Wireless 802.11g
Access Point

User's Manual

Table of contents

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.

Introduction

The **Wireless 802.11g Access Point** is an IEEE802.11g compliant access point, it not only provides a high transfer rate up to 54Mbps, which is almost five times faster than the already existing 11Mbps 802.11b products, but is also backward compatible with the Wireless B equipments.

The **Wireless 802.11g Access Point** provides 64/128 bit WEP encryption and **IEEE802.1x** which ensures a high level of security to protects users' data and privacy. The **MAC Address filter** prevents the unauthorized MAC Addresses from accessing your Wireless LAN. Your network security is therefore double assured.

This device can support three modes, i.e. **Access Point, Repeater** and **Bridge**. With the **Repeater** (**WDS**) functionality, the distance of wireless connection can be extended and wireless clients can roam between Access Points. While acting as a **Bridge**, this device connects wireless stations for inter-LAN connection.

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.

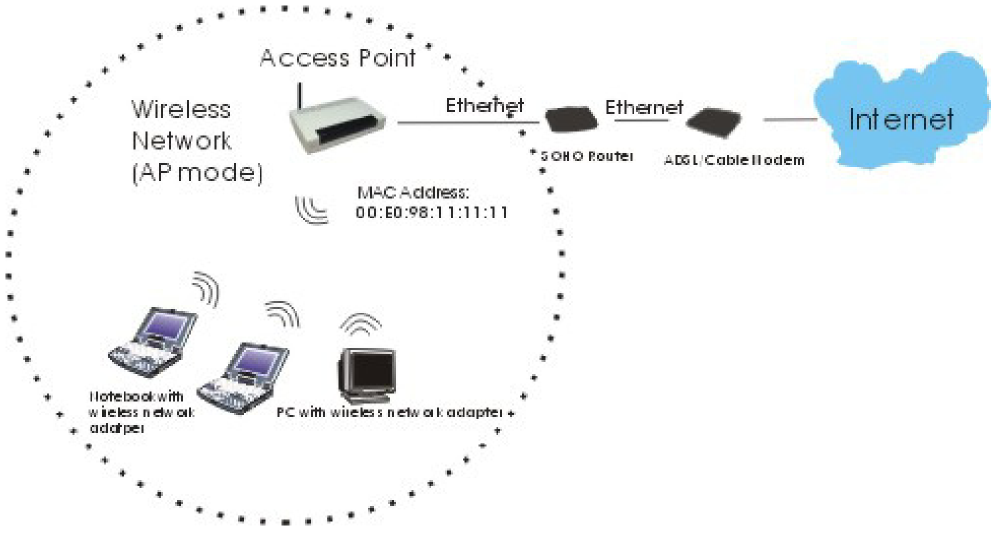
The web-based configuration utility allows users to configure via web browser. Advanced setup and firmware upgrade can be done easily.

About the Operation Modes

This device provides multiple operational applications with **Access Point**, **Repeater** (**WDS**) and **Bridge** (**Infrastructure** and **Ad-hoc**) modes, which are mutually exclusive.

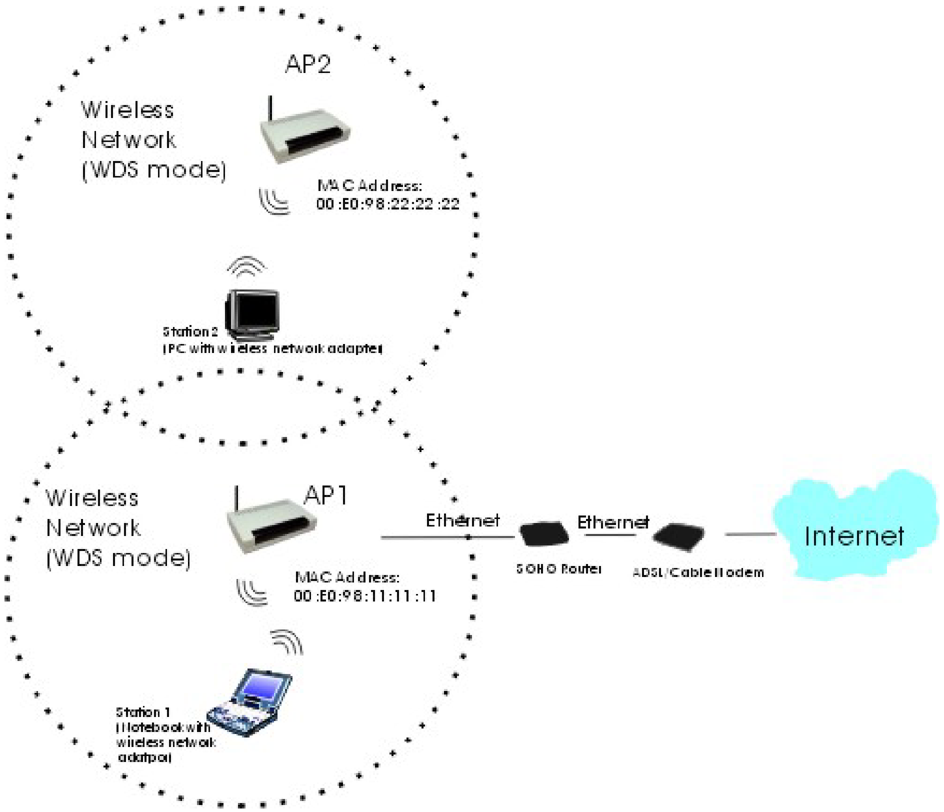
1. **Access Point**: When acting as an access point, this device connects all the wireless points (PCs) to a wired network. See the sample application below.

If you are currently in Bridge mode and want to change to Access Point, perform the **Firmware Upgrade** to upload the firmware from the included CD for Access Point mode. Refer to the section titled "Upgrade system firmware" for details.



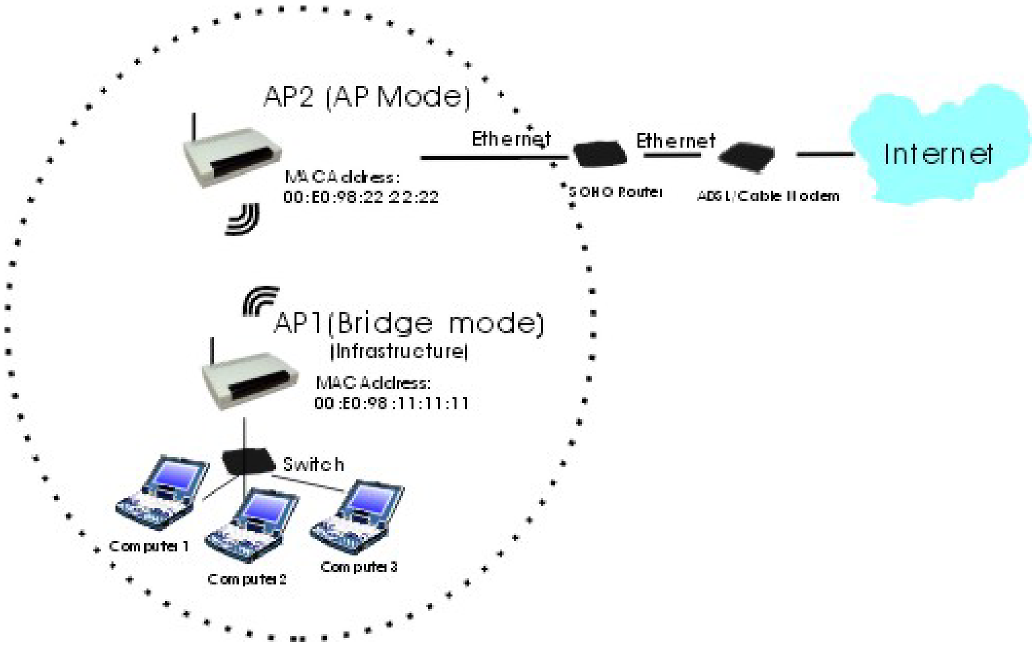
2. **Repeater (WDS)**: When in the **Repeater (WDS)** mode, AP1 (with Station 1 being associated to) and AP2 (with Station 2 being associated) can communicate with each other. Both Station 1 and Station 2 are able to access the Internet if only AP1 or AP2 has the Internet connection.

You can only enable WDS functionality when you are in the Access Point mode. Refer to the section titled **Repeater (WDS)** for more details to set up WDS.

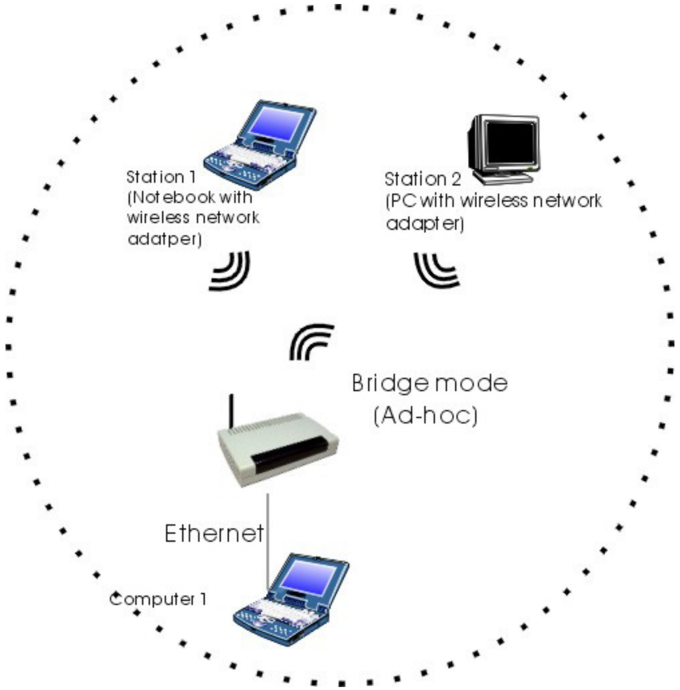


3. **Bridge (Infrastructure):** When acting as a Bridge, this device serves as a wireless client that connects wired stations (refer to the following illustration) to other access point(s). When becomes a wireless station (AP1 plus the connected computer 1, 2 and 3) can have the Internet access if the other Access Point (AP2) has the Internet connection.

If you are currently in Access Point mode and want to change to Bridge, perform the **Firmware Upgrade** to upload the firmware from the included CD for Access Point mode. Refer to the section titled “Upgrade system firmware” for details.



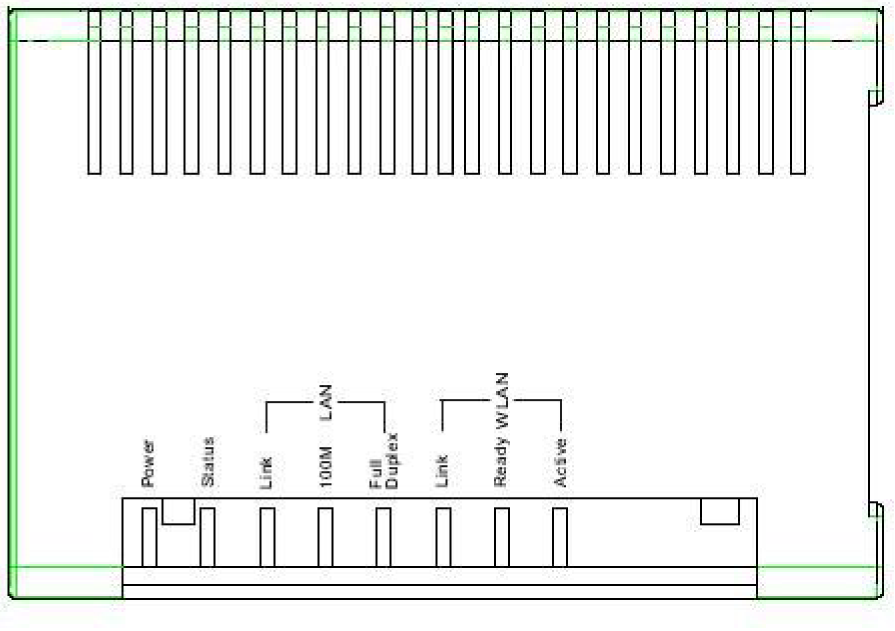
4. **Bridge (Ad-hoc):** When set to the **Bridge (Ad-hoc)** mode, this device can only work when connected to a computer, and will work like a wireless station. You can share files and printers between wireless stations (PC and laptop with wireless network adapter installed). The Bridge (Ad-hoc) mode is only for inter-LAN connection and will not communicate with any wired network.



This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can use the web-based utility provided by the manufacturer as described in the following sections.

LED Indicators

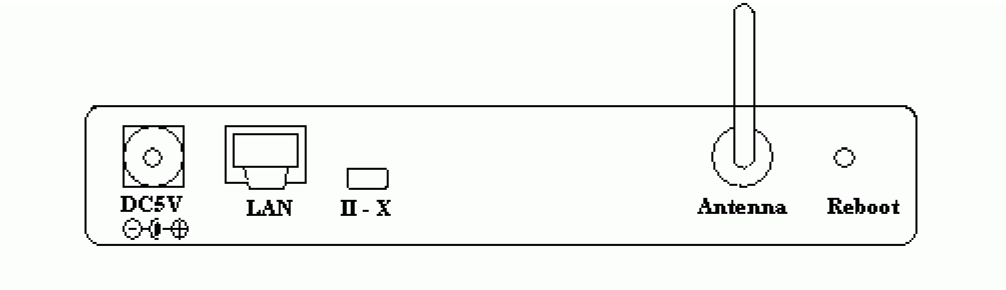
LED Indicators on the Front Panel



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	Dim for 10 Mbps Ethernet

	Ethernet connection.	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
A	***5V DC***	Connects the power adapter plug.
B	***LAN***	Connects to your LAN's network device.
C	***II-X***	Switch this button for choosing different wiring scheme LAN connection; **Switch left** to select using a straight Ethernet cable; **Switch right** to use a Crossover Ethernet cable. .
D	***Antenna***	Adjust to have better performance
E	***Reboot***	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. .

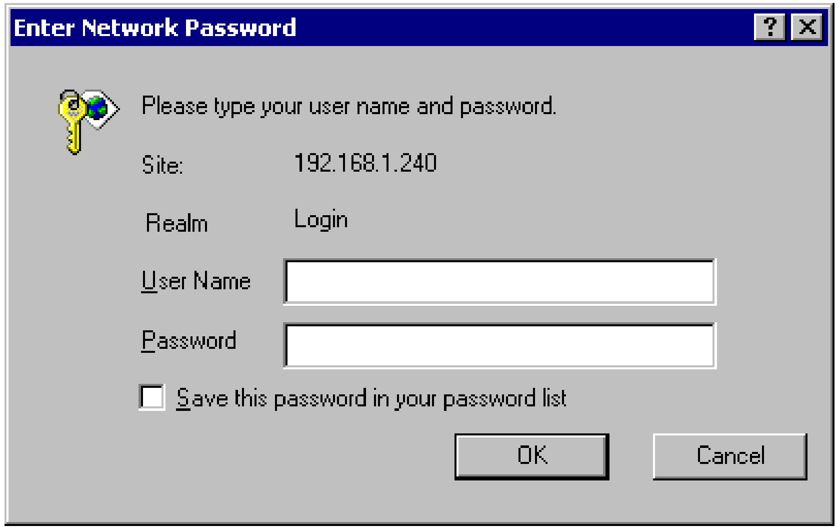
Getting Connected

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.*

WPA AP -Configuration via Web

Login

1. 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.
2. 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

Please type your user name and password.

Site: 192.168.1.240

Realm Login

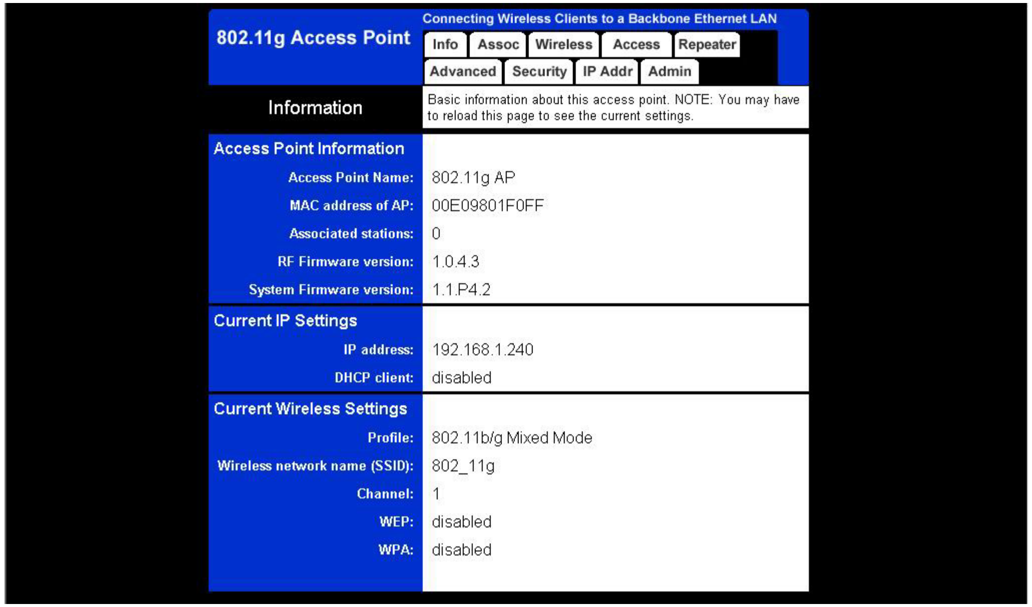
User Name

Password

□ Save this password in your password list

Info(Information)

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



Information

Basic information about this access point. NOTE: You may have to reload this page to see the current settings.

Access Point Information

Access Point Name:	802.11g AP
MAC address of AP:	00E09801F0FF
Associated stations:	0
RF Firmware version:	1.0.4.3
System Firmware version:	1.1.P4.2

Current IP Settings

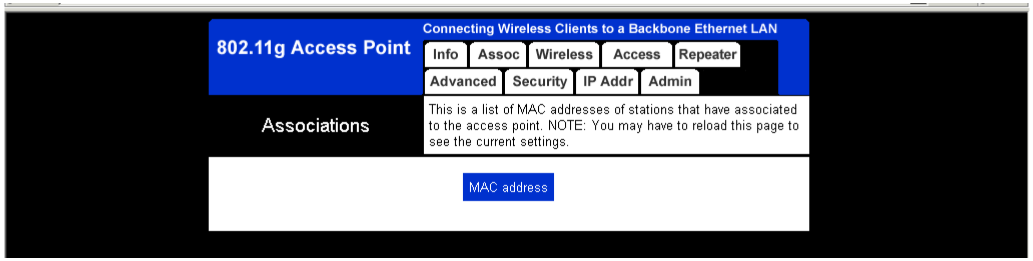
IP address:	192.168.1.240
DHCP client:	disabled

Current Wireless Settings

Profile:	802.11b/g Mixed Mode
Wireless network name (SSID):	802_11g
Channel:	1
WEP:	disabled
WPA:	disabled

Assoc(Associations)

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

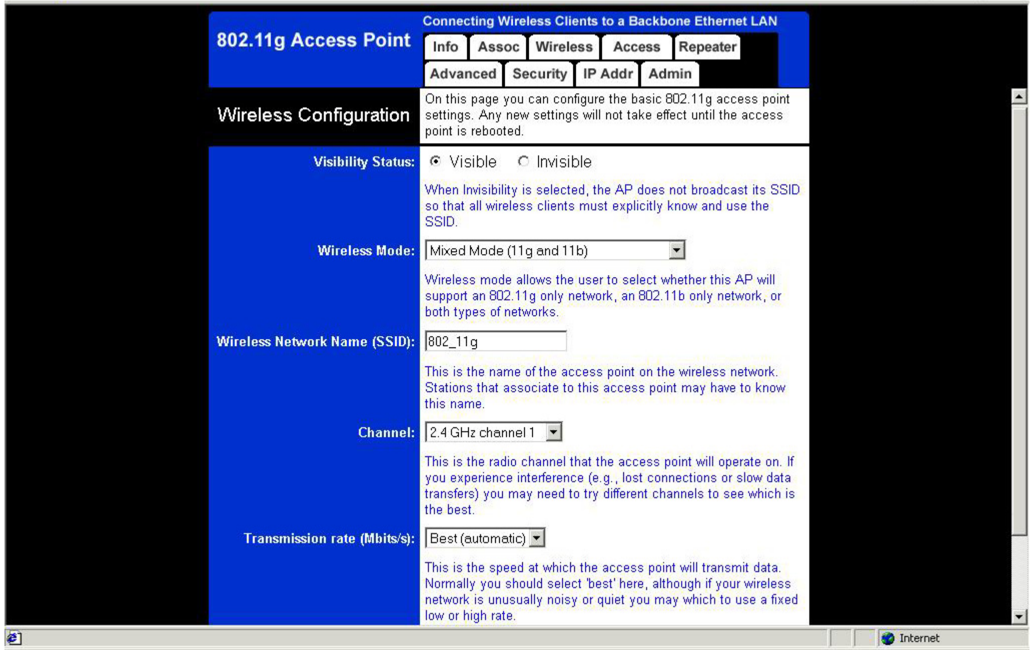


This is a list of MAC addresses of stations that have associated to the access point. NOTE: You may have to reload this page to see the current settings.

Wireless (Wireless Configuration)

Here you can set/change wireless configuration including **visibility status, Wireless Mode, 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.



Wireless Configuration

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

Visibility Status: ● Visible ○ Invisible

When Invisibility is selected, the AP does not broadcast its SSID so that all wireless clients must explicitly know and use the SSID.

Wireless Mode: Mixed Mode (11g and 11b)

Wireless mode allows the user to select whether this AP will support an 802.11g only network, an 802.11b only network, or both types of networks.

Wireless Network Name (SSID): 802_11g

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

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.

Transmission rate (Mbits/s): Best (automatic)

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 which to use a fixed low or high rate.

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.
Wireless Mode	You can select different wireless networking mode to meet your wireless environment or for optimal performance. You can choose from the list.

Wireless Network Name (SSID)	The **SSID** 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	Shows the selected channel that is currently in use. (There are **14** channels available, depending on the country.)
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.)

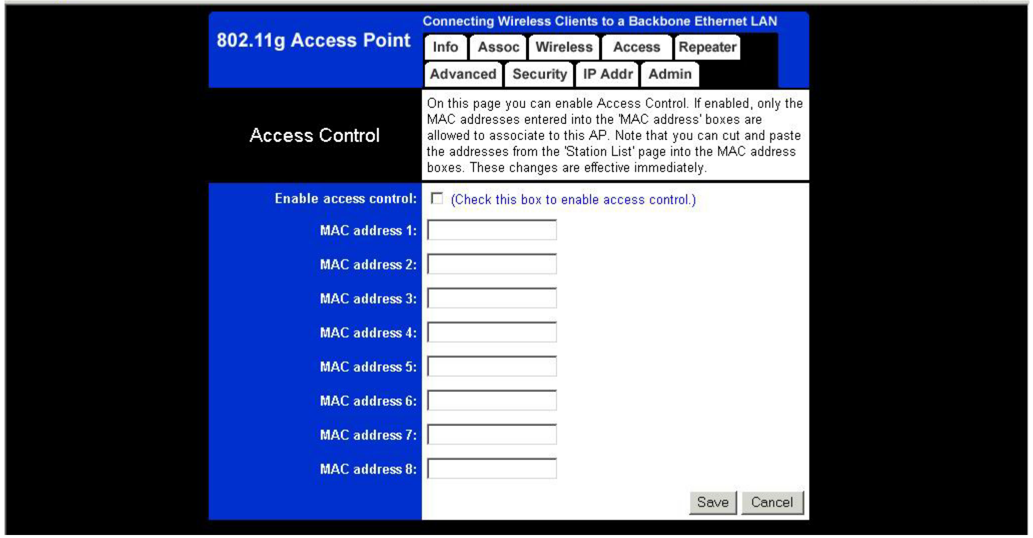
Access (Access Control)

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.



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.

Enable access control: □ (Check this box to enable access control.)

MAC address 1:

MAC address 2:

MAC address 3:

MAC address 4:

MAC address 5:

MAC address 6:

MAC address 7:

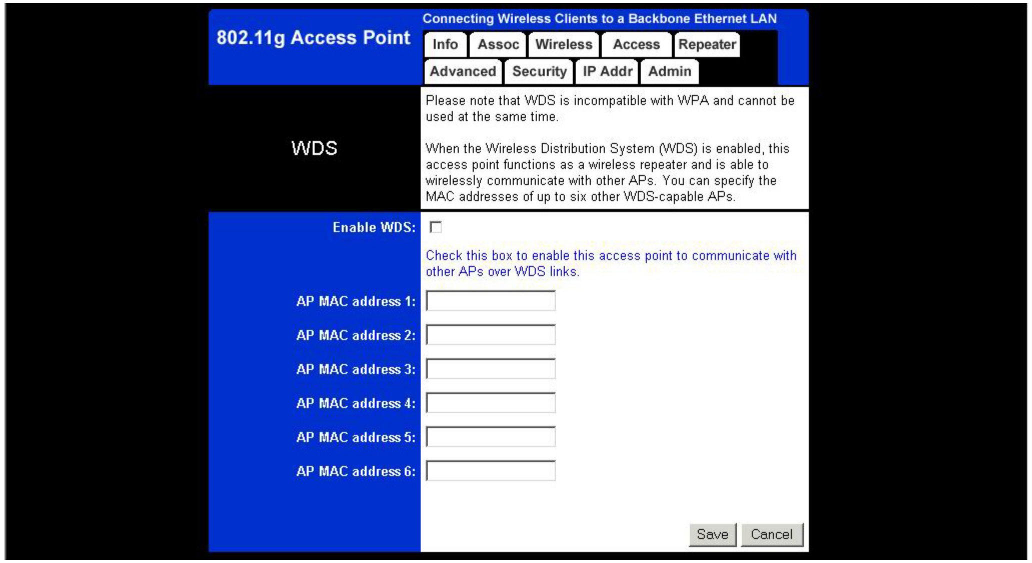
MAC address 8:

Figure: Access Control

Repeater (WDS)

The **Repeater (WDS**) functionality enables this AP to support wireless traffic to other WDS relay Access Points. The distance of wireless networking is thus extended for authenticated client devices that can roam from this Access Point to another.

This Access Point can support up to 6 other Access Points for WDS communication.



Please note that WDS is incompatible with WPA and cannot be used at the same time.

When the Wireless Distribution System (WDS) is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs. You can specify the MAC addresses of up to six other WDS-capable APs.

Enable WDS: □

Check this box to enable this access point to communicate with other APs over WDS links.

AP MAC address 1:

AP MAC address 2:

AP MAC address 3:

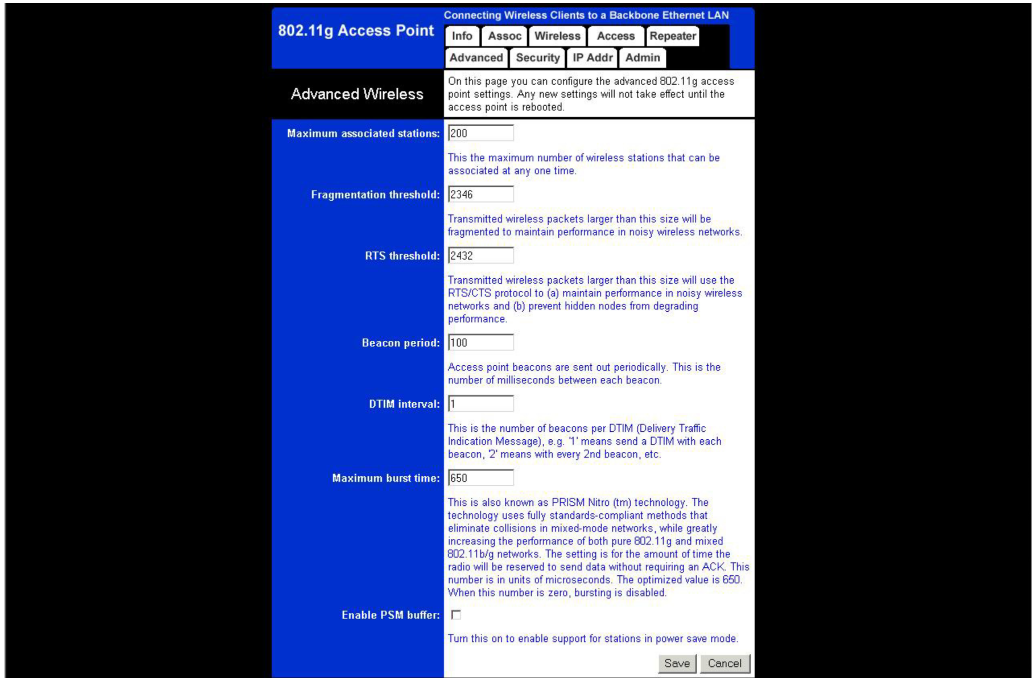
AP MAC address 4:

AP MAC address 5:

AP MAC address 6:

□ **Enable WDS**	Press the radio button to enable WDS.
AP MAC Address #	Enter the MAC Address for the new Access Point to participate the WDS with this Access Point. The MAC Address of this Access Point should be also added in other Access Points so that they can communicate. You can add up to 6 WDS Access points.
Save	Press to save the new settings on the screen.
Cancel	Press to discard the data you have entered since last time you press Save.

Advanced (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: 200

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

Fragmentation threshold: 2346

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

RTS threshold: 2432

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: 100

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

DTIM interval: 1

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 burst time: 650

This is also known as PRISM Nitro (tm) technology. The technology uses fully standards-compliant methods that eliminate collisions in mixed-mode networks, while greatly increasing the performance of both pure 802.11g and mixed 802.11b/g networks. The setting is for the amount of time the radio will be reserved to send data without requiring an ACK. This number is in units of microseconds. The optimized value is 650. When this number is zero, bursting is disabled.

Enable PSM buffer: □

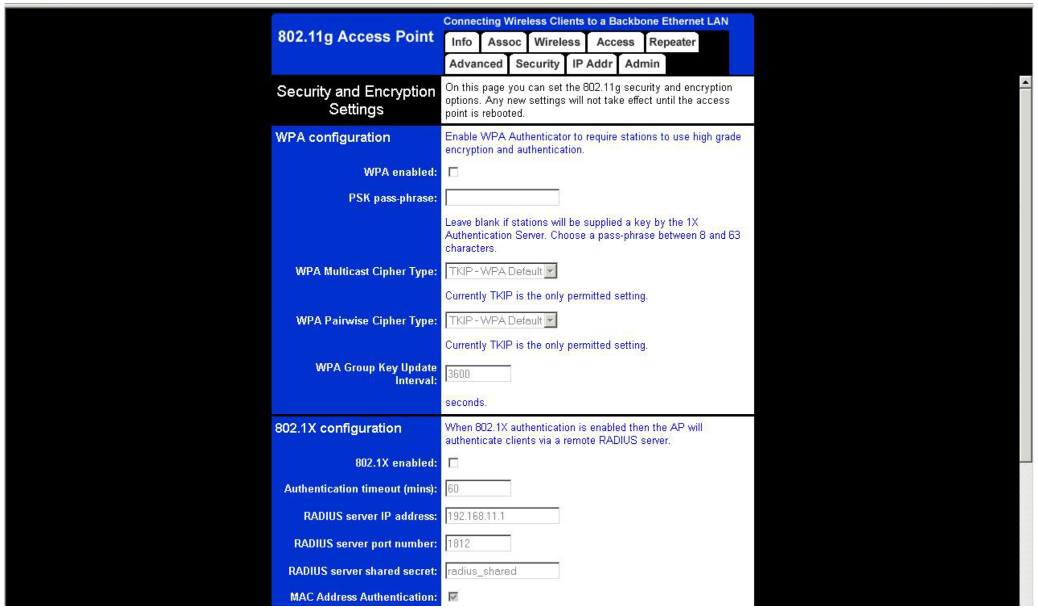
Turn this on to enable support for stations in power save mode.

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 **2346** 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 control frame sent from the transmitting station to the receiving station requesting permission to transmit. This value is recommended to

	remain at its default setting of **2432**. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Beacon period	This is also called **Beacon Interval**. 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 **Delivery Traffic Indication Message**. 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 650 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 configure the security of your wireless network. Selecting different method will enable you to have different level of security.



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 access point is rebooted.

WPA configuration

Enable WPA Authenticator to require stations to use high grade encryption and authentication.

WPA enabled: □

PSK pass-phrase:

Leave blank if stations will be supplied a key by the 1X Authentication Server. Choose a pass-phrase between 8 and 63 characters.

WPA Multicast Cipher Type: TKIP - WPA Default

Currently TKIP is the only permitted setting.

WPA Pairwise Cipher Type: TKIP - WPA Default

Currently TKIP is the only permitted setting.

WPA Group Key Update Interval: 3600 seconds.

802.1X configuration

When 802.1X authentication is enabled then the AP will authenticate clients via a remote RADIUS server.

802.1X enabled: □

Authentication timeout (mins): 60

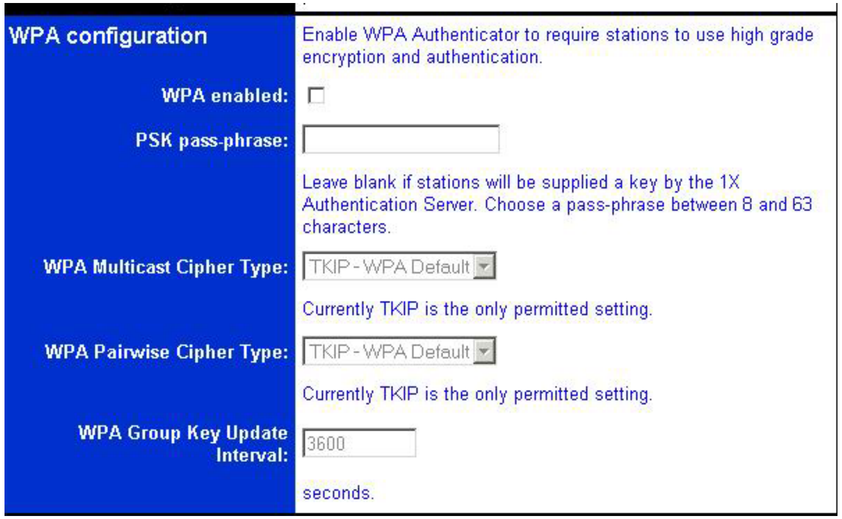
RADIUS server IP address: 192.168.11.1

RADIUS server port number: 1812

RADIUS server shared secret: radius_shared

MAC Address Authentication: ☑

WPA (Wi-Fi Protected Access) is the new wireless LAN security standard for 802.11 networks, which was developed to replace the existing standard WEP. **WPA** authorizes and identifies users based on a secret key that changes periodically.



WPA configuration

Enable WPA Authenticator to require stations to use high grade encryption and authentication.

WPA enabled: □

PSK pass-phrase:

Leave blank if stations will be supplied a key by the 1X Authentication Server. Choose a pass-phrase between 8 and 63 characters.

WPA Multicast Cipher Type: TKIP - WPA Default

Currently TKIP is the only permitted setting.

WPA Pairwise Cipher Type: TKIP - WPA Default

Currently TKIP is the only permitted setting.

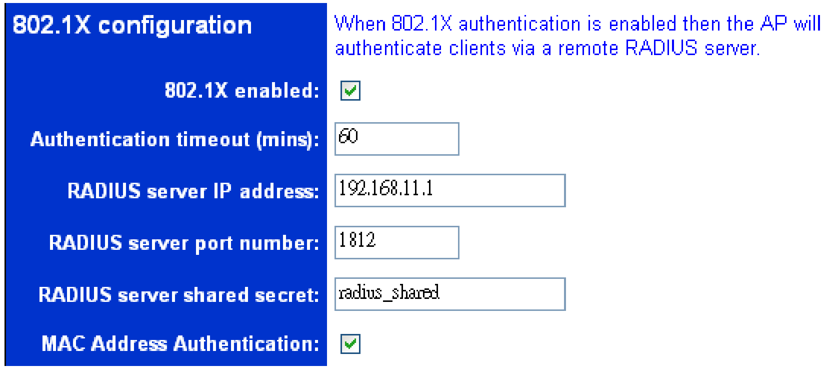
WPA Group Key Update Interval: 3600 seconds.

PSK pass-phrase	PSK stands for Pre-Shared-Key and serves as a password. User may key in a 8 to 63 characters string to set the password or leave it blank, in which the 802.1x Authentication will be activated. Note that if user key in own password, make sure to use the same password on client's end.
WPA Multicast Cipher Type	Select **TKIP - WPA Default**
WPA Pairwise Cipher Type	Select **TKIP - WPA Default**
WPA Group Key Update Interval	This shows the time period for the next key change. The default value is **3600 (seconds**). Users may set the values of

	their preference.

**Note that WPA Multicast Cipher Type & WPA Pairwise Cipher Type are the same.*

802.1x Authentication in conjunction with the RADIUS SERVER verifies the identity of would be clients.



802.1X configuration

When 802.1X authentication is enabled then the AP will authenticate clients via a remote RADIUS server.

802.1X enabled: ☑

Authentication timeout (mins): 60

RADIUS server IP address: 192.168.11.1

RADIUS server port number: 1812

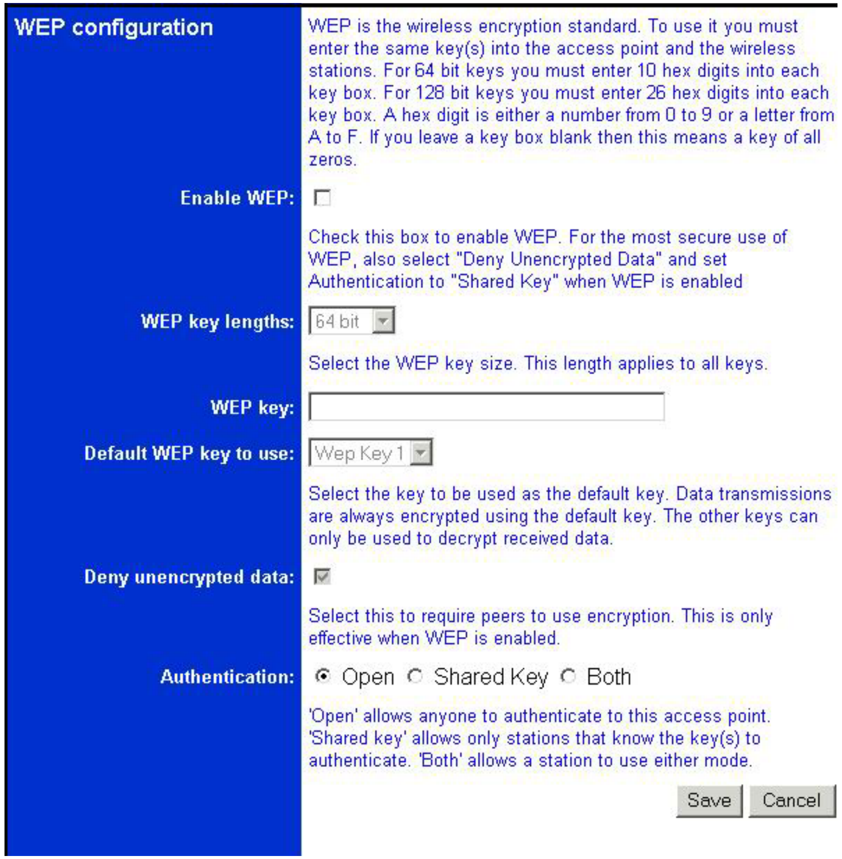
RADIUS server shared secret: radius_shared

MAC Address Authentication: ☑

Authentication timeout (mins)	The default value is **60** (minutes). When the time expires, the device will re-authenticate with RADIUS server.
RADIUS server IP address	Enter the RADIUS server IP.
RADIUS server port number	Port used for RADIUS, the number of ports must be the same as the RADIUS server , normally the port is **1812**
RADIUS server shared secret	When registered with a RADIUS server, a **password** will be assigned. This would be

secret	the RADIUS server shared secret.
MAC Address Authentication	Use client mac address for authentication with RAIDUS server

WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64-bit/128-bit shared key algorithm. WEP encryption scrambles the communication between your access points and client devices to keep the communication private. However, if an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network.



WEP configuration

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. 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

WEP key lengths: 64 bit

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

WEP key:

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 ○ Both

'Open' allows anyone to authenticate to this access point. 'Shared key' allows only stations that know the key(s) to authenticate. 'Both' allows a station to use either mode.

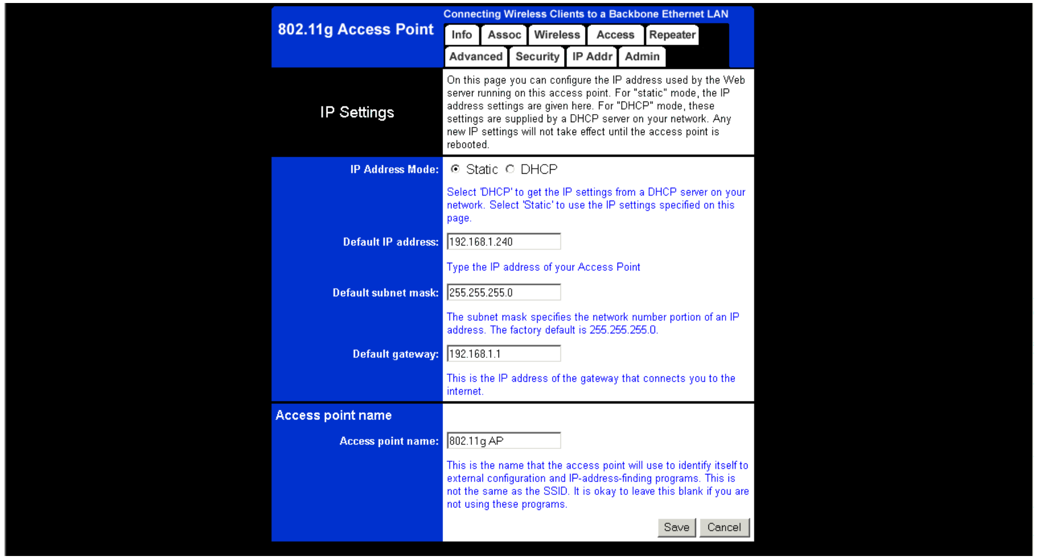
Enable WEP	WEP (Wired Equivalent Privacy) encryption can be used to ensure the security of your wireless network. The window allows you to set to **64bit** or **128bit** Encryption (WEP) by using either **Passphrase** or **Manual Entry** methods. ***Note***: To allow Decryption and communication, all 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 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	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 **Open**, **Shared Authentication**, and **Both**. If the access point is using "**Open Authentication**", then the wireless adapter will need to be set to the same authentication mode. **Shared Authentication** is when both the sender and the recipient share a secret key. Select **Both** for the network adapter to select the Authentication mode automatically depending on the access point Authentication mode.

IP Addr (IP Address Settings)

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, you select **Static**, you will have to manually set the device IP address.



On this page you can configure the IP address used by the Web server running on this access point. For "static" mode, the IP address settings are given here. For "DHCP" mode, these settings are supplied by a DHCP server on your network. Any new IP settings will not take effect until the access point is rebooted.

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: 192.168.1.240

Type the IP address of your Access Point

Default subnet mask: 255.255.255.0

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

Default gateway: 192.168.1.1

This is the IP address of the gateway that connects you to the internet.

Access point name

Access point name: 802.11g AP

This is the name that the access point 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.

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:

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.

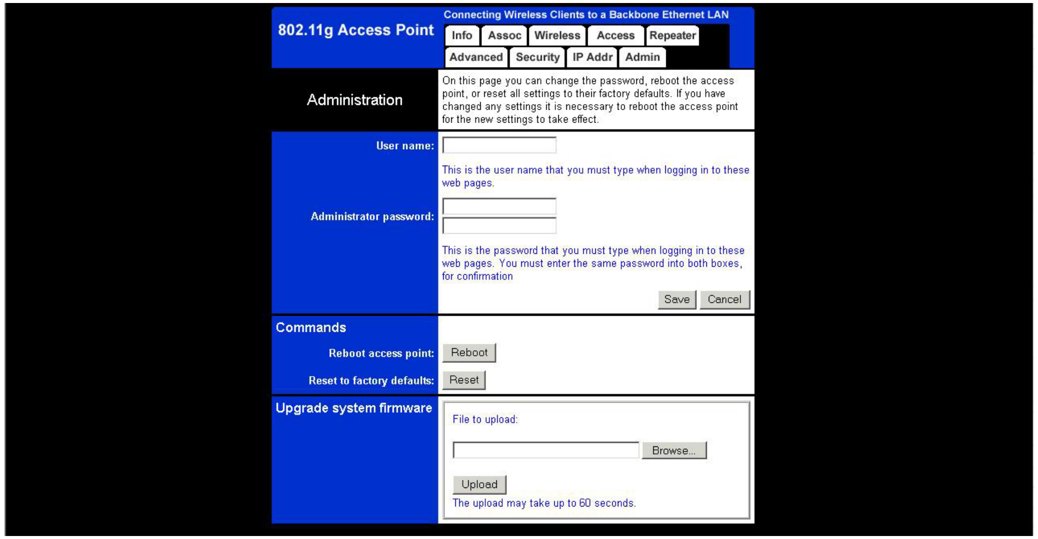
Reboot/Reset this device**.**

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

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 press the Reset button so that the new settings can take effect.



Administration

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.

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 access point:

Reset to factory defaults:

Upgrade system firmware

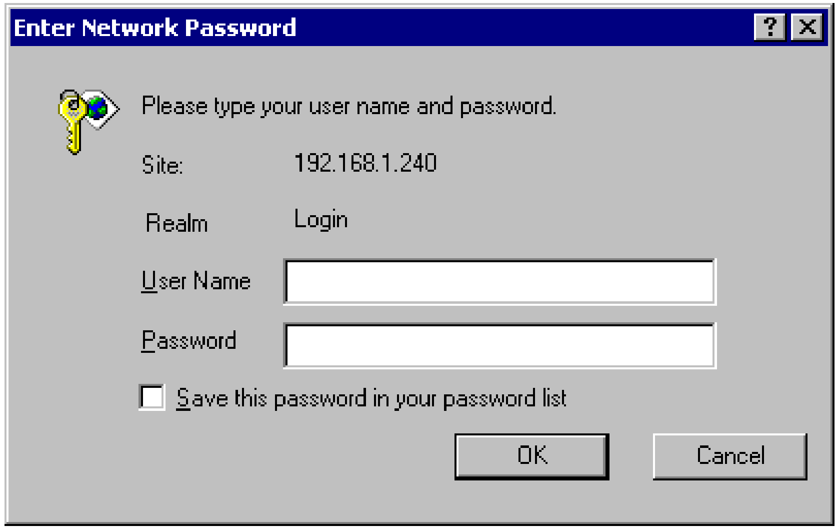
File to upload:

The upload may take up to 60 seconds.

Bridge -Configuration via Web

Login

3. 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.
4. 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

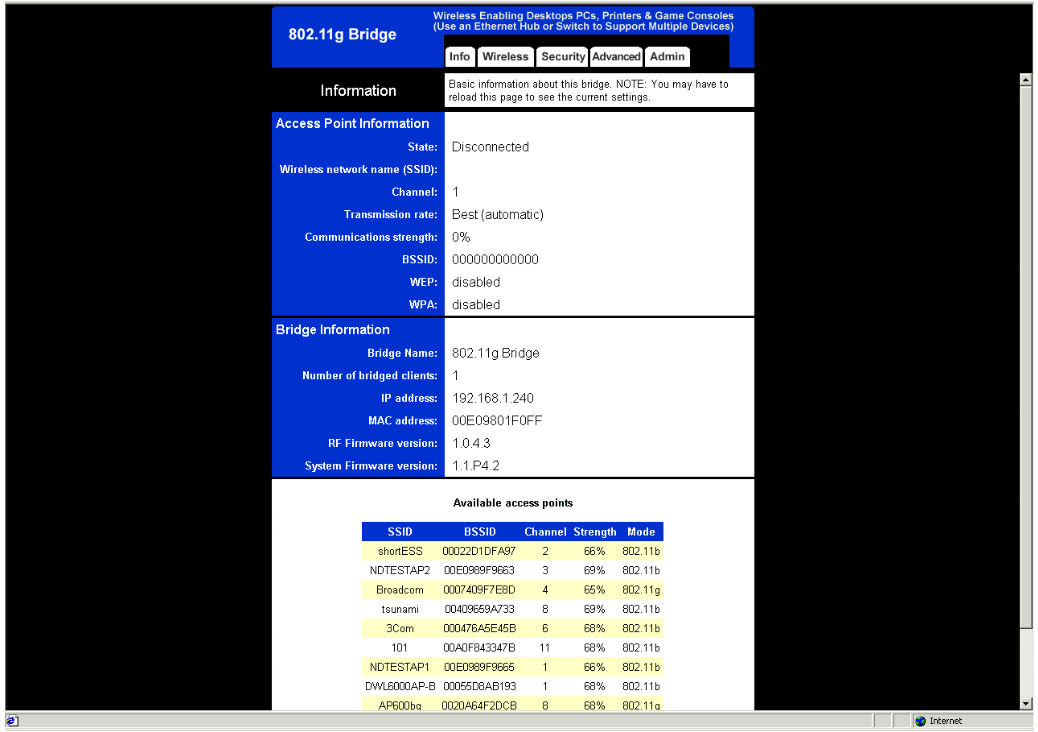
Please type your user name and password.

Site: 192.168.1.240

Realm Login

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)

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:	1
Transmission rate:	Best (automatic)
Communications strength:	0%
BSSID:	000000000000
WEP:	disabled
WPA:	disabled

Bridge Information	
Bridge Name:	802.11g Bridge
Number of bridged clients:	1
IP address:	192.168.1.240
MAC address:	00E09801F0FF
RF Firmware version:	1.0.4.3
System Firmware version:	1.1.P4.2

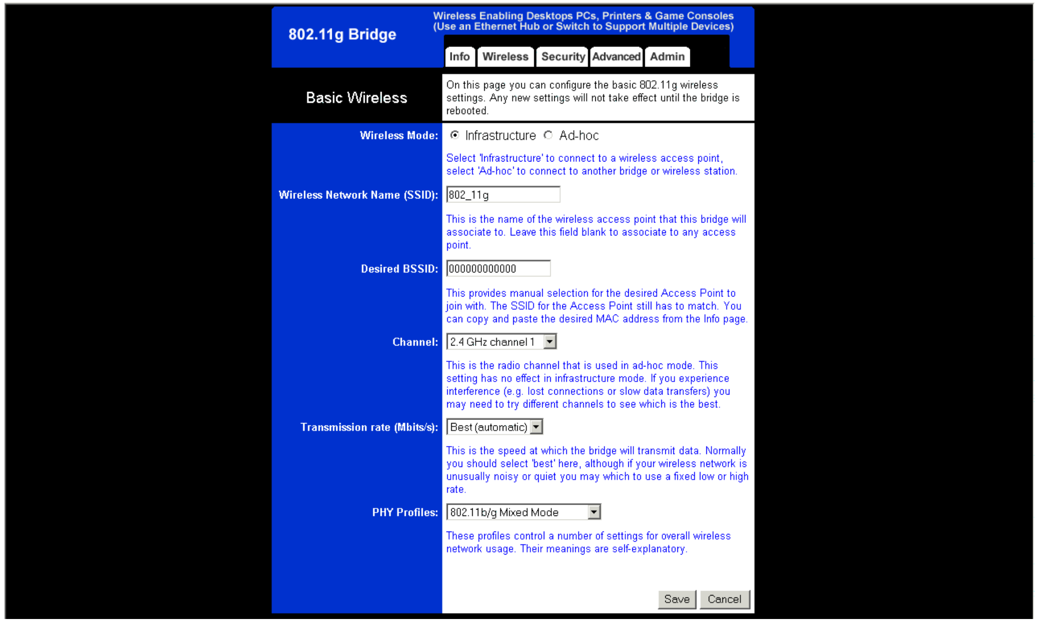
Available access points

SSID	BSSID	Channel	Strength	Mode
shortESS	00022D1DFA97	2	66%	802.11b
NDTESTAP2	00E0989F9663	3	69%	802.11b
Broadcom	0007409F7E8D	4	65%	802.11g
tsunami	00409659A733	8	69%	802.11b
3Com	000476A5E45B	6	68%	802.11b
101	00A0F843347B	11	68%	802.11b
NDTESTAP1	00E0989F9665	1	66%	802.11b
DWL6000AP-B	00055D8AB193	1	68%	802.11b
AP600bq	0020A64F2DCB	8	68%	802.11q

Wireless (Wireless Configuration)

Here you can set/change wireless configuration including **Wireless Mode, Wireless Mode, SSID, BSSID, channel, transmission rate, and PHY profiles**. 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.


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
Save
Cancel

Basic Wireless

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

Wireless Mode: ● Infrastructure ○ Ad-hoc

Select 'Infrastructure' to connect to a wireless access point, select 'Ad-hoc' to connect to another bridge or wireless station.

Wireless Network Name (SSID): 802_11g

This is the name of the wireless access point that this bridge will associate to. Leave this field blank to associate to any access point.

Desired BSSID: 000000000000

This provides manual selection for the desired Access Point to join with. The SSID for the Access Point still has to match. You can copy and paste the desired MAC address from the Info page.

Channel: 2.4 GHz channel 1

This is the radio channel that is used in ad-hoc mode. This setting has no effect in infrastructure mode. 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.

Transmission rate (Mbits/s): Best (automatic)

This is the speed at which the bridge will transmit data. Normally you should select 'best' here, although if your wireless network is unusually noisy or quiet you may which to use a fixed low or high rate.

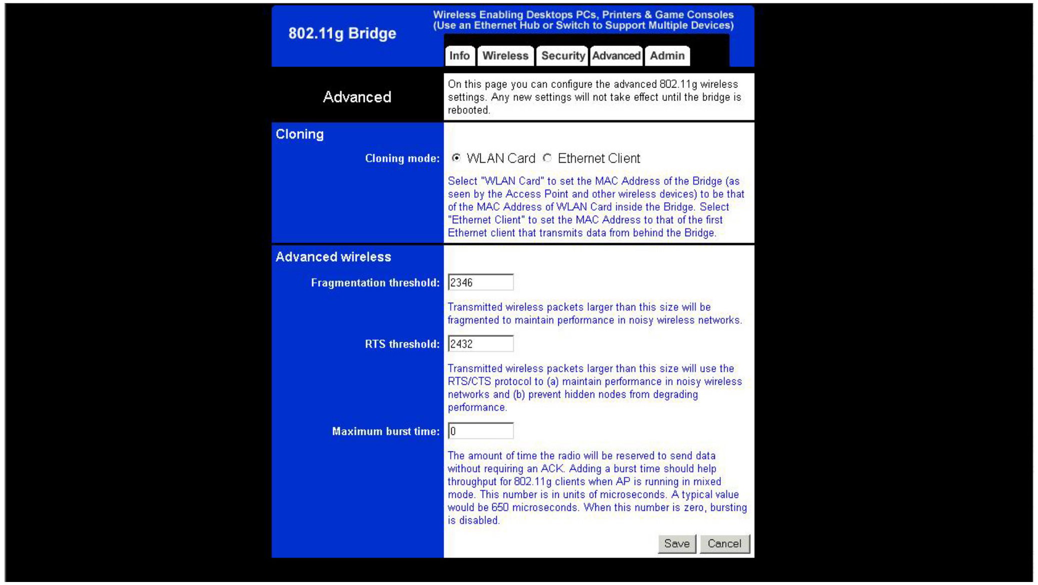
PHY Profiles: 802.11b/g Mixed Mode

These profiles control a number of settings for overall wireless network usage. Their meanings are self-explanatory.

Wireless Mode	Select “**Infrastructure**” to connect to a wireless access point, select “**Ad-hoc**” to connect to another bridge or wireless station.
Wireless Network Name (SSID)	The **SSID** 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.

Desired BSSID	The BSSID displays the ID of current BSS, which uniquely identifies each BSS. You copy the MAC address from the Info page and paste it directly to this field as BSSID.
Channel	Shows the selected channel that is currently in use. (There are **14** channels available, depending on the country.)
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	You can select different wireless networking mode to meet your wireless environment or for optimal performance. You can choose from the list.

Advanced (Advanced Wireless)



802.11g Bridge

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

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: 2346

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

RTS threshold: 2432

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: 0

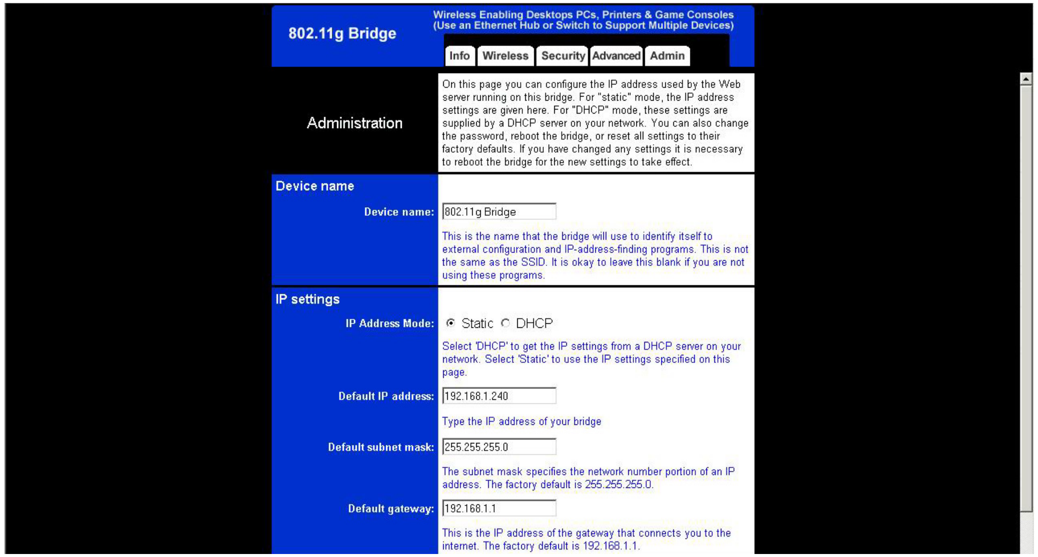
The amount of time the radio will be reserved to send data without requiring an ACK. Adding a burst time should help throughput for 802.11g clients when AP is running in mixed mode. This number is in units of microseconds. A typical value would be 650 microseconds. When this number is zero, bursting is disabled.

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 **2346** 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 control frame sent from the transmitting station to the receiving station requesting permission to transmit. This value is recommended to remain at its default setting of **2432**. Should you encounter inconsistent data flow,

	only minor modifications of this value are recommended.
Beacon period	This is also called **Beacon Interval**. 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 **Delivery Traffic Indication Message**. 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 650 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.

Admin (Administration)

In this Administration page, you can set:



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

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: 192.168.1.240

Type the IP address of your bridge

Default subnet mask: 255.255.255.0

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

Default gateway: 192.168.1.1

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

Device Name

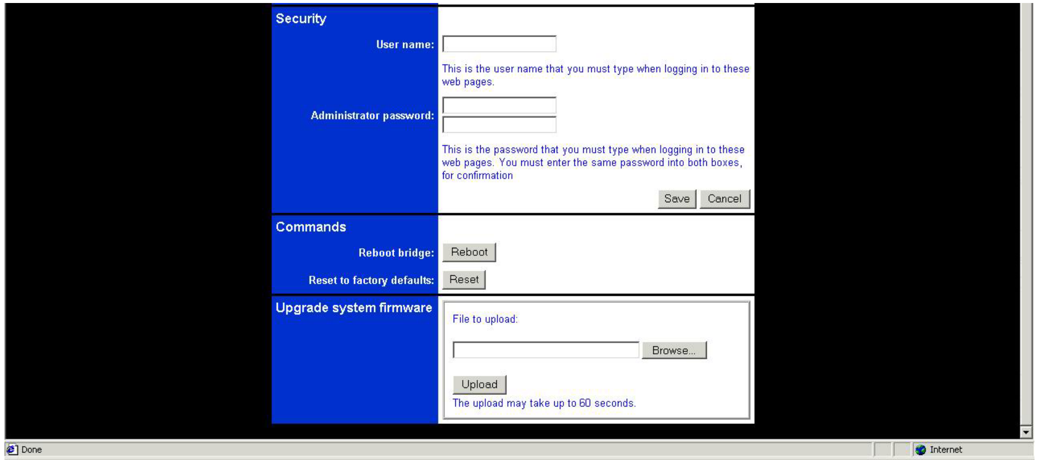
You can name this access point for identification. You can leave it blank without entering anything. However, the name for the access point will be useful for identification especially when there are more than on access points in your wireless network.

IP Settings

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

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.


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.

Security/ 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.

Commands: 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

1. You will have to download the file to your computer.

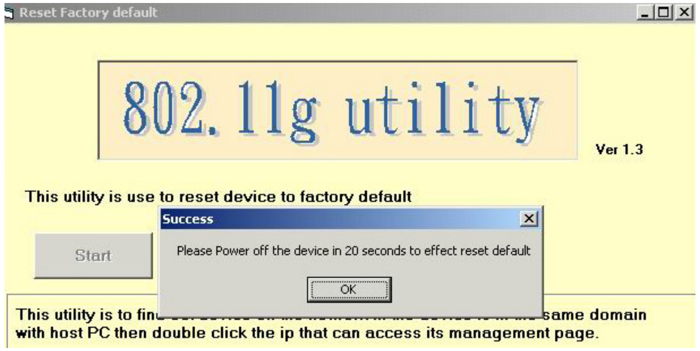
2. Enter the file name and path in the field next to the Browse button. Or you can click Browse to find the file you previously downloaded.
3. Click the **Upload** button to start upgrading. Wait for about 1 minute for the upgrade.
4. When the firmware upgrade is complete, remember to press the Reset button so that the new settings can take effect.

Reset to the Factory Defaults

In the case that you forgotten your password and could not access the device, you can use the provided Utility to reset to factory defaults. Or if you forgotten the IP address of this device and could not access it for configuration, you can locate this device in your network and find its IP address to configure it.

Reset

1. Open the provided CD-ROM\utility.
2. Double-click setdefault.
3. When the utility screen appears, click **Start**
4. Click **OK** and power off this device within **20** seconds for the device to reset to factory defaults. If there’s a delay, and this device is not powered off in 20 seconds, this action will be automatically cancelled.



Reset Factory default

802.11g utility

Ver 1.3

This utility is use to reset device to factory default

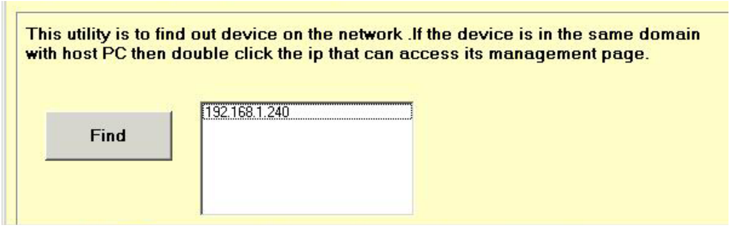
Success

Please Power off the device in 20 seconds to effect reset default

This utility is to fin… same domain with host PC then double click the ip that can access its management page.

Find

Click **Find** and you will be prompted the **login** screen. If user name and password have been previously assigned, however, it is still required that you enter them to enter the management page.



This utility is to find out device on the network .If the device is in the same domain with host PC then double click the ip that can access its management page.

檔名:	AP900mnl
目錄:	\\Nas\rd-2\Eleen\Sharing\Manual\English\Wireless\AccessPoint\AP900\MNL+QIG
範本:	C:\Documents and Settings\brenda\Application Data\Microsoft\Templates\Normal.dot
標題:	
主旨:	
作者:	Brook Lu
關鍵字:	
註解:	
建檔日期:	2003/11/26 下午 07:11
修訂版編號:	38
前次更新日期:	2003/12/3 下午 07:30
前次存檔人員:	writer
編修總時間:	1,872 分鐘
最後列印在:	2003/12/3 下午 07:31
最後列印的字數	
頁數:	41
字數:	3,844 (約)
字元數:	21,911 (約)