# Dual Band Wireless Access Point

# **User's Manual**

Version: 1.0

# **Table of Contents**

Chapter 1 – Introduction 1.1 Features & Benefits 1.2 Package Contents	4 4 5
Chapter 2 – Understanding the Hardware	5
2.1 Hardware Configuration	5
2.2 Hardware Installation	5
Chapter 3 – PC Configuration	5
3.1 TCP/IP Configuration	5
3.2 Wireless LAN Configuration	7
	_
Chapter 4 – web Configuration	8
4.1 Logging In	8
4.2 Getting Familiar with the GUI	9
4.3 System.	9
4.3.1 Administrator Settings	9
4.3.2 Firmware Upgrade	10
4.3.3 Configuration Loois	10
4.3.4 Factory Defaults	11
4.4 LAN	12
4.5 WIREless.	12
4.5.1 General	12
4.5.2 802.118	13
4.5.2.1 Security Setting.	14
4.5.2.2 Security Server Settings	15
4.5.2.5 ACL Settings	10
4.5.3 802. I Ty	10
4.5.3.1 Security Settings	19
4533 ACI Settings	20
46 Statistics	20
4 6 1 5GHz Statistics	
462 24GHz Statistics	

## 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.

eneral	Authenticatio	n Ad	vanced				
Connec	st using:						
B 🦉	roadcom 440	: 10/10	0 Integrat	ed Cont	roller		
						Configure.	
This c <u>o</u>	nnection uses	the foll	owing iten	ns:			
V 🖻	Client for Mic	rosoft N	Vetworks				
	File and Print	er Shar	rina for Mi	A thosos	Jetwor	ks	
	0 oS Packet	Sched	ular		10.110		
		JUNEU	uici				
		1.07.0					
2 7	Internet Prote	ocol (Ti	CP/IP)				
<b>•</b> *	Internet Prote	ocol (T(	CP/IP)				
<b>⊻</b> *	Internet Prot	ocol (T(	CP/IP)		F	<sup>o</sup> roperties	
	Internet Prote	ocol (T(	CP/IP) Uninstall		F	<sup>o</sup> roperties	(
	Internet Prote		CP/IP)		F	P <u>r</u> operties	(
Desc Uran	nstall	ol Proto	CP/IP)	et Proto	F	<sup>p</sup> roperties he default	ĺ
Desc Tran wide	nstall ription smission Contri area network sc diverse inter	ocol (T(	CP/IP)	et Proto vides co	F col. T mmuni	P <u>r</u> operties he default ication	i i
Desc     Tran     wide     acro	Internet Prote nstall ription smission Contr area network ss diverse inter	ocol (T ( ol Proto protoco connec	CP/IP)	et Proto vides co orks.	F Icol. Ti mmuni	<sup>p</sup> roperties he default ication	t
Desc Tran wide acro	Internet Prote nstall ription smission Contr area network ss diverse inter	ocol (T( ol Proto protoco connec	CP/IP)	et Proto vides co orks.	F col. Ti mmuni	P <u>roperties</u> he default ication	í t
Desc     Tran     wide     acro     Sho	Internet Prote <u>n</u> stall ription smission Contr area network ss diverse inter <u>w</u> icon in notifi	ocol (T( ol Proto protoco connec cation a	CP/IP)	et Proto vides co orks.	F Icol. T mmuni	P <u>roperties</u> he default ication	í t
Tran wide acro	Internet Prote <u>n</u> stall smission Contr srea network ss diverse inter <u>w</u> icon in notifi	ol Proto protoco connec cation a	CP/IP)	et Proto vides co orks.	F Icol. Ti mmuni	P <u>r</u> operties he default ication	
Interview       Interview     Interview     Interview      Interview      Interview      In	Internet Prote <u>n</u> stall smission Contr srea network ss diverse inter <u>w</u> icon in notifi	ol Proto protoco connec cation a	DP/IP)	et Proto vides co orks.	F col. T mmuni	<sup>9</sup> roperties he default ication	i i
Desc     Tran     wide     acro     Sho	Internet Prote <u>n</u> stall ription smission Contr area networkt ss diverse inter <u>w</u> icon in notifi	ocol (T( ol Proto protoco connect cation a	CP/IP)	et Proto vides co orks.	F col. T mmuni	Properties he default ication	ĺ

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) Pro	operties 🛛 🛛 🛛 🥐 🔀
General	
You can get IP settings assigned a this capability. Otherwise, you need the appropriate IP settings.	automatically if your network supports d to ask your network administrator for tically
→ Use the following IP address:	
IP address:	192.168.1.2
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	N 1 2
<ul> <li>Obtain DNS server address a</li> <li>Use the following DNS server</li> </ul>	utomatically r addresses:
Preferred DNS server:	2 1 1
Alternate DNS server:	
	Ad <u>v</u> anced
	OK Cancel

- 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.

wireless - WLAN	Wireless Settings	×
Status Configural	tion Encryption Site_Survey About	
Profile Name:	wireless	NN
Network Name:	wireless	_
Network Type:	Access Point	
	Peer-to-Peer Channel: 1 💼 Defaults	
Power Save Mod	e: Off 💌	
Transmit Rate:	Fully Automatic	
8	OK Cancel <u>A</u> pply	

- 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.

Connect to 192	.168.1.1 🛛 🖓 🔀
	<b>G</b> E
Test	
<u>U</u> ser name:	🖸 admin 🕑
Password:	•••••
	Remember my password
	OK Cancel

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.

AN	Status		▲ I
Virelese	LAN		
	P	192.168.1.1	C
	Subnet Mask	255.255.255.0	C
$\frown$	Gateway	0000	
	MAC Address	00:02:6F:E0:00:17	
	Wireless 11a		<b>▲</b> Ď
A	SSID	Wireless Network	
	Channel	SmartSelect	
	Wireless MAC Address	00:02:6F:8E:FD:F5	
	Wireless 11g		
	SSID	Wireless Network	
	Channel	SmartSelect	
	Wireless MAC Address	00:02:6F:8E:FD:F6	
	System Information		
	System Up time	02:02:49	
	Firmware Version	1.1	
	Serial Number	123455789	
			2
			HELP

#### 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	admin	
Password	••••	
System Name		
Enable Telnet		

**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.

Firmware Upgrade	
Host Name	
User Name	
Password	
Image Path	
Image Name	
	HELP APPLY CANCEL

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.

Configuration Scrip	t
Host Name	
User Name	
Password	
Script Path	
Script Name	
	HELP APPLY CANCEL

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.

Restore Factor	y Default
To restore the factory be asked to confirm y	default settings of the Access Point, click on the "Restore" button. You will our decision.
	Restore
	BACK

#### 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.

LAN Settings	
IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 0
Default Gateway Address	0.0.0.0
	HELP APPLY CANCEL

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	UNITED STATES - US
5GHz Radio	◯ Disable
2.4GHz Radio	◯ Disable ⊙ Enable

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	Wireless Network
Suppress SSID	
Wireless Mode	5GHz 54Mbps (802.11a)
Radio Frequency	SmartSelect
Security	WPA-Only Edit Security Setting
Advanced Settings	
Data Rate	best 👻
Transmit Power	Full
Antenna Diversity	Best 💌
Beacon Interval (20 - 1000)	100
Data Beacon Rate (DTIM) (1 - 16384)	1
Fragment Length (256 - 2346)	2346
RTS/CTS Threshold (256 - 2346)	2346

**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	💽 Disa	ıbled 🔘 Pre-shared Key 🔘 Dynamic
Security Server		dit Security Server Settings
	Key Entry Method	⊙ Hexadecimal ○ Ascii Text
Default Shared ≺ey	Encryption Key	Key Length
01.		None
O 2. [		None
O 3.		None
04.		None 64 bit (10 hex digits/ 5 ascii keys) 128 bit (26 hex digits/13 ascii keys) 152 bit (32 hex digits/16 ascii keys)
Accore	Control List: Disable	Edit ACL Settings

Security Mode: select a security mode; options available are Disabled, Preshared 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

Domain Name Server IP Address				
Domain Name Server				
RADIUS Server				
RADIUS Port	1812			
RADIUS Secret				
5GHz Key Source	Local 🗹	Remote 🔲		
			?	

**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

GHz ACI		
MAC Address	ACL Type	
00:11:22:33:44:55	allowed	Delete
22:33:44:55:66:77	denied	Delete
33:44:55:66:77:88	allowed with default shared key	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

5GHz New ACL	
MAC Address	55:66:77:88:99:11 (MAC Address format: aa:bb:co:dd:ee:ff)
ACL Type	Allow
Unique Key	(If unique key is used in ACL type)
BACK	HELP APPLY CANCEL

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	Wireless Network
Suppress SSID	
Wireless Mode	2.4GHz 54Mbps (802.11g) 💌
Radio Frequency	SmartSelect
Security	WPA-Only Edit Security Setting
Advanced Settings	
Data Rate	best 👻
Transmit Power	Full
Antenna Diversity	Best 💌
Beacon Interval (20 - 1000)	100
Data Beacon Rate (DTIM) (1 - 16384)	1
Fragment Length (256 - 2346)	2346
RTS/CTS Threshold (256 - 2346)	2346
Short Preamble	ODisable OEnable
Allow 2.4GHz 54Mbps Stations Only	⊙Disable ○Enable
Protection Mode	Auto 💌
Protection Rate	11 Mbps 💌
Protection Type	⊙ CTS-only ORTS-CTS
Short Slot Time	O Disable 💿 Enable

**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	<ul> <li>Disa</li> </ul>	abled 🔘 Pre-shared Key 🔘 Dynamic	
Security Server		Edit Security Server Settings	
	Key Entry Method	💿 Hexadecimal 🔘 Ascii Text	
Default Shared Key	Encryption Key	Key Length	
01.		None	~
O 2.		None	~
O 3.		None	~
0 4.		None 64 bit (10 hex digits/ 5 ascii keys) 128 bit (26 hex digits/13 ascii keys) 152 bit (32 hex digits/16 ascii keys)	

Security Mode: select a security mode; options available are Disabled, Preshared 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 ACI		
MAC Address	ACL Type	
00:11:22:33:44:55	allowed with default shared key	Delete
<u>11:22:33:44:55:66</u>	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 format: aa:bb:cc:dd:ee:ff)
ACL Type	Deny
Jnique Key	

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.

5GHz Stati	stics						
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:F5	up					

	Authent Ope	ication n System	Гуре I		no no	Cipher Adv Non	ertised
uthentical	tion Dea	uthenti	cation Asso	ciation	Disassociat	ion Reass	ociation
0		0		0	0		0
	MSDU	Data	Multicast	Mai	nagement	Control	Errors
leceive	0	0	0		0	0	16551
ransmit	343	325	343		18	0	0
Receive Errors	Discard Frame	ed s	Duplicate Frames	CRC Errors	Decrypt Errors	PHY Errors	DMA Errors
16551	0		0	0	0	16551	0

Click on the MAC address to view detailed statistics.

### 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 2.4GHz <sup>Wireless Mod</sup>	BSS S AP is de: 2.4GHz Authen Ope	Stats UP 54Mbps ication n System	(802.11g) [ype		Encryption NO	Cipher Ad Noi	<b>vertised</b> ne
Authentical	tion Dea	uthentic	ation Ass	ociation	Disassocial	tion Reas	sociation
7		9		7	3		0
	MSDU	Data	Multicast	: Ma	nagement	Control	Errors
Receive	817603	292	99		817311	0	3058529
Transmit	12501	318	329		19700	0	7523
Receive	Discarde	ed Di	unlicate	CRC	Decrypt	рну	DMA
Errors	Frame	5 F	rames	Errors	Errors	Errors	Errors
3058529	10		10	223954	0	2834575	0
Transı Frror	nit 's	Dis	scarded rames		Excessive Retries		DMA
7523	3		7518		7523		0

Click on the MAC address to view detailed statistics.

#### **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.