>
</tr>
<tr>
<td>Associated Clients</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP/IP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attain IP Protocol</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Default Gateway</td>
</tr>
<tr>
<td>DHCP</td>
</tr>
<tr>
<td>MAC Address</td>
</tr>
</tbody>
</table>

- **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.

**Operation Mode**

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

- **Bridge**: Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.

- **Bridge Router**: Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.

- **AP**: Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.

  ![Apply Change]  ![Reset]

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

  ![Apply Change]  ![Reset]

  Please wait...

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

- Click on the OK button and then enter the specified IP address into the web-browser.
• Please wait and then enter the specified IP address into the web-browser. The previous settings will be retained in AP mode.
• Refer to Chapter 4 to learn how to configure this device in Bridge/Bridge Router mode.

5.2.2 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.

Access Point Status

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

<table>
<thead>
<tr>
<th>System</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>9day 1h 8m 54s</td>
<td></td>
</tr>
<tr>
<td>Firmware Version</td>
<td>v1.39.06</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless Configuration</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>AP+WDS</td>
<td></td>
</tr>
<tr>
<td>Band</td>
<td>2.4 GHz (B+G)</td>
<td></td>
</tr>
<tr>
<td>SSID</td>
<td>wireless_g</td>
<td></td>
</tr>
<tr>
<td>Channel Number</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Disabled(40), Disabled(WDS)</td>
<td></td>
</tr>
<tr>
<td>BSSID</td>
<td>00:02:ef:49:1b:66</td>
<td></td>
</tr>
<tr>
<td>Associated Clients</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP/IP Configuration</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>192.168.1.2</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Default Gateway</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:02:ef:49:1b:66</td>
<td></td>
</tr>
</tbody>
</table>

• 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.
**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.

### 5.2.3 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.

**Statistics**

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

<table>
<thead>
<tr>
<th>Network</th>
<th>Sent Packets</th>
<th>Received Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless LAN</td>
<td>56,501</td>
<td>30,076</td>
</tr>
<tr>
<td>Ethernet LAN</td>
<td>2232</td>
<td>1742</td>
</tr>
</tbody>
</table>

**Refresh**

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

### 5.2.4 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.

**System Log**

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

- **Enable Log**
  - **System All**
  - **Wireless**
  - **Enable Remote Log**
  - **Log Server IP Address:**

**Apply Changes**
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.

### 5.2.5 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.

  **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.

  - Select File:
  - [Upload]
  - [Reset]

- 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.

### 5.2.6 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.
Save/Reload Settings

This page allows you to 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.

- 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.

5.2.7 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.

Password Setup

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

- 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.
5.3 TCP/IP Settings

- Click on the TCP/IP Settings link on the navigation drop-down menu. You will then see the LAN Interface and SNMP option. The options are described in detail below.

5.3.1 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 server/client and 802.1d spanning tree feature.

5.3.1.1 Static IP Address

### LAN Interface Setup

This page is used to configure the parameters for local area network which connects to change the setting for IP address, subnet mask, DHCP, etc.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address:</td>
<td>192.168.1.254</td>
</tr>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>DHCP:</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP Client Range:</td>
<td>192.168.1.100 - 192.168.1.200</td>
</tr>
<tr>
<td>DNS Server:</td>
<td></td>
</tr>
<tr>
<td>802.1d Spanning Tree:</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

- **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**: Since a static IP address is used, this option must be set to **Disabled**. 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.

- **802.1d Spanning Tree**: Select **Enabled** from the drop-down list if you would like to use the spanning tree feature.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

### 5.3.1.2 DHCP Client

**LAN Interface Setup**

This page is used to configure the parameters for local area network which connects to the LAN port change the setting for IP addresses, subnet mask, DHCP, etc.

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>192.168.1.254</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>DHCP:</td>
<td>Client</td>
</tr>
<tr>
<td>DHCP Client Range:</td>
<td>192.168.1.100 - 192.168.1.200</td>
</tr>
<tr>
<td>DNS Server:</td>
<td>Show Client</td>
</tr>
<tr>
<td>802.1d Spanning Tree:</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

- **DHCP**: If this device is a DHCP client and will receive its IP settings from a DHCP server, then select **Client** 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.
- **802.1d Spanning Tree**: Select **Enabled** from the drop-down list if you would like to use the spanning tree feature.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.
5.3.1.3 DHCP Server

LAN Interface Setup

This page is used to configure the parameters for the local area network which connects to the LAN port change the setting for IP addresses, subnet mask, DHCP, etc.

- **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**: Select Server from the drop-down list since this device is the DHCP server. This device will distribute the IP addresses to the clients associated.
- **DHCP Client Range**: Enter the first and last IP address of the range. Make sure that the range is on the same subnet as the device. You may click on the Show Client button to view a list of IP addresses that were distributed.
- **DNS Server**: Enter the IP address of the DNS server.
- **802.1d Spanning Tree**: Select Enabled from the drop-down list if you if you would like to use the spanning tree feature.
- **Click on the Apply Changes button to confirm the changes. This device will automatically restart once these changes have been applied.**
5.3.2 SNMP Settings

**SNMP Parameter Setup**

This page is used to configure the parameters for simple network management protocol which can change the setting for SNMP daemon, read-only and read-write community name, Trap daemon, trap.

- **SNMP Daemon**: Select Enable if you would like to use the SNMP feature.
- **Read-Only Community Name**: Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap**: Select Enable if you would like to receive SNMP traps.
- **Send Trap To**: Specify the IP address that would receive the SNMP traps.
- **Trap Community Name**: Specify the password for the SNMP trap community.
- Click on the **Save Settings** button once you have modified the settings.

5.4 Wireless

- Click on the **Wireless** link on the navigation drop-down menu. You will then see five options: basic settings, advanced settings security, access control and WDS. Each option is described below.
5.4.1 Basic Settings

- 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.

**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.

- **Band**: Select the IEEE 802.11 mode from the drop-down list. Options available are 2.4GHz (B), 2.4GHz (G), or 2.4GHz (B+G). Select the appropriate mode based on the type of wireless network. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select 2.4GHz (G) instead of 2.4GHz (B+G) which will reduce the performance of the wireless network.

- **SSID**: The SSID is a unique name 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.

- **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.

- **Show Active Clients**: Click on this button to view a list of associated clients.

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

- **Enable Universal Repeater Mode**: Select Enable to activate Universal Repeater Mode and type below SSID for extended wireless interface.
5.4.2 Advanced Settings

- 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, broadcast SSID, IAPP, and 802.11g protection.

**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**: 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).
- **ACK Timeout**: You may specify a value for the acknowledge timeout.
- **Data Rate**: Select a data rate from the drop-down list. However, it is recommended to select **auto** for the best performance.
- **Data Rate**: If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Output Power Level (OFDM/CCK)**: You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.

- You can arrange the different data rate in distance in Access Point mode. Please refer below table. The table only for 11g and 11b/g mix mode

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>6M-24M</th>
<th>36M</th>
<th>48M</th>
<th>54M</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>Great</td>
</tr>
<tr>
<td>Ultra High</td>
<td>✅</td>
<td>✅</td>
<td>Great</td>
<td>N/A</td>
</tr>
<tr>
<td>Super</td>
<td>✅</td>
<td>Great</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Extreme</td>
<td>Great</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- **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.
- **Broadcast SSID**: This is a security feature that is enabled by default. This allows clients on the wireless network to run a site survey and detect this Access Point. Select **Disabled** if you do not want this Access Point detected in a site survey.
- **IAPP**: It is recommended to **Enable** the Inter-Access Point Protocol (IAPP) if you would like the clients on the wireless network to seamlessly roam between Access Points of the same SSID.
- **802.11g Protection**: If your wireless network is using both 802.11b and 802.11g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **User Isolation**: Click **“Enabled”** to stop packet transmission between Wireless Clients.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.
5.4.3 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 802.1x.

5.4.3.1 Encryption Disabled

**Wireless Security Setup**

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

<table>
<thead>
<tr>
<th>Encryption:</th>
<th>None</th>
<th>Set WEP Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Use 802.1x Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA Authentication Mode:</td>
<td>○ WEP 64bit</td>
<td>○ WEP 128bit</td>
</tr>
<tr>
<td>WPA Cipher Suite:</td>
<td>○ TKIP</td>
<td>○ AES</td>
</tr>
<tr>
<td>WPA2 Cipher Suite:</td>
<td>○ TKIP</td>
<td>○ AES</td>
</tr>
<tr>
<td>Pre-Shared Key Format:</td>
<td>Passphrase</td>
<td></td>
</tr>
<tr>
<td>Pre-Shared Key:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Enable Pre-Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication RADIUS Server:</td>
<td>Port: 012</td>
<td>IP address</td>
</tr>
</tbody>
</table>

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

- **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.
5.4.3.2 WEP 64-bit / 128-bit

Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys of your wireless network.

- **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.

**Wireless WEP Key Setup**

This page allows you to 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**: 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.

### 5.4.3.3 WPA / WPA2 / WPA2 Mixed Passphrase

#### Wireless Security Setup

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

- **Encryption**: Select WPA, WPA2 or WPA2_Mixed 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, AES or both as the cipher suite.
- **Pre-Shared Key Format**: Select Passphrase from the drop-down list.
- **Pre-Shared Key**: Enter the pass phrase; 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.

Note: When encryption WEP is selected, you must set WEP key value.
Wireless Security Setup

This page allows you to set up the wireless security. Turn on WEP or WPA by using Encryption Keys for your wireless network.

- **Encryption:** Select WPA, WPA2 or WPA2_Mixed 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** or both 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.
5.4.4 Access Control

- Click on the Access Control link under the Wireless menu. On this page you can filter the MAC address by allowing or blocking access the network.

**Wireless Access Control**

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

<table>
<thead>
<tr>
<th>Wireless Access Control Mode:</th>
<th>Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address:</td>
<td>Allow Listed</td>
</tr>
<tr>
<td></td>
<td>Deny Listed</td>
</tr>
</tbody>
</table>

- **Wireless Access Control Mode**: You may choose to **Disable**, **Allow Listed**, or **Deny Listed** MAC address from associating with the network. By selecting Allow Listed, only the address listed in the table will have access to the network; all other clients will be blocked. On the other hand, selected Deny Listed, only the listed MAC address will be blocked from access the network; all other clients will have access to the network.
- **MAC Address**: Enter the MAC address.
- **Current Access Control list**: This table lists the blocked or allowed MAC addresses; you may delete selected MAC address or delete all the addresses from the table by clicking on the associated buttons.
- **Click on the Apply Changes button** to confirm the changes. This device will automatically restart once these changes have been applied.
5.4.5 WDS

- Click on the WDS link under the Wireless menu. On this page you can configure the WDS (Wireless Distribution System) which allows the Access Point to function as a repeater.

**WDS Settings**

Wireless Distribution System uses wireless media to communicate with other APs. Enter the same channel and set MAC address of other APs which you want to communicate with.

- **Enable WDS**: Place a check in this box to enable this feature.
- **Add WDS AP**: Enter the MAC address of the Access Point that will join the WDS network along with a comment about the AP.
- **Current WDS AP List**: This table lists MAC addresses; you may delete selected MAC address or delete all the addresses from the table by clicking on the associated buttons.
- Click on the Apply Changes button to confirm the changes. This device will automatically restart once these changes have been applied.
- Click on the Set Security button to configure the security settings.
WDS Security Setup

This page allows you to setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

- **Encryption**: Select WEP 64bits, WEP 128bits, WPA (TKIP) or WPA2 (AES) from the drop-down list if your wireless network uses a specific encryption.
- **Key Format**: Select a key format from the drop-down list. 64bit-hex keys require 10 characters, whereas 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Key Length**: Select a 64-bit or 128-bit from the drop-down list.
- **Pre-Shared Key Format**: Select Passphrase from the drop-down list.
- **Pre-Shared Key**: Enter the pass phrase; 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.
Appendix A – Specifications

Data Rates
1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

Standards
IEEE802.11b/g, IEEE802.1x, IEEE802.3, IEEE802.3u

Compatibility
IEEE 802.11g/IEEE 802.11b

Power Requirements
Active Ethernet (802.3af) – 48 VDC/0.35A

Regulation Certifications
FCC Part 15, ETSI 300/328/CE

RF Information
Frequency Band
2.400 ~ 2.4835 GHz (US, EU)
2.400 ~ 2.484 GHz (JP)

Media Access Protocol
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Modulation Technology
Orthogonal Frequency Division Multiplexing (OFDM)
DBPSK @ 1Mbps
DQPSK @2Mbps
CCK @ 5.5 & 11Mbps
BPSK @ 6 and 9 Mbps
QPSK @ 12 and 18 Mbps
16-QAM @ 24 and 36 Mbps
64-QAM @ 48 and 54 Mbps

Operating Channels
11 for North America, 14 for Japan, 13 for Europe,

Receive Sensitivity (Typical)
-88dBm @ 6Mbps
-70dBm @ 54Mbps

Available transmit power
Up to 26dBm @ 1~24Mbps
23dBm @ 36Mbps
21dBm @ 48Mbps
20dBm @ 54Mbps

Antenna
Option A: 9dBi Internal(Patch)
Option B: 5dBi External (Dipole)
Option C: 16dBi Built-in (Patch)

RF Connector
SMA (Fr) Type (Optional for External Antenna use)

Networking

Topo
Ad-Hoc, Infrastructure

Operation Mode
Point-to-Point/ Point-to-Multipoint Bridge/ Client Router/ AP/ WDS/ Repeater

Interface
• Wireless IEEE802.11b/g
• One 10/100 RJ-45 port
• RS232 connector

Security
IEEE802.1x Authenticator / RADIUS
Client (EAP-MD5/TLS/TTLS) Support in AP Mode
• WPA /WPA2
• MAC address filtering
• Hide SSID in beacons
• User isolation
• NAT in CR mode

IP Auto-configuration
DHCP client/server

Management
Configuration
• Web-based configuration (HTTP)
• SNMP V1, V2c
• Telnet

Firmware Upgrade
Upgrade firmware via web-browser

Physical
Dimensions
163.8(L)mm * 135.2(W)mm * 47.0(H)mm

Weight
1.2 Kg (2.6 lbs)

Environmental
Temperature Range
Operating: 0°C to 60°C (32°F to 140°F) - Storage: -20°Cto 80°C (-4°F to 176°F)

Humidity (non-condensing)
5%~95% Typical

Package Contents
• Outdoor Wireless Client Bridge unit
• 48V, 0.375A AC/DC adapter with wall-plug power code
• Inline Power Injector (PoE)
• 1.8m Grounding Cable
• User’s manual CD-ROM
• Wall mounting kit
• Mast mounting kit
• Waterproof kit
Appendix B – FCC Interference Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Appendix C – IC Statement

IC statement
Operation is subject to the following two conditions:
This device may not cause interference and
This device must accept any interference, including interference that may cause undesired operation of the device.
This device has been designed to operate with an antenna having a maximum gain of 9 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

IMPORTANT NOTE:
IC Radiation Exposure Statement:
This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Règlement d'Industry Canada
Les conditions de fonctionnement sont sujettes à deux conditions:
Ce périphérique ne doit pas causer d'interférence et.
Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.