

11b/g Long Range Multi-function 7+1 AP

ECB3500



User's Manual

Version: 1.1

Table of Contents

TABLE OF CONTENTS	2
REVISION HISTORY	6
1 INTRODUCTION	7
1.1 FEATURES & BENEFITS	7
1.2 PACKAGE CONTENTS	8
1.3 SAFETY GUIDELINES	8
1.4 SYSTEM REQUIREMENTS	9
1.5 APPLICATIONS	9
1.6 NETWORK CONFIGURATION	9
2 UNDERSTANDING THE HARDWARE	11
2.1 HARDWARE INSTALLATION	11
3.1 IP ADDRESS CONFIGURATION	11
3 SWITCHING BETWEEN OPERATING MODES	13
3.1 LOGGING IN	13
4 ACCESS POINT OPERATING MODE	14
4.1 LOGGING IN	15
4.2 STATUS	15
4.2.1 MAIN	16
4.2.2 WIRELESS CLIENT LIST	16
4.2.3 SYSTEM LOG	17
4.3 SYSTEM	17
4.3.1 SYSTEM PROPERTIES	17
4.3.2 IP SETTINGS	18
4.3.3 SPANNING TREE SETTINGS	19
4.4 WIRELESS	20
4.4.1 WIRELESS NETWORK	20
4.4.1.1 WIRELESS SECURITY - WEP	21
4.4.1.2 WIRELESS SECURITY – WPA-PSK, WPA2-PSK, WPA-Mixed	23
4.4.1.3 WIRELESS SECURITY – WPA, WPA2	23
4.4.2 WIRELESS MAC FILTER	24
4.4.3 WDS LINK SETTINGS	25
4.4.4 WIRELESS ADVANCED SETTINGS	25
4.5 MANAGEMENT	27
4.5.1 ADMINISTRATION	27
4.5.2 MANAGEMENT VLAN	28
4.5.3 SNMP SETTINGS	28
4.5.4 BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	29
4.5.5 FIRMWARE UPGRADE	30
4.5.6 TIME SETTINGS	31
4.5.7 LOG	31
5 CLIENT BRIDGE OPERATING MODE	32
5.1 LOGGING IN	32
5.2 STATUS	33
5.2.1 MAIN	33
5.2.2 CONNECTION STATUS	34
5.2.3 SYSTEM LOG	35
5.3 SYSTEM	36

5.3.1	SYSTEM PROPERTIES	36
5.3.2	IP SETTINGS	36
5.3.3	SPANNING TREE SETTINGS	37
5.4	WIRELESS	39
5.4.1	WIRELESS NETWORK	39
5.4.2	WIRELESS SECURITY - WEP	40
5.4.3	WIRELESS SECURITY – WPA-PSK, WPA2-PSK,	41
5.4.4	WIRELESS ADVANCED SETTINGS	41
5.5	MANAGEMENT	42
5.5.1	ADMINISTRATION	43
5.5.2	SNMP SETTINGS	43
5.5.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	44
5.5.4	FIRMWARE UPGRADE	45
5.5.5	TIME SETTINGS	45
5.5.6	LOG	46
6	WDS BRIDGE OPERATING MODE.....	47
6.1	LOGGING IN	47
6.2	STATUS	48
6.2.1	MAIN	48
6.2.2	WDS LINK STATUS	49
6.2.3	SYSTEM LOG	49
6.3	SYSTEM	50
6.3.1	SYSTEM PROPERTIES	50
6.3.2	IP SETTINGS	51
6.3.3	SPANNING TREE SETTINGS	52
6.4	WIRELESS	53
6.4.1	WIRELESS NETWORK	53
6.4.2	WDS LINK SETTINGS	53
6.4.3	WDS SECURITY - WEP	54
6.4.4	WIRELESS ADVANCED SETTINGS	55
6.5	MANAGEMENT	56
6.5.1	ADMINISTRATION	56
6.5.2	SNMP SETTINGS	56
6.5.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	57
6.5.4	FIRMWARE UPGRADE	58
6.5.5	TIME SETTINGS	59
6.5.6	LOG	59
7	REPEATER OPERATING MODE.....	60
7.1	LOGGING IN	60
7.2	STATUS	61
7.2.1	MAIN	61
7.2.2	WIRELESS CLIENT LIST	62
7.2.3	CONNECTION STATUS	62
7.2.4	SYSTEM LOG	63
7.3	SYSTEM	64
7.3.1	SYSTEM PROPERTIES	64
7.3.2	IP SETTINGS	64
7.3.3	SPANNING TREE SETTINGS	65
7.4	WIRELESS	66
7.4.1	WIRELESS NETWORK	66
7.4.2	WIRELESS SECURITY - WEP	67
7.4.3	WIRELESS SECURITY - WPA-PSK, WPA2-PSK	68
7.4.4	WIRELESS MAC FILTER	68
7.4.5	WIRELESS ADVANCED SETTINGS	69

7.5	MANAGEMENT	70
7.5.1	ADMINISTRATION	70
7.5.2	SNMP SETTINGS	70
7.5.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	71
7.5.4	FIRMWARE UPGRADE.....	72
7.5.5	TIME SETTINGS	72
7.5.6	LOG	73
8	AP ROUTER OPERATING MODE.....	74
8.1	LOGGING IN.....	74
8.2	STATUS.....	75
8.2.1	MAIN.....	75
8.2.2	WIRELESS CLIENT LIST	76
8.2.3	DHCP CLIENT LIST	76
8.2.4	SYSTEM LOG.....	77
8.3	SYSTEM	77
8.3.1	SYSTEM PROPERTIES	77
8.4	ROUTER.....	78
8.4.1	WAN SETTINGS	78
8.4.1.1	WAN - DHCP	78
8.4.1.2	WAN – STATIC IP	79
8.4.1.3	WAN – PPPoE	81
8.4.2	VPN PASS THROUGH	82
8.5	WIRELESS.....	82
8.5.1	WIRELESS NETWORK.....	82
8.5.1.1	WIRELESS SECURITY - WEP	83
8.5.1.2	WIRELESS SECURITY – WPA-PSK, WPA2-PSK,.....	84
8.5.2	WIRELESS MAC FILTER.....	85
8.5.3	WDS LINK SETTINGS.....	86
8.5.4	WIRELESS ADVANCED SETTINGS.....	86
8.6	MANAGEMENT	87
8.6.1	ADMINISTRATION	87
8.6.2	SNMP SETTINGS	88
8.6.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	88
8.6.4	FIRMWARE UPGRADE.....	89
8.6.5	TIME SETTINGS	90
8.6.6	LOG	90
9	CLIENT ROUTER OPERATING MODE.....	92
9.1	LOGGING IN.....	92
9.2	STATUS.....	93
9.2.1	MAIN.....	93
9.2.2	CONNECTION STATUS.....	94
9.2.3	SYSTEM LOG.....	95
9.3	SYSTEM	95
9.3.1	SYSTEM PROPERTIES	95
9.4	ROUTER.....	96
9.4.1	WAN SETTINGS	96
9.4.1.1	WAN - DHCP	96
9.4.1.2	WAN – STATIC IP	98
9.4.1.3	WAN – PPPoE	99
9.4.2	VPN PASS THROUGH	100
9.5	WIRELESS.....	101
9.5.1	WIRELESS NETWORK.....	101
9.5.1.1	WIRELESS SECURITY - WEP	102
9.5.1.2	WIRELESS SECURITY – WPA-PSK, WPA2-PSK,.....	103

9.5.2	WIRELESS ADVANCED SETTINGS.....	103
9.6	MANAGEMENT	104
9.6.1	ADMINISTRATION	105
9.6.2	SNMP SETTINGS	105
9.6.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS	106
9.6.4	FIRMWARE UPGRADE.....	107
9.6.5	TIME SETTINGS	107
9.6.6	LOG	108
APPENDIX A – SPECIFICATIONS.....		109
HARDWARE SPECIFICATIONS		109
RF SPECIFICATIONS		109
SOFTWARE FEATURES		110
MANAGEMENT.....		110
APPENDIX B – FCC INTERFERENCE STATEMENT		112
FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT		112
IMPORTANT NOTE:		112
FCC RADIATION EXPOSURE STATEMENT:		112

Revision History

Version	Date	Notes
1.0	September 14, 2008	Initial Version
1.1	December 15, 2008	GUI and product spec

1 Introduction

ECB3500 is a powerful, enhanced, enterprise level product that supports 7 multi-functions to operate for every kind of working environment.

This is a Wireless high transmit output power and high data rate indoor device which plays different roles of Access Point/ Client Bridge / Repeater / WDS AP / WDSBridge / Client Router / AP Router. It operates seamlessly in the 2.4 GHz frequency spectrum supporting the 802.11b (2.4GHz, 11Mbps) and super high speed of 802.11g (2.4GHz, 108Mbps) wireless standards. It supports high output power level settings, bandwidth selection, RSSI indicator and antenna diversity which enable the best transmitting and receiving signal for traffic communication.

For more sensitive security requirements, ECB3500 can encrypt all wireless transmissions through WEP data encryption and WPA/WPA2. ECB3500 also supports IEEE 802.1x Supplicant function in CB mode, and authenticator in AP mode. Those are the enhanced security features in AP/CB mode. The MAC address filter lets you select any stations that should have access to your network. The User isolation function can protect the private network between client users. Normally, ECB3500 offers mighty security function for your network safety.

The attractive design, high performance, and array of features make ECB3500 a suitable wireless solution for your residence or office.

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

1.1 Features & Benefits

Features	Benefits
Super G solution up to 108Mbps	Capable of handling heavy data payloads such as MPEG, video streaming, large file transfer and VoIP
High Output Power up to 28 dBm	Extended excellent Range and Coverage (fewer APs)
IEEE 802.11b/g Compliant	Fully Interoperable with IEEE 802.11b/IEEE802.11g compliant devices
7+1 Multi Functions	Access Point/Client Bridge/Repeater/WDS AP/ WDS Bridge/Client Router/AP Router
Point-to-multipoint Wireless connectivity	Let users transfer data between two buildings or multiple buildings
WDS (Wireless Distributed System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater
Universal Repeater	The easiest way to expand your wireless networking coverage
Support Multi-SSID function (4 BSSID) in AP mode	Allow clients to access different networks through a single access point and assign different policies and functions for each SSID by manager

Antenna diversity support	Enhance the traffic signal
WPA2/WPA/ IEEE 802.1x support	Powerful data security
802.1x Supplicant support (CB mode)	More sensitive data security in Client Bridge mode
MAC address filtering in AP mode(up to 50)	Ensure the security of network connections
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)	Power supply via Ethernet cable which makes the setup more flexible avoids restricting from wiring lines.

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 High power multi-function 7+1 AP (ECB3500)
- 1* 12V/1A Power Adapter
- 1* CAT5 UTP Cable
- 1* QIG
- 1* CD (User's Manual)
- 2* 5dBi 2.4GHz Dipole Antennas

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 expose this unit to direct sunlight.
- 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.

1.6 Network Configuration

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

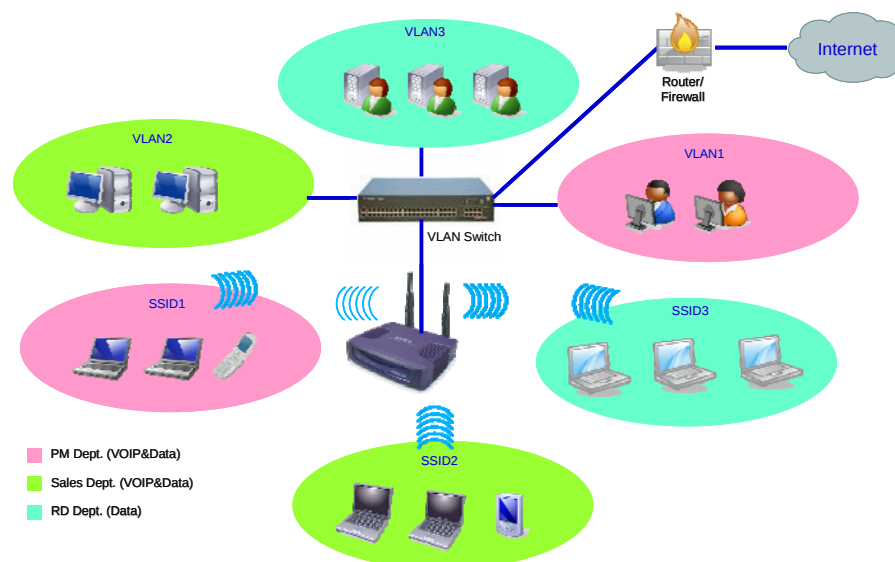
- a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
- b) Infrastructure for enterprise LANs.

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

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

b) Infrastructure Mode

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

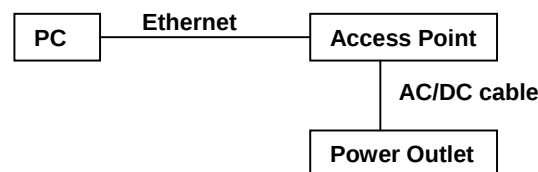


2 Understanding the Hardware

2.1 Hardware Installation

- 1 Place the unit in an appropriate place after conducting a site survey.
- 2 Plug one end of the Ethernet cable into the RJ-45 port on the rear panel of the device and another end into your PC/Notebook.
- 3 Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.

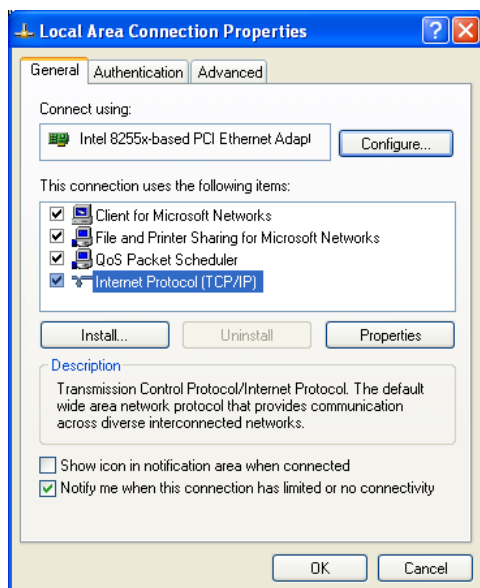
This diagram depicts the hardware configuration



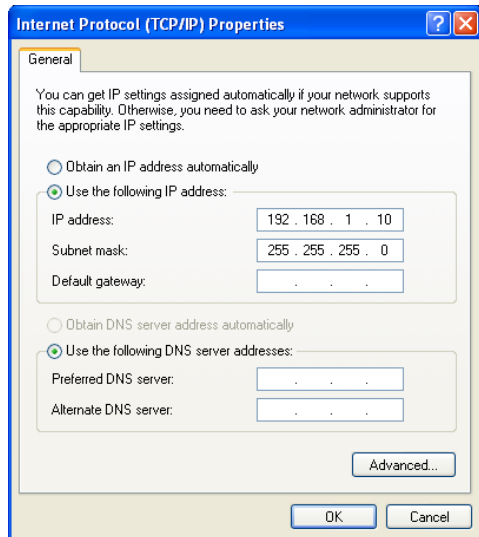
3.1 IP Address Configuration

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: 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 Switching Between Operating Modes

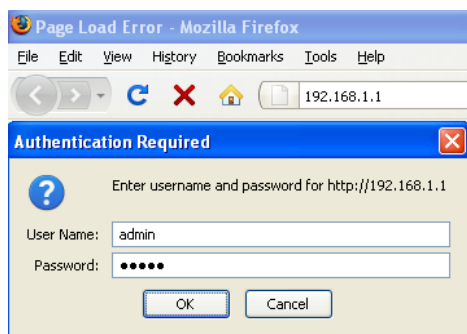
This device can operate in the following modes:

- a) Access Point / WDS AP
- b) Client Bridge
- c) WDS Bridge
- d) Repeater
- e) AP Router
- f) 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.

Home Reset

System Properties	
Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code ▼
Operation Mode	☒ Access Point ☐ Client Bridge ☐ WDS Bridge ☐ Repeater ☐ AP Router ☐ Client Router

Apply Cancel

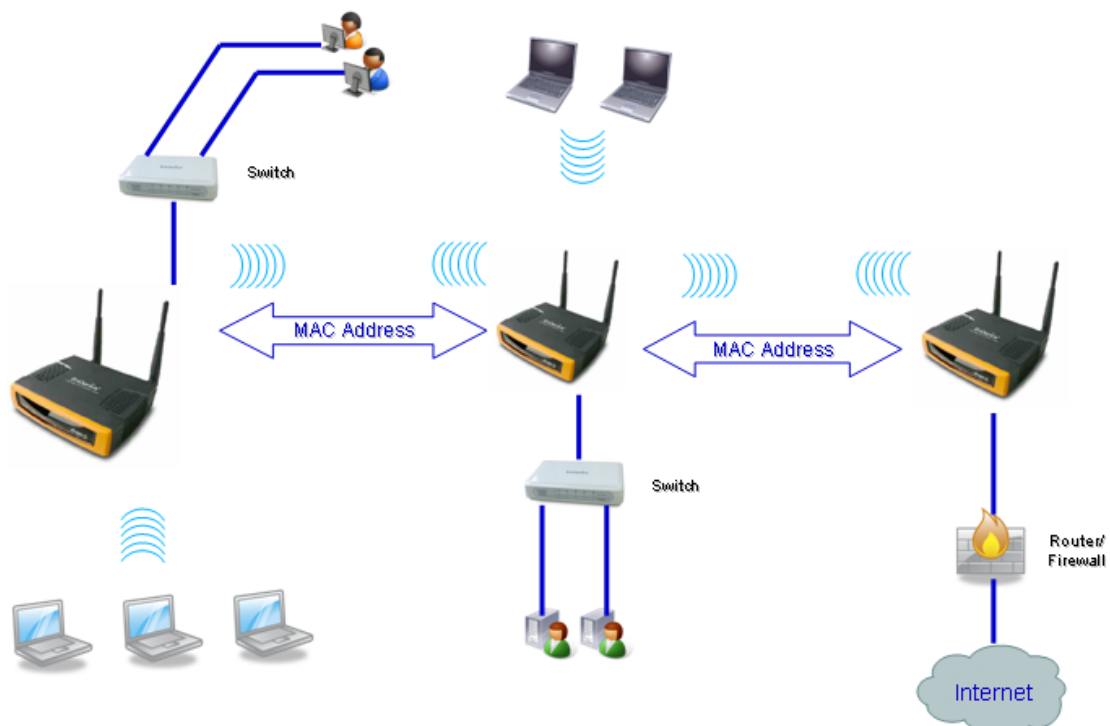
- Select and operating mode from the drop-down list and then click on the **Apply** button.

4 Access Point / WDS Operating Mode

Access Point

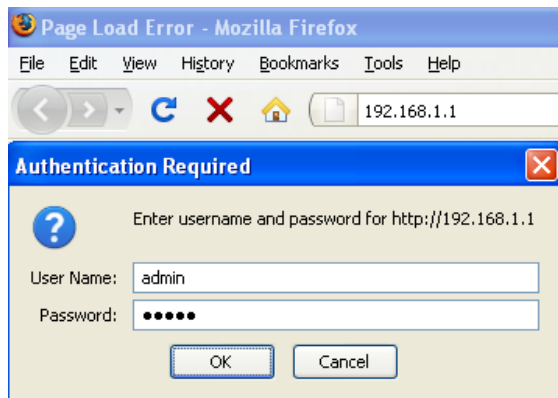


WDS AP

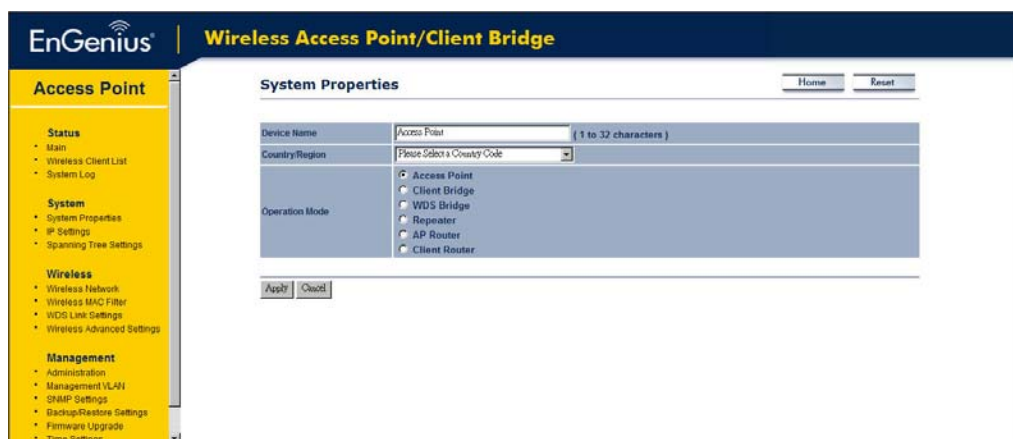


4.1 Logging In

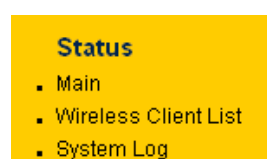
- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure 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, wireless client list, and system log.
 2. **System:** This menu includes the system properties, IP and Spanning Tree settings.
 3. **Wireless:** This menu includes wireless network status, MAC filter, WDS settings, and wireless advanced settings.
 4. **Management:** This menu includes the admin setup, SNMP, VLAN management, 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 operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless' section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed.

Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 00:16:45 UTC 2000
Firmware Version	1.0.27
Management VLAN ID	Untagged

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)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 EnGenius1/Open System/No Encryption/1
	2 N/A
	3 N/A
	4 N/A
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
- NOTE: You will only see the client when you have other wireless devices connected.

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

#	MAC Addr	RSSI(dBm)
1	00:22:43:24:b8:5e	-90

[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 LogShow log type

Local Log is disabled.

[Refresh](#)[Clear](#)

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

Device Name	Access Point (1 to 32 characters)
Country/Region	United States
Operation Mode	☒ Access Point ☐ Client Bridge ☐ WDS Bridge ☐ Repeater ☐ AP Router ☐ 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.

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

IP Network Setting	☐ Obtain an IP address automatically (DHCP) ☒ Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0

- **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

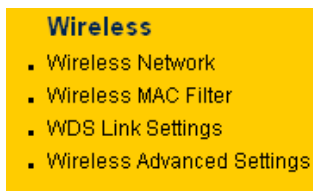
- Click on the **Spanning Tree** link under the **System** drop-down menu Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

Spanning Tree Settings

Spanning Tree Status	☐ On ☒ Off
Bridge Hello Time	1 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	4 seconds (4-30)
Priority	32768 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.

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 Mode: 802.11b/g Mixed (2.4GHz/54Mbps) ▼

Channel / Frequency: Ch1-2.412GHz ▼

Current Profiles				
SSID	Security	VID	Enable	Edit
EnGenius1	Open System/No Encryption	1	☒	Edit
EnGenius2	Open System/No Encryption	2	☐	Edit
EnGenius3	Open System/No Encryption	3	☐	Edit
EnGenius4	Open System/No Encryption	4	☐	Edit

Profile (SSID) Isolation: ☒ No Isolation ☐ Isolate all Profiles (SSIDs) from each other using VLAN (802.1Q) standard

Apply Cancel

- Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **B**, **G**, **B/G-mixed** and **SuperG**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.

Note:

In order to achieve 108Mbps data rate, you will need to check the client card is supporting to 108Mbps as well. If your client device is not super G supported, you can only get 54Mbps throughput only.

The AP default is set as Dynamic Super-G mode, which means if there is any non-super-G supported client surrounded, the AP will switch to normal G automatically.

- 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.
- Current Profiles:** You may configure up to four different wireless profiles. Click on the **Edit** button to modify the profile and place a check in the **Enable** box to activate the profile.

SSID Profile

Wireless Setting	
SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	☐
Station Separation	☐ Enable ☒ Disable

Wireless Security	
Security Mode	Disabled Disabled WEP WPA-PSK WPA2-PSK WPA-PSK Mixed WPA WPA2 WPA Mixed

- **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.
- **VLAN ID:** If you have enabled VLAN tagging on your network, specify the VLAN tag ID.
- **Suppressed SSID:** Place a check in this box if you would like to hide the SSID. By enabling this feature, wireless clients will not be able to scan this access point in a site survey.
- **Station Separation:** This is also known as layer 2 isolation. Clients connected to this Access Point will not be able to directly communicate with each other.
- **Security Mode:** By default, the security is disabled. Refer to the next section to configure the security features such as WEP, WPA, WPA-PSK, WPA2, WPA2-PSK and WPA-Mixed
- Click on the **Apply** button to save the changes.

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.

SSID Profile

Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	☐
Station Separation	☒ Enable ☐ Disable

Wireless Security

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

- **Authentication Type:** Select an authentication method. Options available are **Open System**, **Shared Key**. 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 Hex 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.

SSID Profile

Wireless Setting	
SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	☐
Station Separation	☒ Enable ☐ Disable

Wireless Security	
Security Mode	WPA-PSK
Encryption	Auto
Passphrase	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
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. 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.

SSID Profile

Wireless Setting

SSID	EnGenius1	(1 to 32 characters)
VLAN ID	1	(1~4095)
Suppressed SSID	☐	
Station Separation	☒ Enable ☐ 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)

Save

Cancel

- **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

Home

Reset

ACL Mode
 : : : : :

#	MAC Address	
1	00:11:22:33:44:55	Delete

Apply

- **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 WDS Link Settings

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

WDS Link Settings Home Reset

Notice: When enabling isolation function, WDS function will be disabled automatically.

ID	MAC Address	Mode
1	: : : : :	Disable ▾
2	: : : : :	Disable ▾
3	: : : : :	Disable ▾
4	: : : : :	Disable ▾
5	: : : : :	Disable ▾
6	: : : : :	Disable ▾
7	: : : : :	Disable ▾
8	: : : : :	Disable ▾

Apply Cancel

- **WDS MAC Address:** Specify the MAC address of the Access Points that will join the WDS network and then select Enable or Disable from the drop-down list.
- Click on the **Apply** button to save the changes.

4.4.4 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, antenna diversity, fragmentation threshold, RTS threshold, 802.11g protection and distance.

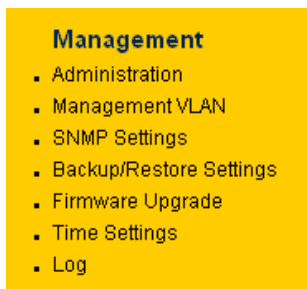
Wireless Advanced Settings

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

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.
- **Antenna:**
- **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:** Choose to enable or disable wireless multimedia mode.
- 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, management VLAN, 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.

Administration

Administrator

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

- **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 Management VLAN

- Click on the **SNMP** link under the **Management** menu. This option allows you to assign a VLAN tag to the packets. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN

Management VLAN Settings

Home

Reset

Caution: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID

☒ No VLAN tag
☐ Specified VLAN ID:
 (must be in the range 1 ~ 4095.)

Apply

Cancel

- Management VLAN ID:** If your network includes VLANs and if tagged packets need to pass through the Access Point, specify the VLAN ID into this field. If not, select the **No VLAN tag** radio button.
- Note:** If you reconfigure the Management VLAN ID, you may lose connectivity to the Access Point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.
- Click on the **Apply** button to save the changes.

4.5.3 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, 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

SNMP Enable/Disable	☒ Enable ☐ Disable
Contact	
Location	
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.
- **Trap Destination IP Address:** Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Destination Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

4.5.4 Backup/Restore settings, 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.

The screenshot shows the 'Backup/Restore Settings' page. At the top, there are two buttons: 'Home' and 'Reset'. Below this, the page is divided into three main sections, each with a label on the left and a button on the right:

- Save A Copy Of Current Settings** with a **Backup** button.
- Restore Saved Settings From A File** with a text input field, a **Browse...** button, and a **Restore** button.
- Revert To Factory Default Settings** with a **Factory Default** button.

- **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](#)

4.5.5 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

HomeReset

Current firmware version: 1.0.27

Locate and select the upgrade file from your hard disk:

Browse...

Upgrade

- 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.

4.5.6 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.

4.5.7 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

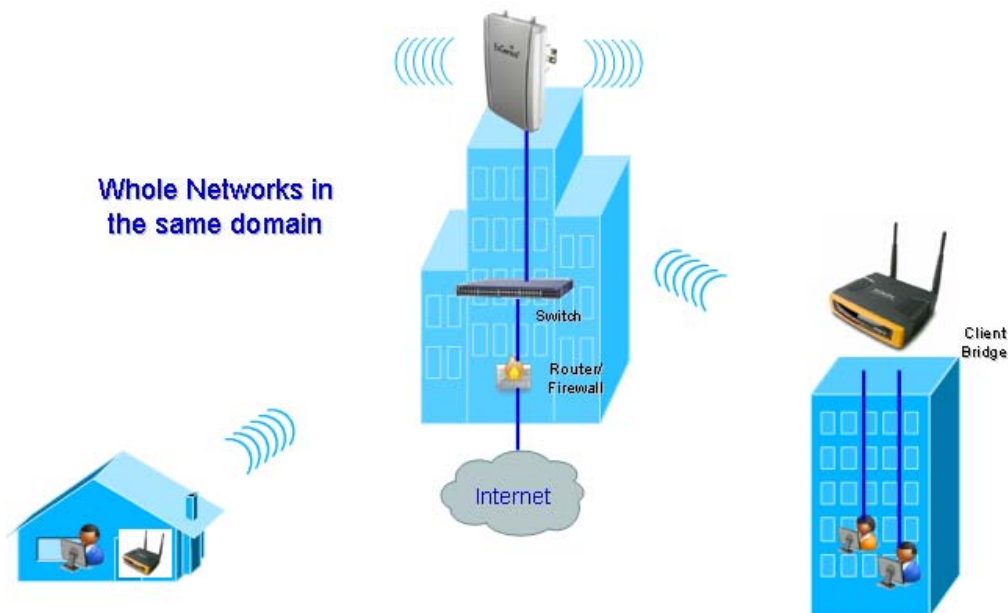
Local log

Local Log Enable

Apply Cancel

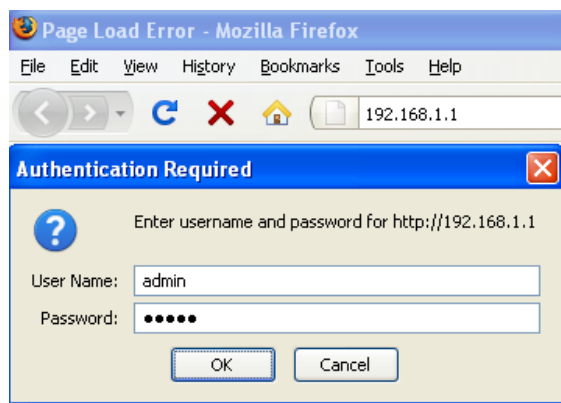
- Syslog:** Choose to enable or disable the system log.
- Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

5 Client Bridge Operating Mode



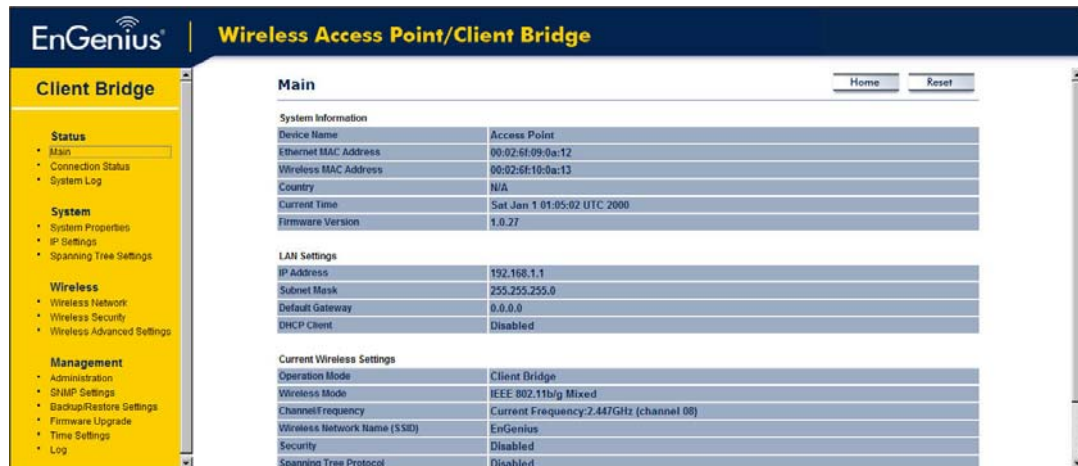
5.1 Logging In

- 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.

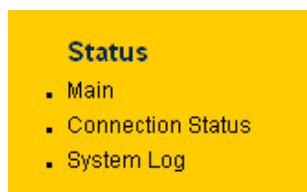


- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
 1. **Status:** Displays the overall status, connection status, and event log.

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, VLAN management, 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 operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless' section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed.

Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 01:06:58 UTC 2000
Firmware Version	1.0.27

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)	EnGenius
Security	Disabled
Spanning Tree Protocol	Disabled
Distance	1 Km

[Refresh](#)

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

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.

System Log

Show log type

Local Log is disabled.

[Refresh](#) [Clear](#)

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.

System Properties

Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	☐ Access Point ☒ Client Bridge ☐ WDS Bridge ☐ Repeater ☐ AP Router ☐ Client Router

Apply Cancel

- **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

IP Network Setting	☐ Obtain an IP address automatically (DHCP) ☒ 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

Spanning Tree Status	☐ On ☒ Off
Bridge Hello Time	1 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	4 seconds (4-30)
Priority	32768 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.

5.4 Wireless



- 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

Wireless Mode	802.11b/g Mixed (2.4GHz/54Mbps) ▼
SSID	Specify the static SSID : EnGenius (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey
Prefer BSSID	☐ : ☐ : ☐ : ☐ : ☐ (Optional)
WDS Support	☒ Enable ☐ Disable

- Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **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 **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.
- Prefer BSSID**
- WDS Support**

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:0f:43	SMC	6	-105 dBm	G	NONE	

Refresh

5.4.2 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 System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

Apply Cancel

- **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 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.

5.4.3 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	WPA-PSK
Encryption	TKIP
Passphrase	(8 to 63 characters) or (64 Hexadecimal 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.

5.4.4 Wireless Advanced Settings

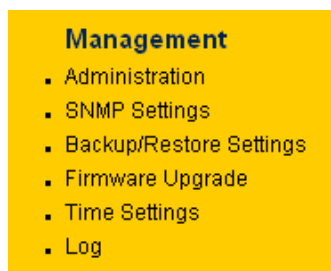
- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, antenna diversity, fragmentation threshold, RTS threshold, 802.11g protection and distance.

Wireless Advanced Settings

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

- **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.
- **Antenna:**
- **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:** Choose to enable or disable wireless multimedia mode.
- Click on the **Apply** button to save the changes.

5.5 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.

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

Administrator

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

- 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, 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

SNMP Enable/Disable	☒ Enable ☐ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0.0.0.0
Trap Destination Community Name	public

- **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 settings, 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	Backup		
Restore Saved Settings From A File		Browse...	Restore
Revert To Factory Default Settings	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](#)

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.

Firmware Upgrade

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

Current firmware version: 1.0.27

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.

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

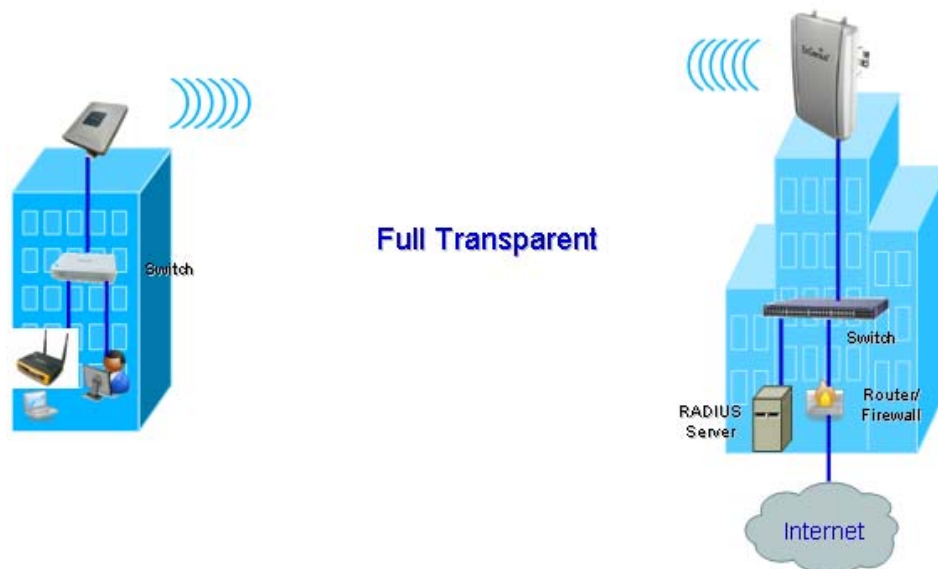
Local log

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

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

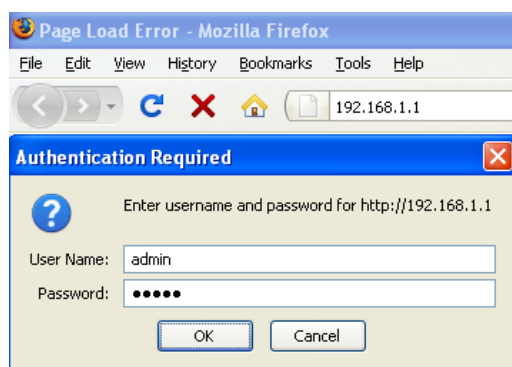
- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

6 WDS Bridge Operating Mode



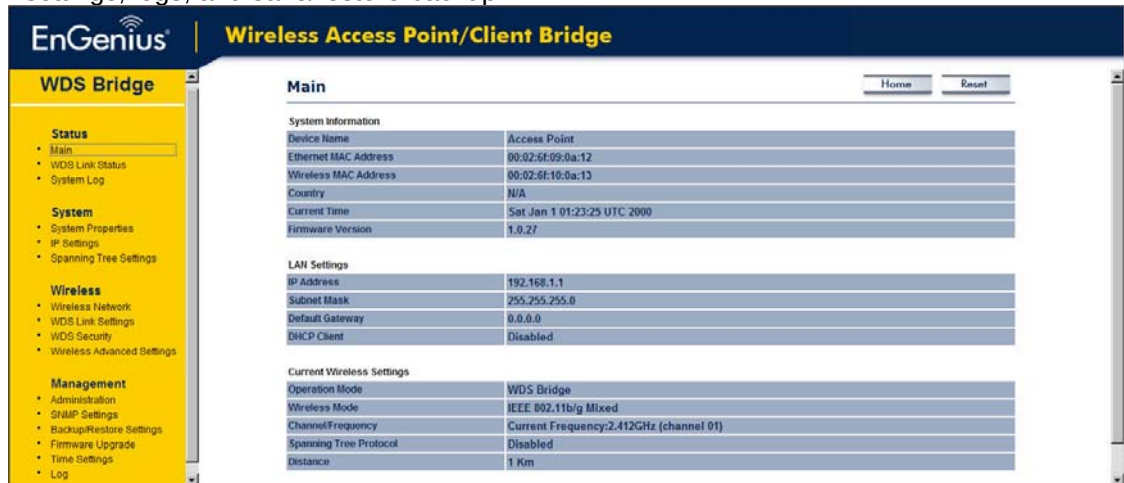
6.1 Logging In

- 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.



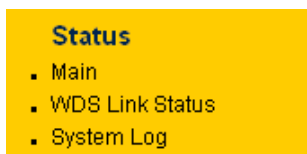
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
 1. **Status:** Displays the overall status, WDS link status, and system log.
 2. **System:** This menu includes the system properties.

3. **Wireless:** This menu includes status, basic, WDS link settings, WDS security, and wireless advanced settings.
4. **Management:** This menu includes the admin setup, SNMP, firmware upgrade, time settings, logs, and save/restore backup



y

6.2 Status



- Click on the **Status** link on the navigation drop-down menu. You will then see three options: Main, WDS Link 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 operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless' section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed.

Main

HomeReset

System Information	
Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 00:28:01 UTC 2000
Firmware Version	1.0.27

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	WDS Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	Current Frequency:2.412GHz (channel 01)
Spanning Tree Protocol	Disabled
Distance	1 Km

Refresh

6.2.2 WDS Link Status

- Click on the **WDS Link Status** link under the **Status** drop-down menu. This page displays the current status of WDS link, including station ID, MAC address, status and RSSI.

WDS Link Status

HomeReset

Station ID	MAC Address	Status	RSSI (dBm)
------------	-------------	--------	------------

Refresh

6.2.3 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

Show log type:

Local Log is disabled.

6.3 System

System

- System Properties
- IP Settings
- Spanning Tree Settings

- Click on the **System** link on the navigation drop-down menu. You will then see 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	WDS Bridge (1 to 32 characters)
Country/Region	United States ▼
Operation Mode	☐ Access Point ☐ Client Bridge ☒ WDS Bridge ☐ Repeater ☐ AP Router ☐ 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.

-

6.3.2 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

IP Network Setting	☐ Obtain an IP address automatically (DHCP) ☒ 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.

▪

6.3.3 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

Spanning Tree Status	☐ On ☒ Off
Bridge Hello Time	1 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	4 seconds (4-30)
Priority	32768 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.

6.4 Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see four options: Wireless Network, WDS Link Settings, WDS Security, and Wireless Advanced Settings. Each option is described below.

6.4.1 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) ▼
Channel / Frequency	Ch1-2.412GHz ▼
SSID	EnGenius

- Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **B**, **G**, **B/G-mixed**, and **SuperG**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- 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.
- 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**.
- Click on the **Apply** button to save the changes.

6.4.2 WDS Link Settings

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

WDS Link Settings

Home

Reset

ID	MAC Address	Mode
1		Disable
2		Disable
3		Disable
4		Disable
5		Disable
6		Disable
7		Disable
8		Disable
9		Disable
10		Disable
11		Disable
12		Disable
13		Disable
14		Disable
15		Disable
16		Disable

Apply Cancel

- **WDS MAC Address:** Specify the MAC address of the Access Points that will join the WDS network and then select Enable or Disable from the drop-down list.
- Click on the **Apply** button to save the changes.

6.4.3 WDS Security - WEP

- Click on the **WDS Security** link. On this page you can configure the settings for the WEP key.

WDS Security

Security	WEP	
WEP Key		40/ 64-bit(10 hex digits)
		40/ 64-bit(10 hex digits) 104/128-bit(26 hex digits) 128/152-bit(32 hex digits)
Apply Cancel		

- **Security:** 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.
- **WEP Key:** Select an encryption type from the drop-down list and then specify the WEP key.
- Click on the **Apply** button to save the changes.

6.4.4 Wireless Advanced Settings

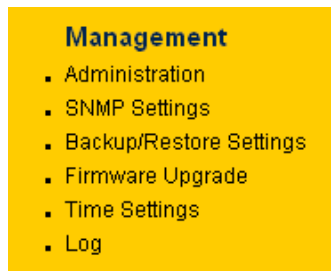
- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, antenna diversity, fragmentation threshold, RTS threshold, 802.11g protection and distance.

Wireless Advanced Settings

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

- 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.
- Antenna:**
- 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:** Choose to enable or disable wireless multimedia mode.
- Click on the **Apply** button to save the changes.

6.5 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.

6.5.1 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

Administrator

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

- **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.

6.5.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, 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	☐ Disable ☒ Enable		
Contact	admin		
Location	US		
Community Name (Read Only)	public		
Community Name (Read/Write)	private		
Trap Destination IP Address	192 . 168 . 1 . 78		
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.

6.5.3 Backup/Restore settings, 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	Backup		
Restore Saved Settings From A File	Browse... Restore		
Revert To Factory Default Settings	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](#)

6.5.4 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: 1.0.27

Locate and select the upgrade file from your hard disk:

 [Browse...](#)[Upgrade](#)

- 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.

6.5.5 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.

6.5.6 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

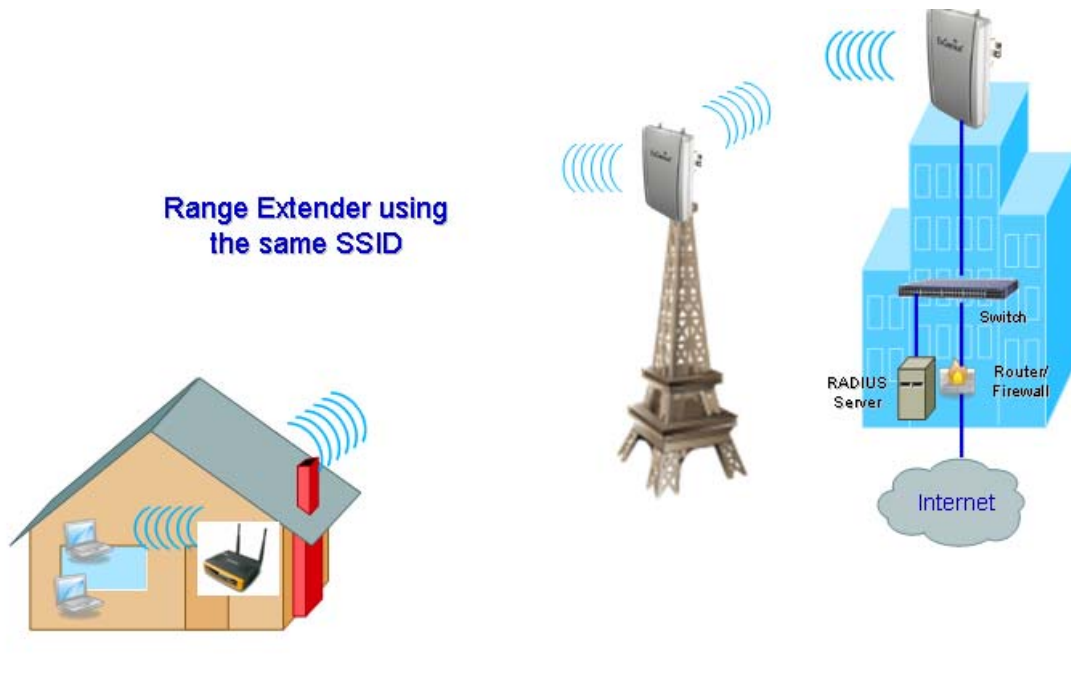
Local log

Local Log Enable

Apply Cancel

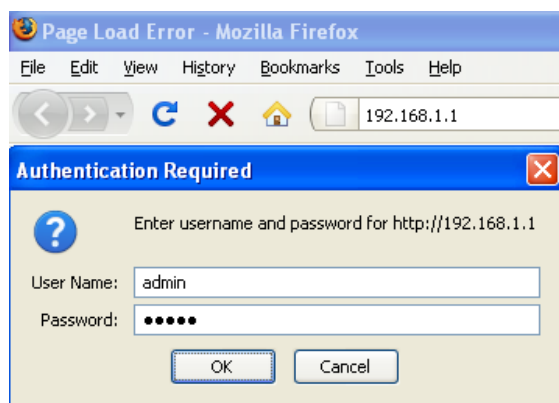
- Syslog:** Choose to enable or disable the system log.
- Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

7 Repeater Operating Mode



7.1 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, wireless client list, connection status, and system 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, time settings, log, and save/restore backup.

EnGenius | **Wireless Access Point/Client Bridge**

Repeater

- Status**
 - Main
 - Wireless Client List
 - Connection Status
 - System Log
- System**
 - System Properties
 - IP Settings
 - Spanning Tree Settings
- Wireless**
 - Wireless Network
 - Wireless Security
 - Wireless MAC Filter
 - Wireless Advanced Settings
- Management**
 - Administration
 - SNMP Settings
 - Backup/Restore Settings
 - Firmware Upgrade
 - Time Settings
 - Log

Main [Home] [Reset]

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 01:49:14 UTC 2000
Firmware Version	1.0.27

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	Repeater
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	Current Frequency:2.442GHz (channel 07)
Spanning Tree Protocol	Disabled
Distance	1 Km

[Refresh]

7.2 Status

Status

- Main
- Wireless Client List
- Connection Status
- System Log

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

7.2.1 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 operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless' section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed.

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 01:49:14 UTC 2000
Firmware Version	1.0.27

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	Repeater
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	Current Frequency:2.442GHz (channel 07)
Spanning Tree Protocol	Disabled
Distance	1 Km

7.2.2 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

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

7.2.3 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

Network Type	Repeater
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

7.2.4 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

Show log type

Local Log is disabled.

7.3 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.

7.3.1 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

Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	☐ Access Point ☐ Client Bridge ☐ WDS Bridge ☒ Repeater ☐ AP Router ☐ 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.

7.3.2 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

IP Network Setting	☐ Obtain an IP address automatically (DHCP) ☒ 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.

7.3.3 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

Spanning Tree Status	☐ On ☒ Off
Bridge Hello Time	1 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	4 seconds (4-30)
Priority	32768 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.

7.4 Wireless

Wireless

- Wireless Network
- Wireless Security
- Wireless MAC Filter
- Wireless Advanced Settings

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

7.4.1 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 : EnGenius (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey
Prefer BSSID	: : : : : (Optional)
WDS Support	☒ Enable ☐ Disable

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **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 **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:0f:43	SMC	6	-105 dBm	G	NONE	

Refresh

- **Prefer BSSID**
- **WDS Support**

7.4.2 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 System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

Apply Cancel

- **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 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.

7.4.3 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	WPA-PSK
Encryption	TKIP
Passphrase	(8 to 63 characters) or (64 Hexadecimal 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.

7.4.4 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 Home Reset

ACL Mode Deny MAC in the List

: : : : : Add

#	MAC Address	
1	00:11:22:33:44:55	Delete

Apply

- **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.

7.4.5 Wireless Advanced Settings

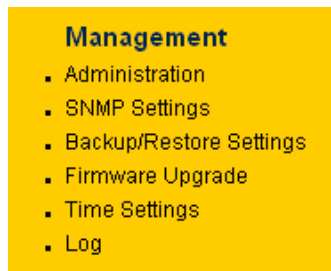
- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, antenna diversity, fragmentation threshold, RTS threshold, 802.11g protection and distance.

Wireless Advanced Settings

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

- **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:** Choose to enable or disable wireless multimedia mode.
- Click on the **Apply** button to save the changes.

7.5 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.

7.5.1 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

Administrator

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

- **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.

7.5.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, 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	☐ Disable ☒ Enable		
Contact	admin		
Location	US		
Community Name (Read Only)	public		
Community Name (Read/Write)	private		
Trap Destination IP Address	192 . 168 . 1 . 78		
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.

7.5.3 Backup/Restore settings, 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	Backup		
Restore Saved Settings From A File	Browse... Restore		
Revert To Factory Default Settings	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](#)

7.5.4 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

HomeReset

Current firmware version: 1.0.27

Locate and select the upgrade file from your hard disk:

Browse...

Upgrade

- 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.

7.5.5 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.

7.5.6 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

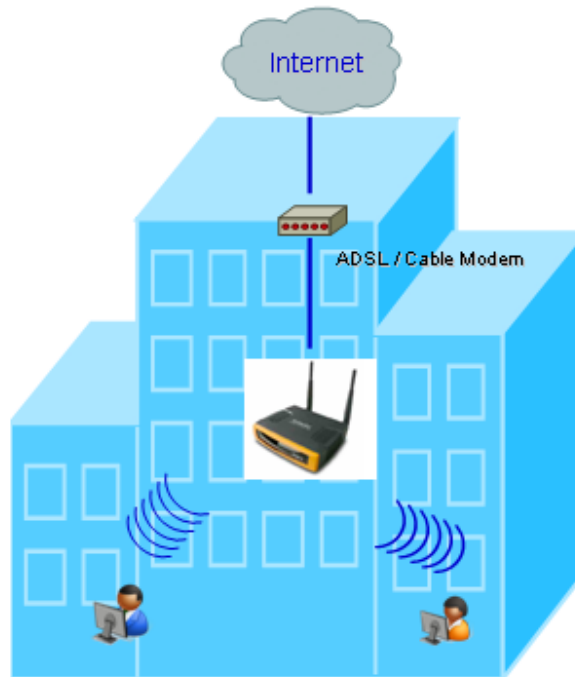
Local log

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

Apply Cancel

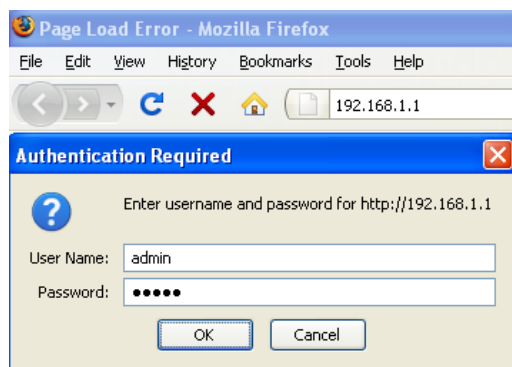
- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

8 AP Router Operating Mode



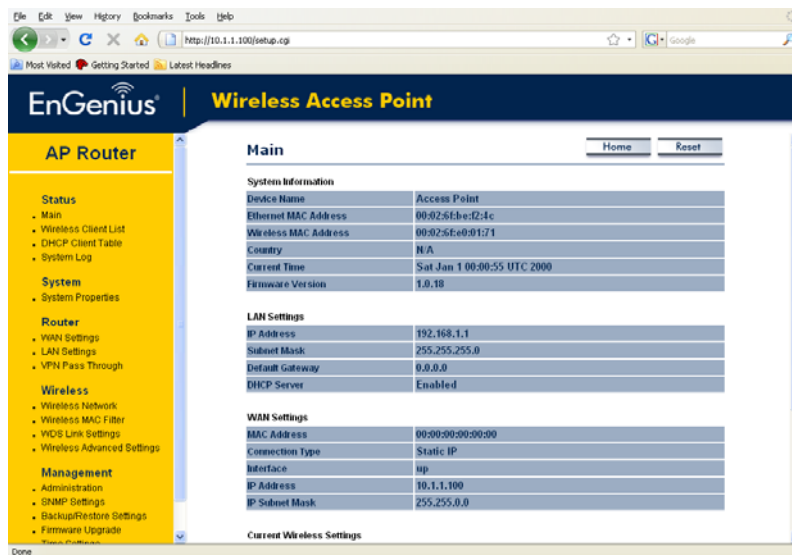
8.1 Logging In

- 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.

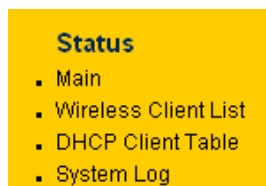


- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
 1. **Status:** Displays the overall status, wireless client list, DHCP client table, and event log.

2. **System:** This menu includes the system properties.
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, time settings, log, firmware upgrade, and save/restore backup.



8.2 Status



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

8.2.1 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 operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless' section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed. The 'WAN' section displays the MAC address, connection type, interface, IP address, and subnet mask.

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

Device Name	Access Point
Ethernet MAC Address	00:02:6f:be:f2:4c
Wireless MAC Address	00:02:6f:e0:01:71
Country	N/A
Current Time	Sat Jan 1 00:14:11 UTC 2000
Firmware Version	1.0.18

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	00:00:00:00:00:00
Connection Type	Static IP
Interface	up
IP Address	10.1.1.100
IP Subnet Mask	255.255.0.0

8.2.2 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](#)**8.2.3 DHCP Client List**

- Click on the **DHCP Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the Access Point through DHCP..
- 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

8.2.4 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

8.3 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.

8.3.1 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

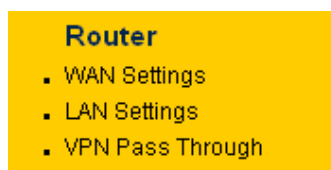
HomeReset

Device Name	AP Router (1 to 32 characters)
Country/Region	United States
Operation Mode	☐ Access Point ☐ Client Bridge ☐ WDS Bridge ☐ Repeater ☒ AP Router ☐ Client Router

ApplyCancel

- **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.

8.4 Router



- 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.

8.4.1 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.

8.4.1.1 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
Secondary DNS	0	0	0
Router MAC Address			
MAC Clone Enable	Disable ▼		
MAC Clone	00	00	00
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.

8.4.1.2 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
Router MAC Address	
MAC Clone Enable	Disable
MAC Clone	00 : 00 : 00 : 00 : 00 : 00 Clone
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.

8.4.1.3 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		Home	Reset
Internet Connection Type	PPPoE		
Options			
MTU	Auto	1492	
PPPoE Options			
Login	ppoe		
Password	•••••		
Service Name (if required)	pppoe		
☐ Connect on Demand: Max idle Time 1 Minutes			
☒ Keep Alive: Redial Period 30 Seconds			
Domain Name Server (DNS) Address			
☒ Get Automatically From ISP			
☐ Use These DNS Servers			
Primary DNS	0	0	0
Secondary DNS	0	0	0
Apply Cancel			

- 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.

8.4.2 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.



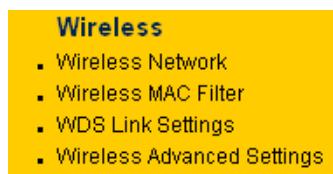
VPN Pass Through Home Reset

☐ PPTP Pass Through
☐ L2TP Pass Through
☐ IPSec Pass Through

Apply Cancel

- **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.

8.5 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.

8.5.1 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 : EnGenius (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **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 **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	

8.5.1.1 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 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	
Key2	
Key3	
Key4	

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

- **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 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.

8.5.1.2 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	(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.

8.5.2 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

Home

Reset

ACL Mode	Disabled ▼	: : : : :	Add
	- Disabled - Deny MAC in the List - Allow MAC in the List		
	MAC Address		
1	00:11:22:33:22:23	Delete	
2	77:88:77:55:77:88	Delete	

Apply

- **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.

8.5.3 WDS Link Settings

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

WDS Link Settings

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

ID	MAC Address	Mode
1	11 : 22 : 33 : 44 : 55 : 66	Enable v
2	22 : 33 : 44 : 55 : 66 : 77	Enable v
3	: : : : :	Disable v
4	: : : : :	Disable v
5	: : : : :	Disable v
6	: : : : :	Disable v
7	: : : : :	Disable v
8	: : : : :	Disable v Enable Disable

- WDS MAC Address:** Specify the MAC address of the Access Points that will join the WDS network and then select Enable or Disable from the drop-down list.
- Click on the **Apply** button to save the changes.

8.5.4 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, antenna diversity, fragmentation threshold, RTS threshold, 802.11g protection and distance.

Wireless Advanced Settings

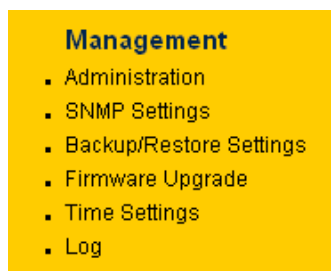
[Home](#)
[Reset](#)

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

- 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.
- Click on the **Apply** button to save the changes.

8.6 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.

8.6.1 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.

Administration

Administrator

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

- **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.

8.6.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, 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	☐ Disable ☒ Enable		
Contact	admin		
Location	US		
Community Name (Read Only)	public		
Community Name (Read/Write)	private		
Trap Destination IP Address	192 . 168 . 1 . 78		
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.

8.6.3 Backup/Restore settings, 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](#)

8.6.4 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: 1.0.27

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.

8.6.5 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.

- 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.

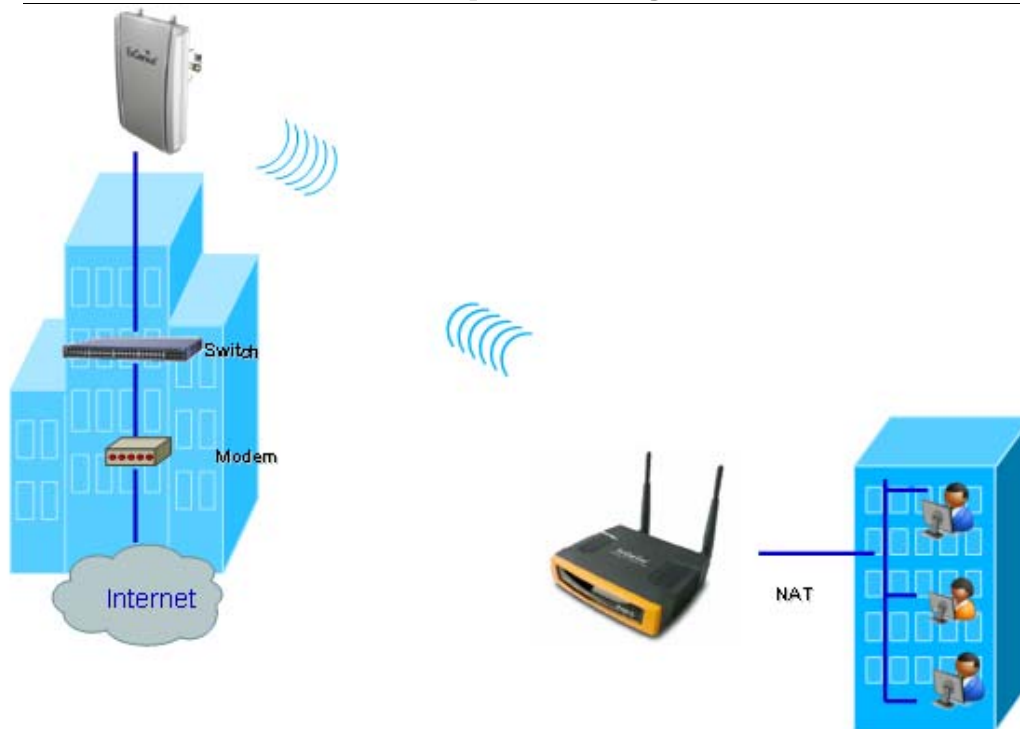
8.6.6 Log

- 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.

- Syslog:** Choose to enable or disable the system log.

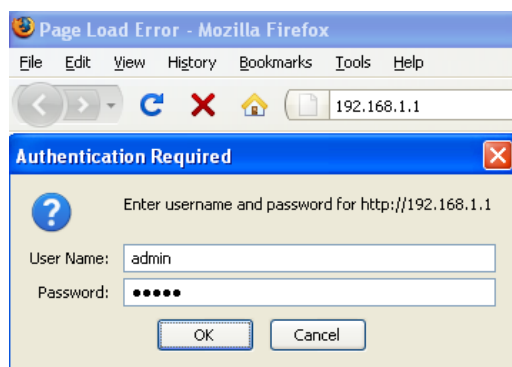
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

9 Client Router Operating Mode



9.1 Logging In

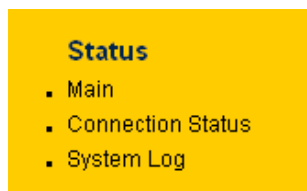
- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure 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.

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, time settings, log, firmware upgrade, and save/restore backup.

9.2 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.

9.2.1 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 operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless' section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed.

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

Main

System Information	
Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 00:40:35 UTC 2000
Firmware Version	1.0.27

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:10:0a:13
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	Current Frequency:2.452GHz (channel 09)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Distance	1 Km

[Refresh](#)

9.2.2 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.

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

Connection Status

Wireless	
Network Type	Client Router
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

WAN	
MAC Address	00:02:6f:e0:01:71
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

9.2.3 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

Show log type

Local Log is disabled.

9.3 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.

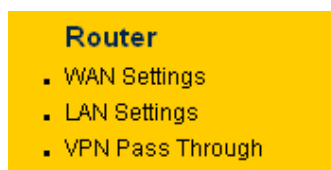
9.3.1 System Properties

- 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	Client Router (1 to 32 characters)		
Country/Region	United States		
Operation Mode	☐ Access Point ☐ Client Bridge ☐ WDS Bridge ☐ Repeater ☐ AP Router ☒ Client Router		
Apply Cancel			

- **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.

9.4 Router



- 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.

9.4.1 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.

9.4.1.1 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

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 Server:** 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.

9.4.1.2 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

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.

- **IP Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.
- **Gateway IP Address:** Specify the IP address of the default gateway, which is assigned by your ISP.
- **Domain Name Server:** Specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

9.4.1.3 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	1 Minutes
☒ Keep Alive: Redial Period	30 Seconds

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 **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 Server:** 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.

9.4.2 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.

9.5 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.

9.5.1 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 : EnGenius (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey
Prefer BSSID	: : : : : (Optional)

- Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **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 **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:0f:43	SMC	6	-105 dBm	G	NONE	

Refresh

- **Prefer BSSID**

9.5.1.1 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 Security

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 System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

Apply Cancel

- **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 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.

9.5.1.2 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

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	WPA-PSK
Encryption	TKIP
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)

- **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.

9.5.2 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, antenna diversity, fragmentation threshold, RTS threshold, 802.11g protection and distance.

Wireless Advanced Settings

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

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.
- **Antenna:**
- **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.
- Click on the **Apply** button to save the changes.

9.6 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.

9.6.1 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.

Administration

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

Remote Access	
Remote Management	☐ Enable ☒ Disable
Remote Upgrade	☐ Enable ☒ Disable
Remote Management Port	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.

9.6.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, 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

SNMP Enable/Disable	☒ Enable ☐ Disable
Contact	admin
Location	US
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

- **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.

9.6.3 Backup/Restore settings, 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

Save A Copy of Current Settings	Backup
Restore Saved Settings from A File	浏览... Restore
Revert to Factory Default Settings	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](#)

9.6.4 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

HomeReset

Current firmware version: 1.0.27

Locate and select the upgrade file from your hard disk:

Browse...

Upgrade

- 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.

9.6.5 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

Time	
☐	Manually Set Date and Time 2000 / 01 / 01 01 : 01
☒	Automatically Get Date and Time Time Zone: UTC+00:00 England ☐ User defined NTP Server: 0 . 0 . 0 . 0
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.

9.6.6 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 Spécifications

Physical Interface	● LAN: One 10/100 Fast Ethernet RJ-45 ● Reset Button ● Power Jack
LEDs Status	● Power/ Status ● Internet (WAN) ● WLAN (Wireless Connection) ● LAN (10/100Mbps)
Power Requirements	● Power Supply: 90 to 240 VDC $\pm$ 10%, 50/60 Hz (depends on different countries) ● Device: 12V/1A
Regulation Certifications	● FCC Part 15, Class B ● R&TTE Directive 1999/5/EC ● EN 300 328 ● EN 301 489 ● EN 60950

RF Spécifications

Frequency Band	2.400~2.484 GHz
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation Technology	● DSSS / BPSK / QPSK / CCK / OFDM
Operating Channels	11 for North America, 13 for Japan, 13 for Europe
Receive Sensitivity (Typical)	● IEEE802.11g 6/9/12/18Mbps@ -97dB ~ -89dB 24/36Mbps@ -80dB 54Mbps@ -74dB ● IEEE802.11b 1/2/5.5/11Mbps@-97dB ~ -89dB
Available transmit power	● IEEE802.11g 26dBm@6/9/12/18 Mbps 24/36dBm@24/36 Mbps 22dBm@54 Mbps ● IEEE802.11b Up to 28dBm@1 ~ 11Mbps
Antenna *2	Detachable omni antenna Peak Gain = 5 dBi

Software Features

Topology	Infrastructure
Operation Mode	Access Point + WDS AP/Client Bridge/Repeater/ WDS Bridge/Client Router/AP Router
LAN	• DHCP Server • DHCP Client
WAN (Client Router /AP Router mode)	• PPPoE
Router	• NAT/ NAPT
VPN	VPN pass-through (PPTP, L2TP, IPSEC)
Wireless	• Wireless Mode – 11b / 11g / Disable • Channel Selection (Setting varies by Country) • Transmission Rate ➢ 11 b/g: 108, 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 in Mbps • Transmit output power control • Signal Strength • RSSI indicator bar (CB/ CR/ Repeater Mode) • Antenna Diversity
Security	• WEP Encryption-64/128bit • WPA Personal (WPA-PSK/WPA2-PSK using TKIP or AES) • WPA Enterprise (WPA-EAP/WPA2-EAP using TKIP) • 802.1x Authenticator • 802.1x Supplicant- TTLS • Hide SSID in beacons • Multiple SSID with 802.1q VLAN tagging (up to 4 SSIDs)(AP mode) • MAC Filter(AP mode) • L2 isolation(AP mode)
QoS	• WMM

Management

Configuration	Web-based configuration (HTTP)/Telnet
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, Statistics and Event Log
SNMP	V1, V2c
MIB	MIB I, MIB II
Backup & Restore	Settings through Web

Environment & Physical

Temperature Range	• Operating: 0°C to 45°C (32°F to 113°F) • Storage: -20°C to 70°C (-4°F to 158°F)
-------------------	--

Humidity (non-condensing)	5%~95% typical
Dimensions	125mm (L) x 108mm (W) x 31mm (H)
Weight	350g

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.