Wireless Multi-Client Bridge / Access Point

User’s Manual

Version: 1.1

Table of Contents

Table of Contents

Revision History

Version	Date	Notes
1.0	September 15, 2003	Initial Version
1.1	October 1, 2003	Updated GUI

1 Introduction

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

1.1 Features & Benefits

Features	Benefits
High RF Output Power	More coverage of regular Multi-Client Bridge.
IEEE 802.11b/g Compliant Point-to-point, Point-to-multipoint Wireless Connectivity	Fully Interoperable with IEEE 802.11b/ IEEE802.11g compliant. Allows users to transfer data between multiple buildings.
Plug and Play	No driver needed, quickly and easily connects your Ethernet device to Wireless.
Power-over-Ethernet	Flexible Access Point locations and cost savings.
64 /128-bit WEP data encryption	Powerful data security.
Hide SSID (AP Mode)	Avoids unauthorized users from sharing the bandwidth and increases efficiency of the network.
DHCP Client/ Server	Simplifies network administration.
WDS (Wireless Distribution System)	Configures wireless AP and Bridge mode simultaneously as a wireless repeater.
MAC address filtering (AP Mode)	Ensures secure network connections.
Seamless Roaming	Allows users to roam between APs without losing their network connection.

1.2 Package Contents

- One Client Bridge/Access Point/Repeater
- One Power Adapter
- One CAT 5 UTP Cable
- One Fast Start Guide
- One CD-ROM with User’s Manual Included

1.3 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.

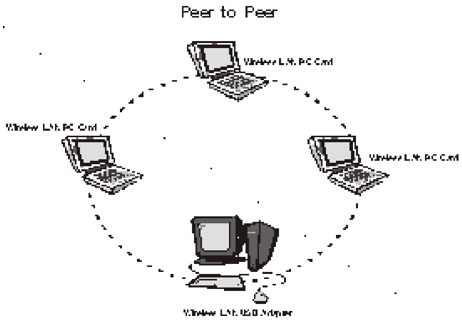
1.4 Network Configuration

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 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.
c) Wireless routing and IP sharing.

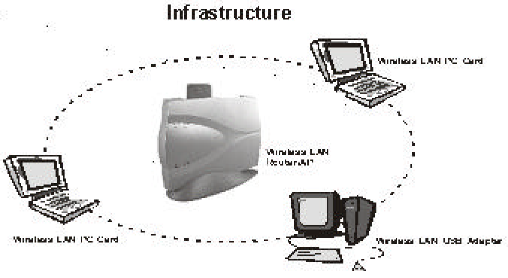
a) Ad-Hoc (peer-to-peer) Mode

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.

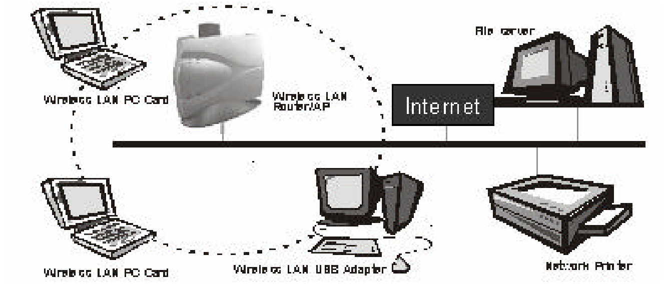


b) Infrastructure Mode

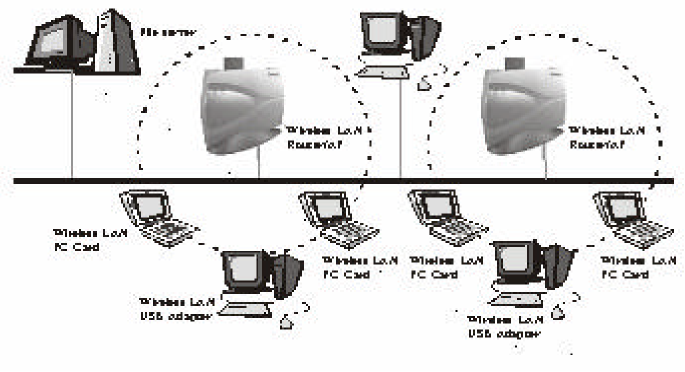
The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn' t matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless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



Extended-range independent WLAN using an AP as a repeater; if wired to an Ethernet network as shown below, the AP serves as a Bridge and provides the link between the server and the wireless clients. The wireless clients can move freely throughout the coverage area of the AP while remaining connected to the server. Since the AP is connected to the wired network, each client would have access to the server's resources as well other clients.

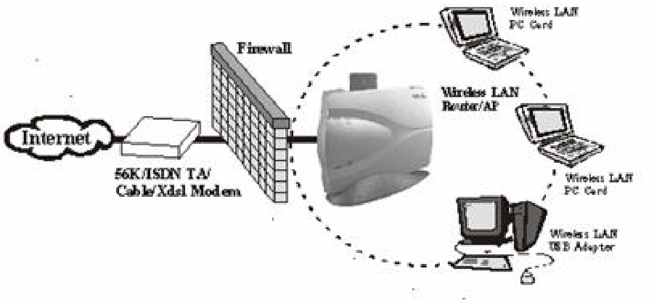


Access points have a finite range, on the order of 50 meters indoor and 100 meters outdoors. In a very large facility such as an enterprise, a warehouse, or on a college campus, it will probably be necessary to install more than one access point to cover an entire building or campus, as shown in the image below. In this scenario, access points hand the client off from one to another in a way that is invisible to the client, ensuring their connectivity. Wireless clients can roam seamlessly between different coverage areas and remain connected to the network.



c) Wireless routing and IP sharing

In infrastructure mode, in addition to acting as a Bridge between an Ethernet and wireless network, the AP can be configured as a wireless router and IP sharing device for Internet access as shown below. You don' t need to buy an expensive router. Nor do you need to buy several modems and set up phone lines. Just share one AP, one modem, a single dial-up account, and one phone line; dozens of network users can surf the Internet simultaneously.



2 Understanding the Hardware

2.1 Hardware Configuration

- **RJ-45 Ethernet Connector –** Provides 10/100 Mbps connectivity to a wired Ethernet LAN.
- **Reset Button –** By holding this down for more than five seconds, the AP will reset to its factory default settings.
- **Power Supply Connector –** Connects to the power adapter.

2.2 Hardware Installation

A. Configure your notebook or PC with a wireless LAN card.
B. For a wired LAN, connect your PC' s Ethernet port to the AP' s LAN port via an Ethernet cable.
C. For WLAN, position the Access Point in a proper location.
D. Plug in the power cord into the power outlet.

2.3 Default IP address

This device can be configured as a Bridge or an Access Point. By default, this device is configured as a Bridge, and the default IP address in Bridge mode is: **192.168.1.1**. The default IP address for Access Point mode is: **192.168.1.2**.

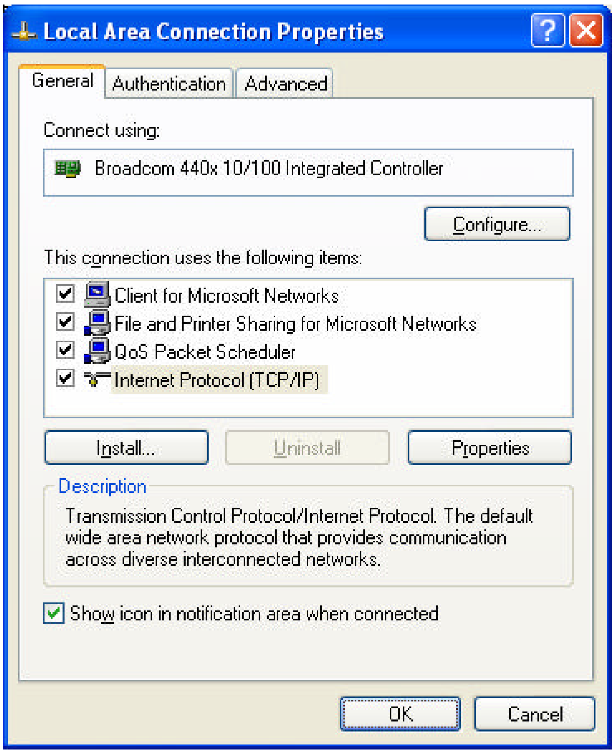
In order to switch between Bridge and Access Point modes refer to **Chapter 4 – Switch Between Bridge & Access Point**.

3 PC Configuration

3.1 TCP/IP Configuration

Follow the steps below in order to configure the TCP/IP settings of your PC.

A. 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.



Local Area Connection Properties

Connect using:

Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

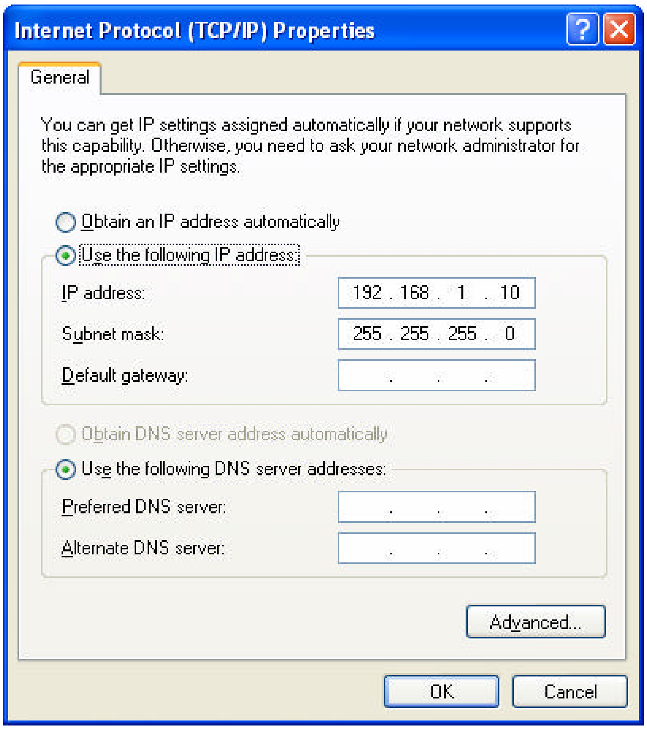
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

B. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the IP address of your PC. You will then see the following screen.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

C. Select **Use the following IP address** radio button, and then enter an IP address and subnet mask for your PC. Make sure that the device and your PC are on the same subnet.

D. Click on the **OK** button, your PC's TCP/IP settings have been configured.

4 Switch Between Bridge & Access Point

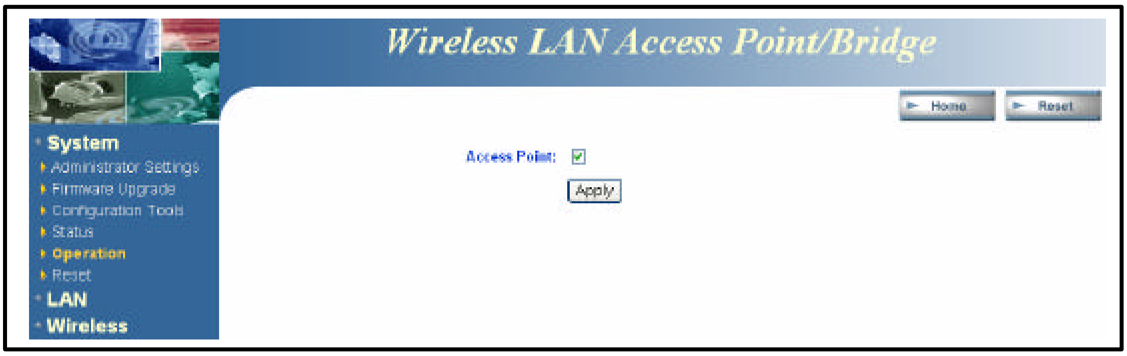
This device can be configured as a Bridge or an Access Point. By default, this device is configured as a Bridge, and the default IP address in Bridge mode is: **192.168.1.1**. The default IP address for Access Point mode is: **192.168.1.2**.

This chapter will describe the steps to switch from Bridge to Access Point, and Access Point to Bridge.

4.1 Bridge to Access Point

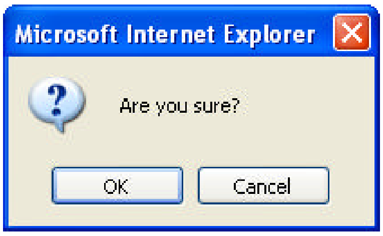
a. Enter the default IP address of the Bridge into the address bar of the web-browser (**192.168.1.1**). Leave the **user name** and **password** fields blank, and click on the **OK** button.

b. After you have logged into the Bridge, click on the **System** link on the navigation bar, and then click on the **Operation** link under it, as the image depicts below.



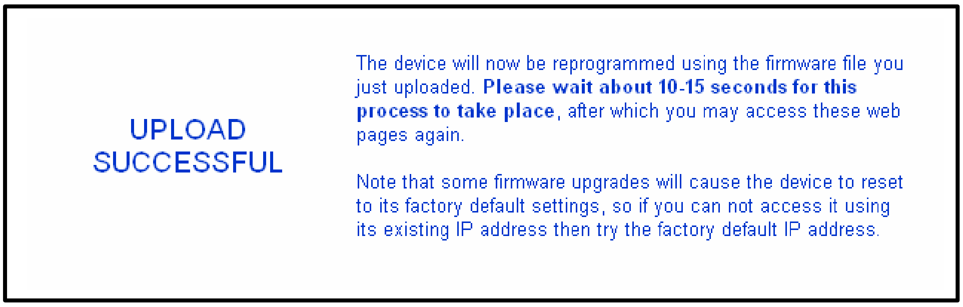
Access Point: ☑

c. Place a check in the **Access Point** check box, and then click on the **Apply** button. A message box will then appear asking you to confirm the switch.



Are you sure?

d. Click on the **OK** button to continue. You will then see the following page.



UPLOAD SUCCESSFUL

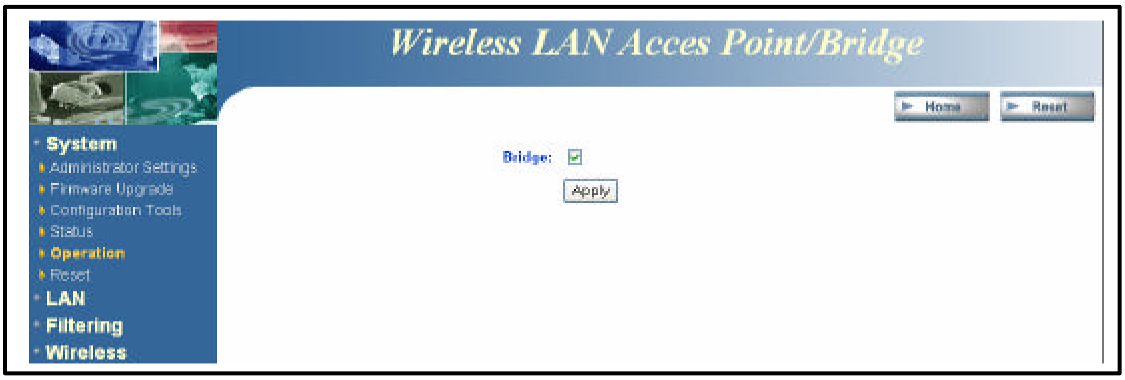
The device will now be reprogrammed using the firmware file you just uploaded. **Please wait about 10-15 seconds for this process to take place**, after which you may access these web pages again.

Note that some firmware upgrades will cause the device to reset to its factory default settings, so if you can not access it using its existing IP address then try the factory default IP address.

e. This message indicates that the firmware has now changed to **Access Point** mode. After about 15 seconds you can re-launch you web-browser to the IP address of the Access Point (**192.168.1.2**)

4.2 Access Point to Bridge

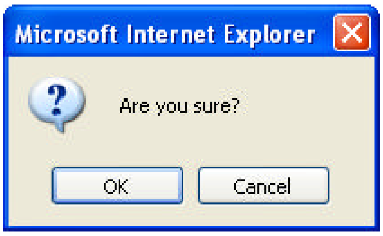
a. Enter the default IP address of the Access Point into the address bar of the web-browser (**192.168.1.2**). Leave the **user name** and **password** fields blank, and click on the **OK** button.
b. After you have logged into the Access Point, click on the **System** link on the navigation bar, and then click on the **Operation** link under it, as the image depicts below.



Bridge: ☑

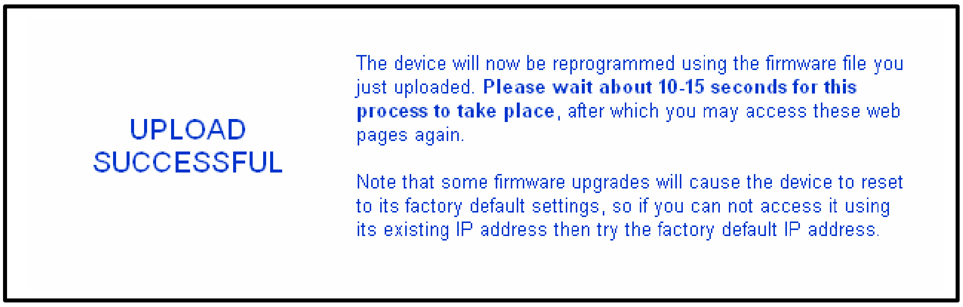
Apply

c. Place a check in the **Bridge** check box, and then click on the **Apply** button. A message box will then appear asking you to confirm the switch.



Are you sure?

d. Click on the **OK** button to continue. You will then see the following page.



UPLOAD SUCCESSFUL

The device will now be reprogrammed using the firmware file you just uploaded. **Please wait about 10-15 seconds for this process to take place**, after which you may access these web pages again.

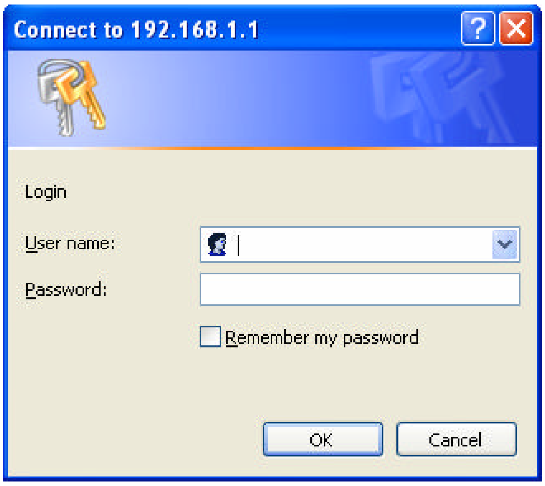
Note that some firmware upgrades will cause the device to reset to its factory default settings, so if you can not access it using its existing IP address then try the factory default IP address.

e. This message indicates that the firmware has now changed to **Bridge** mode. After about 15 seconds you can re-launch you web-browser to the IP address of the Access Point (**192.168.1.1**)

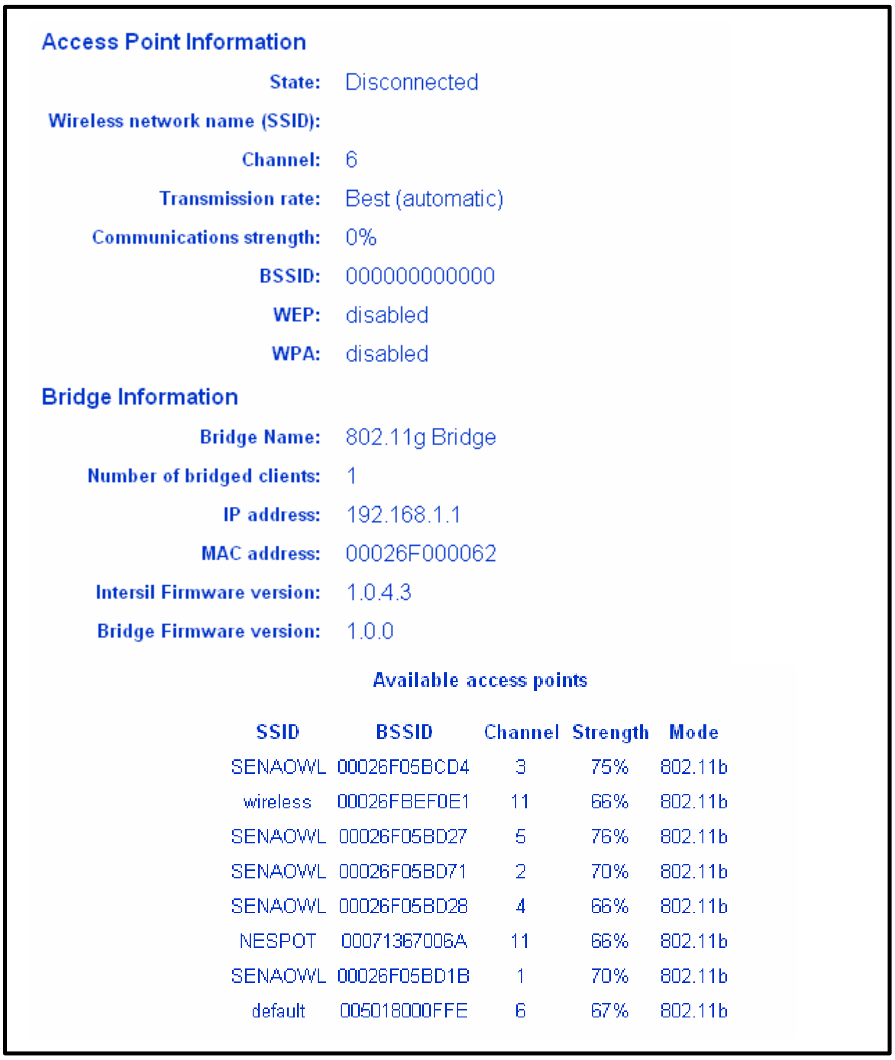
5 Bridge Mode – Web Configuration

5.1 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 on the same subnet. Refer to **Chapter 3** in order to configure the IP address of your computer.
- You will then see the login window. Leave the **User name** and **Password** fields blank and click on the **OK** button.



- You can change the username and password under the **Administrator Settings** option. Refer to section **5.2.1 Administrator Settings** to change the username and password.
- After logging in, you will see the Graphical User Interface (GUI) of the Bridge. The configuration is divided into three major parts: **System, LAN,** and **Wireless**. Each one is described in detail in the next few sections.
- The **Status** page is the first page that is displayed, this page displays the settings of the Bridge, the IP addresses, and the Wireless settings. To understand more about the **Status** page, refer to section **5.2.4 Status**.



Access Point Information

State:	Disconnected
Wireless network name (SSID):	
Channel:	6
Transmission rate:	Best (automatic)
Communications strength:	0%
BSSID:	000000000000
WEP:	disabled
WPA:	disabled

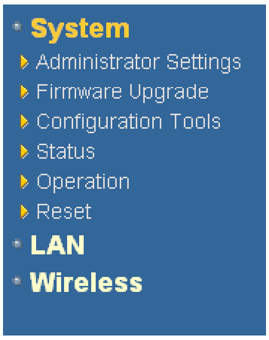
Bridge Information

Bridge Name:	802.11g Bridge
Number of bridged clients:	1
IP address:	192.168.1.1
MAC address:	00026F000062
Intersil Firmware version:	1.0.4.3
Bridge Firmware version:	1.0.0

Available access points

SSID	BSSID	Channel	Strength	Mode
SENAOWL	00026F05BCD4	3	75%	802.11b
wireless	00026FBEF0E1	11	66%	802.11b
SENAOWL	00026F05BD27	5	76%	802.11b
SENAOWL	00026F05BD71	2	70%	802.11b
SENAOWL	00026F05BD28	4	66%	802.11b
NESPOT	00071367006A	11	66%	802.11b
SENAOWL	00026F05BD1B	1	70%	802.11b
default	005018000FFE	6	67%	802.11b

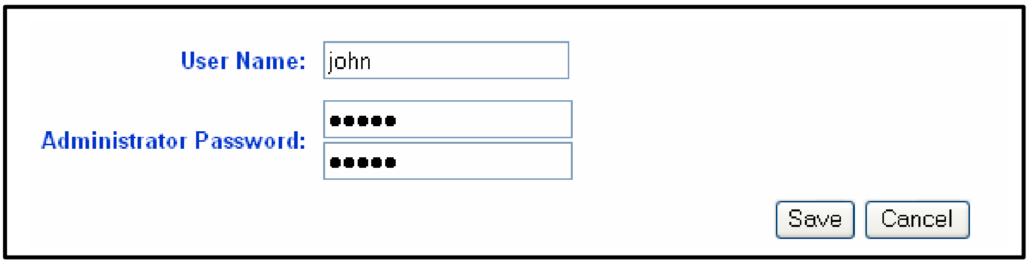
5.2 System



Click on the **System** link on the navigation bar. You will then see the following options: Administrator Settings, Firmware Upgrade, Configuration Tools, Status, Operation, and Rest. Each option is described in detail below.

5.2.1 Administrator Settings

- Click on the **Administrator Settings** link under the **System** menu on the navigation bar. On this page you can configure a user name and password for the Bridge. The image below depicts the administrator settings screen.



User Name: john

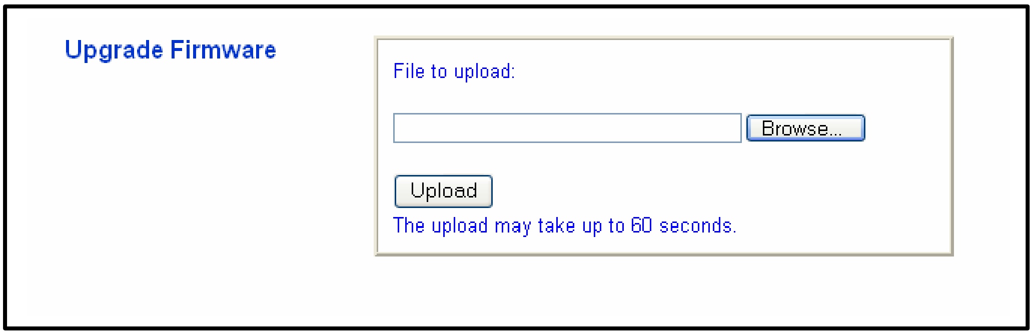
Administrator Password: ●●●●●

●●●●●

- **User name:** enter a new user name.
- **Administrator password:** enter a new password in the first box, and then re-type the password in the second box.
- Click on the **Save** button to save the changes.

5.2.2 Firmware Upgrade

- Click on the **Firmware Upgrade** link under the **System** menu on the navigation bar. Using this page you can upload a new firmware on the Bridge. The image below depicts the Firmware Upgrade screen.



Upgrade Firmware

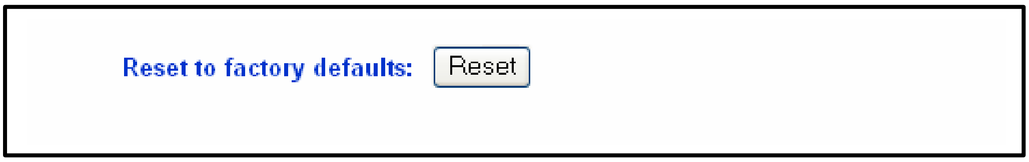
File to upload:

The upload may take up to 60 seconds.

- Click on the **Browse** button to select the firmware, and then click on the **Upload** button.
- The upload may take up to 60 seconds to complete. Do not power off the Bridge while the upgrade is in process.

5.2.3 Configuration Tools

- Click on the **Configuration Tools** link under the **System** menu on the navigation bar. Using this page you can reset the settings of the Bridge to its factory defaults. The image below depicts the Configuration Tools screen.

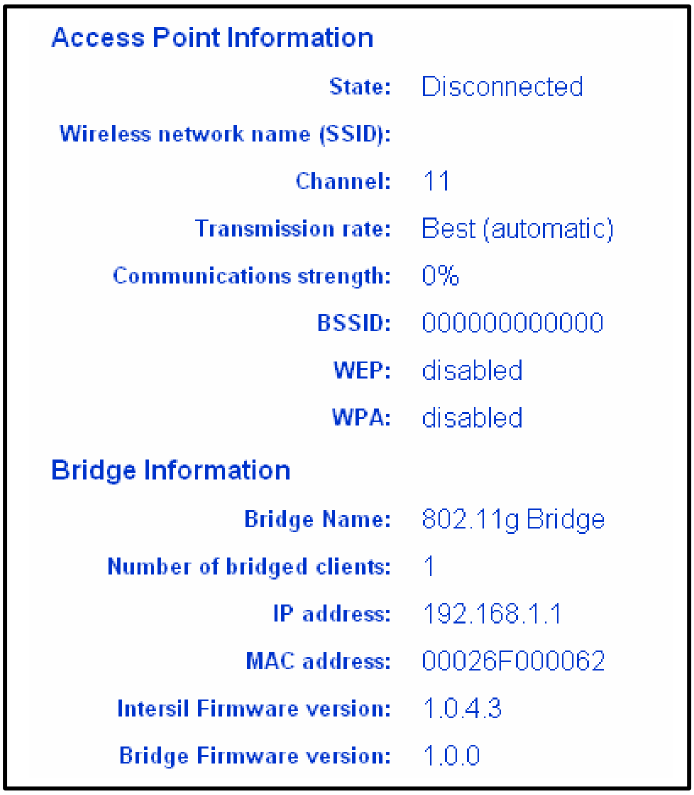


Reset to factory defaults:

- Click on the **Reset** button to reset the Bridge to its factory default settings.

5.2.4 Status

- Click on the **Status** link under the **System** menu on the navigation bar. This page displays the current status of the Bridge. This includes information such as: connection state, SSID, channel number, transmission rate, communication strength, WEP, WPA, Bridge name, number of Bridged clients, IP address, MAC address and firmware version. This page also displays a list of Access Points in the area. The image below depicts the Status screen.

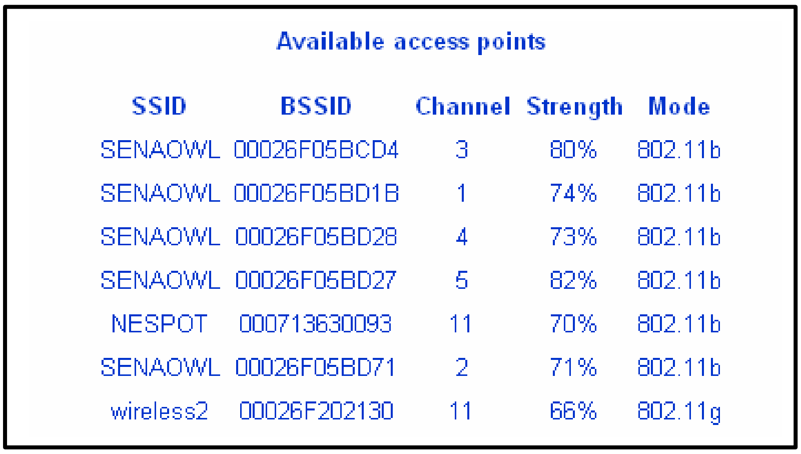


Access Point Information

State:	Disconnected
Wireless network name (SSID):	
Channel:	11
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:	192.168.1.1
MAC address:	00026F000062
Intersil Firmware version:	1.0.4.3
Bridge Firmware version:	1.0.0

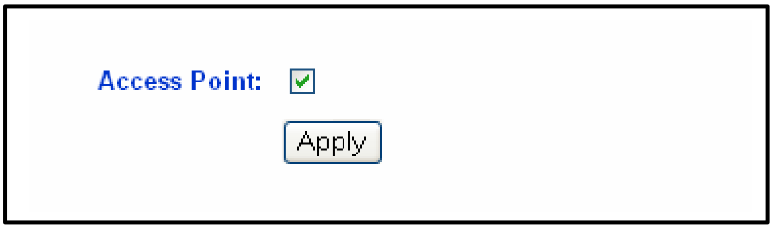


Available access points

SSID	BSSID	Channel	Strength	Mode
SENAOWL	00026F05BCD4	3	80%	802.11b
SENAOWL	00026F05BD1B	1	74%	802.11b
SENAOWL	00026F05BD28	4	73%	802.11b
SENAOWL	00026F05BD27	5	82%	802.11b
NESPOT	000713630093	11	70%	802.11b
SENAOWL	00026F05BD71	2	71%	802.11b
wireless2	00026F202130	11	66%	802.11g

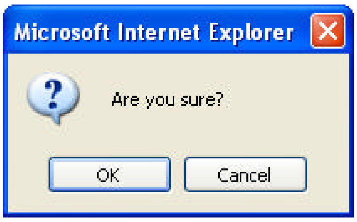
5.2.5 Operation

- Click on the **Operation** link under the **System** menu on the navigation bar. Using this page can switch from the Bridge mode to Access Point mode. The image below depicts the Operation screen.



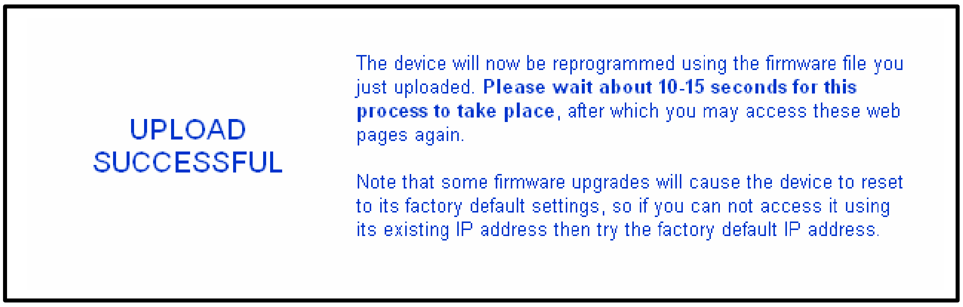
Access Point: ☑

- Place a check in the **Access Point** check box, and then click on the **Apply** button. A message box will then appear asking you to confirm the switch.



Are you sure?

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



UPLOAD SUCCESSFUL

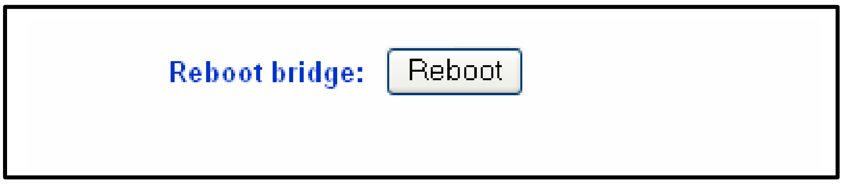
The device will now be reprogrammed using the firmware file you just uploaded. **Please wait about 10-15 seconds for this process to take place**, after which you may access these web pages again.

Note that some firmware upgrades will cause the device to reset to its factory default settings, so if you can not access it using its existing IP address then try the factory default IP address.

- This message indicates that the firmware has now changed to **Access Point** mode. After about 15 seconds you can re-launch you web-browser to the IP address of the Access Point (**192.168.1.2**)
- In order to configure the Access Point, refer to **Chapter 6**.

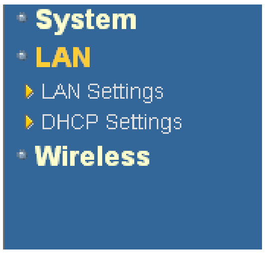
5.2.6 Reset

- Click on the **Reset** link under the **System** menu on the navigation bar. Using this page you can reset the bridge based on the current configuration. The image below depicts the Reset screen.



- Click on the **Reboot** button to reset the bridge based on its current configuration.

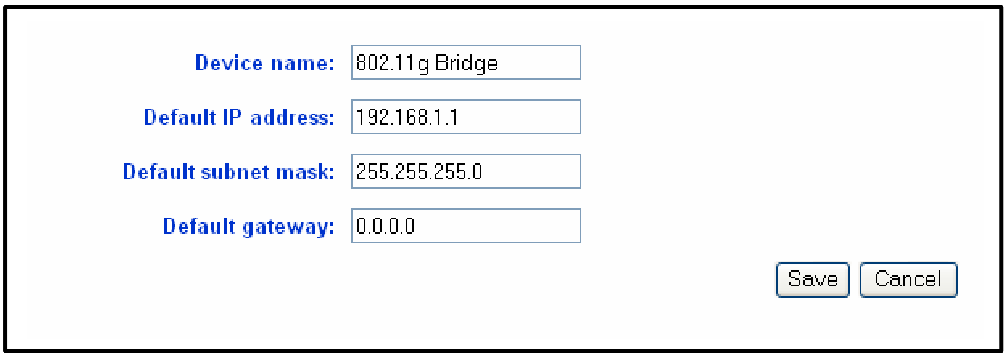
5.3 LAN



Click on the **LAN** link on the navigation bar. You will then see the following options: LAN Settings and DHCP Settings. Each option is described in detail below.

5.3.1 LAN Settings

- Click on the **LAN Settings** link under the **LAN** menu on the navigation bar. Using this you can configure the local IP settings on the bridge. The image below depicts the LAN Settings screen.



Device name: 802.11g Bridge

Default IP address: 192.168.1.1

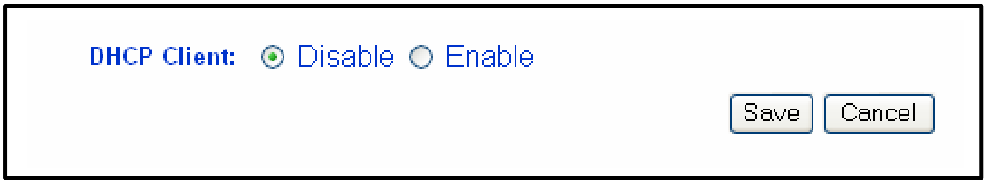
Default subnet mask: 255.255.255.0

Default gateway: 0.0.0.0

- **Device name:** enter a name for the bridge.
- **Default IP address:** enter the IP address.
- **Default subnet mask:** enter the subnet mask.
- **Default gateway:** enter the IP address of the default gateway. The default IP address is 0.0.0.0.
- Click on the **Save** button to confirm the changes.

5.3.2 DHCP Settings

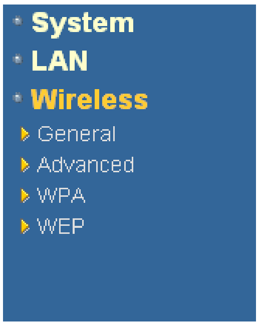
- Click on the **DHCP Settings** link under the **LAN** menu on the navigation bar. Using this you can configure this bridge as a DHCP client, meaning that the network will assign the IP address to it.



DHCP Client: ● Disable ○ Enable

- **DHCP Client:** select **Disable** or **Enable**. By enabling this option, the network will assign an IP address to the Bridge.
- Click on the **Save** button to confirm the changes.

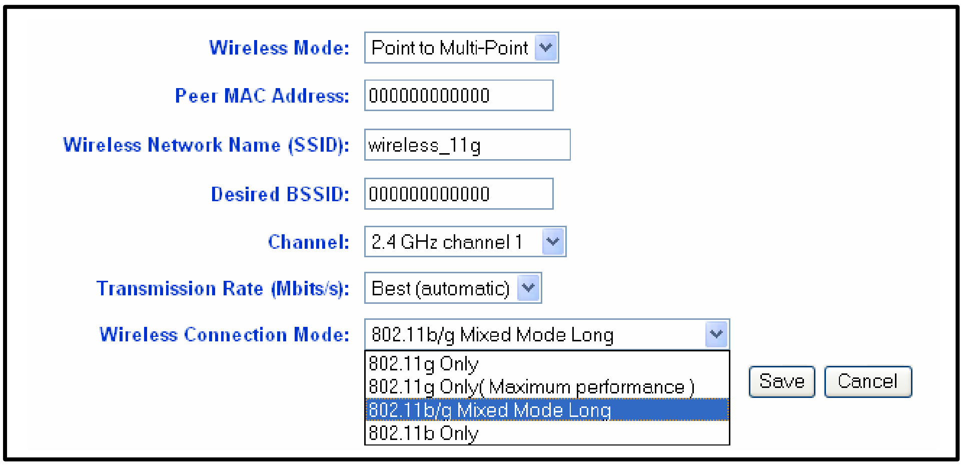
5.4 Wireless



Click on the **Wireless** link on the navigation bar. You will then see the following options: General, Advanced, WPA and WEP. Each option is described in detail below.

5.4.1 General

- Click on the **General** link under the **Wireless** menu on the navigation bar. Using this page you can configure the wireless settings such as: wireless mode, SSID, channel, and transmission rate. The image below depicts the General Wireless screen.



Wireless Mode: Point to Multi-Point

Peer MAC Address: 000000000000

Wireless Network Name (SSID): wireless_11g

Desired BSSID: 000000000000

Channel: 2.4 GHz channel 1

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

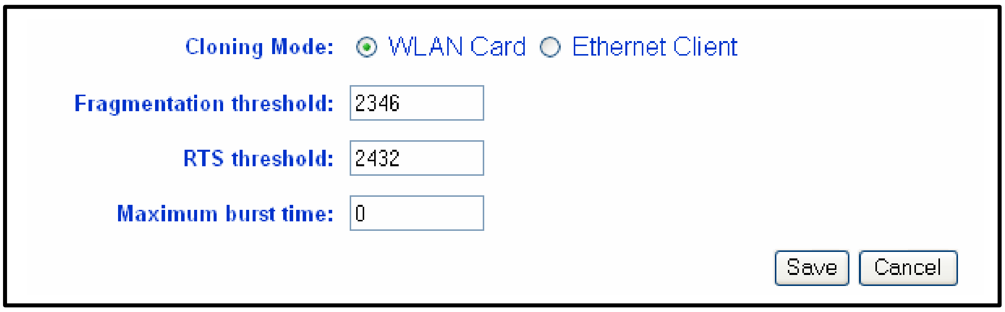
Wireless Connection Mode: 802.11b/g Mixed Mode Long

802.11g Only
802.11g Only(Maximum performance)
802.11b/g Mixed Mode Long
802.11b Only
Save
Cancel

- **Wireless Mode:** select **Point to Multi-Point** or **Point to Point** from the drop-down list. Use Point to Multi-Point to connect to a wireless Access Point, or use Point to Point to connect to another Bridge or Station.
- **Peer MAC Address**: enter the MAC address of the peer WLAN Bridge (P2P Tunnel).
- **Wireless Network Name (SSID)**: the SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network. It is case sensitive and must not exceed 32 characters.
- **Channel:** select a radio frequency from the drop-down list.
- **Transmission Rate (Mbits/s):** select a transmission rate from the drop-down list.
- **Wireless Connection Mode:** select a connection mode from the drop down list. Options available are **802.11g Only**, **802.11g Only (Maximum Performance)**, **802.11b/g Mixed Mode Long,** and **802.11b Only**.
- Click on the **Save** button to confirm the changes.

5.4.2 Advanced

- Click on the **Advanced** link under the **Wireless** menu on the navigation bar. Using this page you can configure the cloning mode and threshold values. The image below depicts the Advanced Wireless screen.



Cloning Mode: ● WLAN Card ○ Ethernet Client

Fragmentation threshold: 2346

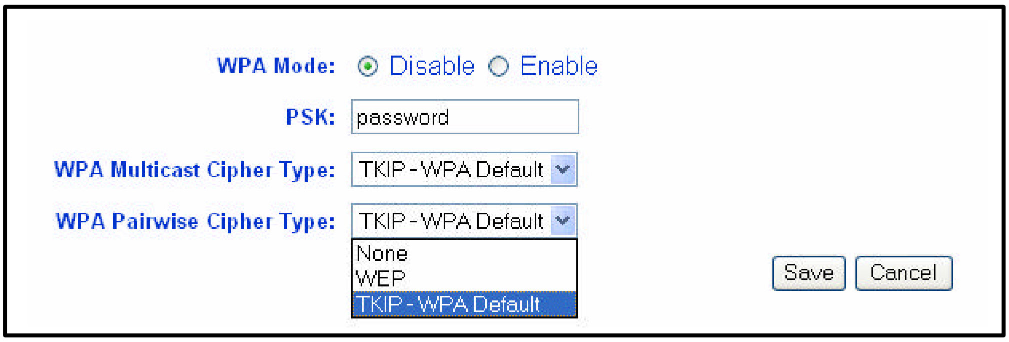
RTS threshold: 2432

Maximum burst time: 0

- **Cloning Mode**: select **WLAN Card** to set the MAC address of the bridge (as seen by the Access Point and other wireless devices) to be the MAC address of the WLAN card inside the bridge. Select **Ethernet Client** to set the MAC address to be that of the first Ethernet client that transmits data from behind the Bridge.
- **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 the Bridge is running in mixed mode. This number is in units of microseconds. A typical value would be 1000 microseconds. When the value if 0, bursting is disabled.
- Click on the **Save** button to confirm the changes.

5.4.3 WPA

- Click on the **WPA** link under the **Wireless** menu on the navigation bar. On this page you may configure WPA, an acronym for Wi-Fi Protected Access, which is a security protocol from the Wi-Fi alliance for 802.11 wireless networks. It uses the Temporal Key Integrity Protocol (TKIP) to provide stronger encryption than the earlier WEP (Wired Equivalent Privacy) method. Derived from, and a subset of, the IEEE 802.11i security standard, WPA includes 802.1x authentication. The image below depicts the configuration screen of the **WPA** option.



WPA Mode: ● Disable ○ Enable

PSK: password

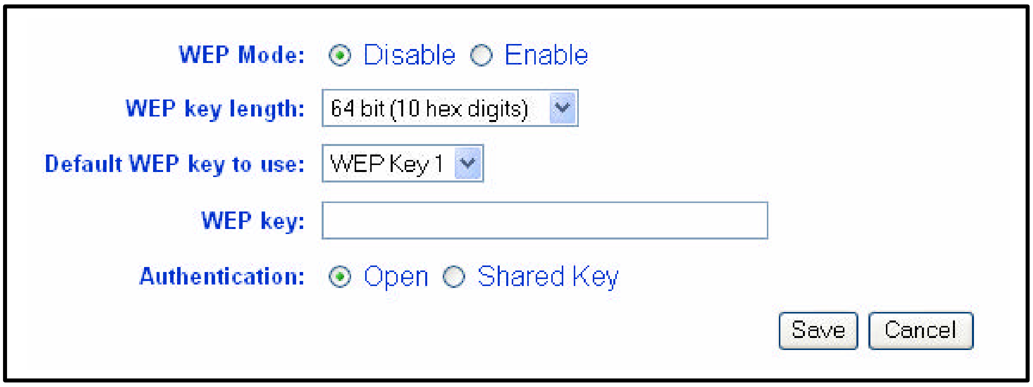
WPA Multicast Cipher Type: TKIP - WPA Default

WPA Pairwise Cipher Type: TKIP - WPA Default

- **WPA Mode:** select **Disable** or **Enable** for WPA.
- **PSK:** leave this blank if the stations will be supplied a key by the 802.1x authentication server. If not, enter a pass-phrase between 8 and 63 characters.
- **WPA Multicast Cipher Type:** currently TKIP is the only permitted setting.
- **WPA Pairwise Cipher Type:** currently TKIP is the only permitted setting.
- Click on the **Save** button to confirm the changes.

5.4.4 WEP

- Click on the **WEP** link under the **Wireless** menu on the navigation bar. On this page you may configure WEP, which is an acronym for Wired Equivalent Privacy, a security protocol for Wireless Local Area Networks (WLANs) defined in the 802.11 standard. WEP is designed to provide the same level of security as a wired LAN. The image below depicts the configuration screen of the **WEP** option.



WEP Mode: ● Disable ○ Enable

WEP key length: 64 bit (10 hex digits)

Default WEP key to use: WEP Key 1

WEP key:

Authentication: ● Open ○ Shared Key

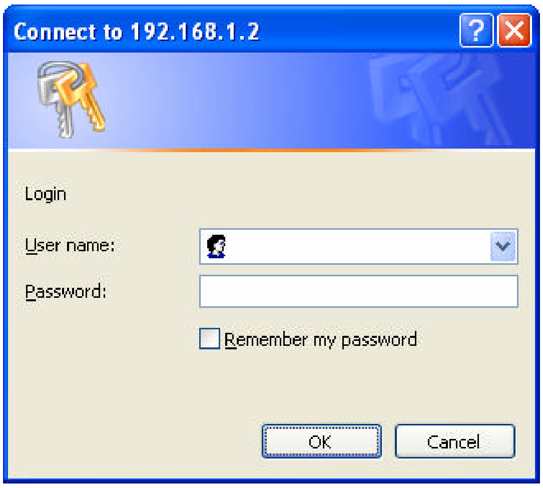
- **WEP Mode:** select **Disable** or **Enable** WEP encryption.
- **WEP key length:** select a WEP key length from the drop-down list. Options available are **64-bit** and **128-bit**.
- **WEP key:** enter the WEP key. If you use WEP you must specify the same key into the Access Point and wireless stations. For **64-bit** keys you must enter 10 hex digits. For **128-bit** keys you must enter 26 hex digits. A hex digit is either a number from 0 through 9 or a letter from A through F. Leaving the box blank indicates a key of all 0's.

- **Default WEP key to use:** select a default WEP key to use.
- **Authentication:** select an authentication method. Options available are **Open**, **Shared Key**. If Open is selected any station can access the Bridge. If **Shared Key** is selected both communicating stations must have the encryption key.

6 Access Point Mode – Web Configuration

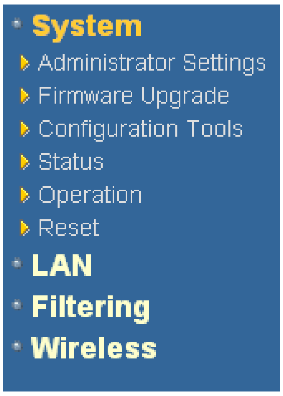
6.1 Logging In

- 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 Access Point and your computers are on the same subnet. Refer to **Chapter 3** in order to configure the IP address of your computer.
- You will then see the login window. Leave the **User name** and **Password** fields blank and click on the **OK** button.



- You can change the username and password under the **Administrator Settings** option. Refer to section **6.2.1 Administrator Settings** to change the username and password.
- After logging in, you will see the Graphical User Interface (GUI) of the Bridge. The configuration is divided into four major parts: **System, LAN, Filtering,** and **Wireless**. Each one is described in detail in the next few sections.
- The **Status** page is the first page that is displayed, this page displays the settings of the Access Point, the MAC/IP addresses, and the Wireless settings. To understand more about the **Status** page, refer to section **6.2.4 Status**.

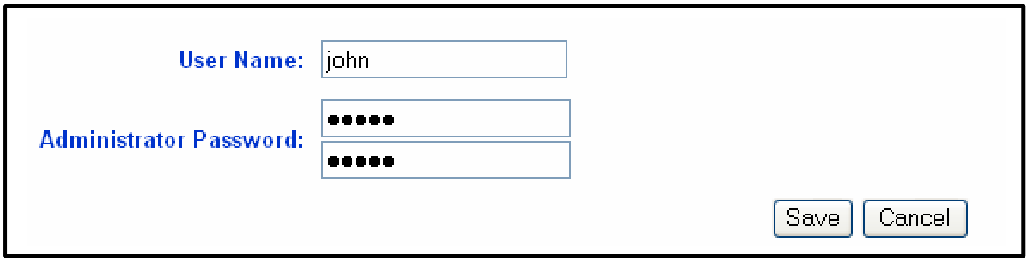
6.2 System



Click on the **System** link on the navigation bar. You will then see the following options: Administrator Settings, Firmware Upgrade, Configuration Tools, Status, Operation, and Rest. Each option is described in detail below.

6.2.1 Administrator Settings

- Click on the **Administrator Settings** link under the **System** menu on the navigation bar. On this page you can configure a user name and password for the Access Point. The image below depicts the administrator settings screen.



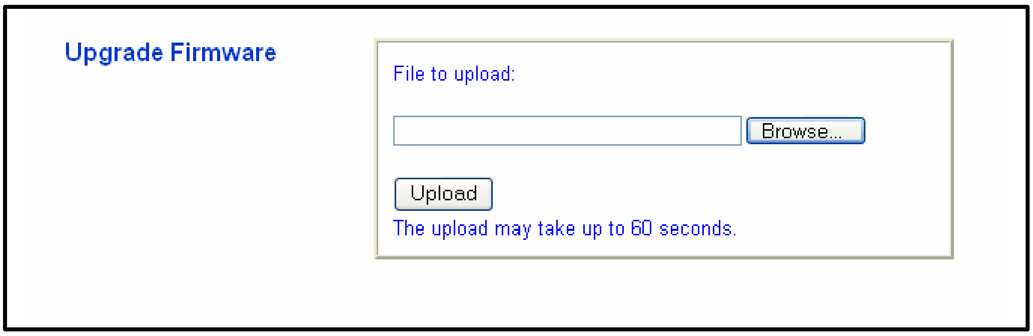
User Name: john

Administrator Password: ●●●●●
●●●●●

- **User name:** enter a new user name.
- **Administrator password:** enter a new password in the first box, and then re-type the password in the second box.
- Click on the **Save** button to save the changes.

6.2.2 Firmware Upgrade

- Click on the **Firmware Upgrade** link under the **System** menu on the navigation bar. Using this page you can upload a new firmware on the Access Point. The image below depicts the Firmware Upgrade screen.

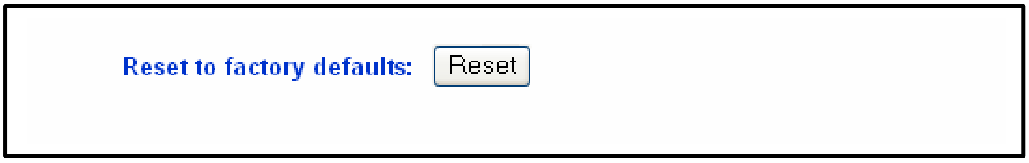


The upload may take up to 60 seconds.

- Click on the **Browse** button to select the firmware, and then click on the **Upload** button.
- The upload may take up to 60 seconds to complete. Do not power off the Access Point while the upgrade is in process.

6.2.3 Configuration Tools

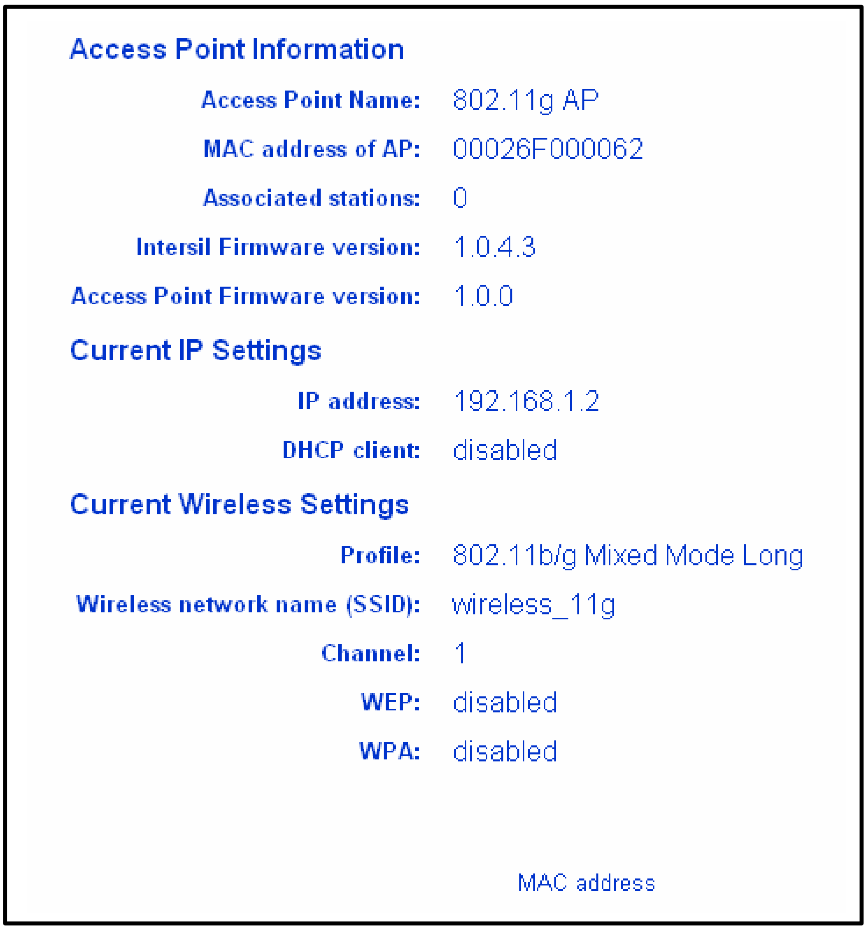
- Click on the **Configuration Tools** link under the **System** menu on the navigation bar. Using this page you can reset the settings of the Access Point to its factory defaults. The image below depicts the Configuration Tools screen.



- Click on the **Reset** button to reset the Access Point to its factory default settings.

6.2.4 Status

- Click on the **Status** link under the **System** menu on the navigation bar. This page displays the current status of the Access Point. This includes information such as: AP name, MAC address, number of associated stations, IP address, SSID, WEP, and WPA. The image below depicts the Status screen.



Access Point Information

Access Point Name: 802.11g AP

MAC address of AP: 00026F000062

Associated stations: 0

Intersil Firmware version: 1.0.4.3

Access Point Firmware version: 1.0.0

Current IP Settings

IP address: 192.168.1.2

DHCP client: disabled

Current Wireless Settings

Profile: 802.11b/g Mixed Mode Long

Wireless network name (SSID): wireless_11g

Channel: 1

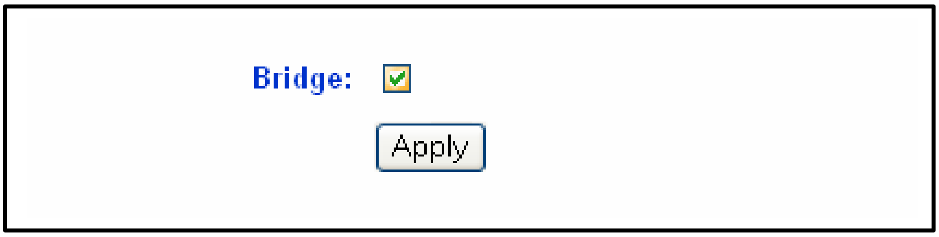
WEP: disabled

WPA: disabled

MAC address

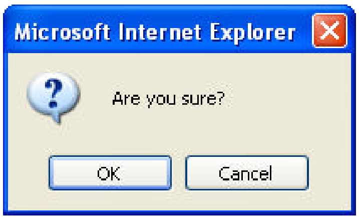
6.2.5 Operation

- Click on the **Operation** link under the **System** menu on the navigation bar. Using this page can switch from the Access Point mode to Bridge mode. The image below depicts the Operation screen.

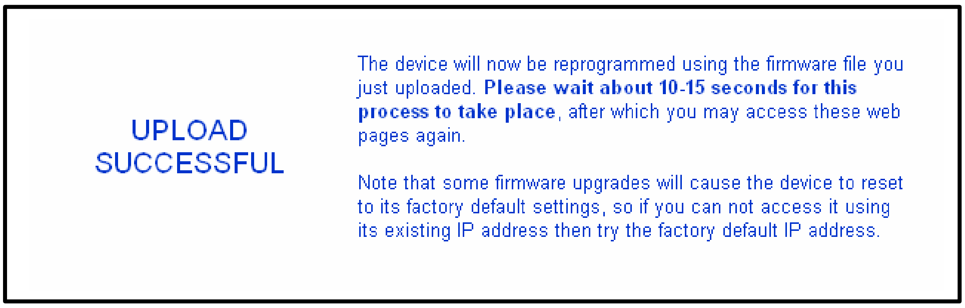


Bridge: ☑

- Place a check in the **Bridge** check box, and then click on the **Apply** button. A message box will then appear asking you to confirm the switch.



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



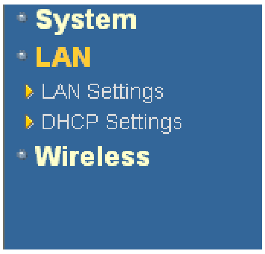
UPLOAD SUCCESSFUL

The device will now be reprogrammed using the firmware file you just uploaded. **Please wait about 10-15 seconds for this process to take place**, after which you may access these web pages again.

Note that some firmware upgrades will cause the device to reset to its factory default settings, so if you can not access it using its existing IP address then try the factory default IP address.

- This message indicates that the firmware has now changed to **Bridge** mode. After about 15 seconds you can re-launch you web-browser to the IP address of the Bridge (**192.168.1.1**)
- In order to configure the Bridge, refer to **Chapter 5**.

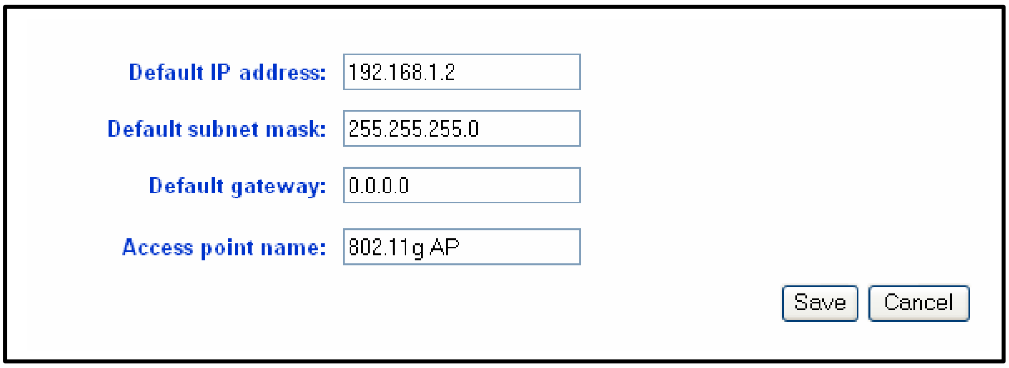
6.3 LAN



Click on the **LAN** link on the navigation bar. You will then see the following options: LAN Settings and DHCP Settings. Each option is described in detail below.

6.3.1 LAN Settings

- Click on the **LAN Settings** link under the **LAN** menu on the navigation bar. Using this you can configure the local IP settings on the Access Point. The image below depicts the LAN Settings screen.



Default IP address: 192.168.1.2

Default subnet mask: 255.255.255.0

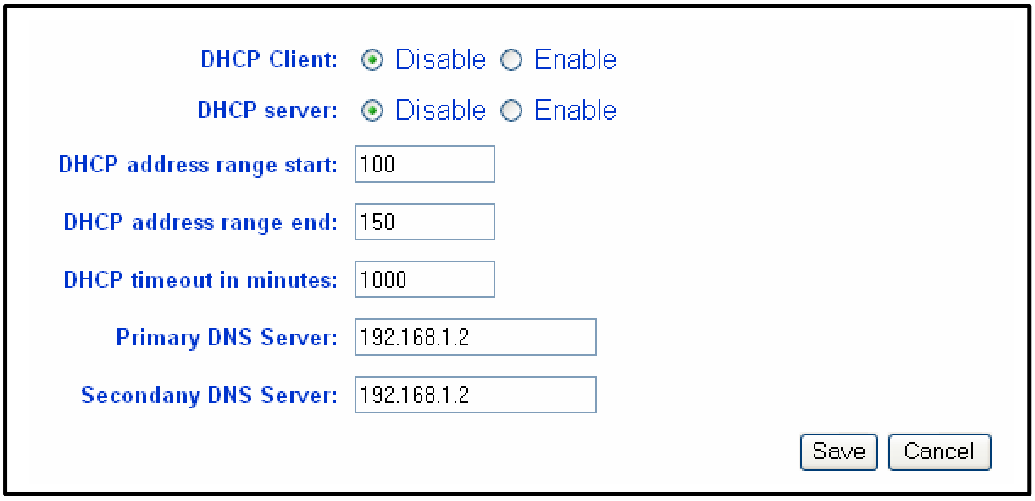
Default gateway: 0.0.0.0

Access point name: 802.11g AP

- **Default IP address:** enter the IP address of the Access Point.
- **Default subnet mask:** enter the subnet mask for the Access Point.
- **Default gateway:** enter the IP address of the default gateway. The default IP address is 0.0.0.0.
- **Access point name:** enter a name for the access point. This is different from the SSID.
- Click on the **Save** button to confirm the changes.

6.3.2 DHCP Settings

- Click on the **DHCP Settings** link on the navigation bar. On this page you can configure this Access Point as a DHCP client or server. If you set this Access Point as a DHCP client, then it will receive its IP address from the network. If you choose to set this device as a DHCP server, then it will assign IP addresses to its clients. The image below depicts the configuration screen of the **DHCP** option.



DHCP Client: ● Disable ○ Enable

DHCP server: ● Disable ○ Enable

DHCP address range start: 100

DHCP address range end: 150

DHCP timeout in minutes: 1000

Primary DNS Server: 192.168.1.2

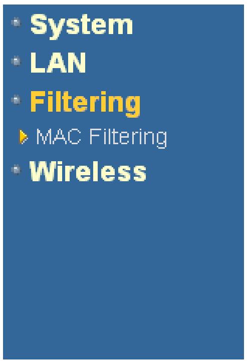
Secondary DNS Server: 192.168.1.2

- **DHCP Client:** select **Disable** or **Enable**. By enabling this option, the network will assign an IP address to the Access Point.
- **DHCP Server:** select **Disable** or **Enable**. If you enable DHCP Server, then the

Access Point will assign IP addresses to the clients based on address ranges specified.

- **DHCP address range start:** enter the starting range for the IP addresses.
- **DHCP address range end:** enter the ending range of the IP addresses.
- **DHCP timeout in minutes:** enter a lease time for the IP addresses. This is specified in minutes.
- **Primary DNS Server:** enter the IP address of the primary DNS server.
- **Secondary DNS Server:** enter the IP address of the secondary DNS server.
- Click on the **Save** button to confirm the changes.

6.4 Filtering

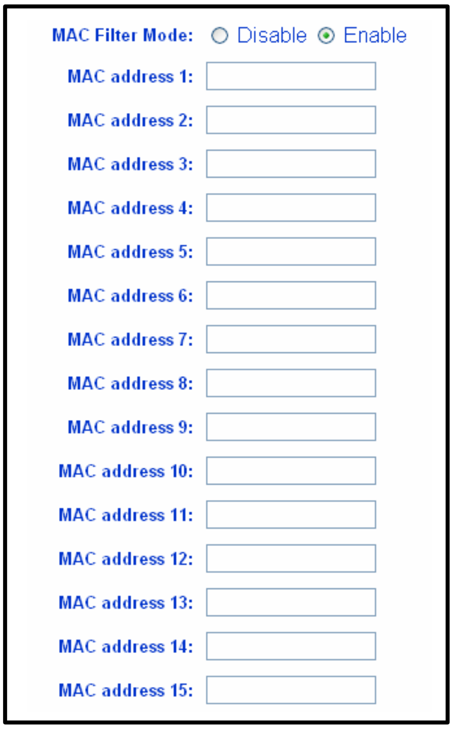


Click on the **Filtering** link on the navigation bar. You will then see the MAC Filtering option, as described below.

6.4.1 MAC Filtering

- Click on the **MAC Filtering** link on the navigation bar. On this page you may list the MAC addresses of clients that you wish to allow or disallow association by the Access Point. This image depicts the configuration screen of the MAC Filtering option.

- **MAC Filter Mode:** select **Disable** or **Enable**. By enabling MAC filtering, only the listed MAC addresses will be able to associate with the Access Point. By disabling MAC filtering, only the listed MAC addresses will not be able to associate with the Access Point.
- **MAC address 1~25:** list the MAC addresses.
- Click on the **Save** button to confirm the changes.



MAC Filter Mode: ○ Disable ● Enable

MAC address 1:

MAC address 2:

MAC address 3:

MAC address 4:

MAC address 5:

MAC address 6:

MAC address 7:

MAC address 8:

MAC address 9:

MAC address 10:

MAC address 11:

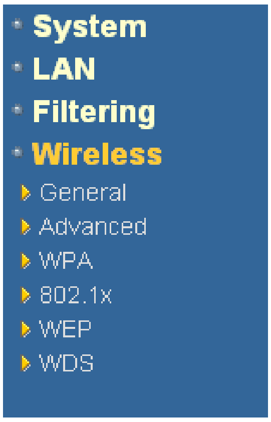
MAC address 12:

MAC address 13:

MAC address 14:

MAC address 15:

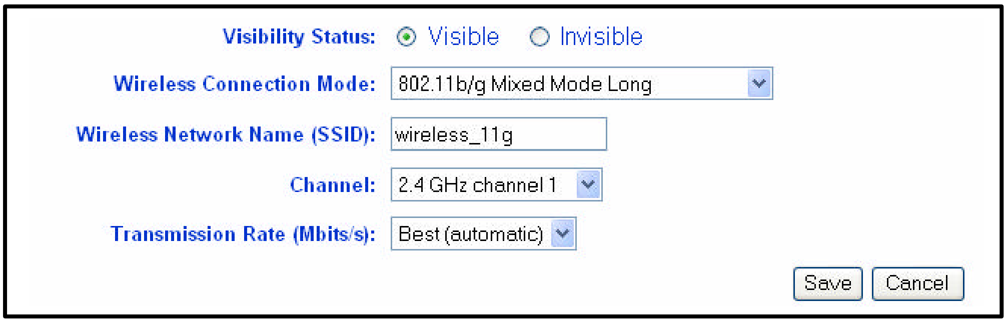
6.5 Wireless



Click on the **Wireless** link on the navigation bar. You will then see the following options: General, Advanced, WPA, 802.1x, WEP, and WDS. Each option is described in detail below.

6.5.1 General

- ➤ Click on the **General** link under the **Wireless** menu on the navigation bar. On this page you can manage 802.11b/g of the Access Point. The image below depicts the configuration screen of the **General** option.

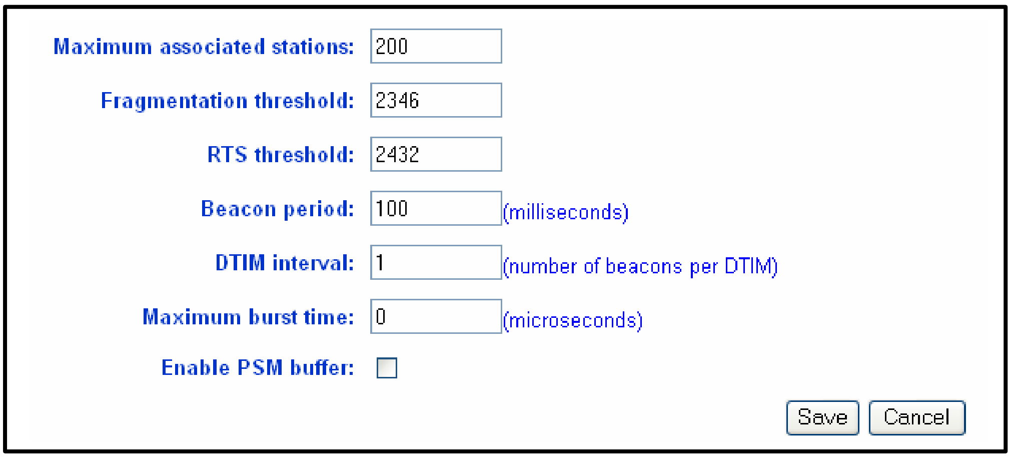


Visibility Status:	● Visible ○ Invisible
Wireless Connection Mode:	802.11b/g Mixed Mode Long
Wireless Network Name (SSID):	wireless_11g
Channel:	2.4 GHz channel 1
Transmission Rate (Mbits/s):	Best (automatic)

- ➤ **Visibility Status:** select **Visible** or **Invisible**. This option displays or hides the SSID of this Access Point from other Access Points.
- ➤ **Wireless Connection Mode:** select an Access Point mode from the drop down list. Options available are **802.11g Only**, **802.11g Only (Maximum Performance)**, **802.11b/g Mixed Mode Long,** and **802.11b Only,**
- ➤ **Wireless Network Name (SSID):** the SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network. It is case sensitive and must not exceed 32 characters.
- ➤ **Channel:** select a radio frequency from the drop-down list.
- ➤ **Transmission Rate (Mbits/s):** select a transmission rate from the drop-down list.
- ➤ Click on the **Save** button to confirm the changes.

6.5.2 Advanced

- Click on the **Advanced** link on the navigation bar. On this page you may configure the maximum associated stations, thresholds, beacon periods, DTIM interval, maximum burst time, PSM mode. The image below depicts the configuration screen of the Advanced option.

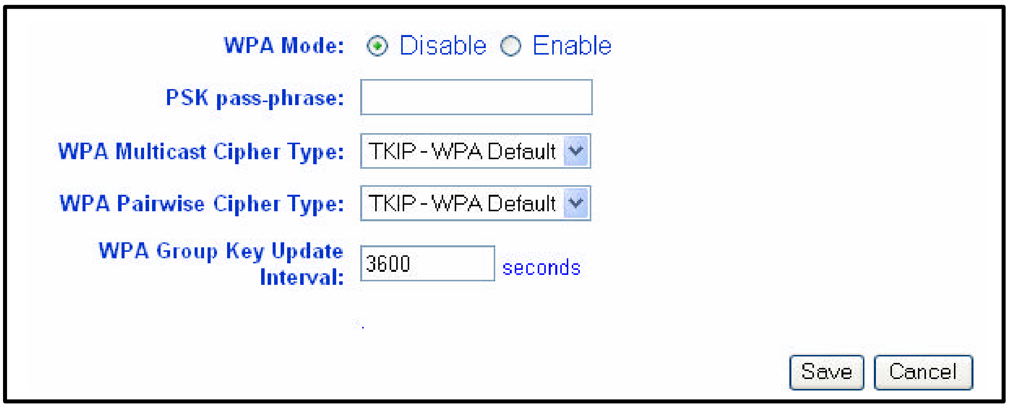


Maximum associated stations: 200
Fragmentation threshold: 2346
RTS threshold: 2432
Beacon period: 100 (milliseconds)
DTIM interval: 1 (number of beacons per DTIM)
Maximum burst time: 0 (microseconds)
Enable PSM buffer: □

- **Maximum associated stations:** enter the maximum number of stations that may associate with this Access Point at 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 burst time:** 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. A typical value would be 1000 microseconds. When this number is zero, bursting is disabled.
- **Enable PSM Buffer:** turn this on to enable support for stations in power save mode.
- Click on the **Save** button to confirm the changes.

6.5.3 WPA

- Click on the **WPA** link on the navigation bar. On this page you may configure WPA, an acronym for Wi-Fi Protected Access, which is a security protocol from the Wi-Fi alliance for 802.11 wireless networks. It uses the Temporal Key Integrity Protocol (TKIP) to provide stronger encryption than the earlier WEP (Wired Equivalent Privacy) method. Derived from, and a subset of, the IEEE 802.11i security standard, WPA includes 802.1x authentication. The image below depicts the configuration screen of the **WPA** option.



WPA Mode: ● Disable ○ Enable

PSK pass-phrase:

WPA Multicast Cipher Type: TKIP - WPA Default

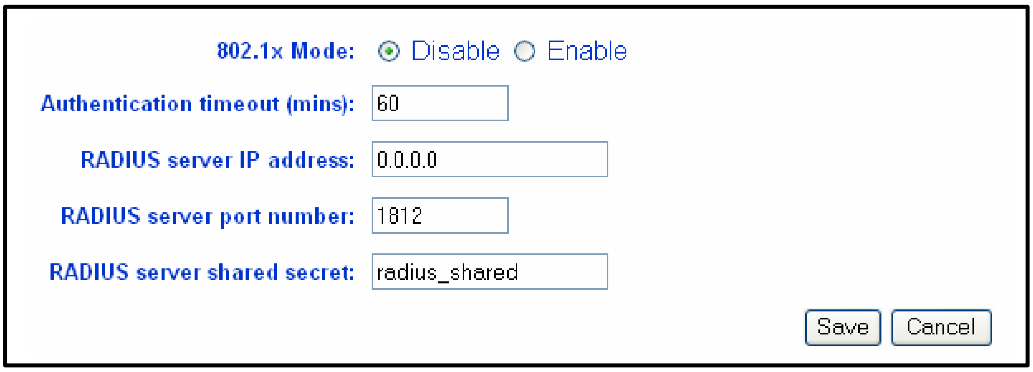
WPA Pairwise Cipher Type: TKIP - WPA Default

WPA Group Key Update Interval: 3600 seconds

- **WPA Mode:** select **Disable** or **Enable** for WPA.
- **PSK pass-phrase:** leave this blank if the stations will be supplied a key by the 802.1x authentication server. If not, enter a pass-phrase between 8 and 63 characters.
- **WPA Multicast Cipher Type:** currently TKIP is the only permitted setting.
- **WPA Pairwise Cipher Type:** currently TKIP is the only permitted setting.
- **WPA Group Key Update Interval:** enter the update value, which is in number of seconds.
- Click on the **Save** button to confirm the changes.

6.5.4 802.1x

- Click on the **8021.x** link on the navigation bar. On this page you may configure IEEE 802.1x, which is a standard designed to enhance the security of wireless local area networks (WLANs) that follow the IEEE 802.11 standard. 802.1x provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. The image below depicts the configuration screen of the 8021.x option.



802.1x Mode: ● Disable ○ Enable

Authentication timeout (mins): 60

RADIUS server IP address: 0.0.0.0

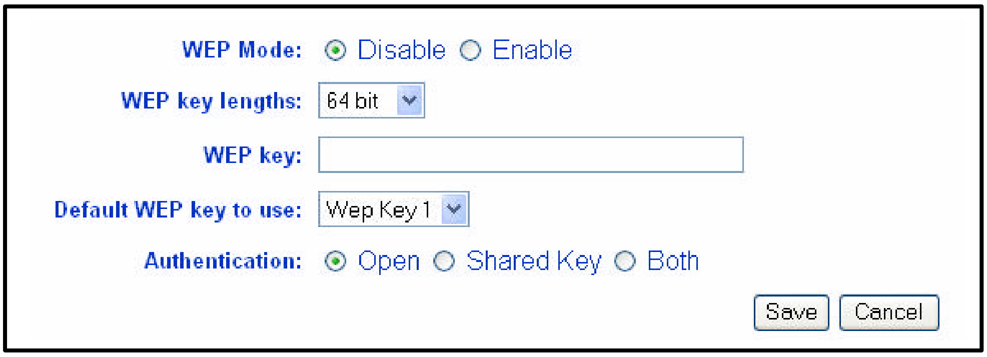
RADIUS server port number: 1812

RADIUS server shared secret: radius_shared

- **802.1x Mode:** select **Disable** or **Enable** for 802.1x
- **Authentication timeout (mns):** enter a value for the authentication time out.
- **RADIUS server IP address:** enter the IP address of the RADIUS server.
- **RADIUS server port number:** enter the port number of the RADIUS server.
- **RADIUS server shared secret:** enter the shared secret of the RADIUS server.
- Click on the **Save** button to confirm the changes.

6.5.5 WEP

- Click on the **WEP** link on the navigation bar. On this page you may configure WEP, which is an acronym for Wired Equivalent Privacy, a security protocol for Wireless Local Area Networks (WLANs) defined in the 802.11 standard. WEP is designed to provide the same level of security as a wired LAN. The image below depicts the configuration screen of the WEP option.



WEP Mode: ● Disable ○ Enable

WEP key lengths: 64 bit

WEP key:

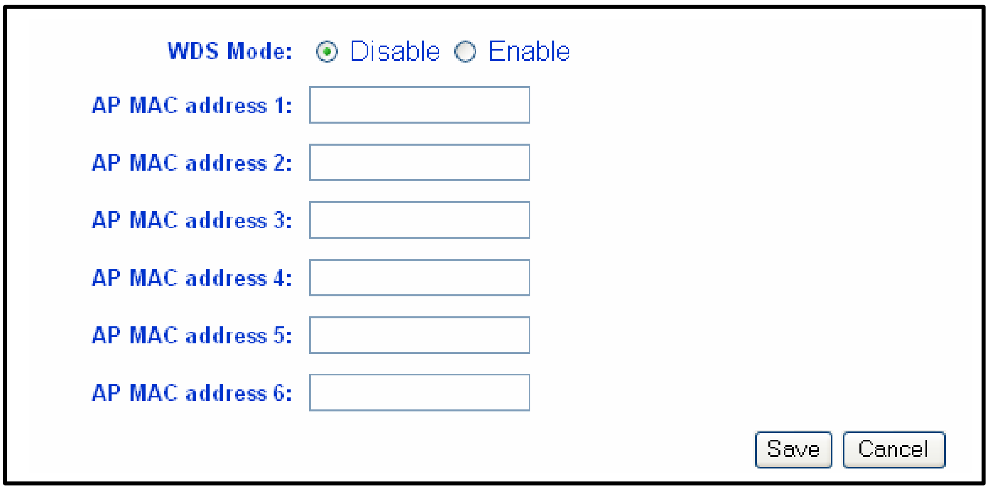
Default WEP key to use: Wep Key 1

Authentication: ● Open ○ Shared Key ○ Both

- **WEP Mode:** select **Disable** or **Enable** WEP encryption.
- **WEP key length:** select a WEP key length from the drop-down list. Options available are **64-bit** and **128-bit**.
- **WEP key:** enter the WEP key.
- **Default WEP key to use:** select a default WEP key to use.
- **Authentication:** select an authentication method. Options available are **Open**, **Shared Key** or **Both**.
- Click on the **Save** button to confirm the changes.

6.5.6 WDS

- Click on the **WDS** link on the navigation bar. On this page you may configure the Wireless Distribution System. The image below depicts the configuration screen of the WDS option.



WDS Mode: ● Disable ○ Enable

AP MAC address 1:

AP MAC address 2:

AP MAC address 3:

AP MAC address 4:

AP MAC address 5:

AP MAC address 6:

- **WDS Mode:** select **Disable** or **Enable** WDS encryption. When Wireless Distribution System (WDS) is enabled, the Access Point functions as a wireless repeater and is able to wirelessly communicate with other Access Points.
- **AP MAC address 1 – 6:** enter the MAC address of WDS capable Access Point.
- Click on the **Save** button to confirm the changes.

Appendix A – Specifications

General	
Data Rates	1,2,5.5,6,9,11,12,18,24,36,48,54 Mbps
Standards	IEEE802.11 b/g, IEEE802.1x, IEEE802.3, IEEE802.3u
Compatibility	IEEE 802.11g/ IEEE 802.11 b compliant
Power Requirements	Power Supply: 90 to 240 VDC ± 10% (depend on different country) Device: 12 V/ 1A
Status LEDs	LAN：Link , WLAN：Link , Power ：on/off
Regulation Certifications	FCC Part 15/UL, ETSI 300/328/CE
RF Information	
Frequency Band	2.400 2.484 GHz
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, 2 for Spain, 4 for France
Receive Sensitivity (Typical)	-94dBm @ 1Mbps -92dBm @ 6Mbps -83dBm @ 24Mbps -92dBm @ 2Mbps -90dBm @ 9Mbps -79dBm @ 36Mbps -89dBm @ 5.5Mbps -88dBm @ 12Mbps -74dBm @ 48Mbps -86dBm @ 11Mbps -86dBm @ 18Mbps -72dBm @ 54Mbps
Available transmit power (Depend on Different Countries' Regulation)	21 ± 2dBm @1, 2, 5.5 and 11 Mbps 20 ± 2dBm @6, 9, 12, 18Mbps 17 ± 2dBm @24, 36Mbps 16 ± 2dBm @48, 54Mbps
RF Connector	TNC Type (Female Reverse—FCC Standard)

Networking Information	
Topology	Ad-Hoc, Infrastructure
Operation Mode	Point-to-Point/ Point-to-Multipoint Bridge/ AP/ Client Bridge/ Repeater
Interface	One 10/100Mbps RJ-45 LAN Port
Security	• IEEE802.1x / RADIUS Client (EAP-MD5/TLS/TTLS) Support • WPA* -- Wi-Fi Protected Access • PSK (Pre share key) with 64/ 128-bit WEP Key • EAP-MD5/TLS/ TTLS authenticator support • TKIP • MAC address filtering (WLAN) • Hide SSID in beacons
IP Auto-configuration	DHCP client / server
Management	
Configuration	Web-based configuration (HTTP)
Firmware Upgrade	Upgrade firmware via Web Browser
Physical	
Dimensions (HxWxD)	125(L)mm * 108(W)mm * 31(H)mm 4.9 (L)in* 4.3(W)in * 1.2(H)in
Weight	350 g (0.8 lb.)
Environmental	
Temperature Range	-10°C to 45°C (14°F to 113°F) - Operating -40°Cto 70°C (-40°F to 158°F) - Storage
Humidity (non-condensing)	5%~95% Typical

Appendix B – Regulatory Compliance Information

Mobile of end product

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.

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.

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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