



ALL0258

Wireless Outdoor Access Point & Client Bridge



User's Manual

V1.0

Table of Contents

1	INTRODUCTION.....	4
1.1	FEATURES	5
1.2	PACKAGE CONTENTS	6
1.3	SAFETY GUIDELINES	6
1.4	SYSTEM REQUIREMENTS	6
1.5	APPLICATIONS	7
2	UNDERSTANDING THE HARDWARE.....	8
2.1	HARDWARE INSTALLATION	8
2.2	HARDWARE DESCRIPTION.....	8
2.3	MOUNTING KITS.....	9
2.4	IP ADDRESS CONFIGURATION	9
3	SWITCHING BETWEEN OPERATING MODES.....	11
3.1	LOGGING IN.....	11
4	ACCESS POINT OPERATING MODE	12
4.1	LOGGING IN.....	12
4.2	STATUS	13
4.2.1	MAIN	13
4.2.2	WIRELESS CLIENT LIST	14
4.2.3	SYSTEM LOG.....	15
4.3	SYSTEM.....	15
4.3.1	SYSTEM PROPERTIES.....	15
4.3.2	IP SETTINGS	16
4.3.3	SPANNING TREE SETTINGS	17
4.4	WIRELESS.....	17
4.4.1	WIRELESS NETWORK	18
4.4.1.1	WIRELESS SECURITY - WEP.....	19
4.4.1.2	WIRELESS SECURITY – WPA-PSK, WPA2-PSK, WPA-MIXED	20
4.4.1.3	WIRELESS SECURITY – WPA, WPA2	21
4.4.2	WIRELESS MAC FILTER	22
4.4.3	WIRELESS ADVANCED SETTINGS	23
4.5	MANAGEMENT	24
4.5.1	ADMINISTRATION	24
4.5.2	SNMP SETTINGS	24
4.5.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	25
4.5.4	FIRMWARE UPGRADE	26
4.5.5	TIME SETTINGS	27
4.5.6	LOG	27
5	CLIENT BRIDGE OPERATING MODE	28
5.1	LOGGING IN.....	28
5.2	STATUS	29
5.2.1	MAIN	29
5.2.2	CONNECTION STATUS	30
5.2.3	SYSTEM LOG.....	31
5.3	SYSTEM.....	31
5.3.1	SYSTEM PROPERTIES.....	31
5.3.2	IP SETTINGS	32
5.3.3	SPANNING TREE SETTINGS	32

5.4	WIRELESS.....	33
5.4.1	WIRELESS NETWORK	34
5.4.2	WIRELESS SECURITY	35
5.4.2.1	WIRELESS SECURITY - WEP.....	35
5.4.2.2	WIRELESS SECURITY – WPA-PSK, WPA2-PSK	36
5.4.3	WIRELESS ADVANCED SETTINGS	36
5.5	MANAGEMENT	37
5.5.1	ADMINISTRATION	38
5.5.2	SNMP SETTINGS	38
5.5.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	39
5.5.4	FIRMWARE UPGRADE	40
5.5.5	TIME SETTINGS	40
5.5.6	LOG	41
6	CLIENT ROUTER OPERATING MODE.....	42
6.1	LOGGING IN.....	42
6.2	STATUS	43
6.2.1	MAIN	43
6.2.2	DHCP CLIENT TABLE.....	44
6.2.3	CONNECTION STATUS	44
6.2.4	SYSTEM LOG.....	45
6.3	SYSTEM.....	46
6.3.1	SYSTEM PROPERTIES.....	46
6.4	ROUTER	46
6.4.1	WAN SETTINGS	47
6.4.1.1	WAN - DHCP	47
6.4.1.2	WAN – STATIC IP.....	48
6.4.1.3	WAN – PPPoE.....	49
6.4.2	LAN SETTING.....	51
6.4.3	VPN PASS THROUGH.....	51
6.5	WIRELESS.....	52
6.5.1	WIRELESS NETWORK	52
6.5.2	WIRELESS SECURITY	53
6.5.2.1	WIRELESS SECURITY - WEP.....	53
6.5.2.2	WIRELESS SECURITY – WPA-PSK, WPA2-PSK	54
6.5.2.3	WIRELESS ADVANCED SETTINGS	55
6.6	MANAGEMENT	56
6.6.1	ADMINISTRATION	56
6.6.2	SNMP SETTINGS	57
6.6.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	57
6.6.4	FIRMWARE UPGRADE	58
6.6.5	TIME SETTINGS	59
6.6.6	LOG	60
	APPENDIX A – SPECIFICATIONS.....	61
	APPENDIX B – FCC INTERFERENCE STATEMENT.....	64

Revision History

Version	Date	Notes
1.0	January 08, 2009	Initial Version

1 Introduction

ALL0258 is a long range outdoor wireless Access Point / Client Bridge that operates in both **5GHz and 2.4GHz** frequency. It provides high bandwidth up to 54Mbps with Super Mode (SuperA/G) and features high transmitted output power as well as superior sensitivity. ALL0258 extends radio coverage, avoids unnecessary roaming between Access Points and ensures a stable wireless connection while reduces the number of required equipments.

ALL0258 provides user friendly interface including user friendly distance control ranges from 1Km up to 30Km and RSSI LED indicator offering real time signal status. It comes with PoE injector for convenient outdoor installation.

ALL0258 enforces transmission security with full support of latest encryption mechanism including 64/128-bit WEP, WPA and WPA2. With 13dBi internal antenna and superior performance, ALL0258 makes an optimal wireless solution for both small and large scale projects.

1.1 Features

Wireless

- **5GHz / 2.4GHz** It works in 5GHz / 2.4GHz frequency spectrum
- **High output power** Transmit output power programmable for different country selections
- **High Data Rate** High speed transmitting rate up to 54Mbps with Super Mode, supports large payload such as MPEG video streaming
- **Multifunction application** Access Point/Client Bridge/Client Router
- **Long range transmitting** Transmit power control and distance control (ACK timeout)
- **Signal Strength** LED indicators have the best transmit and receive signal for traffic communication
- **Public wireless solution** An AP interface that is especially useful in public areas such as hotspots and enterprise
- **Signal Strength Display** RF signal strength status shown LEDs of 3 colors, making network build-up easier
- **BSSID** Basic Service Set ID, supports 4 MAC address

Networking

- **QoS(WMM)** Enhance performance and density
- **PPPoE** Point-to-Point Protocol over Ethernet at Client Router mode. This function will keep trying when failed or disconnected

Security

- **802.11i** WEP, WPA, WPA2 (Encryption support TKIP/AES)
- **MAC address functions** MAC address filter (AP mode)
- **802.1x** IEEE802.1x Authenticator
- **Station isolation**

Management

- **Firmware Upgrade** Upgrading firmware via web browser, setting are reserved after upgrade
- **Reset & Backup** Reset to factory default. User can export all setting into a file via WEB
- **MIB** MIB I, MIB II(RFC1213)
- **SNMP** V1, V2c

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.

- 1* Wireless 802.11a/b/g Outdoor Device(ALL0258)
- 1* PoE Injector (EPE-1212)
- 1* Power Adaptor(24V/0.6A)
- 1* CD with User's Manual
- 1* QIG
- 1* Metal strap
- 1* Special screw set

1.3 Safety Guidelines

In order to reduce the risk of fire, electric shock and injury, please adhere to the following safety guidelines.

- Carefully follow the instructions in this manual; also follow all instruction labels on this device.
- Except for the power adapter supplied, this device should not be connected to any other adapters.
- Do not spill liquid of any kind on this device.
- Do not place the unit on an unstable stand or table. This unit may drop and become damaged.
- Do not place any hot devices close to this unit, as they may degrade or cause damage to the unit.
- Do not place any heavy objects on top of this unit.
- Do not use liquid cleaners or aerosol cleaners. Use a soft dry cloth for cleaning.

1.4 System Requirements

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

- PC/AT compatible computer with an 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

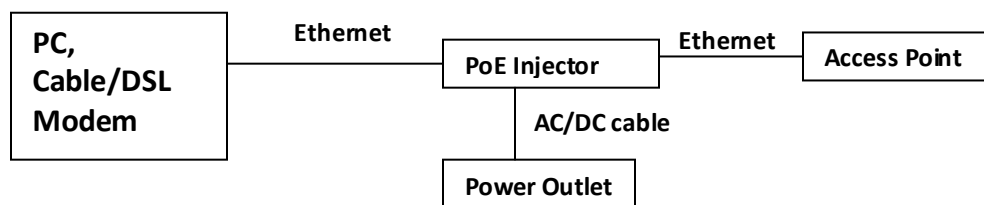
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

2 Understanding the Hardware

2.1 Hardware Installation

- 1 Place the unit in an appropriate location after conducting a site survey.
- 2 Plug one end of the Ethernet cable into the Network port of the PoE injector and another end into your PC/Notebook.
- 3 Plug one end of another Ethernet cable to AP/Bridge port of the PoE injector and the other end into you cable/DSL modem (Internet)
- 4 Insert the DC-inlet of the power adapter into the 24V port of the PoE injector and the other end into the power socket on the wall.

This diagram depicts the hardware configuration



2.2 Hardware Description

The images below depict the front and rear panel of the Access Point / Client Bridge.

Front Panel



Rear Panel



2.3 Mounting Kits

The images below depict the standard and optional mounting kits.

**Standard
Pole Mount**



**Optional
Wall Mount**



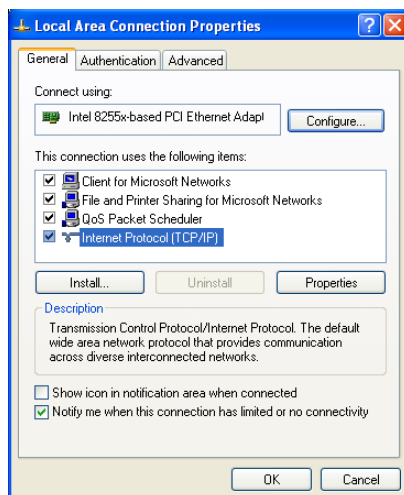
**Optional
Window Mount**



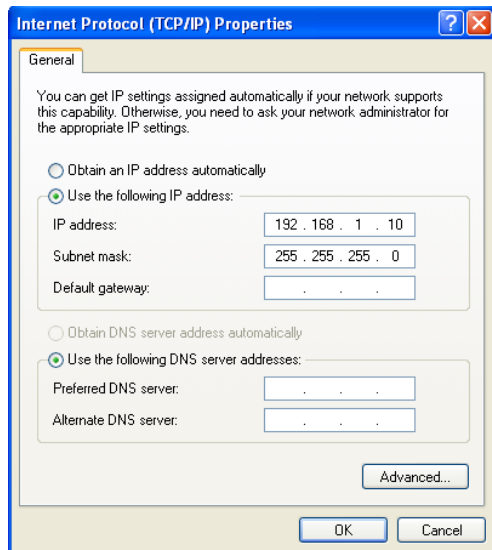
2.4 IP Address Configuration

This device can be configured as a Bridge/Router 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.



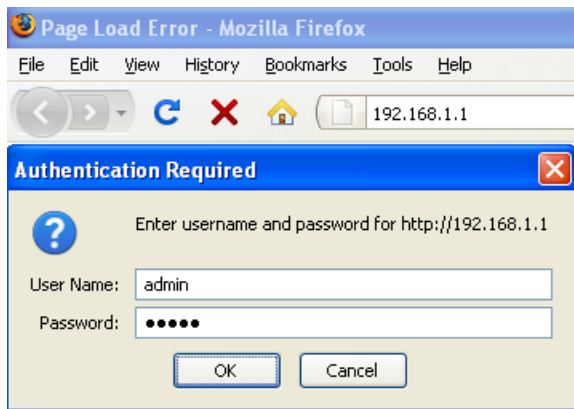
3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.
For Example:
PC IP address: 192.168.1.10
PC subnet mask: 255.255.255.0
4. Click on the **OK** button to close this window, and once again to close LAN properties window.

3 Switching Between Operating Modes

This device can operate in three modes: Access Point, Client Bridge, and Client Router. This chapter will describe how to switch between operating modes.

3.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.



- After logging in, you will see the graphical user interface of the device. Click on the **System Properties** link under the **System** navigation drop-down menu.

System Properties Home Reset

Device Name	Access Point (1 to 32 characters)
Country/Region	United States
Operation Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> Client Bridge <input type="radio"/> Client Router

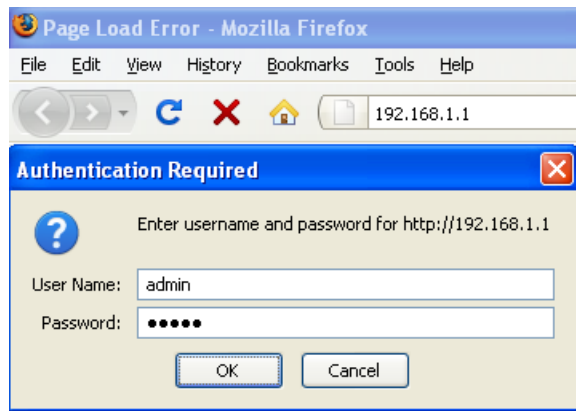
Apply Cancel

- Select and operating mode from the list (Access Point, Client Bridge, or Client Router) and then click on the **Apply** button.

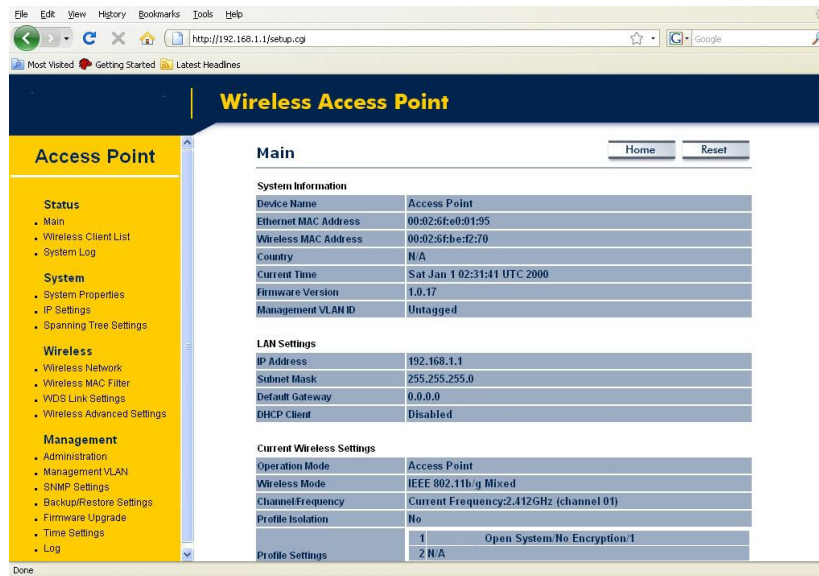
4 Access Point Operating Mode

4.1 Logging In

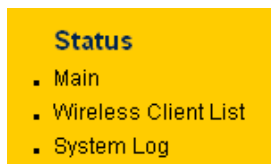
- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.



- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
 1. **Status:** Displays the overall status, connection status, and event log.
 2. **System:** This menu includes the system properties, IP and Spanning Tree settings.
 3. **Wireless:** This menu includes status, basic, advanced, and security.
 4. **Management:** This menu includes the admin setup, SNMP, firmware upgrade, and save/restore backup.



4.2 Status



- Click on the **Status** link on the navigation drop-down menu. You will then see three options: Main, Wireless Client List, and System Log. Each option is described in detail below.

4.2.1 Main

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, Country, Firmware version, Ethernet MAC Address, Wireless MAC Address and Current Time are displayed in the 'System' section. LAN IP Address, Subnet Mask, Default Gateway and DHCP Client are displayed in the 'LAN' section. In the 'Wireless section, the frequency, channel is displayed.

Main[Home](#)[Reset](#)**System Information**

Device Name	Access Point
Ethernet MAC Address	00:02:6f:54:65:a6
Wireless MAC Address	00:02:6f:54:65:a7
Country	N/A
Current Time	Sat Jan 1 00:41:59 UTC 2000
Firmware Version	1.0.25

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	Current Frequency:2.412GHz (channel 01)
Wireless Network Name (SSID)	default
Security	Open System/No Encryption
Spanning Tree Protocol	Disabled
Distance	1 Km

4.2.2 Wireless Client List

- Click on the **Wireless Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the Access Point.
- The MAC addresses and signal strength for each client is displayed. Click on the **Refresh** button to refresh the client list

Client List[Home](#)[Reset](#)

#	MAC Addr	RSSI
1	00:02:6f:01:cf:4f	66

[Refresh](#)

4.2.3 System Log

- Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

System Log Home Reset

Show log type: All

Local Log i

- All
- Debug
- Information
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

4.3 System

System

- System Properties
- IP Settings
- Spanning Tree Settings

- Click on the **System** link on the navigation drop-down menu. You will then see three options: System Properties, IP Settings, and Spanning Tree Settings. Each option is described

in detail below.

4.3.1 System Properties

- Click on the **System Properties** link under the **System** drop-down menu. This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

System Properties Home Reset

Device Name	Access Point <small>(1 to 32 characters)</small>
Country/Region	Please Select a Country Code <input type="button" value="v"/>
Operation Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> Client Bridge <input type="radio"/> Client Router

- Device Name:** Specify a name for the device (this is not the SSID),
- Country/Region:** Select a country from the drop-down list.

- **Operating Mode:** Select and operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

4.3.2 IP Settings

- Click on the **IP Settings** link under the **System** drop-down menu This page allows you to configure the device with a static IP address or a DHCP client.

IP Settings Home Reset

IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0

Apply Cancel

- **IP Network Setting:** Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- **IP Address:** Specify an IP address
- **IP Subnet Mask:** Specify the subnet mask for the IP address
- **Default Gateway:** Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

4.3.3 Spanning Tree Settings

- Click on the **Spanning Tree** link under the **System** drop-down menu. Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

Spanning Tree Settings

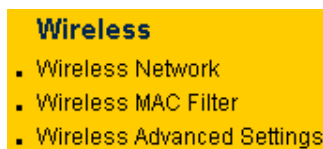
Home Reset

Spanning Tree Status	<input checked="" type="radio"/> On <input type="radio"/> Off
Bridge Hello Time	1 <input type="text"/> seconds (1-10)
Bridge Max Age	20 <input type="text"/> seconds (6-40)
Bridge Forward Delay	4 <input type="text"/> seconds (4-30)
Priority	8000 <input type="text"/> seconds (0-65535)

Apply Cancel

- Spanning Tree Status:** Choose to enable or disable the spanning tree feature.
- Bridge Hello Time:** Specify the number of seconds for the hello time.
- Bridge Max Age:** Specify the number of seconds for the max age.
- Bridge Forward Delay:** Specify the number of seconds for the bridge forward delay.
- Priority:** Specify the number of seconds for the priority.
- Click on the **Apply** button to save the changes.

4.4 Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see four options: wireless network, wireless MAC filter, WDS link settings, and wireless advanced settings. Each option is described below.

4.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

Wireless Network
Home
Reset

Wireless Setting

Wireless Mode	802.11b/g Mixed (2.4GHz/54Mbps) ▼
Channel / Frequency	Ch1-2.412GHz ▼
SSID	default (1 to 32 characters)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Wireless Security

Security Mode	Disabled ▼
----------------------	------------

Apply
Cancel

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **A, B, G, B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **A** or **B/G-mixed** for the best performance.
- **Turbo Mode** is a proprietary mode which combines all channels into a single channel to maximize the through-put up to 200%. Please be aware that Turbo Mode works only with other Turbo Mode supported devices.
- **Channel:** Select a channel from the drop-down list. The channels available are based on the country's regulation.

4.4.1.1 Wireless Security - WEP

- **Security Mode:** 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.

Wireless Setting

SSID	default	(1 to 32 characters)
VLAN ID	1	(1~4095)
Suppressed SSID	<input type="checkbox"/>	
Station Separation	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

Wireless Security

Security Mode	WEP
Auth Type	Open Key
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	40/64-bit (10 hex digits or 5 ASCII char)
	104/128-bit (26 hex digits or 13 ASCII char)
	128/152-bit (32 hex digits or 16 ASCII char)
Key1	<input type="text"/>
Key2	<input type="text"/>
Key3	<input type="text"/>
Key4	<input type="text"/>

- **Authentication Type:** Select an authentication method. Options available are **Open Key**, **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 Access Point. 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.
- **Input Type:** Select He or ASCII from the drop-down list
- **Key Length:** 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 Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply** button to save the changes.

4.4.1.2 Wireless Security – WPA-PSK, WPA2-PSK, WPA-Mixed

- **Security Mode:** Select **WPA-PSK**, **WPA2-PSK**, or **WPA-Mixed** from the drop-down list if your wireless network uses WPA pre-shared key.

Wireless Setting

Wireless Mode	802.11b/g Mixed (2.4GHz/54Mbps) ▾	
Channel / Frequency	Ch1-2.412GHz ▾	
SSID	default	(1 to 32 characters)
Suppressed SSID	<input type="checkbox"/>	
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

Wireless Security

Security Mode	WPA-PSK ▾	
Encryption	Auto ▾	
Passphrase	passphrasel	(8 to 63 characters)
Group Key Update Interval	3600	seconds(30~3600, 0: disabled)

Apply Cancel

- **Encryption:** Select **TKIP** or **AES** 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.
- **Passphrase:** Specify a passphrase that is shared amongst the Access Points and clients.
- **Group Key Update Interval:** Specify the number of seconds after which the Access Point will probe the client for the passphrase.
- Click on the **Apply** button to save the changes.

4.4.1.3 Wireless Security – WPA, WPA2

- **Security Mode:** Select **WPA** or **WPA2** from the drop-down list if your wireless network uses WPA. 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.

Wireless Setting

Wireless Mode	802.11b/g Mixed (2.4GHz/54Mbps) ▾
Channel / Frequency	Ch1-2.412GHz ▾
SSID	EnGenius (1 to 32 characters)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Wireless Security

Security Mode	WPA ▾
Encryption	Auto ▾
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

- **Encryption:** Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption.
- **RADIUS IP Address:** Enter the IP address of the RADIUS server.
- **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.
- **RADIUS Secret:** Enter the shared password of the RADIUS server.
- **Group Key Update Interval:** Specify the number of seconds after which the Access Point will probe the client for the secret.
- Click on the **Apply** button to save the changes.

4.4.2 Wireless MAC Filter

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

Wireless MAC Filter

ACL Mode:

: : : : :

	MAC Address	
1	00:11:22:33:22:23	<input type="button" value="Delete"/>
2	77:88:77:55:77:88	<input type="button" value="Delete"/>

- ACL (Access Control) Mode:** You may choose to **Disable**, **Allow Listed**, or **Deny Listed** MAC addresses from associating with the network. By selecting **Allow MAC in the List**, 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 MAC in the List**, only the listed MAC addresses will be blocked from accessing the network; all other clients will have access to the network.
- MAC Address:** Enter the MAC address.
- 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 **Delete** button.
- Click on the **Apply** button to save the changes.

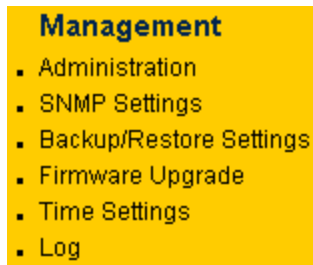
4.4.3 Wireless Advanced Settings

- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.

Wireless Advanced Settings	
Data Rate	Auto ▾
Transmit Power	20 dBm ▾
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable ▾
WMM	Disable ▾
Distance (1-30km)	1 km

- 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.
- Transmit Power:** 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.
- Fragment:** 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.
- Protection Mode:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- WMM:** Enable wireless Quality of Service
- Distance (1-30km):** Specify a distance between 1 and 30Km.
- Click on the **Apply** button to save the changes.

4.5 Management



- Click on the **Management** link on the navigation drop-down menu. You will then see seven options: administration, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

4.5.1 Administration

- Click on the **Administration** 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 **admin**. For security reasons it is highly recommended that you create a new user name and password.

The image shows a web interface for the "Administration" page. At the top right, there are two buttons: "Home" and "Reset". Below the title "Administration", there is a section titled "Administrator" with three input fields:

Name	admin
Password	•••••
Confirm Password	•••••

At the bottom of the form, there are two buttons: "Apply" and "Cancel".

- **Name:** Specify a user name into the first field.
- **Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

4.5.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases. .

SNMP Settings

Home

Reset

SNMP Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

Apply

Cancel

- **SNMP Enable/Disable:** Choose to **enable** or **disable** the SNMP feature.
- **Contact:** Specify the contact details of the device.
- **Location:** Specify the location of the device.
- **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:** Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

4.5.3 Backup/Restore, Reset to factory default settings

- Click on the **Backup/Restore 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.

Backup/Restore Settings

Home

Reset

Save A Copy Of Current Settings	<input type="button" value="Backup"/>
Restore Saved Settings From A File	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Restore"/>
Revert To Factory Default Settings	<input type="button" value="Factory Default"/>

- **Save a copy of the current settings:** Click on the Backup button to save the current configuration.
- **Restore saved settings from a file:** Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings:** Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1

System Rebooting...

Rebooting, Please wait... 

[Click here when AP is ready](#)

4.5.4 Firmware Upgrade

- 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.

Firmware Upgrade [Home](#) [Reset](#)

Current firmware version: 1.0.25

Locate and select the upgrade file from your hard disk:

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** 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.

4.5.5 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

Time Settings Home Reset

Time

Manually Set Date and Time
 2000 / 01 / 01 00 : 02

Automatically Get Date and Time
 Time Zone: UTC+00:00 England

User defined NTP Server: 192 . 168 . 1 . 99

Apply Cancel

- Manually Set Date and Time:** Specify the date and time
- Automatically Get Date and Time:** Select the time zone from the drop down list and then specify the IP address of the NTP server.
- Click on the **Apply** button to save the changes.

4.5.6 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.

Log Home Reset

Syslog

Syslog Enable

Log Server IP Address 192 . 168 . 1 . 67

Local log

Local Log Enable

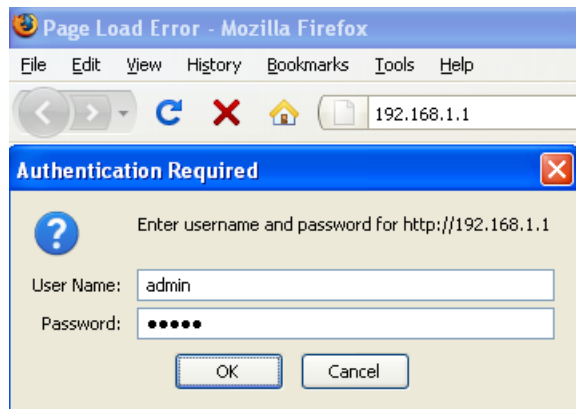
Apply Cancel

- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

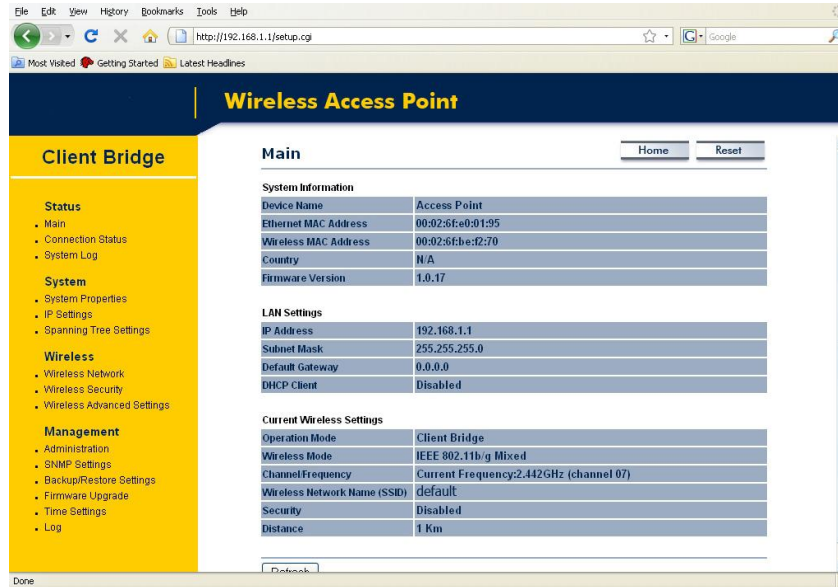
5 Client Bridge Operating Mode

5.1 Logging In

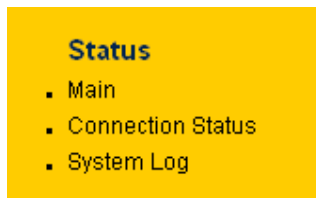
- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.



- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
 1. **Status:** Displays the overall status, connection status, and event log.
 2. **System:** This menu includes the system properties, IP and Spanning Tree settings.
 3. **Wireless:** This menu includes status, basic, advanced, and security.
 4. **Management:** This menu includes the admin setup, SNMP, firmware upgrade, and save/restore backup.



5.2 Status



- Click on the **Status** link on the navigation drop-down menu. You will then see three options: Main, Connection Status, and System Log. Each option is described in detail below.

5.2.1 Main

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, Country, Firmware version, Ethernet MAC Address, Wireless MAC Address and Current Time are displayed in the 'System' section. LAN IP Address, Subnet Mask, Default Gateway and DHCP Client are displayed in the 'LAN' section. In the 'Wireless section, the frequency, channel is displayed.

Main[Home](#)[Reset](#)**System Information**

Device Name	Access Point
Ethernet MAC Address	00:02:6f:e0:01:95
Wireless MAC Address	00:02:6f:be:f2:70
Country	N/A
Firmware Version	1.0.17

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Client Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	Current Frequency:2.422GHz (channel 03)
Wireless Network Name (SSID)	default
Security	Disabled
Distance	1 Km

5.2.2 Connection Status

- Click on the **Connection Status** link under the **Status** drop-down menu. This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.

Connection Status[Home](#)[Reset](#)

Network Type	Client Bridge
SSID	EnGenius
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rate(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

[Refresh](#)

5.2.3 System Log

- Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

5.3 System

System

- System Properties
- IP Settings
- Spanning Tree Settings

- Click on the **System** link on the navigation drop-down menu. You will then see three options: System Properties, IP Settings, and Spanning Tree Settings. Each option is described

in detail below.

5.3.1 System Properties

- Click on the **System Properties** link under the **System** drop-down menu. This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

- **Device Name:** Specify a name for the device (this is not the SSID),
- **Country/Region:** Select a country from the drop-down list.
- **Operating Mode:** Select an operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

5.3.2 IP Settings

- Click on the **IP Settings** link under the **System** drop-down menu. This page allows you to configure the device with a static IP address or a DHCP client.

IP Settings Home Reset

IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0

Apply Cancel

- **IP Network Setting:** Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- **IP Address:** Specify an IP address
- **IP Subnet Mask:** Specify the subnet mask for the IP address
- **Default Gateway:** Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

5.3.3 Spanning Tree Settings

- Click on the **Spanning Tree** link under the **System** drop-down menu. Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

Spanning Tree Settings

[Home](#)
[Reset](#)

Spanning Tree Status	<input checked="" type="radio"/> On <input type="radio"/> Off
Bridge Hello Time	1 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	4 seconds (4-30)
Priority	8000 seconds (0-65535)

- **Spanning Tree Status:** Choose to enable or disable the spanning tree feature.
- **Bridge Hello Time:** Specify the number of seconds for the hello time.
- **Bridge Max Age:** Specify the number of seconds for the max age.
- **Bridge Forward Delay:** Specify the number of seconds for the bridge forward delay.
- **Priority:** Specify the number of seconds for the priority.
- Click on the **Apply** button to save the changes.

5.4 Wireless

Wireless

- Wireless Network
- Wireless Security
- Wireless Advanced Settings

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

5.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

Wireless Network
Home
Reset

Wireless Mode

802.11b/g Mixed (2.4GHz/54Mbps) ▼

SSID

Specify the static SSID :
 (1 to 32 characters)
 Or press the button to search for any available WLAN Service.

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **A**, **B**, **G**, or **B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **A** or **B/G-mixed** for the best performance.
- **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. You may specify an SSID or select one from the **Site Survey**.
- **Site Survey:** Click on the **Site Survey** button in order to scan the 2.4GHz frequency for devices that broadcast their SSID. Click on the **BSSID** link to connect to the Access Point. Click on the **Refresh** button to re-scan the frequency.

Site Survey

2.4GHz Site Survey i:Infrastructure Ad_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:31:86:21	DinoNet	1	-86 dBm	B	WEP	i
00:13f7:7c:6f:43	SMC	6	-105 dBm	G	NONE	i

5.4.2 Wireless Security

The **Wireless Security** page allows you to configure the wireless security.

5.4.2.1 Wireless Security - WEP

- **Security Mode:** 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.

Wireless Security		Home	Reset
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.			
Security Mode	WEP		
Auth Type	Open Key		
Input Type	Hex		
Key Length	40/64-bit (10 hex digits or 5 ASCII char)		
Default Key	1		
Key1	<input type="text"/>		
Key2	<input type="text"/>		
Key3	<input type="text"/>		
Key4	<input type="text"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **Authentication Type:** Select an authentication method. Options available are **Open Key**, **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 Access Point. 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.
- **Input Type:** Select He or ASCII from the drop-down list
- **Key Length:** 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 Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply** button to save the changes.

5.4.2.2 Wireless Security – WPA-PSK, WPA2-PSK

- **Security Mode:** Select **WPA-PSK**, or **WPA2-PSK** from the drop-down list if your wireless network uses WPA pre-shared key.

Wireless Security Home Reset

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA2-PSK
Encryption	TKIP
Passphrase	<input type="text"/> (8 to 63 characters)

Apply Cancel

- **Encryption:** Select **TKIP** or **AES** 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.
- **Passphrase:** Specify a passphrase that is shared amongst the Access Points and clients.
- Click on the **Apply** button to save the changes.

5.4.3 Wireless Advanced Settings

- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.

Wireless Advanced Settings

Home

Reset

Data Rate	Auto
Transmit Power	20 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Distance (1-30km)	1 km

Apply

Cancel

- **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.
- **Transmit Power:** 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.
- **Fragment:** 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.
- **Protection Mode:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM:** You can select Enable or Disable WMM when doing the communication by wireless.
- **Distance (1-30km):** Specify a distance between 1 and 30Km.
- Click on the **Apply** button to save the changes.

5.5 Management

Management

- Administration
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Log

- Click on the **Management** link on the navigation drop-down menu. You will then see six options: administration, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

5.5.1 Administration

- Click on the **Administration** 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 **admin**. For security reasons it is highly recommended that you create a new user name and password.

Administration		Home	Reset
Administrator			
Name	<input type="text" value="admin"/>		
Password	<input type="password" value="•••••"/>		
Confirm Password	<input type="password" value="•••••"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- Name:** Specify a user name into the first field.
- Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

5.5.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

SNMP Settings		Home	Reset
SNMP Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Contact	<input type="text"/>		
Location	<input type="text"/>		
Community Name (Read Only)	<input type="text" value="public"/>		
Community Name (Read/Write)	<input type="text" value="private"/>		
Trap Destination IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Trap Destination Community Name	<input type="text" value="public"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **SNMP Enable/Disable:** Choose to **enable** or **disable** the SNMP feature.
- **Contact:** Specify the contact details of the device.
- **Location:** Specify the location of the device.
- **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:** Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

5.5.3 Backup/Restore, Reset to factory default settings

- Click on the **Backup/Restore 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.

Backup/Restore Settings Home Reset

Save A Copy Of Current Settings

Restore Saved Settings From A File

Revert To Factory Default Settings

- **Save a copy of the current settings:** Click on the Backup button to save the current configuration.
- **Restore saved settings from a file:** Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings:** Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1

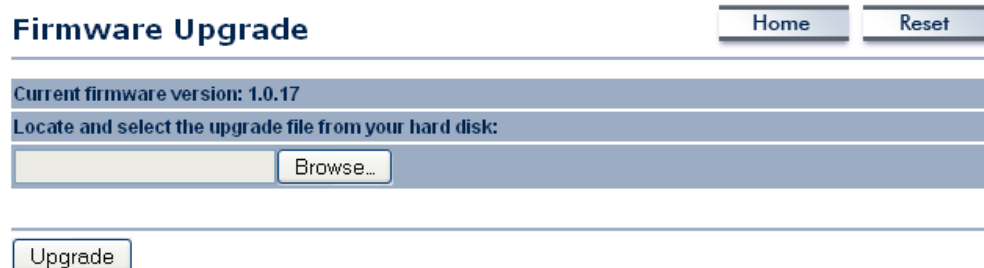
System Rebooting...

Rebooting, Please wait... 

[Click here when AP is ready](#)

5.5.4 Firmware Upgrade

- 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.



The screenshot shows the 'Firmware Upgrade' page. At the top right are 'Home' and 'Reset' buttons. Below the title, it displays 'Current firmware version: 1.0.17' and the instruction 'Locate and select the upgrade file from your hard disk:'. There is a text input field followed by a 'Browse...' button. At the bottom of the form is an 'Upgrade' button.

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** 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.

5.5.5 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

[Home](#) [Reset](#)

Time Settings

Time

Manually Set Date and Time
 2000 / 01 / 01 00 : 02

Automatically Get Date and Time
 Time Zone: UTC+00:00 England

User defined NTP Server: 192 . 168 . 1 . 99

[Apply](#) [Cancel](#)

- **Manually Set Date and Time:** Specify the date and time
- **Automatically Get Date and Time:** Select the time zone from the drop down list and then specify the IP address of the NTP server.
- Click on the **Apply** button to save the changes.

5.5.6 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.

[Home](#) [Reset](#)

Log

Syslog

Syslog

Log Server IP Address 192 . 168 . 1 . 67

Local log

Local Log

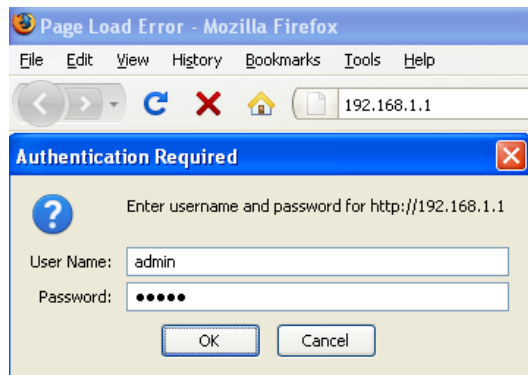
[Apply](#) [Cancel](#)

- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

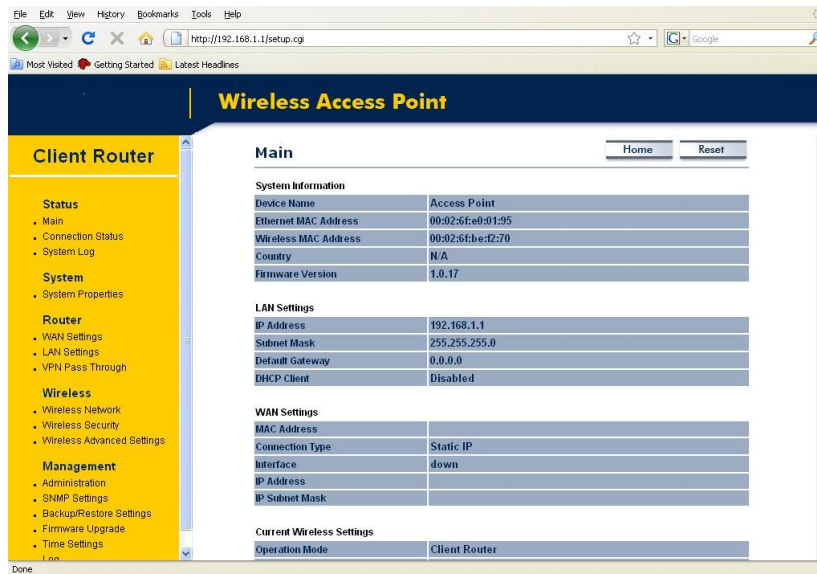
6 Client Router Operating Mode

6.1 Logging In

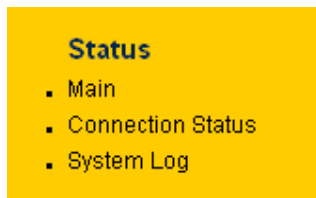
- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.



- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
 1. **Status**: Displays the overall status, connection status, and event log.
 2. **System**: This menu includes the system properties, IP and Spanning Tree settings.
 3. **Router**: This includes WAN, LAN, and VPN settings.
 4. **Wireless**: This menu includes status, basic, advanced, and security.
 5. **Management**: This menu includes the admin setup, SNMP, firmware upgrade, and save/restore backup.



6.2 Status



- Click on the **Status** link on the navigation drop-down menu. You will then see three options: Main, Connection Status, and System Log. Each option is described in detail below.

6.2.1 Main

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, Country, Firmware version, Ethernet MAC Address, Wireless MAC Address and Current Time are displayed in the 'System' section. LAN IP Address, Subnet Mask, Default Gateway and DHCP Server are displayed in the 'LAN' section. In the 'Wireless section, Operation Mode, Wireless Mode, SSID, Security, Channel are displayed. The 'WAN' section displays the MAC address, Connection Type, Interface, IP Address, and Subnet Mask.

Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:e0:00:09
Wireless MAC Address	00:02:6f:12:34:5c
Country	N/A
Current Time	Sat Jan 1 00:06:26 UTC 2000
Firmware Version	1.0.29

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Enabled

WAN Settings

MAC Address	00:02:6f:12:34:5c
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

Current Wireless Settings

Operation Mode	Client Router
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.417GHz (channel 02)
Wireless Network Name (SSID)	default
Security	Disabled
Distance	1 Km

6.2.2 DHCP Client Table

The List shows all connection with DHCP clients.

DHCP Client List

MAC addr	IP	Expires
<input type="button" value="Refresh"/>		

6.2.3 Connection Status

- Click on the **Connection Status** link under the **Status** drop-down menu. This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.

Connection Status

[Home](#) [Reset](#)

Network Type	Client Router
SSID	SMC
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rate(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

[Refresh](#)

6.2.4 System Log

- Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

System Log

[Home](#) [Reset](#)

Show log type: All

Local Log i:
 All
 Debug
 Information
 Notice
 Warning
 Error
 Critical
 Alert
 Emergency

6.3 System

System

- System Properties

- Click on the **System** link on the navigation drop-down menu. You will then see System Properties setting, which is described below.

6.3.1 System Properties

- Click on the **System Properties** link under the **System** drop-down menu. This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

System Properties		Home	Reset
Device Name	<input type="text" value="Client Router"/> (1 to 32 characters)		
Country/Region	<input type="text" value="Please Select a Country Code"/>		
Operation Mode	<input type="radio"/> Access Point <input type="radio"/> Client Bridge <input checked="" type="radio"/> Client Router		

- Device Name:** Specify a name for the device (this is not the SSID),
- Country/Region:** Select a country from the drop-down list.
- Operating Mode:** Select an operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

6.4 Router

Router

- WAN Settings
- LAN Settings
- VPN Pass Through

- Click on the **Router** link on the navigation drop-down menu. You will then see three options: WAN settings, LAN settings, and VPN Pass Through. Each section is described in detail below.

6.4.1 WAN Settings

- Click on the **WAN Settings** link under the **Router** drop-down menu. This page allows you to configure the WAN interface as DHCP, Static IP, or PPPoE.

6.4.1.1 WAN - DHCP

- The WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.

WAN Settings

Home
Reset

Internet Connection Type DHCP ▾

Options

Account Name (if required) none

Domain Name (if required) none

MTU Auto ▾ 1500

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

Apply
Cancel

- Internet Connection Type:** Select the **DHCP** from the drop-down list.
- Account Name:** Specify an account name if your ISP has provided you with one.
- Domain Name:** Specify a domain name if the ISP has provided you with one.
- MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in

extreme cases may be unable to establish some connections. In either case, network performance can suffer.

- **Domain Name Service:** Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- **Router MAC Address:** If you need to change the MAC address of the router's WAN interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on the **Clone MAC** button.
- Click on the **Apply** button to save the changes.

6.4.1.2 WAN – Static IP

- The WAN interface can be configured as Static IP address. In this type of connection, your ISP provides you with a dedicated IP address (which does not change as DHCP).

WAN Settings

[Home](#)
[Reset](#)

Internet Connection Type

Static IP

Options

Account Name (if required)

none

Domain Name (if required)

none

MTU

Auto

1500

Internet IP Address

IP Address

10 . 1 . 1 . 100

IP Subnet Mask

255 . 255 . 0 . 0

Gateway IP Address

10 . 1 . 1 . 150

Domain Name Server (DNS) Address

Primary DNS

0 . 0 . 0 . 0

Secondary DNS

0 . 0 . 0 . 0

Apply

Cancel

- **Internet Connection Type:** Select the **Static IP** from the drop-down list.
- **Account Name:** Specify an account name if your ISP has provided you with one.

- **Domain Name:** Specify a domain name if the ISP has provided you with one.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **IP Address:** Specify the IP address for this device, which is assigned by your ISP.
- **Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.
- **Default Gateway:** Specify the IP address of the default gateway, which is assigned by your ISP.
- **Domain Name Service:** Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- **Router MAC Address:** If you need to change the MAC address of the router's WAN interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on the **Clone** MAC button.
- Click on the **Apply** button to save the changes.

6.4.1.3 WAN – PPPoE

- The WAN interface can be configured as PPPoE. This type of connection is usually used for a DSL service and requires a username and password to connect.

WAN Settings

Internet Connection Type PPPoE ▾

Options

MTU Auto ▾ 1492

PPPoE Options

Login

Password

Service Name (if required)

Connect on Demand: Max idle Time **Minutes**
 Keep Alive: Redial Period **Seconds**

Domain Name Server (DNS) Address

Get Automatically From ISP
 Use These DNS Servers

Primary DNS . . .

Secondary DNS . . .

- **Internet Connection Type:** Select **PPPoE** from the drop-down list.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **Login:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Service Name:** Specify the name of the ISP.
- **Type:** Select a reconnection type: **Keep Alive** (A connection to the Internet is always maintained), **Connect on Demand:** You have to open up the Web-based management interface and click the **Connect** button manually any time that you wish to connect to the Internet.
- **Domain Name Service:** Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

6.4.2 LAN Setting

LAN Settings

LAN IP Setup

IP Address	192	168	1	1
IP Subnet Mask	255	255	255	0
WINS Server IP	0	0	0	0

Use Router As DHCP Server

Starting IP Address	192	168	1	2
Ending IP Address	192	168	1	254

6.4.3 VPN Pass Through

- Click on the **VPN Pass Through** link under the **Router** drop-down menu. This page allows you to enable the pass through feature.

VPN Pass Through

PPTP Pass Through
 L2TP Pass Through
 IPSec Pass Through

- PPTP Pass Through:** Place a check in this box if you would like to enable this pass through. PPTP is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels"
- L2TP Pass Through:** Place a check in this box if you would like to enable this pass through. Layer 2 Tunneling Protocol is a transport protocol that enables tunneling through the Internet for the establishment of virtual private networks.
- IPSec Pass Through:** Place a check in this box if you would like to enable this pass through. IPSec is a VPN protocol used to implement secure exchange of packets at the IP layer.
- Click on the **Apply** button to save the changes.

6.5 Wireless



option is described below.

- Click on the **Wireless** link on the navigation drop-down menu. You will then see three options: wireless network, wireless security, and wireless advanced settings. Each

6.5.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

Wireless Network	
Wireless Mode	802.11b/g Mixed (2.4GHz/54Mbps) ▼
SSID	Specify the static SSID : default (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey

Apply Cancel

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **A**, **B**, **G**, or **B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **A** or **B/G-mixed** for the best performance.
- **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. You may specify an SSID or select one from the **Site Survey**.
- **Site Survey:** Click on the **Site Survey** button in order to scan the 2.4GHz frequency for devices that broadcast their SSID. Click on the **BSSID** link to connect to the Access Point. Click on the **Refresh** button to re-scan the frequency.

Site Survey

2.4GHz Site Survey

:Infrastructure :Ad_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:81:86:21	DinoNet	1	-86 dBm	B	WEP	
00:13:f7:7c:6f:43	SMC	6	-105 dBm	G	NONE	

Refresh

6.5.2 Wireless Security

The **Wireless Security** page allows you to configure the wireless security.

6.5.2.1 Wireless Security - WEP

- **Security Mode:** 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.

Wireless Security

Home

Reset

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WEP
Auth Type	Open Key
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	<input type="text"/>
Key2	<input type="text"/>
Key3	<input type="text"/>
Key4	<input type="text"/>

Apply

Cancel

- **Authentication Type:** Select an authentication method. Options available are **Open Key**, **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 Access Point. 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.

- **Input Type:** Select He or ASCII from the drop-down list
- **Key Length:** 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 Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply** button to save the changes.

6.5.2.2 Wireless Security – WPA-PSK, WPA2-PSK

- **Security Mode:** Select **WPA-PSK**, or **WPA2-PSK** from the drop-down list if your wireless network uses WPA pre-shared key.

Wireless Security		Home	Reset
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.			
Security Mode	WPA2-PSK ▼		
Encryption	TKIP ▼		
Passphrase	<input type="text"/>		(8 to 63 characters)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **Encryption:** Select **TKIP** or **AES** 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.
- **Passphrase:** Specify a passphrase that is shared amongst the Access Points and clients.
- Click on the **Apply** button to save the changes.

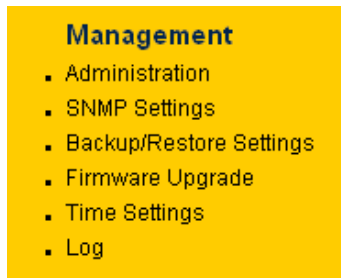
6.5.2.3 Wireless Advanced Settings

- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.

Wireless Advanced Settings	
Data Rate	Auto
Transmit Power	20 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Distance (1-30km)	1 km

- 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.
- Transmit Power:** 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.
- Fragment:** 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.
- Protection Mode:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- WMM:** Enable wireless Quality of Service
- Distance (1-30km):** Specify a distance between 1 and 30Km.
- Click on the **Apply** button to save the changes.

6.6 Management



- Click on the **Management** link on the navigation drop-down menu. You will then see six options: administration, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

6.6.1 Administration

- Click on the **Administration** 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 **admin**. For security reasons it is highly recommended that you create a new user name and password.

Administrator	
Name	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>
Confirm Password	<input type="password" value="•••••"/>
Remote Access	
Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Upgrade	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Management Port	<input type="text" value="8080"/>

- **Name:** Specify a user name into the first field.
- **Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.
- **Remote Management:** Choose to enable or disable remote management.
- **Remote Upgrade:** Choose to enable or disable remote firmware upgrade.
- **Remote Management Port:** Specify a port for remote management. For example, if you specify 8080, then you will need to specify *<IP address>:<port>* 192.168.1.1:8080 to connect to the web interface of the device.
- Click on the **Apply** button to save the changes.

6.6.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases. .

SNMP Settings Home Reset

SNMP Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

Apply Cancel

- SNMP Enable/Disable:** Choose to **enable** or **disable** the SNMP feature.
- Contact:** Specify the contact details of the device.
- Location:** Specify the location of the device.
- 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:** Specify the IP address of the computer that will receive the SNMP traps.
- Trap Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

6.6.3 Backup/Restore, Reset to factory default settings

- Click on the **Backup/Restore 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.

Backup/Restore Settings

[Home](#)[Reset](#)

Save A Copy Of Current Settings

Restore Saved Settings From A File

Revert To Factory Default Settings

- **Save a copy of the current settings:** Click on the Backup button to save the current configuration.
- **Restore saved settings from a file:** Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings:** Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1

System Rebooting...

Rebooting, Please wait... [Click here when AP is ready](#)

6.6.4 Firmware Upgrade

- 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.

Firmware Upgrade

[Home](#)[Reset](#)

Current firmware version: 1.0.17

Locate and select the upgrade file from your hard disk:

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** 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.

6.6.5 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

Time Settings Home Reset

Time

Manually Set Date and Time
2000 / 01 / 01 00 : 02

Automatically Get Date and Time
Time Zone: UTC+00:00 England

User defined NTP Server: 192 . 168 . 1 . 99

Apply Cancel

- **Manually Set Date and Time:** Specify the date and time
- **Automatically Get Date and Time:** Select the time zone from the drop down list and then specify the IP address of the NTP server.
- Click on the **Apply** button to save the changes.

6.6.6 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.

Log Home Reset

Syslog

Syslog	Enable
Log Server IP Address	192 . 168 . 1 . 67

Local log

Local Log	Enable
-----------	--------

Apply Cancel

- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

Appendix A – Specifications

Hardware Specification	
MCU/RF	Atheros AR2313+AR5112
Memory	32MB SDRAM
Flash	8MB
Physical Interface	1 x 10/100 Fast Ethernet RJ-45 1 x Reset Button 1 x Antenna Switch 2 x SMA Connector
LED indicators	Power/ Status LAN (10/100Mbps) WLAN (Wireless is up) 3 x Link Quality (Client Bridge mode) <ul style="list-style-type: none"> • Green: Good Quality • Yellow: Marginally Acceptable Quality • Red: Bad Quality
Power Requirements	Active Ethernet (Power over Ethernet) Proprietary PoE design Power Adapter 24V / 1A DC
Regulation Certifications	FCC Part 15C/15B/15E, EN 300 328/EN 301 489-1/-17

RF Specification															
Frequency Band	802.11a = 5.150~5.350GHz, 5.470~5.725GHz, 5.725~5.825GHz 802.11b/g = 2.412~2.472GHz														
Modulation Technology	OFDM = BPSK, QPSK, 16-QAM, 64-QAM DSSS = DBPSK, DQPSK, CCK														
Operating Channels	802.11a = See the Table1 802.11b/g = 11 for North America, 14 for Japan, 13 for Europe														
Receive Sensitivity (Typical)	802.11a -88dBm @ 6Mbps, -70dBm @ 54Mbps	802.11g -92 dBm @ 6Mbps, -75 dBm @ 54Mbps	802.11b -93 dBm @ 1Mbps -91 dBm @ 11Mbps												
Available transmit power (Average power)	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">FCC</th> <th colspan="2">ETSI</th> </tr> <tr> <th>Frequency</th> <th>Power</th> <th>Frequency</th> <th>Power</th> </tr> </thead> <tbody> <tr> <td>5.150~5.350 GHz</td> <td>28dBm @6~24Mbps 26dBm @36Mbps</td> <td>5.150~5.350 GHz</td> <td>28dBm @6~24Mbps s</td> </tr> </tbody> </table>			FCC		ETSI		Frequency	Power	Frequency	Power	5.150~5.350 GHz	28dBm @6~24Mbps 26dBm @36Mbps	5.150~5.350 GHz	28dBm @6~24Mbps s
FCC		ETSI													
Frequency	Power	Frequency	Power												
5.150~5.350 GHz	28dBm @6~24Mbps 26dBm @36Mbps	5.150~5.350 GHz	28dBm @6~24Mbps s												

	<table border="1"> <tbody> <tr> <td>IEEE802.11a</td> <td>24dBm @48Mbps 22dBm @54Mbps</td> <td>IEEE802.11a</td> <td>26dBm @36Mbps 24dBm @48Mbps 22dBm @ 54Mbps</td> </tr> <tr> <td>5.470~5.725 GHz IEEE802.11a</td> <td>28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps</td> <td>5.470~5.725 GHz IEEE802.11a</td> <td>28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps</td> </tr> <tr> <td>5.725~5.825 GHz IEEE802.11a</td> <td>28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps</td> <td>5.725~5.825 GHz IEEE802.11a</td> <td>28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps</td> </tr> <tr> <td>2.412~2.462 GHz IEEE802.11g</td> <td>28dBm @6~24Mbps 26dBm @36Mbps 25dBm @48Mbps 24dBm @54Mbps</td> <td>2.412~2.472 GHz IEEE802.11g</td> <td>28dBm @6~24Mbps 26dBm @36Mbps 25dBm @48Mbps 24dBm @54Mbps</td> </tr> <tr> <td>2.412~2.462 GHz IEEE802.11b</td> <td>28dBm @1~11Mbps</td> <td>2.412~2.472 GHz IEEE802.11b</td> <td>28dBm @1~11Mbps</td> </tr> </tbody> </table>	IEEE802.11a	24dBm @48Mbps 22dBm @54Mbps	IEEE802.11a	26dBm @36Mbps 24dBm @48Mbps 22dBm @ 54Mbps	5.470~5.725 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps	5.470~5.725 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps	5.725~5.825 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps	5.725~5.825 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps	2.412~2.462 GHz IEEE802.11g	28dBm @6~24Mbps 26dBm @36Mbps 25dBm @48Mbps 24dBm @54Mbps	2.412~2.472 GHz IEEE802.11g	28dBm @6~24Mbps 26dBm @36Mbps 25dBm @48Mbps 24dBm @54Mbps	2.412~2.462 GHz IEEE802.11b	28dBm @1~11Mbps	2.412~2.472 GHz IEEE802.11b	28dBm @1~11Mbps
IEEE802.11a	24dBm @48Mbps 22dBm @54Mbps	IEEE802.11a	26dBm @36Mbps 24dBm @48Mbps 22dBm @ 54Mbps																		
5.470~5.725 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps	5.470~5.725 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps																		
5.725~5.825 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps	5.725~5.825 GHz IEEE802.11a	28dBm @6~24Mbps 26dBm @36Mbps 24dBm @48Mbps 22dBm @54Mbps																		
2.412~2.462 GHz IEEE802.11g	28dBm @6~24Mbps 26dBm @36Mbps 25dBm @48Mbps 24dBm @54Mbps	2.412~2.472 GHz IEEE802.11g	28dBm @6~24Mbps 26dBm @36Mbps 25dBm @48Mbps 24dBm @54Mbps																		
2.412~2.462 GHz IEEE802.11b	28dBm @1~11Mbps	2.412~2.472 GHz IEEE802.11b	28dBm @1~11Mbps																		
Internal Antenna	1 x 5dBi 2.4GHz Panel Antenna + 1 x 13dBi 5GHz Panel Antenna																				
External Antenna	2 x SMA connector (for 2.4GHz and 5GHz individually)																				

Software Features	
General	
Topology	Infrastructure
Protocol / Standard	IEEE 802.3 (Ethernet) IEEE 802.3u (Fast Ethernet) IEEE 802.11b/g (2.4GHz WLAN)
Operation Mode	802.11 a/b/g Access Point Client Bridge Client Router
LAN	DHCP Server DHCP Client
VPN	VPN – pass through

Wireless	Channel Selection (Setting varies by countries) Transmission Rate 11 a/b/g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps Long distance transmission : 1km to 30km (Ack timeout) Transmit power table Signal Strength indication using LEDs PPPoE(CR mode)
Security	WEP Encryption-64/128/152 bit WPA/WPA2 Personal (WPA-PSK using TKIP or AES) WPA/WPA2 Enterprise (WPA-EAP using TKIP) 802.1x Authenticator Hide SSID in beacons MAC address filtering, up to 50 field Wireless STA (Client) connected list
QoS	WMM
Management	
Configuration	Web-based configuration (HTTP)
Firmware Upgrade	- Upgrade firmware via web-browser - Keep latest setting when f/w update
Administrator Setting	Administrator password change
Reset Setting	- Reboot (Press 1 second) - Reset to Factory Default (Press 5 seconds)
System monitoring	Status, Event Log
SNMP	V1, V2c
MIB	MIB I, MIB II (RFC1213)
Backup & Restore	Settings through Web
Time setting	NTP (Auto-setting of time) Time setting manually

Environment & Mechanical	
Temperature Range	Operating -20°C~70°C Storage -30°C to 80°C
Humidity (non-condensing)	0% ~ 90% typical
Dimensions	260mm (L) x 84mm (W) x 55mm (H)
Weight	300g

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.

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.

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.

IMPORTANT NOTE: FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



30.06.2009

EC – Declaration of conformity

For the following product

ALL0258 Gigabit Wireless-N Client Bridge



This equipment conforms with the requirements of the Council Directive **R&TTE 1999/5/EC** on the approximation of the laws of the member states relating to Radio and Telecommunication Terminal Equipment and the mutual recognition of their conformity.

The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The ALL0258 Gigabit Wireless-N Client Bridge conforms to the European Directives 1989/336/EEC.

This equipment meets the following conformance standards:

EN 300 328
EN 301489-1/-17
EN 301 893
EN 50385
EN 60950

This equipment is intended to be operated in all countries.
This declaration is made by

ALLNET Computersysteme GmbH
Maistraße 2
82110 Germering
Germany

and can be downloaded from <http://www.allnet.de/ce-certificates/>

Copyright © 2009. All rights reserved.

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission of the owner. Product specifications contained in this document are subject to change without notice. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

Manufacturer:

ALLNET GmbH



ALLNET Deutschland GmbH
Maistrasse 2
82110 Germering
Tel. +49 89 894 222 22
Fax +49 89 894 222 33
email: info@allnet.de