

**Wireless 802.11g  
Access Point  
User's Manual**

# Table of contents

<b>INTRODUCTION</b> .....	<b>1</b>
<b>Features</b> .....	<b>1</b>
<b>LED Indicators</b> .....	<b>2</b>
Solid .....	2
<b>Ports on the Rear Panel</b> .....	<b>2</b>
<b>GETTING CONNECTED</b> .....	<b>4</b>
<b>AP MODES:</b> .....	<b>5</b>
<b>CONFIGURATION VIA WEB</b> .....	<b>6</b>
<b>Login</b> .....	<b>6</b>
<b>Info(Information)</b> .....	<b>7</b>
<b>Assoc(Associations)—Only for Access Point mode</b> .....	<b>8</b>
<b>Wireless (Wireless Configuration)</b> .....	<b>9</b>
<b>Access (Access Control)-Only for Access Point mode</b> .....	<b>11</b>
<b>Advanced (Advanced Wireless)</b> .....	<b>12</b>
<b>Security</b> .....	<b>15</b>
<b>IP Addr (IP Address Settings) -Only for Access Point mode</b> .....	<b>17</b>
IP Address Mode .....	17
Access point name .....	18
<b>Admin (Administration)</b> .....	<b>19</b>
Change password. ....	19
Reboot/Reset this device.....	19
Upgrade system firmware.....	19
<b>Help</b> .....	<b>21</b>

# Introduction

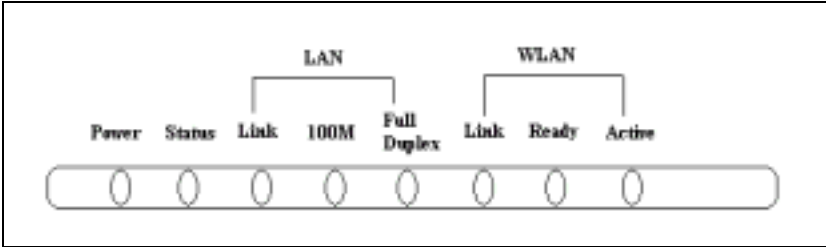
The Wireless 802.11g Access Point is a [54 Mbps Access Point \(AP\)](#) that can also act as a Media Access Control (MAC) bridge between wired Local Area Networks, and one or more LAN wireless networks. Placed anywhere along with an Ethernet LAN, the Wireless 802.11g Access Point allows up to 200 wireless stations within its area of coverage to access transparently to the corporate network.

## Features

- ◆ [High speed for wireless LAN connection, 54 Mbps.](#)
- ◆ Web browser-based configuration utility.
- ◆ Wireless security of 128-bit WEP Encryption/ MAC Address Filtering
- ◆ AP Visibility Modes
- ◆ Firmware upgrades
- ◆ Static IP Address or DHCP
- ◆ Automatic Device Discovery

# LED Indicators

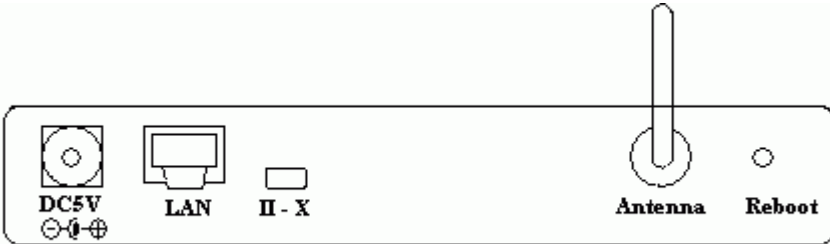
## LED Indicators on the Front Panel



LED Indicator	Status	
	Solid	Dim/ Flashing
Power	Glows when power is applied to this device, the LED turns solid yellow.	Dim when no power is applied.
Status	Normal	Flashing when upgrading firmware.
LAN-Link	Glows when Ethernet is connected.	Dim when no Ethernet is connected. Flashing when this device is sending/receiving data
LAN-100M	Glows for 100Mbps Ethernet connection.	Dim for 10 Mbps Ethernet connection
LAN-Full Duplex	Glows for Full duplex mode	Dim for half duplex
WLAN-Link	Glows when this device is associated	Dim when it is not associated
WLAN-Ready	Glows when WLAN is connected.	Dim when no WLAN is connected.

		Flashing when trying to connect to WLAN.
WLAN-Active	N/A	Flashing when this device is actively sending/receiving data over the wireless LAN connection.

## Ports on the Rear Panel



	Port/button	Functions
<b>A</b>	<b>5V DC</b>	Connects the power adapter plug.
<b>B</b>	<b>LAN</b>	Connects to your LAN's network device.
<b>C</b>	<b>II-X</b>	Switch this button for choosing different wiring scheme LAN connection; <b>Switch left</b> to select using a straight Ethernet cable; <b>Switch right</b> to use a Crossover Ethernet cable. .
<b>D</b>	<b>Antenna</b>	Adjust to have better performance
<b>E</b>	<b>Reboot</b>	Use a pin-shape item, for example a pin tip, to press this button to re-boot this device when the device stop working properly. .

# Getting Connected

1. **Find a Location:** choose a location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations.
2. **Adjust the Antenna:** usually the higher the antenna is placed, the better will be the performance.
3. **Connect to your local area network:** connect a straight or a crossover **Ethernet cable** to one of the **Ethernet** port of the Access Point, and the other end to a hub or switch. (If you are using a straight Ethernet cable, make sure the II-X button is switched right; the other way for Cross Ethernet cable.)
4. **Power on the device:** connect the included AC power adapter to the Access Point's power port and the other end to a wall outlet. *Note: use only the power adapter that provided with the Access Point. Using a different power adapter may cause permanent damage to the device.*

## **AP MODES:**

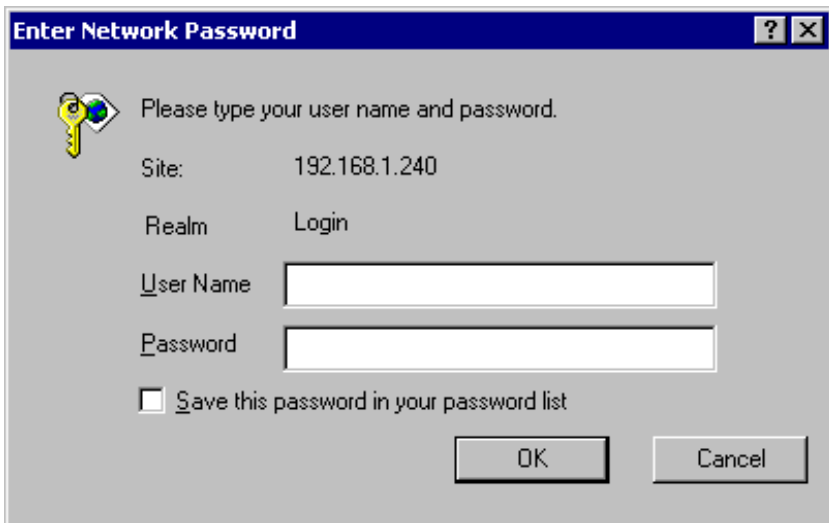
This device is shipped with configuration that can be utilized right out of the box. The default configuration is as a AP/bridge depending on your purchase. If you want to change the settings in order to perform more advanced configuration or just configure into the other mode, namely Access Point to bridge or the other way, you can use the web-based utility provided by the manufacturer as described below.

# Configuration via Web


## Login

Open the browser, enter the local port IP address of the Device (default at **192.168.1. 240**), and click “Go” to get the login page.

The user name and password are not required and should be left blank for the first-time login. Just click **OK** to enter.



**Enter Network Password** ? X

 Please type your user name and password.

Site: 192.168.1.240

Realm Login

User Name

Password

Save this password in your password list

OK Cancel



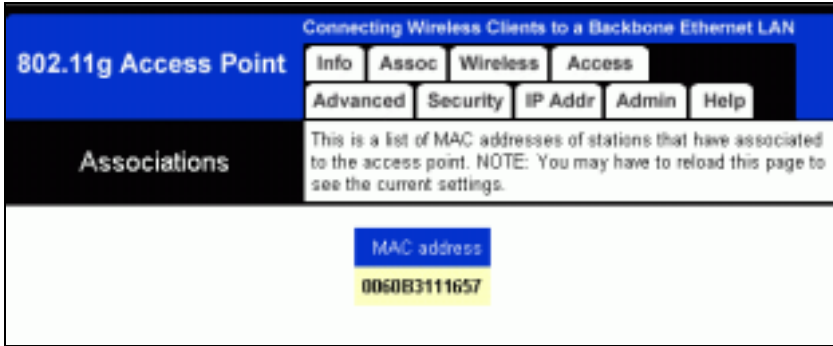
# Info(Information)

The setup home page will display the information about the current settings of this access point.

802.11g Access Point	
Connecting Wireless Clients to a Backbone Ethernet LAN	
<a href="#">Info</a> <a href="#">Assoc</a> <a href="#">Wireless</a> <a href="#">Access</a>	
<a href="#">Advanced</a> <a href="#">Security</a> <a href="#">IP Addr</a> <a href="#">Admin</a> <a href="#">Help</a>	
<b>Information</b>	Basic information about this access point. NOTE: You may have to reload this page to see the current settings.
<b>Access Point Information</b>	
Access Point Name:	802.11g AP
MAC address of AP:	0060B31A002D
Associated stations:	1
RF Firmware version:	1.0.4.3
System Firmware version:	1.0.P_1
<b>Current IP Settings</b>	
IP address:	192.168.1.240
DHCP client:	disabled
<b>Current Wireless Settings</b>	
Profile:	802.11b/g Mixed Mode
Wireless network name (SSID):	802_11g
Channel:	1
WEP:	disabled
WPA:	disabled

## Assoc(Associations)—Only for Access Point mode

This page shows the **MAC addresses** of devices connected to this Wireless 802.11g Access Point.



The screenshot shows a web interface for an 802.11g Access Point. The title is "802.11g Access Point" and the subtitle is "Connecting Wireless Clients to a Backbone Ethernet LAN". The navigation menu includes "Info", "Assoc", "Wireless", "Access", "Advanced", "Security", "IP Addr", "Admin", and "Help". The "Assoc" tab is selected. The main content area is titled "Associations" and contains a note: "This is a list of MAC addresses of stations that have associated to the access point. NOTE: You may have to reload this page to see the current settings." Below the note, there is a table with one row containing a MAC address: 0060B3111657.

MAC address
0060B3111657

## Wireless (Wireless Configuration)

Here you can set/change wireless configuration including **visibility status**, **PHY profiles**, **SSID**, **channel**, **transmission rate** ... etc. See the description that comes after each function.

When you are done with the change, remember to restart this access point to let the new settings take effect.


The screenshot shows a web interface for configuring an 802.11g Access Point. The page title is "802.11g Access Point" and the subtitle is "Connecting Wireless Clients to a Backbone Ethernet LAN". There are several tabs: "Info", "Assoc", "Wireless", "Access", "Advanced", "Security", "IP Addr", "Admin", and "Help". The "Wireless" tab is selected. The "Wireless Configuration" section contains the following settings:

- Visibility Status:**  Visible  Invisible. Description: "When Invisibility is selected, the AP is protected against discovery by wireless sniffers, and all wireless clients must explicitly know and use the SSID."
- PHY Profiles:** 802.11 b/g Mixed Mode. Description: "These profiles control a number of settings for overall wireless network usage. Their meanings are self-explanatory. For more details, please see Intersil documentation."
- Wireless Network Name (SSID):** 802\_11g. Description: "This is the name of the access point on the wireless network. Stations that associate to this access point may have to know this name."
- Channel:** 2.4 GHz channel 1. Description: "This is the radio channel that the access point will operate on. If you experience interference (e.g. lost connections or slow data transfers) you may need to try different channels to see which is the best. Channels 1-14 are in the 2.4 GHz band and channels 36-64 are in the 5 GHz band."
- Transmission rate (Mbits/s):** Best (automatic). Description: "This is the speed at which the access point will transmit data. Normally you should select 'best' here, although if your wireless network is unusually noisy or quiet you may wish to use a fixed low or high rate."

At the bottom right of the configuration area are "Save" and "Cancel" buttons.

Visibility Status

If you select **invisible**, this AP can not be detected by wireless sniffers; which means all the wireless clients can not associated to this AP unless they know/use the SSID.

PHY Profiles	<p>You can select different wireless networking hardware (PHY) to meet your wireless environment or for optimal performance. You can thus choose from the list.</p> 
Wireless Network Name (SSID)	<p>The <b>SSID</b> is the unique name shared among all points in your wireless network. The name must be identical for all devices and points attempting to connect to the same network.</p>
Channel	<p>Shows the selected channel that is currently in use. (There are <b>14</b> channels available, depending on the country.)</p>
Transmission rate (Mbps)	<p>Shows the current transfer rate There are Best (Automatic), Fixed 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54Mbps. )</p>

## Access (Access Control)-Only for Access Point mode

This AP provides MAC Address filtering, which prevents the unauthorized MAC Addresses from accessing your Wireless LAN.

Once you check to enable access control, only MAC addresses entered in following fields are allowed to associate to this AP.

Note:

1. You can enter 16 MAC Addresses to associate to this AP.
2. You can copy the MAC addresses shown on the Station List and past them to the MAC address table to save the effort of typing and avoid typo as well.

The screenshot shows a web interface for configuring an 802.11g Access Point. The title is "802.11g Access Point" and the subtitle is "Connecting Wireless Clients to a Backbone Ethernet LAN". There are several tabs: "Info", "Assoc", "Wireless", "Access", "Advanced", "Security", "IP Addr", "Admin", and "Help". The "Access" tab is selected. The main heading is "Access Control". Below this, there is a paragraph of text: "On this page you can enable Access Control. If enabled, only the MAC addresses entered into the 'MAC address' boxes are allowed to associate to this AP. Note that you can cut and paste the addresses from the 'Station List' page into the MAC address boxes. These changes are effective immediately." Below the text, there is a checkbox labeled "Enable access control:" with the text "(Check this box to enable access control.)" next to it. Below the checkbox, there are eight input fields labeled "MAC address 1:" through "MAC address 8:". At the bottom right, there are "Save" and "Cancel" buttons.

**Figure: Access Control**

# Advanced (Advanced Wireless)

Connecting Wireless Clients to a Backbone Ethernet LAN

**802.11g Access Point**

---

**Advanced Wireless**

On this page you can configure the advanced 802.11g access point settings. Any new settings will not take effect until the access point is rebooted.

---

**Maximum associated stations:**

This the maximum number of wireless stations that can be associated at any one time.

**Fragmentation threshold:**

Transmitted wireless packets larger than this size will be fragmented to maintain performance in noisy wireless networks.

**RTS threshold:**

Transmitted wireless packets larger than this size will use the RTS/CTS protocol to (a) maintain performance in noisy wireless networks and (b) prevent hidden nodes from degrading performance.

**Beacon period:**

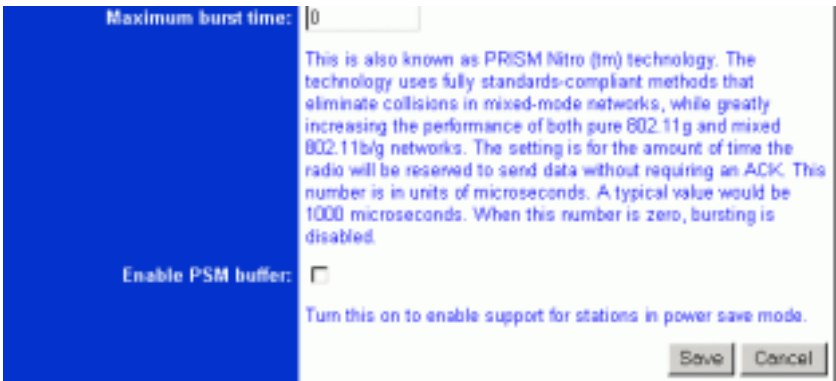
Access point beacons are sent out periodically. This is the number of milliseconds between each beacon.

**DTIM interval:**

This is the number of beacons per DTIM (Delivery Traffic Indication Message), e.g. '1' means send a DTIM with each beacon, '2' means with every 2nd beacon, etc.

Maximum associated stations	200
Fragmentation threshold	To fragment MSDU or MMPDU into small sizes of frames for increasing the reliability of frame (The maximum value of <b>2346</b> means no fragmentation is needed) transmission. The performance will be decreased as well, thus a noisy environment is recommended.
RTS Threshold	RTS (Request To Send) is a <a href="#">control frame</a> sent from the transmitting station to the

	receiving station requesting permission to transmit. This value is recommended to remain at its default setting of <b>2432</b> . Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Beacon period	This is also called <b>Beacon Interval</b> . This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network. The default value is 100.
DTIM interval	DTIM stands for <b>Delivery Traffic Indication Message</b> . A DTIM is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast message for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point clients hear and awaken to receive the broadcast and multicast messages.



Maximum burst time	The amount of time the radio will be reserved to send data without requiring an ACK. Adding a burst time should help throughput for 802.11g clients when AP is running in mixed mode. This number is in units of microseconds. A typical value would be 1000 microseconds. When this number is zero, bursting is disabled.
Enable PSM buffer	PSM stands for Power Save Mechanisms. Turn this on to enable support for stations in power save mode.

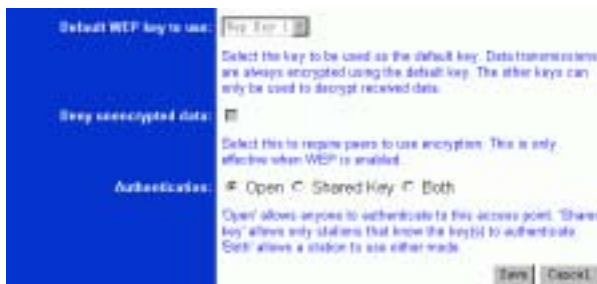


# Security

Here you can enable the WEP and set the WEP key, if you enable the WEP, the client PC also need to set the WEP key.



Enable WEP	WEP (Wired Equivalent Privacy) encryption can be used to ensure the security of your wireless network. The window allows you to set to <b>64bit</b> or <b>128bit</b> Encryption (WEP) by using either <b>Passphrase</b> or <b>Manual Entry</b> methods. <i>Note:</i> To allow Decryption and communication, all wireless devices must share the identical encryption key on the same network.
WEP key lengths	Select between 64-bit and 128-bit.
WEP key	You can enter WEP key here or use the default settings shown in the next field.



Default WEP key to use	Select one of the four keys to encrypt your data. Only
------------------------	--

	<p>the key you select it in the “Default WEP key to use” will take effect.</p>
Deny unencrypted data	<p>To access this wireless network clients are required to use encryption. This should be checked together with the item “Enable WEP”.</p>
Authentication	<p>The authentication mode defines configuration options for the sharing of wireless networks to verify identity and access privileges of roaming wireless network cards. You may choose between <b>Open</b>, <b>Shared Authentication</b>, and <b>Both</b>.</p> <p>If the Access Point is using "<b>Open Authentication</b>", then the wireless adapter will need to be set to the same authentication mode.</p> <p><b>Shared Authentication</b> is when both the sender and the recipient share a secret key.</p> <p>Select <b>Both</b> for the network adapter to select the Authentication mode automatically depending on the Access Point Authentication mode.</p>

# IP Addr (IP Address Settings) -Only for Access Point mode

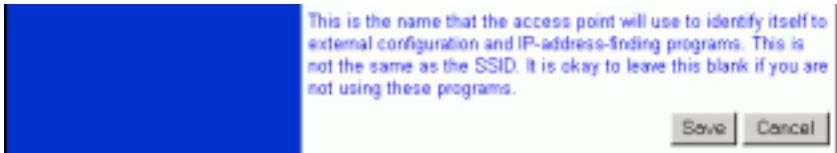
Set the management IP for the Wireless 802.11g Access Point, the default IP address is 192.168.1.240.

## IP Address Mode

If you select **DHCP**, DHCP server will automatically assign IP addresses to [this device](#). And the fields that follow will be grayed out and need no settings. If, otherwise you select **Static**, you will have to manually set the [device IP address](#).

The screenshot shows the configuration interface for an 802.11g Access Point. The page title is "802.11g Access Point" and the subtitle is "Connecting Wireless Clients to a Backbone Ethernet LAN". The navigation menu includes "Info", "Assoc", "Wireless", "Access", "Advanced", "Security", "IP Addr", "Admin", and "Help". The "IP Settings" section contains the following fields and options:

- IP Address Mode:**  Static  DHCP
- Default IP address:**  (Note: Type the IP address of your Access Point)
- Default subnet mask:**  (Note: The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.255.0.)
- Default gateway:**  (Note: This is the IP address of the gateway that connects you to the internet.)
- Access point name:**



### **Access point name**

You can name this Access Point for identification. You can leave it blank without entering anything. However, the name for the access point will be useful for identification especially when there are more than on Access Points in your wireless network.

## **Admin (Administration)**

In this Administration page, you can

### **Change password.**

The device has no password at default. It is recommended that you set a password to ensure that no one can adjust the device's settings;

#### **To set/change password:**

1. Enter your password to the first password box.
2. Enter the password again in the next box to confirm.
3. Click **SAVE** to save the setting.

### **Reboot/Reset this device.**

By **Reboot**, the device will re-boot itself and while still keep your original settings. You will probably do this if problems occur with this Access Point.

By **Reset**, the device will reset itself to the factory default settings.

*(Note that all your original settings will be replaced by factory default settings.)*

### **Upgrade system firmware.**

#### **To upgrade system firmware,**

1. You will have to download the file to your computer.
2. Enter the file name and path in the field next to the Browse button. Or you can click Browse to find the file you previously downloaded.
3. Click the **Upload** button to start upgrading. Wait for about 1 minute for the upgrade.
4. When the firmware upgrade is complete, remember to reboot the device.

802.11g Access Point		Connecting Wireless Clients to a Backbone Ethernet LAN	
		Info	Assoc
		Wireless	Access
		Advanced	Security
		IP Addr	Admin
		Help	
Administration	<p>On this page you can change the password, reboot the access point, or reset all settings to their factory defaults. If you have changed any settings it is necessary to reboot the access point for the new settings to take effect.</p>		
User name:	<input type="text"/>		
Administrator password:	<p>This is the user name that you must type when logging in to these web pages.</p>		
	<input type="text"/>		
	<input type="text"/>		
	<p>This is the password that you must type when logging in to these web pages. You must enter the same password into both boxes, for confirmation</p>		
			<input type="button" value="Save"/> <input type="button" value="Cancel"/>
Commands			
Reboot access point:	<input type="button" value="Reboot"/>		
Reset to factory defaults:	<input type="button" value="Reset"/>		
Upgrade system firmware	<p>File to upload:</p>		
	<input type="text"/>		<input type="button" value="Browse..."/>
	<input type="button" value="Upload"/>		
	<p>The upload may take up to 60 seconds.</p>		

# Help

802.11g Access Point

Connecting Wireless Clients to a Backbone Ethernet LAN

Info Assoc Wireless Access

Advanced Security IP Addr Admin Help

Help

This is where some helpful information will go. There is nothing here right now.

# Bridge MODES:

## Info(Information)

The setup home page will display the information about the current settings of this access point.

**802.11g Bridge** Wireless Enabling Desktops PCs, Printers & Game Consoles  
(Use an Ethernet Hub or Switch to Support Multiple Devices)

[Info](#) [Wireless](#) [Security](#) [Advanced](#) [Admin](#) [Help](#)

**Information** Basic information about this bridge. NOTE: You may have to reload this page to see the current settings.

---

**Access Point Information**

State: Disconnected

Wireless network name (SSID):

Channel: 6

Transmission rate: Best (automatic)

Communications strength: 0%

BSSID: 000000000000

WEP: disabled

---

**Bridge Information**

Bridge Name: 802.11g Bridge

Number of bridged clients: 12

IP address: 192.168.1.241

MAC address: 00E09814EAA2

RF Firmware version: 1.0.4.3

System Firmware version: 1.0.P\_3

### Available access points

SSID	BSSID	Channel	Strength	Mode
CISCO1200AP_B	000D28A45E0B	1	76%	802.11b
Genesis Microchip	009096284395	6	71%	802.11b
Abocom	00E0984C041E	10	73%	802.11g
ATC	0010E7F5C823	1	66%	802.11b
WP	000D28A45E00	6	67%	802.11b



# Wireless (Wireless Configuration)


Here you can set/change wireless configuration including **visibility status**, **PHY profiles**, **SSID**, **channel**, **transmission rate** ... etc. See the description that comes after each function.

When you are done with the change, remember to restart this access point to let the new settings take effect.

The screenshot shows the configuration interface for an 802.11g Bridge. At the top, there's a title '802.11g Bridge' and a subtitle 'Wireless Enabling Desktops PCs, Printers & Game Consoles (Use an Ethernet Hub or Switch to Support Multiple Devices)'. Below the title are navigation tabs: 'Info', 'Wireless', 'Security', 'Advanced', 'Admin', and 'Help'. The 'Wireless' tab is selected. The main heading is 'Basic Wireless'. A descriptive paragraph states: 'On this page you can configure the basic 802.11g wireless settings. Any new settings will not take effect until the bridge is rebooted.' The configuration options are: 'Wireless Mode' with radio buttons for 'Infrastructure' (selected) and 'Ad-hoc'; 'Wireless Network Name (SSID)' with a text input field containing '802.11g'; 'Channel' with a dropdown menu set to '24 GHz channel 1'; 'Transmission rate (Mbps)' with a dropdown menu set to 'Best (automatic)'; and 'PHY Profiles' with a dropdown menu set to '802.11g Mixed Mode'. Each option has a detailed explanatory text block. At the bottom right, there are 'Save' and 'Cancel' buttons.

Wireless Mode

Infrastructure mode: to connect to a AP  
Ad-hoc mode to connect to other bridge station.

Wireless Network Name (SSID)	The <b>SSID</b> is the unique name shared among all points in your wireless network. The name must be identical for all devices and points attempting to connect to the same network.
Channel	Select channel that is currently in use. (There are <b>14</b> channels available, depending on the country.) only for Ad-hoc mode
Transmission rate (Mbps)	Shows the current transfer rate There are Best (Automatic), Fixed 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54Mbps. )
PHY Profiles	<p>You can select different wireless networking hardware (PHY) to meet your wireless environment or for optimal performance. You can thus choose from the list.</p> 

# Security

Here you can enable the WEP and set the WEP key, if you enable the WEP, the client PC also need to set the WEP key.

**802.11g Bridge**  
Wireless Enabling Desktops PCs, Printers & Game Consoles  
(Use an Ethernet Hub or Switch to Support Multiple Devices)

Info Wireless **Security** Advanced Admin Help

**Security and Encryption Settings**  
On this page you can set the 802.11g security and encryption options. Any new settings will not take effect until the bridge is rebooted.

**WEP configuration**  
WEP is the wireless encryption standard. To use it you must enter the same key(s) into the bridge and the 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. If you leave a key box blank then this means a key of all zeros.

Enable WEP:

Check this box to enable WEP. For the most secure use of WEP, also select "Deny Unencrypted Data" and set Authentication to "Shared Key" when WEP is enabled

Default WEP key to use: WEP Key 1

Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.

Deny unencrypted data:

Select this to require peers to use encryption. This is only effective when WEP is enabled.

Authentication:  Open  Shared Key

Select the type of authentication used when connecting to an access point. 'Open' is used if anyone can connect to the AP. 'Shared key' is used if both devices must know the encryption key.

WEP key length: 64 bit (10 hex digits)

Select the WEP key size. This length applies to all keys.

WEP key 1:

WEP key 2:

WEP key 3:

WEP key 4:

Save Cancel

Enable WEP	WEP (Wired Equivalent Privacy) encryption can be used to ensure the security of your wireless network.
------------	--

	<p>The window allows you to set to <b>64bit</b> or <b>128bit</b> Encryption (WEP) by using either <b>Passphrase</b> or <b>Manual Entry</b> methods.</p> <p><i>Note:</i> To allow Decryption and communication, all wireless devices must share the identical encryption key on the same network.</p>
Default WEP key to use	Select one of the four keys to encrypt your data. Only the key you select it in the “Default WEP key to use” will take effect.
Deny unencrypted data	To access this wireless network clients are required to use encryption. This should be checked together with the item “Enable WEP”.
Authentication	<p>The authentication mode defines configuration options for the sharing of wireless networks to verify identity and access privileges of roaming wireless network cards. You may choose between <b>Open</b>, <b>Shared Authentication</b>, and <b>Both</b>.</p> <p>If the Access Point is using "<b>Open Authentication</b>", then the wireless adapter will need to be set to the same authentication mode.</p> <p><b>Shared Authentication</b> is when both the sender and the recipient share a secret key.</p> <p>Select <b>Both</b> for the network adapter to select the Authentication mode automatically depending on the Access Point Authentication mode.</p>
WEP key lengths	Select between 64-bit and 128-bit.
WEP key	Enter WEP key here .

# Advanced (Advanced Wireless)

802.11g Bridge  
Wireless Enabling Desktops PCs, Printers & Game Consoles  
(Use an Ethernet Hub or Switch to Support Multiple Devices)

Info Wireless Security **Advanced** Admin Help

**Advanced**  
On this page you can configure the advanced 802.11g wireless settings. Any new settings will not take effect until the bridge is rebooted.

**Cloning**  
Cloning mode:  WLAN Card  Ethernet Client  
Select "WLAN Card" to set the MAC Address of the Bridge (as seen by the Access Point and other wireless devices) to be that of the MAC Address of WLAN Card inside the Bridge. Select "Ethernet Client" to set the MAC Address to that of the first Ethernet client that transmits data from behind the Bridge.

**Advanced wireless**  
Fragmentation threshold:   
Transmitted wireless packets larger than this size will be fragmented to maintain performance in noisy wireless networks.  
RTS threshold:   
Transmitted wireless packets larger than this size will use the RTS/CTS protocol to (a) maintain performance in noisy wireless networks and (b) prevent hidden nodes from degrading performance.  
Maximum burst time:   
The amount of time the radio will be reserved to send data without requiring an ACK. Adding a burst time should help throughput for 802.11g clients when AP is running in mixed mode. This number is in units of microseconds. A typical value would be 1000 microseconds. When this number is zero, bursting is disabled.

Save Cancel

Cloning mode	WLAN Card : set MAC address by internal MAC address, Ethernet Client: Set MAC address as the first LAN client.
Fragmentation threshold	To fragment MSDU or MMPDU into small

	<p>sizes of frames for increasing the reliability of frame (The maximum value of <b>2346</b> means no fragmentation is needed) transmission. The performance will be decreased as well, thus a noisy environment is recommended.</p>
RTS Threshold	<p>RTS (Request To Send) is a <b>control frame</b> sent from the transmitting station to the receiving station requesting permission to transmit. This value is recommended to remain at its default setting of <b>2432</b>. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.</p>
Maximum burst time	<p>The amount of time the radio will be reserved to send data without requiring an ACK.</p>

## **Admin (Administration)**

In this Administration page, you can

### **Change device name.**

This is the name that the bridge will use to identify itself to external configuration and IP-address-finding programs. It is okay to leave this blank if you are not using these programs

### **IP address setting.**

Set the IP address for this device or use dhcp to get a ip for this device.

### **Change password.**

The device has no password at default. It is recommended that you set a password to ensure that no one can adjust the device's settings;

#### **To set/change password:**

4. Enter your password to the first password box.
5. Enter the password again in the next box to confirm.
6. Click **SAVE** to save the setting.

### **Reboot/Reset this device.**

By **Reboot**, the device will re-boot itself and while still keep your original settings. You will probably do this if problems occur with this Access Point.

By **Reset**, the device will reset itself to the factory default settings.

*(Note that all your original settings will be replaced by factory default settings.)*

## Upgrade system firmware.

### **To upgrade system firmware,**

5. You will have to download the file to your computer.
6. Enter the file name and path in the field next to the Browse button. Or you can click Browse to find the file you previously downloaded.
7. Click the **Upload** button to start upgrading. Wait for about 1 minute for the upgrade.
8. When the firmware upgrade is complete, remember to reboot the device.



## 802.11g Bridge

Wireless Enabling Desktops PCs, Printers & Game Consoles  
(Use an Ethernet Hub or Switch to Support Multiple Devices)

Info Wireless Security Advanced **Admin** Help

### Administration

On this page you can configure the IP address used by the Web server running on this bridge. For "static" mode, the IP address settings are given here. For "DHCP" mode, these settings are supplied by a DHCP server on your network. You can also change the password, reboot the bridge, or reset all settings to their factory defaults. If you have changed any settings it is necessary to reboot the bridge for the new settings to take effect.

#### Device name

Device name:

This is the name that the bridge will use to identify itself to external configuration and IP-address-finding programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.

#### IP settings

IP Address Mode:  Static  DHCP

Select 'DHCP' to get the IP settings from a DHCP server on your network. Select 'Static' to use the IP settings specified on this page.

Default IP address:

Type the IP address of your bridge

Default subnet mask:

The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.255.0.

Default gateway:

This is the IP address of the gateway that connects you to the internet. The factory default is 192.168.1.1

#### Security

User name:

This is the user name that you must type when logging in to these web pages.

Administrator password:

This is the password that you must type when logging in to these web pages. You must enter the same password into both boxes, for confirmation

#### Commands

Reboot bridge:

Reset to factory defaults:

#### Upgrade system firmware

File to upload:

The upload may take up to 60 seconds.

## **FEDERAL COMMUNICATIONS 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 or more 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.

### **CAUTION:**

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

### **FCC RF Radiation Exposure Statement**

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.