

11b/g Wireless Multi-Client Bridge/AP



User's Manual

Version: 1.0

Table of Contents

1	INTRODUCTION	5
1.1	FEATURES & BENEFITS	5
1.2	PACKAGE CONTENTS	6
1.3	UNIT DESCRIPTION	6
1.4	SYSTEM REQUIREMENTS	6
1.5	APPLICATIONS	7
1.6	NETWORK CONFIGURATION.....	7
2	UNDERSTANDING THE HARDWARE	9
2.1	HARDWARE INSTALLATION	9
2.2	IP ADDRESS CONFIGURATION.....	9
3	CLIENT BRIDGE MODE – WEB CONFIGURATION	11
3.1	LOGGING IN.....	11
3.2	SYSTEM	13
3.2.1	ADMINISTRATOR SETTINGS.....	13
3.2.1.1	SAVE CONFIGURATION TO A FILE	15
3.2.1.2	RESTORE THE CONFIGURATION FROM A FILE.....	15
3.2.1.3	SWITCH FROM BRIDGE TO AP MODE	16
3.2.2	FIRMWARE UPGRADE.....	17
3.2.3	SYSTEM REBOOT AND RESTORE SETTINGS TO DEFAULT	18
3.2.3.1	SYSTEM REBOOT	18
3.2.3.2	RESTORE SETTINGS TO DEFAULT	19
3.2.4	SYSTEM TIME CONFIGURATION.....	19
3.3	WIRELESS	21
3.3.1	WIRELESS NETWORK SETTINGS	21
3.3.2	INFRASTRUCTURE / AD-HOC MODE	22
3.3.3	WIRELESS SECURITY	23
3.3.3.1.1	WEP (WIRED EQUIVALENT PRIVACY)	23
3.3.3.1.2	WPA – PERSONAL (WI-FI PROTECTED ACCESS).....	24
3.3.4	ADVANCED WIRELESS SETTINGS.....	25
3.3.5	SNMP	26
3.4	LAN SETTINGS (STATIC / DHCP)	27
3.5	STATISTICS.....	29
3.6	LOGS	30
4	ACCESS POINT MODE – WEB CONFIGURATION	31
4.1	LOGGING IN.....	31
4.2	SYSTEM	32
4.2.1	ADMINISTRATOR SETTINGS.....	32
4.2.1.1	SAVE CONFIGURATION TO A FILE	33
4.2.1.2	RESTORE THE CONFIGURATION FROM A FILE.....	34
4.2.2	FIRMWARE UPGRADE.....	34
4.2.3	SYSTEM REBOOT AND RESTORE SETTINGS TO DEFAULT	36
4.2.3.1	SYSTEM REBOOT	36
4.2.3.2	RESTORE SETTINGS TO DEFAULT	36
4.2.3.3	SWITCH FROM AP TO BRIDGE MODE	37
4.2.4	SYSTEM TIME CONFIGURATION.....	38
4.3	WIRELESS NETWORK SETTINGS	39
4.3.1.1	WEP (WIRED EQUIVALENT PRIVACY)	39
4.3.1.2	WPA PERSONAL (WI-FI PROTECTED ACCESS).....	40
4.3.1.3	WPA ENTERPRISE (WI-FI PROTECTED ACCESS & 802.1X).....	41

Table of Contents

4.3.2	ADVANCED WIRELESS AND WDS.....	43
4.3.3	SNMP	44
4.4	LAN	45
4.5	DHCP SERVER	46
4.6	MAC ADDRESS FILTER	48
4.7	LOGS	49
4.8	STATISTICS.....	50
APPENDIX A – SPECIFICATIONS.....		51
APPENDIX B – FCC INTERFERENCE STATEMENT		52
APPENDIX C – INDEX.....		54

Revision History

Version	Date	Notes
1.0	August 12, 2007	Initial Version

1 Introduction

NCB-3610S Wireless High Power and High Gain Client Bridge/Access Point/ WDS (wireless distribution system) operates in the 2.4 GHz frequency spectrum supporting the 802.11b (2.4GHz, 11Mbps) and the newer, faster 802.11g (2.4GHz, 54Mbps) wireless standards. It's the best way to add wireless capability to your existing wired network, or to add bandwidth to your wireless installation.

To protect your wireless connectivity, it can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA. The MAC address filter lets you select exactly which stations should have access to your network. With the Wireless Multi-Client Bridge/Access Point/WDS, you'll experience the best wireless connectivity available today.

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

1.1 Features & Benefits

Features	Benefits
High Speed Data Rate Up to 54Mbps	Capable of handling heavy data payloads such as MPEG video streaming
High Output Power up to 28dBm	Excellent output power spreads the operation distance
IEEE 802.11b/g Compliant	Fully Interoperable with IEEE 802.11b/IEEE802.11g compliant devices
Point-to-point, Point-to-multipoint Wireless Connectivity	Let users transfer data between two buildings or multiple buildings
Plug and Play	No driver needed, easy and quick to connect your Ethernet device to Wireless
WPA/WPA2/ IEEE 802.1x support	Powerful data security
Hide SSID (AP Mode)	Avoids unallowable users sharing bandwidth, increases efficiency of the network
DHCP Client/ Server	Simplifies network administration
WDS (Wireless Distributed System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater
MAC address filtering (AP Mode)	Ensures secure network connection
Power-over-Ethernet (IEEE802.3af)	Flexible Access Point locations and cost savings

1.2 Package Contents

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

- One AP/ CB Device
- One TNC Dipole Antenna
- One Power Adapter
- One CAT5 UTP Cable
- One Quick Start Guide
- One CD-ROM with User's Manual

1.3 Unit Description



1.4 System Requirements

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

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

1.5 Applications

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

- a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
- b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
- c) **The ability to access real-time information**
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
- d) **Frequently changed environments**
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
- e) **Small Office and Home Office (SOHO) networks**
SOHO users need a cost-effective, easy and quick installation of a small network.
- f) **Wireless extensions to Ethernet networks**
Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- g) **Wired LAN backup**
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
- h) **Training/Educational facilities**
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

1.6 Network Configuration

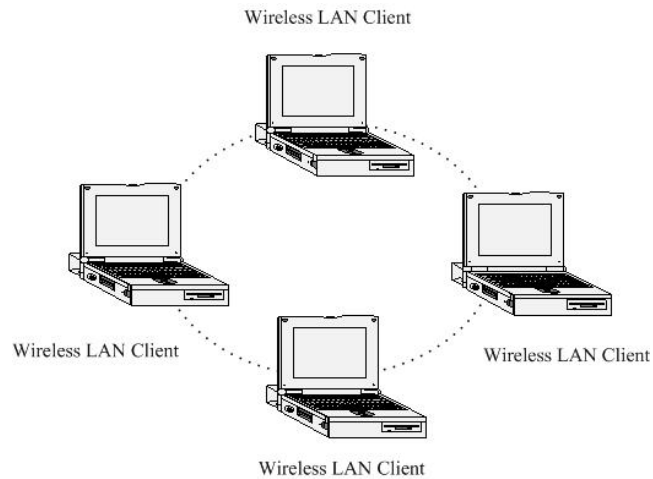
To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

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

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

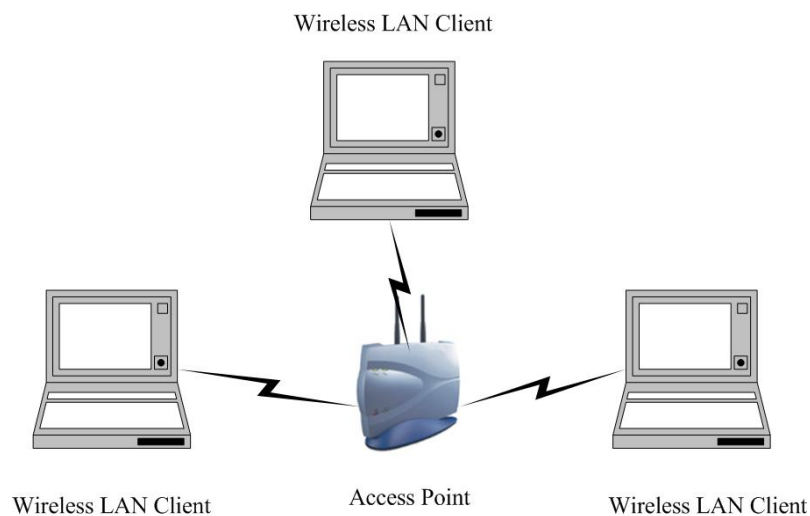
This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they

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



b) Infrastructure Mode

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

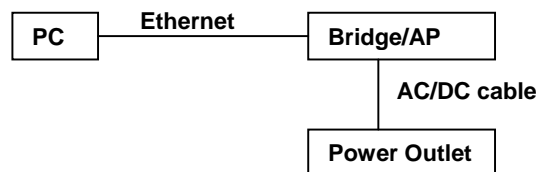


2 Understanding the Hardware

2.1 Hardware Installation

- 1 Place the unit in an appropriate place after conducting a site survey.
- 2 Plug one end of the Ethernet cable into the RJ-45 port 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.

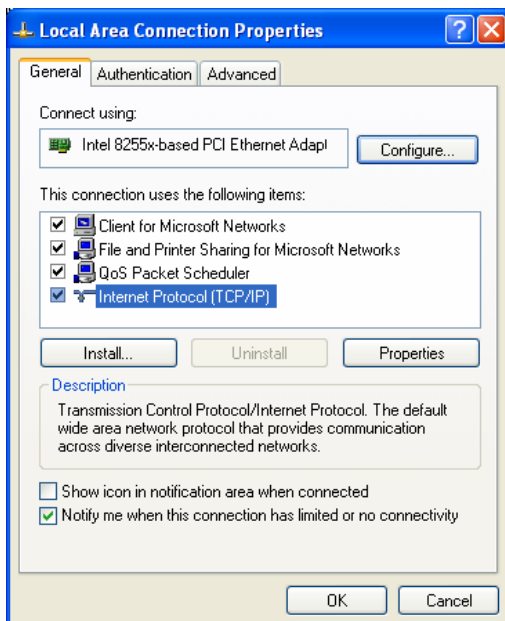
This diagram depicts the hardware configuration



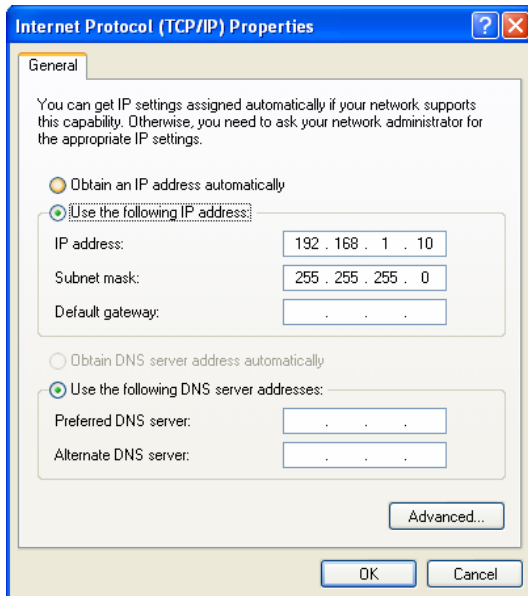
2.2 IP Address Configuration

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

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



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



3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.
For Example: Device IP address: 192.168.1.1
 PC IP address: 192.168.1.10
 PC subnet mask: 255.255.255.0
4. Click on the **OK** button to close this window, and once again to close LAN properties window.

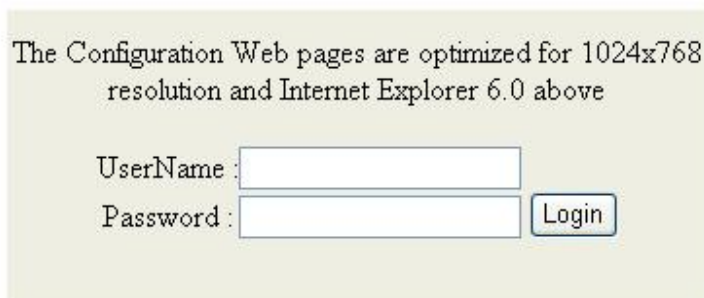
3 Client Bridge Mode – Web Configuration

3.1 Logging In

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



- Make sure that the Bridge and your computers are 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 the **User Name** and **Password**. The device does not have a password configured by default, therefore please leave the password field blank and then click on the **Login** button.



- After logging in you will graphical user interface (GUI) of the bridge. The navigation drop-down menu on left is divided into six main sections:
 - System:** This menu includes the administrator settings, Also included are other system related settings such as firmware upgrade, reset to factory defaults, and system date/time configuration.
 - Wireless:** This menu includes the settings such as network type (infrastructure/ad-hoc), data rate, and security. Advanced wireless settings such as wireless MAC clone and RTS/fragmentation threshold. Are also included.
 - LAN:** This menu includes the configuration of the LAN port and settings for the LAN IP, subnet mask, default gateway and DHCP client.
 - Statistics:** This menu displays the wired and wireless interface statistics.
 - Log:** This menu displays a log of the critical and informational events that are triggered on the device.
 - Help:** This menu describes the features of the device and the parameters for each setting.



- The Bridge status page is also displayed once you have logged in. This includes details about the system date and firmware, LAN IP address and MAC address and the wireless settings such as the radio status, MAC address, SSID, RF channel, and security.

The screenshot displays the Bridge status page with three main sections: General, LAN, and Wireless LAN. Each section contains specific configuration and status information.

General	
Firmware Version :	1.0.0.03 , 2007/07/16

LAN	
MAC Address :	00:02:6F:4A:61:8C
IP Address :	192.168.1.1
Subnet Mask :	255.255.255.0
Default Gateway :	0.0.0.0

Wireless LAN	
Status :	Not associated with any AP
Wireless Radio :	On
MAC Address :	00:02:6F:4A:61:8C
Network Name (SSID) :	Engenius
Channel :	9
Security Type :	None
802.11 Mode :	Mixed 802.11g and 802.11b
Associated BSSID :	00:00:00:00:00:00

- **General:**
 - Displays firmware version and system date.
- **LAN:**
 - Displays the MAC address, IP address, and subnet mask of the LAN interface.
- **Wireless LAN:**
 - Displays the status, MAC address, SSID, RF channel, and security settings of the wireless interface.

3.2 System



- Click on the **System** link on the navigation drop-down menu. You will then see four options: Administrators Settings, Firmware, System, and Time. Each option is described below.

3.2.1 Administrator Settings

- Click on the **Administrator Settings** link under the **System** menu. This page allows you to configure the password to access this device from the web-browser. You can also specify a name for the bridge as well as backup and restore the system settings.
- The first part of this page gives you the option to save the changes that were made on this page. Click on the **Save Settings** button once you have configured the administrator settings.



- The second part of this page allows you to configure the user name and password for accessing the device. Specify a user name and password and then re-type it once again for verification. Click on the **Save Settings** button to store the changes.

Admin User Name

Please enter the user name into both boxes, for confirmation.

User Name :

User Password

Please enter the same password into both boxes, for confirmation.

Password :

Verify Password :

- The third part of this page allows you to specify a name for this device as well as save or restore a configuration. Click on the **Save Settings** button to store the changes.

Administration

Bridge Name :

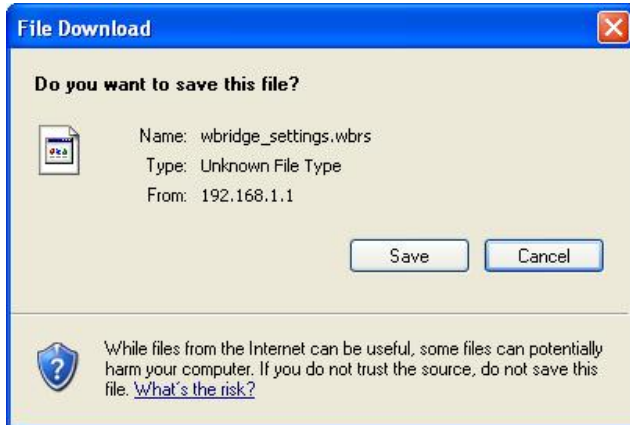
Web Idle Timeout : (minutes)

Save And Restore Configuration

- **Bridge Name:** Specify a name for this bridge.
- **Web Idle Timeout:** Specify a time in minutes. If there is no activity on the configuration pages, then web page will close the session at the specified time.

3.2.1.1 Save Configuration to a File

- This option allows you to save the current configuration of the device into a file. Click on the **Save Configuration** button to begin.
- Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.



3.2.1.2 Restore the Configuration from a File

- This option allows you to restore a backup configuration from a file to the device. Click on the **Browse** button to select the file and then click on **Restore Configuration from a File** button.
- The system then prompts you to reboot the device.



- Click on the **OK** button to continue. You will then see the **Rebooting** page.



- Please wait while the system is rebooting.
Note: Do not unplug the device during this process as this may cause permanent damage.

3.2.1.3 Switch from Bridge to AP Mode

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



- Click on the **Switch Device to AP Mode** and then you will see a confirmation dialog box. Click on the **OK** button to continue.



- Please wait while the system is rebooting.
Note: Do not un-plug the device during this process as this may cause permanent damage.
- Once the device has restarted you may need to access the management page through a different IP address. The default IP address for Access Point mode is **192.168.1.2**. Refer to **Chapter 4** to configure the device in Access Point mode.

3.2.2 Firmware Upgrade

- Click on the **Firmware** link under the **System** menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance. This page also displays the current firmware version and its release date.

Firmware Information

Current Firmware Version : 1.0.0.03
Current Firmware Date : 2007/07/16

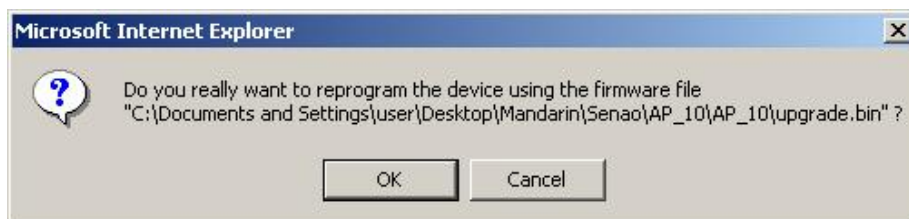
Firmware Upgrade

Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the System - > Administrator Settings screen.

To upgrade the firmware, your PC must have a wired connection to the bridge. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

- Ensure that you have downloaded the appropriate firmware from the vendor's website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded using the wireless interface.
- Click on the **Browse** button to select the firmware and then click on the **Upload** button.

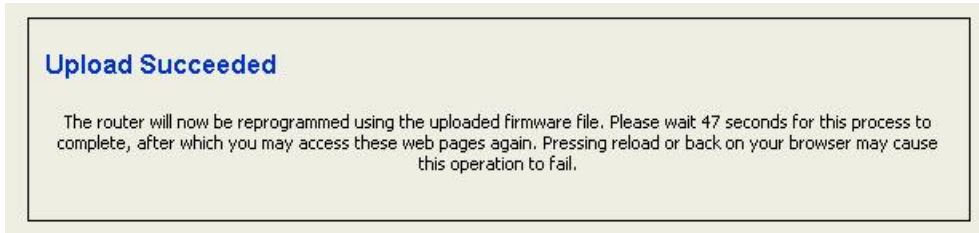


- The above dialog box requests you to confirm the upgrade process. Click on the **OK** button to continue.
- Once you click on the **OK** button, you will return to the previous page which indicates that the upgrade process may take up to one minute.

Upload :

Note: Now uploading. The upload may take up to 1 minute.

- After a few seconds the firmware will start to re-program the device and you will see a countdown on the **Success** page.



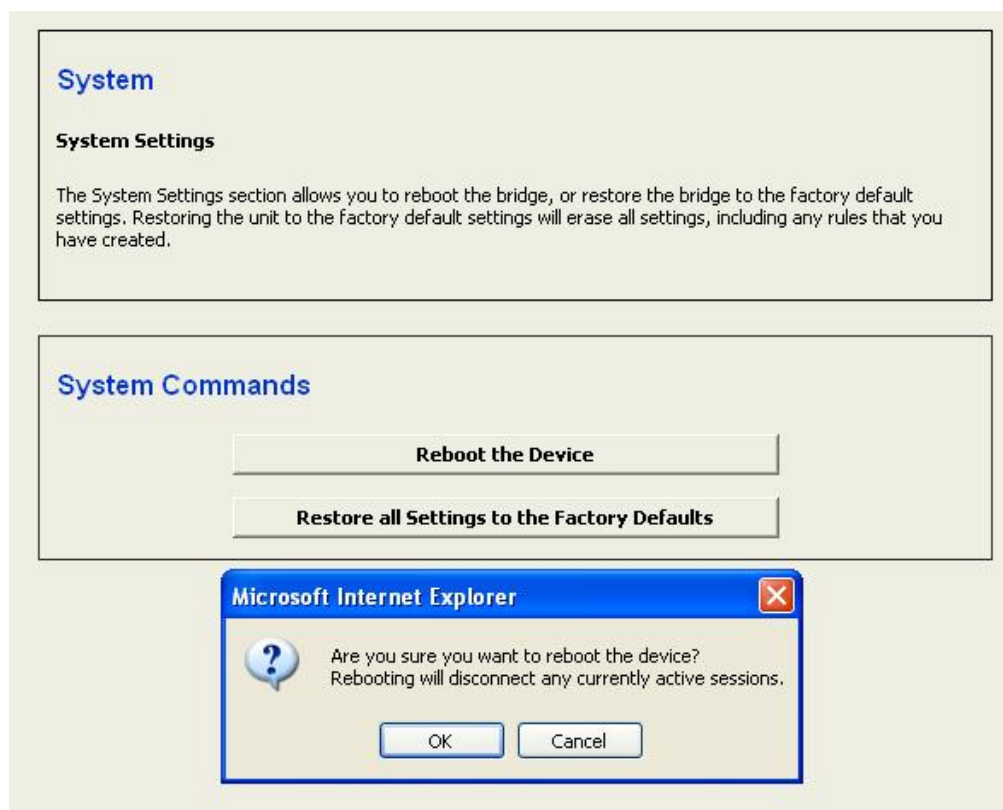
Note: Do not un-plug the device during this process. Some firmware upgrades may restore the configuration back to the factory default settings. Therefore you may need to restore a configuration from a file. Refer to **Administrator Settings** for details.

3.2.3 System Reboot and Restore Settings to Default

- Click on the **System** link under the **System** menu. This page allows you to reboot the device using the current settings or restore all the settings to the factory defaults.

3.2.3.1 System Reboot

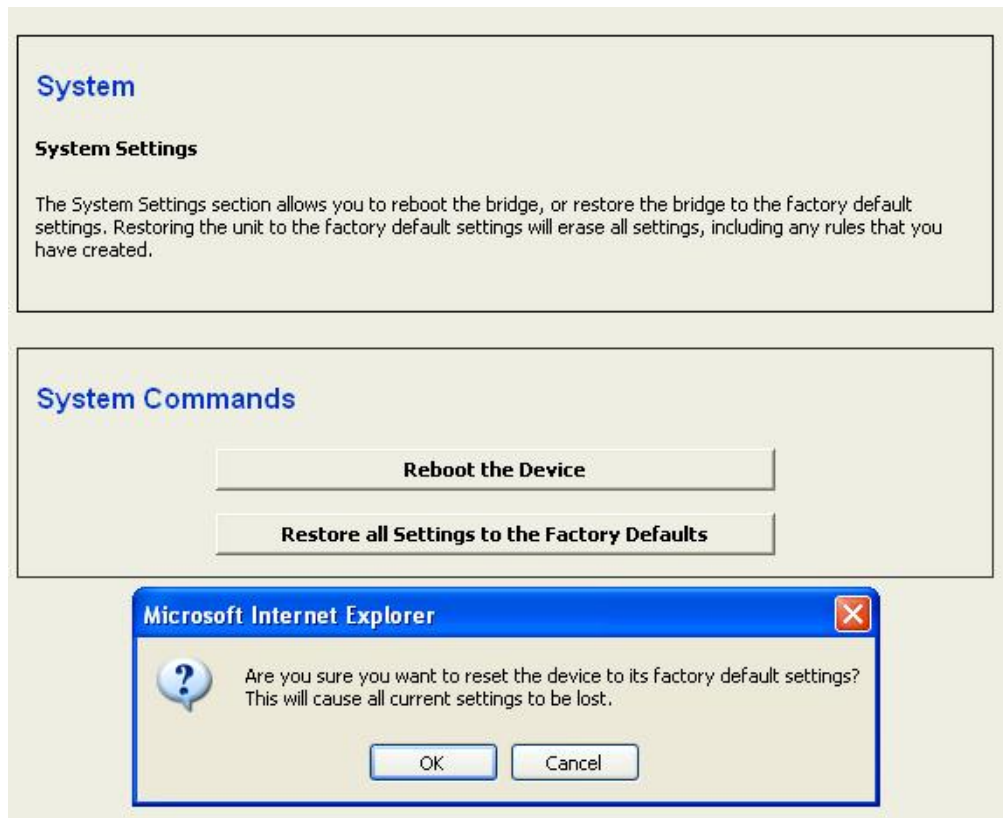
- Click on the **Reboot the Device** button to reboot the device using its current settings. Once the dialog box appears, click on the **OK** button to confirm the action.



3.2.3.2 Restore Settings to Default

- Click on the **Restore all Settings to Factory Defaults** button. This option restores all configuration settings back to the settings that were in effect at the time when the device was shipped from the factory. Once the dialog box appears, click on the **OK** button to confirm the action.

Note: The current settings will be lost.



3.2.4 System Time Configuration

- Click on the **Time** link under the **System** menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by copying the time on the PC that it is wired to.

Note: If the bridge loses power for any reason, it will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.

Time

Time Configuration

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in.

Time Configuration

Time Zone :

Set the Date and Time Manually

Current Bridge Time : **Saturday, January 31, 2004 10:47:52 AM**

Year	<input type="text" value="2004"/>	Month	<input type="text" value="Jan"/>	Day	<input type="text" value="31"/>		
Hour	<input type="text" value="10"/>	Minute	<input type="text" value="47"/>	Second	<input type="text" value="32"/>		<input type="text" value="AM"/>

- **Time Zone:** Select your time zone from the drop-down list.
- **Set the Date and Time:** Select a date and time from the drop-down list or do to use computer's time and date click on the **Copy Your Computer's Time Settings** button.
- Click on the **Save Settings** button once you have modified the settings.

3.3 Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see three options: **Wireless_Setting**, **Advanced**, and **SNMP**. The configuration steps are the same for both radios.

Wireless

Access Point List

Use this option to view the list of Access Points around.

Number Of Access Points : 1

MAC Address	SSID	Channel	Mode	Privacy	Type	Signal (%)	Noise Level (dbm)
00:20:ED:0D:26:96	DinoNet	11	11b	WEP	AP	33	-93

- MAC Address:** The MAC address or BSSID of the Access Point.
- SSID:** The name used to identify the wireless network. 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.
- Channel:** The channel used to communicate on the wireless network.
- Mode:** Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
- Privacy:** The type of security used on this network. It may be disabled, WEP, WPA, etc.
- Type:** Wireless configuration mode such as Ad-Hoc or AP.
- Signal (%):** The wireless signal strength. Signal quality can be reduced by distance, by interference from other radio frequency devices and obstruction from obstacles between the bridge and AP.

3.3.1 Wireless Network Settings

- Click on the **Wireless_Setting** link under the **Wireless** menu. The first part of this page allows you to save the configuration. Click on the **Save Settings** button once you have modified the settings.

Wireless_Setting

Wireless Network Settings

Use this section to configure the wireless settings for your Wireless Client Bridge. Please note that changes made on this section may also need to be duplicated on your Wireless Access Point.

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WEP and WPA-Personal. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server.

3.3.2 Infrastructure / Ad-hoc Mode

- Click on the **Wireless Setting** link under the **Wireless** menu. The second part of this page allows you to configure the device in infrastructure or ad-hoc mode.

Basic Wireless Settings

Wireless Mode : Infrastructure Ad-Hoc

Wireless Network Name : (Also called the SSID)

Channel :

Transmission Rate : (Mbit/s)

802.11 Mode :

Setting ACK_B Timeout: μ s (0..372)

Preferred BSSID

Preferred BSSID Enable : Disable Enable

Preferred BSSID MAC :

Basic Wireless Settings

Wireless Mode : Infrastructure Ad-Hoc

Wireless Network Name : (Also called the SSID)

Channel :

Transmission Rate : (Mbit/s)

802.11 Mode :

Setting ACK_B Timeout: μ s (0..372)

- Wireless Mode:** Select the **Infrastructure** or **Ad-Hoc** radio button. Infrastructure is a point-to-multipoint (PtMp) topology where as Adhoc is a point-to-point topology (PtP).
- Wireless Network Name:** 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.
- 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.
- Transmission Rate:** Select a transmission rate from the drop-down list. It is recommended to use the **Best (automatic)** option.
- 802.11 Mode:** Select the IEEE 802.11 mode from the drop-down list. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select **802.11g** only instead of **Mixed 802.11g and 802.11b** which will reduce the performance of the wireless network.

- **ACK Timeout:** You may specify a value for the acknowledge timeout. However, it is recommended to use the default setting: 48.
- Click on the **Save Settings** button once you have modified the settings.

3.3.3 Wireless Security

- Click on the **Wireless_Setting** link under the **Wireless** menu. The third part of this page allows you to configure the security settings of this device. To protect your privacy this mode supports two types of wireless security: WEP and WPA-Personal. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server.
- Select the **None** radio button in order to disable security.



3.3.3.1.1 WEP (Wired Equivalent Privacy)

- Select the **WEP** radio button 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 is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the bridge and the wireless access point. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : (length applies to all keys)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Default WEP Key :

Authentication :

Open
Shared Key

- **WEP Key Length:** Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **WEP Key 1-4:** You may enter four different WEP keys.
- **Default WEP Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Authentication:** Select **Open**, or **Shared Key**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Click on the **Save Settings** button once you have modified the settings.

3.3.3.1.2 WPA – Personal (Wi-Fi Protected Access)

- Select the **WPA-Personal** radio button if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

WPA

WPA requires stations to use high grade encryption and authentication.

WPA Mode : WPA

Cipher Type : TKIP and AES

TKIP
AES
TKIP and AES

Pre-Shared Key

Pre-Shared Key :

- **WPA Mode:** Select the **WPA** or **WPA2** from the drop-down list.
- **Cipher Type:** Select **TKIP** or **AES** as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.
- Click on the **Save Settings** button once you have modified the settings.

3.3.4 Advanced Wireless Settings

- Click on the **Advanced** link under the **Wireless** menu. This page allows you to enable wireless MAC cloning as well as configure the fragmentation threshold, RTS threshold, 802.11d, and the transmit power.

Advanced Wireless

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

Wireless MAC Cloning

Cloning Mode : WLAN Card Ethernet Client

Advanced Wireless Settings

Fragmentation Threshold : (256..2346)

RTS Threshold : (0..2347)

Transmit Power :

- **Bridge Name:** This feature controls the MAC address of the Bridge as seen by other devices (wired or wireless). If set to **Ethernet Client**, the MAC address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful when connected to an Xbox or if there is only one Ethernet device connected to the Bridge. When multiple Ethernet devices are connected to the Bridge, it may not be obvious which MAC address is being used. If set to **WLAN Card**, the MAC address of the WLAN card will be used. When multiple Ethernet devices are connected to the Bridge, the MAC address of the Bridge will not change.
- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 65535. The default value is 2346.
- **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. Specify a value between 1 and 65535. The default value is 2346.
- **Transmit Power:** You may control the output power 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.
- Click on the **Save Settings** button once you have modified the settings.

3.3.5 SNMP

- Click on the **SNMP** link under the **Wireless** menu. This page allows you to SNMP community and trap settings. The feature is useful while remotely monitoring and maintaining the device.

SNMP

SNMP Parameter Settings

Use this section to configure the SNMP settings of your bridge.

SNMP Settings

Support WebAdmin Control: Disable Enable

Read-Only Community Name:

Read-Write Community Name:

Send SNMP Trap: Disable Enable

Send Trap To:

Trap Community Name:

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

3.4 LAN Settings (Static / DHCP)



- Click on the **LAN** link on the navigation drop-down menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP client. This IP address is also used to access the web-based interface.

LAN Settings

IP Address Mode : Static DHCP

IP Address :

Subnet Mask :

Default Gateway :

LAN Settings

IP Address Mode : Static DHCP

IP Address :

Subnet Mask :

Default Gateway :

- **IP Address Mode:** Select the Static or DHCP radio button. If you select **DHCP** radio button, you are not required to enter the rest of the fields, as the IP address will be provided to the device by the AP or DHCP server. If you select the **Static** radio button, you must enter the IP address, subnet mask, and default gateway.
 - **IP Address:** Enter an IP address for this device.
 - **Subnet Mask:** Enter the subnet mask for this IP address.
 - **Default Gateway:** Enter the IP address of the default gateway.
 - Click on the **Save Settings** button once you have modified the settings.
- Note:** If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

3.5 Statistics

- Click on the **Statistics** link on the navigation drop-down menu. This page displays the transmitted and received packet statistics of the wired and wireless interface.

The screenshot displays the Statistics page with three main sections:

- Statistics**
 - Network Traffic Stats**

Traffic Statistics display Receive and Transmit packets passing through your bridge.

Refresh Statistics Clear Statistics
- LAN Statistics**

Sent : 1824	Received : 1848
TX Packets Dropped : 0	RX Packets Dropped : 0
Collisions : 0	Errors : 0
- Wireless Statistics**

Sent : 15025	Received : 0
TX Packets Dropped : 0	Errors : 0

- Sent:** The number of packets sent from the bridge.
- Received:** The number of packets received by the bridge.
- TX Packets Dropped:** The number of packets that were dropped while being sent, due to errors, collisions, or bridge resource limitations.
- RX Packets Dropped:** The number of packets that were dropped while being received, due to errors, collisions, or bridge resource limitations.
- Collisions:** The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).
- Errors:** The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.
- Click on the **Refresh Statistics** button to refresh the events or click on the **Clear Statistics** button to clear the events.

3.6 Logs

- Click on the **Logs** link on the navigation drop-down menu. Logs display 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.

The screenshot shows a web interface for managing logs. It is divided into two main sections: 'Log Options' and 'Log Details'.
Log Options: This section contains two rows of checkboxes. The first row is labeled 'What to View' and has checkboxes for 'System' and 'Status', both of which are checked. The second row is labeled 'View Levels' and has checkboxes for 'Critical', 'Warning', and 'Informational', all of which are checked. Below these options is a button labeled 'Apply Log Settings Now'.
Log Details: This section contains three buttons: 'Refresh', 'Clear', and 'Save Log'. Below the buttons, there are two lines of log entries: '[INFO] Sat Jan 31 10:30:06 2004 Stored configuration to non-volatile memory' and '[INFO] Thu Jan 01 00:00:00 1970 Loaded configuration from non-volatile memory'.

- **Log Options:** Select the type of warning that you would like recorded and place a check in the appropriate box. Then click on the **Apply Log Settings Now** button.
- **Log Details:** The events are logged in this section. Click on the **Refresh** button to refresh the events or click on the **Clear** button to clear the events. Click on the **Save Log** button to save the log on your PC.

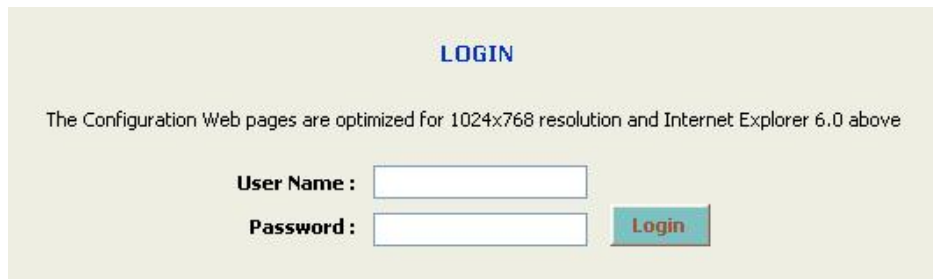
4 Access Point Mode – Web Configuration

4.1 Logging In

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



- Make sure that the Bridge 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 the **User Name** and **Password**. The device does not have a password configured by default, therefore please leave the password field blank and then click on the **Login** button.



4.2 System



- Click on the **System** link on the navigation drop-down menu. You will then see four options: Administrator Settings, Firmware, System, and Time. Each option is described below.

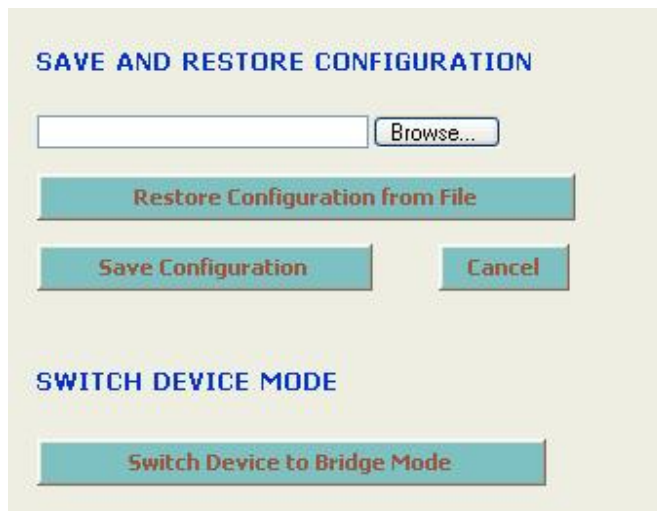
4.2.1 Administrator Settings

- Click on the **Administrator Settings** link under the **System** menu. This page allows you to configure the password to access this device from the web-browser. You can also backup and restore the system settings.

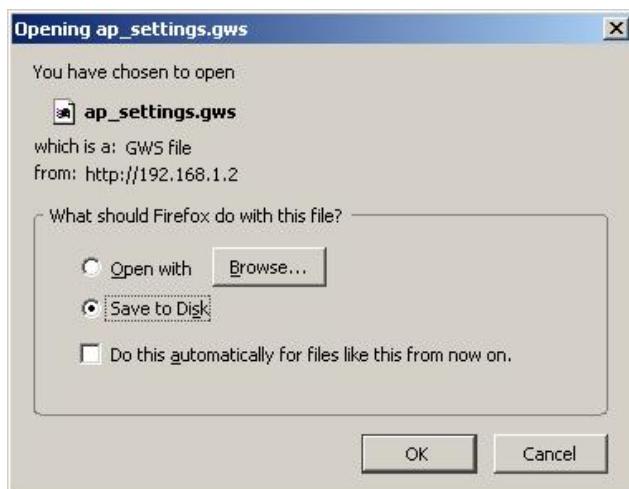
A screenshot of a web form for Administrator Settings. It has a light beige background. The first section is titled 'USER NAME' in blue. Below it is the instruction 'Please enter the user name into box.' followed by a text input field labeled 'User Name :'. The second section is titled 'ADMIN PASSWORD' in blue. Below it is the instruction 'Please enter the same password into both boxes, for confirmation.' followed by two text input fields labeled 'Password :' and 'Verify Password :'. At the bottom right, there are two buttons: 'Save Settings' and 'Don't Save Settings'.

- Specify a user name and password and then re-type it once again for verification. Click on the **Save Settings** button to store the changes.

4.2.1.1 Save Configuration to a File



- This option allows you to save the current configuration of the device into a file. Click on the **Save Configuration** button to begin.
- Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.



4.2.1.2 Restore the Configuration from a File

- This option allows you to restore a backup configuration from a file to the device. Click on the **Browse** button to select the file and then click on **Restore Configuration from a File** button.
- The system then prompts you to reboot the device.



- Click on the **OK** button to continue. You will then see the **Rebooting** page.



- Please wait while the system is rebooting.

Note: Do not un-plug the device during this process as this may cause permanent damage.

4.2.2 Firmware Upgrade

- Click on the **Firmware** link under the **System** menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance. This page also displays the current firmware version and its release date.

Firmware Upgrade

The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance.

FIRMWARE INFORMATION

Current Firmware Version : 1.0.0.03
Current Firmware Date : 2007/07/16

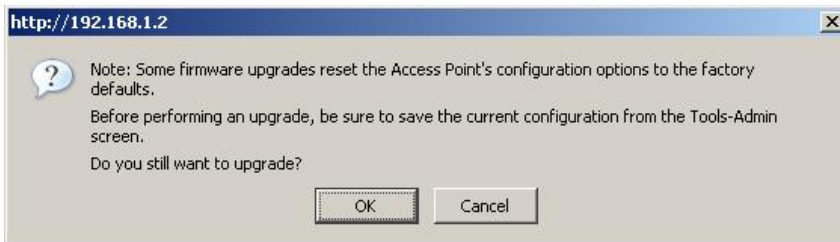
FIRMWARE UPGRADE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the System -> Administrator Settings screen.

To upgrade the firmware, your PC must have a wired connection to the Access Point. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

- Ensure that you have downloaded the appropriate firmware from the vendor's website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded using the wireless interface.
- Click on the **Browse** button to select the firmware and then click on the **Upload** button.



- The above dialog box requests you to confirm the upgrade process. Click on the **OK** button to continue.
- Once you click on the **OK** button, you will return to the previous page which indicates that the upgrade process may take up to one minute.



- After a few seconds the firmware will start to re-program the device and you will see a countdown on the **Success** page.

UPLOAD SUCCEEDED

The Access Point will now be reprogrammed using the uploaded firmware file. Please wait 56 seconds for this process to complete, after which you may access these web pages again. Pressing reload or back on your browser may cause this operation to fail.

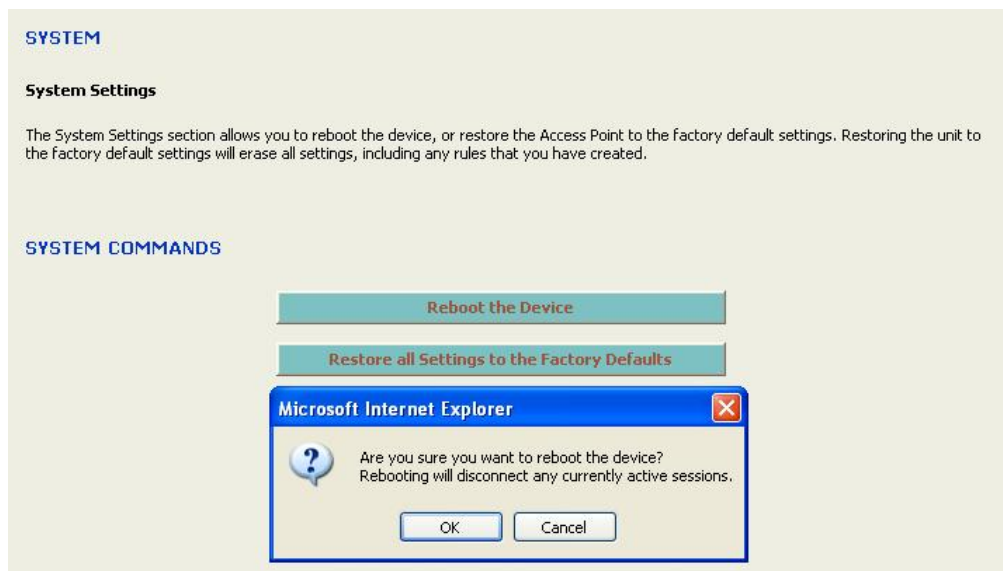
Note: Do not un-plug the device during this process. Some firmware upgrades may restore the configuration back to the factory default settings. Therefore you may need to restore a configuration from a file. Refer to **Administrator Settings** for details.

4.2.3 System Reboot and Restore Settings to Default

- Click on the **System** link under the **System** menu. This page allows you to reboot the device using the current settings or restore all the settings to the factory defaults.

4.2.3.1 System Reboot

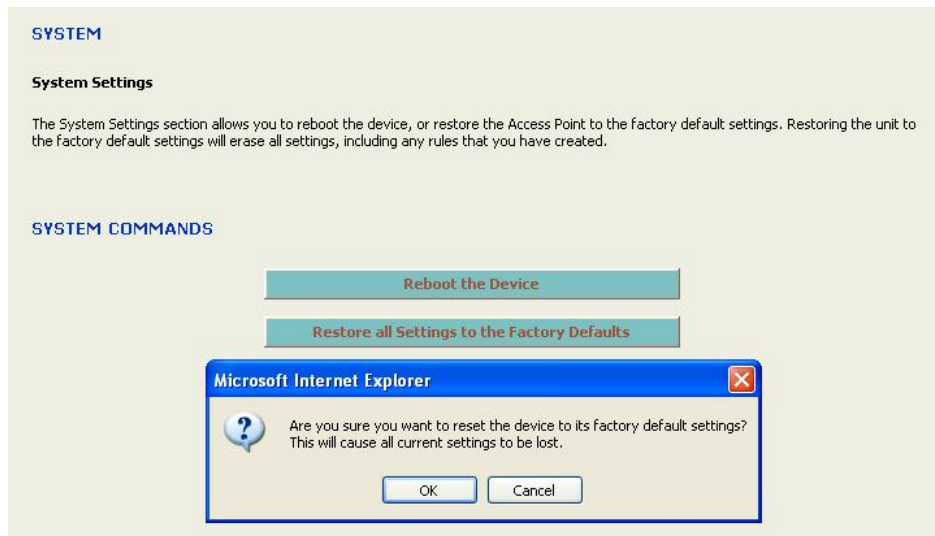
- Click on the **Reboot the Device** button to reboot the device using its current settings. Once the dialog box appears, click on the **OK** button to confirm the action.



4.2.3.2 Restore Settings to Default

- Click on the **Restore all Settings to Factory Defaults** button. This option restores all configuration settings back to the settings that were in effect at the time when the device was shipped from the factory. Once the dialog box appears, click on the **OK** button to confirm the action.

Note: The current settings will be lost.



4.2.3.3 Switch from AP to Bridge Mode

This device can be configured as a Access Point or Bridge. The default IP address of the device is **192.168.1.2** in Access Point mode. This section will describe the steps to switch from Access Point to Bridge mode.



- Click on the **Switch Device to Bridge Mode** and then you will see a confirmation dialog box. Click on the **OK** button to continue.



- Please wait while the system is rebooting.
Note: Do not un-plug the device during this process as this may cause permanent damage.

- Once the device has restarted you may need to access the management page through a different IP address. The default IP address for Access Point mode is **192.168.1.2**. Refer to **Chapter 3** to configure the device in Bridge mode.

4.2.4 System Time Configuration

- Click on the **Time** link under the **System** menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by copying the time on the PC that it is wired to.

Note: If the device loses power for any reason, it will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.

TIME

Time Configuration

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME CONFIGURATION

Time Zone: (GMT-08:00) Pacific Time (US/Canada), Tijuana

Daylight Saving Settings:

Enable Daylight Saving

Daylight Saving Offset: +1:00

	Month	Week	Day of Week	Time
DST Start	Apr	1st	Sun	2 am
DST End	Oct	5th	Sun	2 am

SET THE DATE AND TIME MANUALLY

Current Gateway Time: Wednesday, May 31, 2006 12:40:54 AM

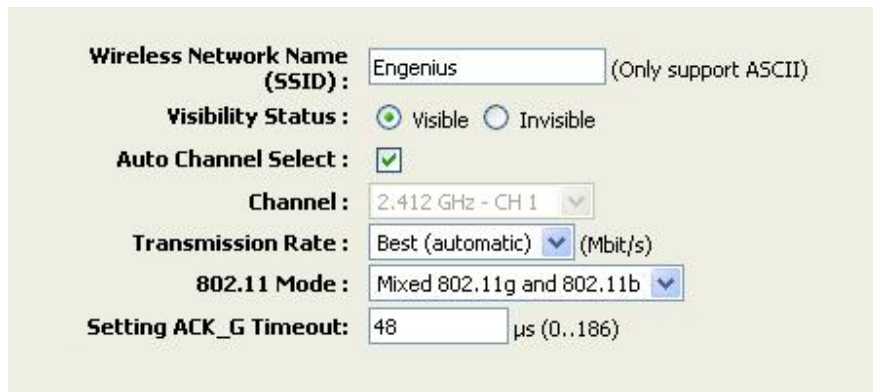
Year	2006	Month	May	Day	31		
Hour	1	Minute	23	Second	8		PM

[Copy Your Computer's Time Settings](#)

- Time Zone:** Select your time zone from the drop-down list.
- Set the Date and Time:** Select a date and time from the drop-down list or do to use computer's time and date click on the **Copy Your Computer's Time Settings** button.
- Click on the **Save Settings** button once you have modified the settings.

4.3 Wireless Network Settings

- Click on the [Wireless_Setting](#) link under the Wireless menu. On this page you may configure the 802.11b/g radio.



Wireless Network Name (SSID): Engenius (Only support ASCII)

Visibility Status: Visible Invisible

Auto Channel Select:

Channel: 2.412 GHz - CH 1

Transmission Rate: Best (automatic) (Mbit/s)

802.11 Mode: Mixed 802.11g and 802.11b

Setting ACK_G Timeout: 48 μs (0..186)

- Wireless Network Name:** 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.
- Visibility Status:** Select **Visible** or **Invisible**. This is the SSID broadcast feature. If you set this value to Visible, then the clients will be able to find this SSID on a site survey.
- Channel:** Select a channel from the drop-down list. The channels available are based on the country's regulation. Place a check in the Auto Channel Select box if you would like the Access Point to select the cleanest channel.
- Transmission Rate:** Select a transmission rate from the drop-down list. It is recommended to use the **Best (automatic)** option.
- 802.11 Mode:** Select the IEEE 802.11 mode from the drop-down list. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select **802.11g** only instead of **Mixed 802.11g and 802.11b** which will reduce the performance of the wireless network. Click on the **Save Settings** button once you have modified the settings.
- ACK Timeout:** You may specify a value for the acknowledge timeout. However, it is recommended to use the default setting: 48.

4.3.1.1 WEP (Wired Equivalent Privacy)

- Select the **WEP** radio button 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 is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier

to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

WIRELESS SECURITY MODE

Security Mode : None WEP WPA-Personal WPA-Enterprise

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the Access Point and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Default WEP Key :

Authentication :

- **WEP Key Length:** Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **WEP Key 1-4:** You may enter four different WEP keys.
- **Default WEP Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Authentication:** Select **Open**, or **Shared Key**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Click on the **Save Settings** button once you have modified the settings.

4.3.1.2 WPA Personal (Wi-Fi Protected Access)

- Select the **WPA-Personal** radio button if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

WPA

WPA requires stations to use high grade encryption and authentication. NOTE: WDS will not function with WPA security.

WPA Mode :

Cipher Type :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Pre-Shared Key :

- **WPA Mode:** Select the **WPA / WPA2** from the drop-down list.
- **Cipher Type:** Select TKIP or AES as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval:** Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.
- Click on the **Save Settings** button once you have modified the settings.

4.3.1.3 WPA Enterprise (Wi-Fi Protected Access & 802.1x)

- Select the WPA-Enterprise radio button if your wireless network uses WPA 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.
- This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

WIRELESS SECURITY MODE

Security Mode : None WEP WPA-Personal WPA-Enterprise

WPA

WPA requires stations to use high grade encryption and authentication. NOTE: WDS will not function with WPA security.

WPA Mode :

Cipher Type :

Group Key Update Interval : (seconds)

EAP (802.1X)

When WPA enterprise is enabled, the Access Point uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : (minutes)

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

MAC Address Authentication :

[<< Advanced](#)

Optional backup RADIUS server:

Second RADIUS server IP Address :

Second RADIUS server Port :

Second RADIUS server Shared Secret :

Second MAC Address Authentication :

[Save Settings](#) [Don't Save Settings](#)

- **WPA Mode:** Select the WPA / WPA2 from the drop-down list.
- **Cipher Type:** Select TKIP or AES as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval:** Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Authentication Timeout:** Specify the number of minutes after which the client will be required to re-authenticate.
- **RADIUS Server IP Address:** Specify the IP address of the RADIUS server.
- **RADIUS Server Port:** Specify the port number of the RADIUS server, the default port is 1812.
- **RADIUS Server Shared Secret:** Specify the pass-phrase that is matched on the RADIUS Server.
- **MAC Address Authentication:** Place a check in this box if you would like the user to always authenticate using the same computer.
- **Optional Backup RADIUS server:** This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the

primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding.

- Click on the **Save Settings** button once you have modified the settings.

4.3.2 Advanced Wireless and WDS

- Click on the **Advanced** link under the **Wireless** menu. This page allows you to configure the fragmentation threshold, RTS threshold, transmit power, layer 2 isolation, and WDS (wireless distribution system).

ADVANCED

If you are not familiar with these Advanced settings, please read the help section before attempting to modify these settings.

ADVANCED SETTINGS

Fragmentation Threshold: (256..2346)

RTS Threshold: (0..2347)

Beacon Period: (20..1000)

DTIM Interval: (1..255)

Transmit Power: High

Layer2 Isolation Enable:

WDS Enable:

WDS AP MAC Address:

1:

2:

3:

4:

5:

6:

(Leave blank to disable WDS for that slot)

- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 65535. The default value is 2346.
- **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. Specify a value between 1 and 65535. The default value is 2346.
- **Beacon Period:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.
- **DTIM Interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

- **Transmit Power:** You may control the output power 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.
- **Layer 2 Isolation:** Place a check in this box if you would like to enable the layer 2 isolation feature. This feature will hide the node from the windows network neighborhood. It is recommended to enable this feature in a hotspot environment.
- **WDS:** Place a check in this box to enable WDS (Wireless Distribution System). When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links.
Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel number.
- **WDS AP MAC Address:** Specify one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.
- Click on the **Save Settings** button once you have modified the settings.

4.3.3 SNMP

- Click on the **SNMP** link under the **Wireless** menu. This page allows you to SNMP community and trap settings. The feature is useful while remotely monitoring and marinating the device.

SNMP

SNMP Parameter Settings

Use this section to configure the SNMP settings for your Wireless Access Point. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

SNMP SETTINGS

Support WebAdmin Control : Disable Enable

Read-Only Community Name:

Read-Write Community Name:

Send SNMP Trap: Disable Enable

Send Trap To:

Trap Community Name:

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

4.4 LAN

- Click on the **LAN** link under the **LAN** menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP client/server. This IP address is also used to access the web-based interface.

LAN

Network Settings

Use this section to configure the internal network settings of your Access Point. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

LAN SETTINGS

Get LAN IP from:

IP Address:

Subnet Mask:

Gateway:

Local Domain Name: (optional)

- Get LAN IP from:** Select **Static IP (Manual)** or **DHCP (Dynamic)** from the drop down list. Choose **DHCP (Dynamic)** if your router supports DHCP and you want the router to assign an IP address to this device. In this case, you do not need to fill in the following fields. Choose **Static IP (Manual)** if your router does not support DHCP or if for any other reason you need to assign a fixed address to this device.
Note: You cannot choose DHCP (Dynamic) if you have enabled the DHCP Server option on the DHCP page; this device cannot be both a DHCP client and a DHCP server.

LAN

Network Settings

Use this section to configure the internal network settings of your Access Point. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

LAN SETTINGS

Get LAN IP from:

IP Address:

Subnet Mask:

Gateway:

Local Domain Name: (optional)

- IP Address:** Enter an IP address for this device.
- Subnet Mask:** Enter the subnet mask for this IP address.
- Gateway:** Enter the IP address of the default gateway.
- Local Domain Name:** Enter a local domain name. This field is optional.
- Click on the **Save Settings** button once you have modified the settings.
Note: If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

4.5 DHCP Server

- Click on the **DHCP** link under the **LAN** menu. DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN). In most situations, the router provides DHCP services, and you can leave this option disabled. However, if for any reason the router does not provide DHCP services, enable this option. The AP's DHCP Server will then manage the IP addresses and other network configuration information for wireless clients associated with the AP. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to **DHCP** or **Obtain an IP address automatically**.

DHCP

DHCP Server

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

ENABLE

Enable DHCP Server :

DHCP SETTINGS

DHCP IP Address Range : to (addresses within the LAN subnet)

Primary DNS :

Secondary DNS :

DHCP Lease Time : (minutes)

Always broadcast : (compatibility for some DHCP Clients)

NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address

- Enable DHCP Server:** Place a check in this box if you would like this device to function as a DHCP Server.
- DHCP IP Address Range:** Enter the first and last IP address of the range. Make sure that the range is on the same subnet as the device. These two IP values (from and to) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.
- Primary / Secondary DNS:** Enter an IP address for the primary and secondary DNS servers. This field is optional.
- DHCP Lease Time:** The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

- **Always Broadcast:** If all the computers on the LAN successfully obtain their IP addresses from the Access Point's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the Access Point's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the Access Point to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.
- Click on the **Save Settings** button once you have modified the settings.
-

ADD DHCP RESERVATION

Enable:

IP Address: << Select Machine

MAC Address:

Copy Your PC's MAC Address

Computer Name:

Save Clear

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address		
<input checked="" type="checkbox"/>	node03	00:40:D0:58:17:33	192.168.1.103	●	✕
<input type="checkbox"/>	node02	00:40:D0:58:17:31	192.168.1.102	●	✕
<input checked="" type="checkbox"/>	node01	00:40:D0:58:17:30	192.168.1.101	●	✕

- **Enable DHCP Reservation:** You may use this feature to reserve a specific IP address for a specific MAC address (node). Place a check in this box to enable this feature.
- **IP Address:** Specify the IP address
- **MAC Address:** Specify the MAC address of the node which will used the reserved IP address.
- **Copy your PCs MAC address:** Click on this button if you would like to reserve an IP address for the PC you are logged on to.
- **Computer Name:** Specify a name for the specified IP address.
- Click on the **Save** button to insert the entry into the DHCP reservations list.

4.6 MAC Address Filter

- Click on the **MAC Address Filter** link under the **Filter** menu. The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

ENABLE

Enable MAC Address Filter :

FILTER SETTINGS

Mode :

Filter Wireless Clients :

Filter Wired Clients :

ADD MAC ADDRESS

Enable :

MAC Address : <<

Computer Name :

MAC ADDRESS LIST

Deny access to all except the machines in this list (subject to "Filter Settings"):

Enable	MAC Address	Computer Name		
<input checked="" type="checkbox"/>	00:40:D0:58:17:30	node01	<input type="checkbox"/>	<input type="checkbox"/>

- Enable MAC Address Filter:** You may use this feature to filter the wired and wireless clients. Place a check in this box to enable this feature.
- Mode:** Select a filter setting from the drop-down list. When **only allow listed machines** is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When **only deny listed machines** is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.
- Filter Wireless Clients:** Place a check in this box if you would like to filter wireless clients.
- Filter Wired Clients:** Place a check in this box if you would like to filter wired clients.
- MAC Address:** Specify the MAC address of the node which you would like to filter.
- Copy your PCs MAC address:** Click on this button if you would like to filter the MAC address for the PC you are logged on to.
- Computer Name:** Specify a name for the specified MAC address.
- Click on the **Save** button to insert the entry into the MAC address list.

4.7 Logs

- Click on the **Logs** link on the navigation menu. Logs display 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.

The screenshot shows a web interface for configuring logs. It has three main sections: LOGS, LOG OPTIONS, and LOG DETAILS. The LOGS section has a heading 'System Logs' and a paragraph explaining the option. The LOG OPTIONS section has two rows of checkboxes: 'What to View' with 'System' checked, and 'View Levels' with 'Critical', 'Warning', and 'Informational' all checked. Below these is a blue button labeled 'Apply Log Settings Now'. The LOG DETAILS section has three buttons: 'Refresh', 'Clear', and 'Save Log'. Below the buttons is a list of log entries, each starting with '[INFO]' followed by a timestamp and a message.

LOGS

System Logs

Use this option to view the Access Point logs. You can define what types of events you want to view and the event levels to view. This Access Point also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

LOG OPTIONS

What to View : System

View Levels : Critical Warning Informational

[Apply Log Settings Now](#)

LOG DETAILS

[Refresh](#) [Clear](#) [Save Log](#)

[INFO] Wed May 31 00:44:37 2006 Log viewed by IP address 192.168.1.21
[INFO] Wed May 31 00:24:03 2006 Stored configuration to non-volatile memory
[INFO] Wed May 31 00:23:18 2006 Allowed configuration authentication by IP address 192.168.1.21
[INFO] Wed May 31 00:22:35 2006 Initialization complete, starting DHCP server
[INFO] Wed May 31 00:22:33 2006 DHCP Server Parameter 19 was added to the parameter database
[INFO] Wed May 31 00:22:33 2006 DHCP Server Parameter 3 was added to the parameter database
[INFO] Wed May 31 00:22:33 2006 DHCP Server Parameter 1 was added to the parameter database
[INFO] Wed May 31 00:22:29 2006 Device initialized
[INFO] Wed May 31 00:22:29 2006 Wireless Link is up
[INFO] Wed May 31 00:22:29 2006 Stored configuration to non-volatile memory
[INFO] Thu Jan 01 00:00:00 1970 Loaded configuration from non-volatile memory

- Log Options:** Select the type of warning that you would like recorded and place a check in the appropriate box. Then click on the **Apply Log Settings Now** button.
- Log Details:** The events are logged in this section. Click on the **Refresh** button to refresh the events or click on the **Clear** button to clear the events. Click on the **Save Log** button to save the log on your PC.

4.8 Statistics

- Click on the **Statistics** link on the navigation menu. This page displays the transmitted and received packet statistics of the wired and wireless interface.

The screenshot displays the 'STATISTICS' page. At the top, it says 'Network Traffic Stats' and 'Traffic Statistics display Receive and Transmit packets passing through your Access Point.' Below this are two buttons: 'Refresh Statistics' and 'Clear Statistics'. The page is divided into three sections: 'LAN STATISTICS' and 'WIRELESS STATISTICS'. Each section shows 'Sent' and 'Received' counts, as well as 'TX Packets Dropped' and 'RX Packets Dropped' counts. 'Collisions' and 'Errors' are also listed for both sections.

Category	Sent	Received	TX Packets Dropped	RX Packets Dropped	Collisions	Errors
LAN STATISTICS	2068	1335	0	0	0	0
WIRELESS STATISTICS	64	0	0	0		0

- **Sent:** The number of packets sent from the bridge.
- **Received:** The number of packets received by the bridge.
- **TX Packets Dropped:** The number of packets that were dropped while being sent, due to errors, collisions, or bridge resource limitations.
- **RX Packets Dropped:** The number of packets that were dropped while being received, due to errors, collisions, or bridge resource limitations.
- **Collisions:** The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).
- **Errors:** The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.
- Click on the **Refresh Statistics** button to refresh the events or click on the **Clear Statistics** button to clear the events.

Appendix A – Specifications

Data Rates

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

Standards

IEEE802.11b/g,
IEEE802.3, IEEE802.3u,
IEEE802.3af,
IEEE802.1f, IEEE802.1x

Compatibility

IEEE 802.11g/ IEEE
802.11b

Power Requirements

Power Supply: 90 to
240 VDC \pm 10%
(depends on different
countries)
Device: 12 V/ 1A

Status LEDs

LAN: Link, WLAN: Link,
Power: on/off

Regulation Certifications

FCC Part 15 B & C,
CE: EN 300328, EN
301489
EN 60950

RF Information

Frequency Band

802.11b/g: U.S., Europe
and Japan product
covering 2.4 to 2.484
GHz, programmable for
different country
regulations

Media Access Protocol

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

Modulation Technology

Orthogonal Frequency
Division Multiplexing
(OFDM)
DBPSK @ 1Mbps
DQPSK @2Mbps
CCK @ 5.5 & 11Mbps
BPSK @ 6 and 9 Mbps
QPSK @ 12 and 18

Mbps

16-QAM @ 24 and 36

Mbps

64-QAM @ 48 and 54

Mbps

Operating Channels

11 for North America
14 for Japan
13 for Europe

Receive Sensitivity (Typical)

- 2.412~2.472G(IEEE802
.11g)
6Mbps@ -91dBm;
54Mbps@ -74dBm
- 2.412~2.472G(IEEE802
.11b)
11Mbps@ -90dBm
1Mbps@ -95dBm

Available Transmit Power

(Typical)

- 2.412~2.472G(802.11g)
27dBm @6 ~ 24Mbps
25dBm@36Mbps
24 dBm@48Mbps
23dBm@54Mbps
- 2.412~2.472G(802.11b)
28 dBm@1, 2, 5.5 and
11Mbps

RF Connector

TNC Type (Female
Reverse)

Networking

Topology

Ad-Hoc, Infrastructure

Operation Mode

Point-to-Point/ Point-to-
Multipoint Bridge/ AP/
Client Bridge/ WDS

Interface

One 10/100Mbps RJ-45
LAN Port

Security

- IEEE802.1x
Authenticator /
RADIUS Client (EAP-
MD5/TLS/TTLS)
Support in AP Mode
- IEEE802.1x
Supplicant (EAP-
MD5/TLS/TTLS,
PEAP) support in
Client Bridge Mode
- WPA /WPA2/ Pre
Share KEY (PSK) with
TKIP/AES
- MAC address filtering
(AP only)
- Hide SSID in beacons
- VLAN Pass-through

IP Auto-configuration

DHCP client/server

Management

Configuration

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

Firmware Upgrade

Upgrade firmware via
web-browser

Environmental

Temperature Range

Operating: 0°C to 45°C
(32°F to 113°F)
Storage: -40°C to 70°C
(-40°F to 158°F)

Humidity (non- condensing)

5%~95% Typical

Package Contents

One AP/ CB Device
One TNC Dipole
Antenna
One Power Adapter
One CAT5 UTP Cable
One Quick Start Guide
One CD-ROM with
User's Manual

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.

IC statement

Operation is subject to the following two conditions:

This device may not cause interference and

This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 9 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

IMPORTANT NOTE: IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

Ce périphérique ne doit pas causer d'interférence et.

Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

Appendix C – Index

- 1
- 128-bit, 4, 22, 23, 38, 39
- 8
- 802.11b, 4, 21, 38, 50
802.11d, 24
802.11g, 4, 21, 38, 50
802.1x, 4, 40
- A
- ACK Timeout, 22, 38
Ad-hoc, 6, 21
Administrator Settings, 12, 17, 31, 35
Advanced Wireless Settings, 24
Applications, 6
ASCII, 22, 24, 38, 40
- B
- Beacon Period, 42
Bridge Name, 13, 25
Broadcast, 46
- C
- Channel, 20, 21, 38
Client Bridge Mode, 10, 50
Community Name, 26, 43
- D
- DHCP, 4, 10, 26, 27, 30, 44, 45, 46, 50
dipole antenna, 5, 50
DITM Interval, 42
DNS, 45
- F
- Features & Benefits, 4
Filter, 30, 47
Firmware Upgrade, 16, 33, 50
Fragment Threshold, 25, 42
- G
- Grounding Cable, 5, 50
- H
- Hardware Installation, 8
HEX, 22, 38
- I
- Infrastructure, 6, 7, 21, 50
Infrastructure Mode, 7
IP Address Configuration, 8
- L
- LAN Settings, 26
Logging In, 10, 30
- Logs, 29, 30, 48
- M
- MAC Address, 20, 41, 43, 46, 47
- N
- Network Configuration, 6
NIC, 8
- O
- Open, 5, 23, 39
operation mode, 20
- P
- Package Contents, 5
Password, 10, 30
PoE, 5, 8, 50
Power Injector, 5, 50
Privacy, 20, 22, 23, 38, 39, 40
- R
- RADIUS, 40, 41, 50
Restore Settings to Default, 17, 18, 35
Restore the Configuration from a File, 14, 33
RTS Threshold, 25, 42
- S
- Save Configuration to a File, 14, 32
Shared Key., 23, 39
Signal, 20
site survey, 8
SNMP, 20, 25, 26, 43, 50
SSID, 4, 11, 20, 21, 38, 50
Static, 26, 27, 44
Statistics, 10, 28, 30, 49
subnet mask, 9
Switch from Bridge to AP Mode, 15
System, 5, 10, 12, 16, 17, 18, 30, 31, 33, 35, 37, 43
System Requirements, 5
- T
- Transmission Rate, 21, 38
Transmit Power, 25, 43
Trap, 26, 43
- U
- User Name, 10, 30
- W
- WDS, 4, 42, 43, 50
Wireless Network Settings, 20, 38
Wireless Security, 22
WPA, 4, 20, 22, 23, 24, 38, 39, 40, 41, 43, 50

