Dual Band Wireless

Access Point

User's Manual

Version: 1.0

Table of Contents

Revision History

Version	Date	Notes
1.0	September 12, 2003	Initial Version

1 Introduction

The Dual Band Wireless Access Point operates seamlessly and simultaneously in both the 2.4 GHz and 5 GHz frequency spectrums supporting the 802.11b (2.4GHz, 11Mbps) and the newer, faster 802.11a (5GHz, 54Mbps) and 802.11g (2.4GHz, 54Mbps) wireless standards. It's the best way to add wireless capability to your existing wired network, or to add bandwidth to your wireless installation.

To protect your wireless connectivity, the Dual Band Wireless Access Point can encrypt all wireless transmissions through 64/128/152-bit WEP data encryption. The MAC address filter lets you select exactly which station has access to your wireless network. Dynamic Frequency Selection (DFS) puts your network on the cleanest channel in your location. With the Dual Band Wireless Access Point, you'll experience the best wireless connectivity available today.

1.1   Features & Benefits

Features	Benefits
2.4GHz IEEE802.11b/g (draft) standard and 5GHz IEEE802.11a standard compliant	Fully interoperable with IEEE802.11a/b/g (draft) compliant products.
Dual Radios for Atheros 802.11a and Atheros 802.11g/b	The 802.11a and 802.11g wireless LANs can be used simultaneously.
3-way bridging for 802.3 and 802.11a/g networks	Enable the transfer of data among different kinds of networks.
Wi-Fi Protected Access	Enhance authentication and security.
High speed data rate up to 54Mbps/ 108Mbps in "Turbo" mode in 11a mode	Capable of handling heavy data payloads such as MPEG video streaming.
DFS/TPC for European operation (IEEE802.11h)	Meets requirements of vertical applications using 802.11a and 802.11g in Europe.
Multi country Roaming (802.11d)	Automatically adjusts regulatory domain to operate in different countries.
64/128/152-bit WEP data encryption	Powerful data security.
MAC address filtering	Ensures secure network connections.
Remote Configuration via Web-browser/Telnet	Easy to configure or manage the device remotely.
Firmware upgrade through Web-browser	Easy to upgrade the firmware to reduce operations overhead.

1.2   Package Contents

One Access Point
One Power Adapter
One CAT 5 UTP Cable
One RS-232 Cable
One Fast Start Guide
One CD-ROM with User's Manual Included

2 Understanding the Hardware

2.1 Hardware Configuration

RJ-45 Ethernet Connector – Provides 10/100 Mbps connectivity to a wired Ethernet LAN.
RS-232 Console Connector – Provides Command Line Interface (CLI) to view and modify the configuration of the AP from a terminal or PC through a telnet connection.
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 position.
D. Plug in the power cord into the power outlet.

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.
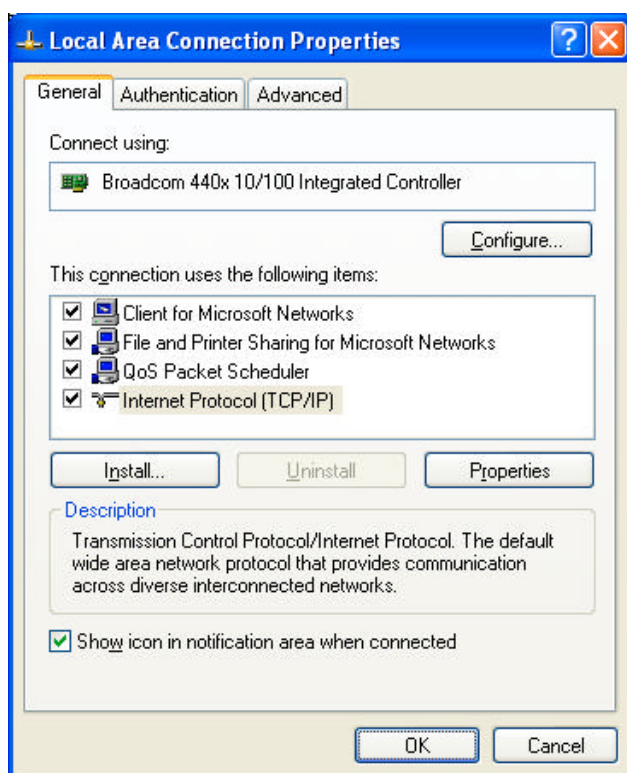
B. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the IP address of your PC. You will then see the following screen.
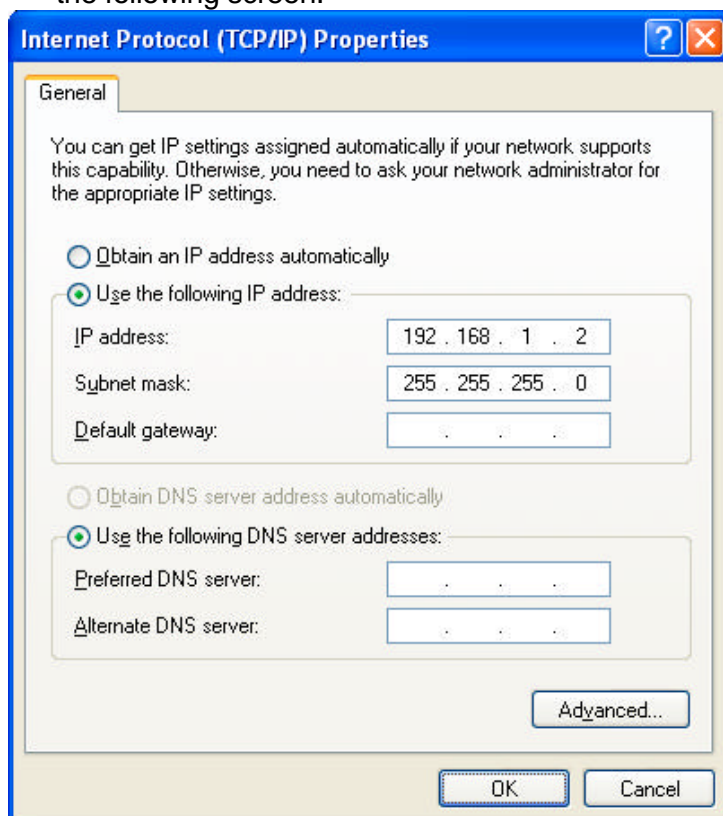
C. Select **Use the following IP address** radio button, and then enter an IP address and subnet mask for your PC. Make sure that the Access Point and your PC are on the same subnet. The default IP address and subnet mask of the Access Point are **192.168.1.1** and **255.255.255.0** respectively.

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

3.2   Wireless LAN Configuration

Follow the steps below in order to configure the Wireless LAN settings.

A. Launch the **WLAN Client Utility** and click on the **Configuration** tab.
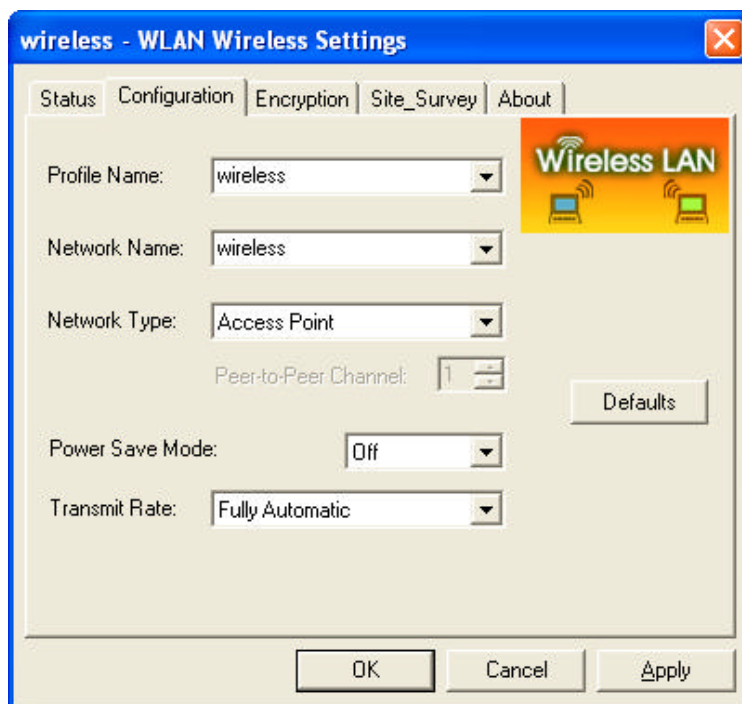
B. **Profile Name**: enter a name for this profile.
C. **Network Name**: enter the SSID. (Default name: Any)
D. **Network Type**: select **Access Point** from the drop-down list.
E. **Power Save Mode**: Select **Off** or **On** from the drop-down list.
F. **Transmit Rate**: select **Fully Automatic** from the drop-down list.
G. Click on the **OK** button.

4 Web Configuration

4.1   Logging In

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

You will then see the login window. Enter **admin** as the User name and **iktpw** as the Password and then click on the **OK** button.
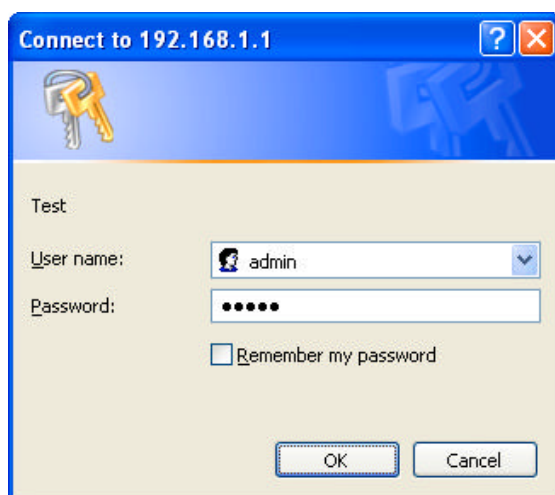
You can also change the username and password under the **Administrator Settings** option. Refer to section **4.3.1 Administrator Settings** to change the username and password.

4.2   Getting Familiar with the GUI

After logging in, the first page that is displayed in the **Status** page.

The GUI consists of three parts and is displayed in the image below:
A. **Navigation Bar**: used to navigate through the available options.
B. **Main Page**: used to view and configure the AP's settings.
C. **Top Right-hand Corner**: quick buttons for **Home**, **Exit**, and **Reset**. Click on the **Home** button to return to the status page. Click on the **Exit** button to logout, and click on the **Reset** button to restart the AP.

4.3   System

Click on the **System** link on the navigation bar, you will then see five options: Administrator Settings, Firmware Upgrade, Configuration Tools, Factory Default, and Rest. Each one is described in detail below.

4.3.1   Administrator Settings

Click on the **Administrator Settings** link. On this page you can configure the user name, password, system name and telnet.
Set another username and password to restrict management access to the Access Point.

Username: enter a new user name.
Password: enter a new password.

System Name: enter a unique name for this AP.
Enable Telnet: place a check in this box if you would like to allow telnet access to this device.
Click on the **Apply** button to confirm and save the changes.

4.3.2 Firmware Upgrade

Click on the **Firmware Upgrade** link. This page is used to upgrade the firmware on the AP.

Host Name: enter the host name or host IP address.
User Name: enter the user name for the host.
Password: enter the password for the host.
Image Path: enter the path of the image file.
Image Name: enter the name of the image file.
Click on the **Apply** button to confirm and save the changes.

4.3.3 Configuration Tools

Click on the **Configuration Tools** link on the navigation bar, you will then see the **Configuration Script** page. This page allows you to develop a script for an application.

Host Name: enter the host name for the script resides.
User Name: enter the user name of the host.
Password: enter the password of the host.
Script Path: enter the path of the script file.
Script Name: enter the name of the script file.
Click on the **Apply** button to confirm and save the changes.

4.3.4 Factory Defaults

Click on the **Restore** button of the Access Point to perform a reset and restore the original factory settings.

4.4   LAN

Click on the **LAN** link on the navigation bar, and then click on **LAN Settings.** You will then see the LAN Settings page. On this page you can configure the LAN IP, subnet mask, and default gateway IP addresses.

IP Address: enter the IP address of the Access Point.
Subnet Mask: enter a subnet mask for the IP address.
Default Gateway Address: enter a gateway IP for the Access Point.
Click on the **Apply** button to confirm and save the changes.

4.5   Wireless

Click on the **Wireless** link on the navigation bar, you will then see three options: General, 802.11a, and 80211g.. Each one is described in detail below.

4.5.1 General

Click on the **General** link on the navigation bar. On this page you can select and set the country for the Access Point, and choose to enable or disable the 5GHz and 2.4GHz radios.

Country Code: select your country from the drop-down list.
5 GHz Radio: select **Disable** or **Enable** for the 5GHz radio.
2.4 GHz Radio: select **Disable** or **Enable** for the 2.4GHz radio.
Click on the **Apply** button to confirm and save the changes.

4.5.2   802.11a

Click on the **802.11a** link on the navigation bar. On this page you can configure the 802.11a settings.

SSID: enter the SSID of the wireless network. 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, and is case-sensitive.
Suppress SSID: place a check in this box if you would like the SSID to be hidden from other Access Points or a site survey.
Wireless Mode: select a data rate from the drop-down menu. One option is 54Mbps and the other is 108Mbps in turbo mode.
Radio Frequency: select a radio frequency from the drop-down list. **SmartSelect** is the default setting.

Security: place a check is this box if you would like to use **WPA** only. If you would like to configure a more detailed security, click on the **Edit Security Setting** button. This option is described in the next section.

Data Rate: select a data rate from the drop-down list; by default **Best** is selected.

Transmit Power: select a transmit power from the drop-down list; by default **full** is selected.

Antenna Diversity: select **Best**, **1** or **2** from the drop-down list.

Beacon Interval (20-1000): enter a value between 20 and 1000 for the beacon interval. Beacons announce the existence for the 802.11 networks at regular intervals.

Data Beacon Rate DTIM (1-16384): enter the data beacon rate, the default rate is 1.

Fragment Length (256-2346): enter a value between 256 and 2346 for the fragment length.

RTS/CTS Threshold (256-2346): enter a value between 256 and 2346 for the RTS/CTS threshold. Any packet in the RTS/CTS handshake larger than the specified size will be discarded.

Click on the **Apply** button to confirm and save the changes.

4.5.2.1   Security Setting

Security Mode: select a security mode; options available are **Disabled**, **Pre-shared Key**, or **Dynamic**.

Key Entry Method: select a type of key method; options available are **Hexadecimal** or **Ascii Text**.

Default Shared Key: select a default-shared key, and then enter the key in the **Encryption Key** text box. From the **Key Length** drop down list, select **none**, **64-bit**, **128-bit** or **152-bit**.

Access Control List: select Enable or Disable for MAC access control lists. Then click on the **Edit ACL Settings** button.

4.5.2.2   Security Server Settings

RADIUS Server

Domain Name Server IP Address	[ ] . [ ] . [ ] . [ ]
Domain Name Server	[ ]
RADIUS Server	[ ]
RADIUS Port	[1812]
RADIUS Secret	[ ]
5GHz Key Source	Local ☑ Remote ☐

BACK   HELP APPLY CANCEL

Domain Name Server IP address: enter the IP address of the domain name server.

Domain Name Server: enter the name of the domain name server.

RADIUS Server: enter the IP address of the RADIUS server.

RADIUS Port: enter the port of the RADIUS server.

RADIUS Secret: enter the password of the RADIUS server.

5GHz Key Source: select a location of the RADIUS key. **Local** specifies that the RADIUS key is located in the AP. **Remote** specifies that the RADIUS key is located in the RADIUS server.

Click on the **Apply** button to confirm and save the changes.

4.5.2.3   ACL Settings

To delete an existing MAC ACL, click on the **Delete** button.
Click on the **Add** button to add another MAC ACL.

Add New ACL

MAC Address: enter the MAC address.
ACL Type: select an ACL type from the drop-down list. Options available are **Allow, Deny, Default Shared Key, 64-bit, 128-bit** or **152-bit.**
Unique Key: this is only required if a unique key is used in the ACL type.
Click on the **Apply** button to confirm and save the changes.

4.5.3   802.11g

Click on the **802.11g** link on the navigation bar. On this page you can configure the 802.11g settings.

SSID: enter the SSID of the wireless network. 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, and is case-sensitive.

Suppress SSID: place a check in this box if you would like the SSID to be hidden from other Access Points or a site survey.

Wireless Mode: select a data rate from the drop-down menu. One option is 11Mbps and the other is 54Mbps.

Radio Frequency: select a radio frequency from the drop-down list. **SmartSelect** is the default setting.

Security: place a check is this box if you would like to use **WPA** only. If you would like to configure a more detailed security, click on the **Edit Security Setting** button. This option is described in the next section.

Data Rate: select a data rate from the drop-down list; by default **Best** is selected.

Transmit Power: select a transmit power from the drop-down list; by default **full** is selected.

Antenna Diversity: select **Best**, **1** or **2** from the drop-down list.

Beacon Interval (20-1000): enter a value between 20 and 1000 for the beacon interval. Beacons announce the existence for the 802.11 networks at regular intervals.

Data Beacon Rate DTIM (1-16384): enter the data beacon rate; the default rate is 1.

Fragment Length (256-2346): enter a value between 256 and 2346 for the fragment length.

RTS/CTS Threshold (256-2346): enter a value between 256 and 2346 for the RTS/CTS threshold. Any packet in the RTS/CTS handshake larger than the specified size will be discarded.

Short Preamble: use this radio button to specify short preamble usage. When **Enable** is selected, both short and long preambles are used. When **Disable** is selected only long preambles are used.

Allow 2.4GHz 54Mbps Stations Only: use this radio button to Enable or Disable the association of 2.4GHz Mbps station only.

Protection Mode: select a protection mode from the drop-down list for the CTS operation mode. By default, **auto** is selected.

Protection Rate: select a protection rate from the drop-down list for the CTS operation. By default, **11Mbps** is selected.

Protection Type: Select a **CTS-only** or **RTS-CTS** radio button. By default, **CTS-only** is selected.

Short Slot Time: use this radio button to **Enable** or **Disable** short time slot usage.

Click on the **Apply** button to confirm and save the changes.

4.5.3.1   Security Setting

Security Mode: select a security mode; options available are **Disabled**, **Pre-shared Key**, or **Dynamic**.

Key Entry Method: select a type of key method; options available are **Hexadecimal** or **Ascii Text**.

Default Shared Key: select a default-shared key, and then enter the key in the **Encryption Key** text box. From the **Key Length** drop down list, select **none**, **64-bit**, **128-bit** or **152-bit**.

Access Control List: select Enable or Disable for MAC access control lists. Then click on the **Edit ACL Settings** button.

4.5.3.2   Security Server Settings

RADIUS Server

Domain Name Server IP Address	⬜ . ⬜ . ⬜ . ⬜
Domain Name Server	
RADIUS Server	
RADIUS Port	1812
RADIUS Secret	
5GHz Key Source	Local ☑ Remote ☐

BACK   HELP APPLY CANCEL

Domain Name Server IP address: enter the IP address of the domain name server.

Domain Name Server: enter the name of the domain name server.

RADIUS Server: enter the IP address of the RADIUS server.

RADIUS Port: enter the port of the RADIUS server.

RADIUS Secret: enter the password of the RADIUS server.

5GHz Key Source: select a location of the RADIUS key. **Local** specifies that the RADIUS key is located in the AP. **Remote** specifies that the RADIUS key is located in the RADIUS server.

Click on the **Apply** button to confirm and save the changes.

4.5.3.3   ACL Settings

2.4GHz ACl

MAC Address	ACL Type	
00:11:22:33:44:55	allowed with default shared key	Delete
11:22:33:44:55:66	denied	Delete

BACK   HELP ADD

To delete an existing MAC ACL, click on the **Delete** button.

Click on the **Add** button to add another MAC ACL.

Add New ACL

MAC Address: enter the MAC address.
ACL Type: select an ACL type from the drop-down list. Options available are
Allow, Deny, Default Shared Key, 64-bit, 128-bit or **152-bit.**
Unique Key: this is only required if a unique key is used in the ACL type.
Click on the **Apply** button to confirm and save the changes.

4.6   Statistics

Click on the **Statistics** link on the navigation bar, you will then see two options:
5GHz Statistics and 2.4GHz Statistics.   Each one is described in detail below.

4.6.1 5 GHz Statistics

Click on the **5GHz Statistics** link on the navigation bar. You will then see a list
of stations that are currently part of the BSS.

Click on the MAC address to view detailed statistics.

5GHz BSS Stats
5GHz AP is up
Wireless Mode: 5GHz 54Mbps (802.11a)

Authentication Type		Encryption	Cipher Advertised
Open System		no	None

Authentication	Deauthentication	Association	Disassociation	Reassociation
0	0	0	0	0

	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	0	0	16551
Transmit	343	325	343	18	0	0

Receive Errors	Discarded Frames	Duplicate Frames	CRC Errors	Decrypt Errors	PHY Errors	DMA Errors
16551	0	0	0	0	16551	0

Transmit Errors	Discarded Frames	Excessive Retries	DMA Errors
0	2	0	0

4.6.2   2.4 GHz Statistics

Click on the **2.4GHz Statistics** link on the navigation bar. You will then see a list of stations that are currently part of the BSS.

2.4GHz Statistics

This shows the Access Point and the stations that are currently part of the BSS.

ID	MAC Address	State
AP	00:02:6F:BE:F0:F6	up

Click on the MAC address to view detailed statistics.

2.4GHz BSS Stats
2.4GHz AP is up
Wireless Mode: 2.4GHz 54Mbps (802.11g)

Authentication Type		Encryption	Cipher Advertised
Open System		no	None

Authentication	Deauthentication	Association	Disassociation	Reassociation
7	9	7	3	0

	MSDU	Data	Multicast	Management	Control	Errors
Receive	817603	292	99	817311	0	3058529
Transmit	12501	318	329	19700	0	7523

Receive Errors	Discarded Frames	Duplicate Frames	CRC Errors	Decrypt Errors	PHY Errors	DMA Errors
3058529	10	10	223954	0	2834575	0

Transmit Errors	Discarded Frames	Excessive Retries	DMA Errors
7523	7518	7523	0

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.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

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