# 802.11b/g/n Wireless iNIC Module

**User's Guide** 

### **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.

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.

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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

#### **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.

#### **IMPORTANT NOTE:**

This module is intended for OEM integrator. The OEM integrator is still responsible for the FCC compliance requirement of the end product, which integrates this module.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the FCC radiation exposure limits set forth for an population/uncontrolled environment can be satisfied.

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

### USERS MANUAL OF THE END PRODUCT:

In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. If the size of the end product is smaller than 8x10cm, then additional FCC part 15.19 statement is required to be available in the users manual: This device complies with Part 15 of 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.

### LABEL OF THE END PRODUCT:

The final end product must be labeled in a visible area with the following " Contains TX FCC ID:U4P-E45 ". If the size of the end product is larger than 8x10cm, then the following FCC part 15.19 statement has to also be available on the label: This device complies with Part 15 of 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.

# **Table of Content**

CHAPTER 1: INTRODUCTION
FEATURES
CHAPTER 2: ABOUT THE OPERATION MODES
ACCESS POINT MODE
CHAPTER 3: CONFIGURATION
LOGIN8CONFIGURATION VIA WEB10INTERNET SETTINGS10WIRELESS SETTINGS12ADMINISTRATION23
CHAPTER 4: PC CONFIGURATION
Overview27WINDOWS CLIENTS27MACINTOSH CLIENTS32LINUX CLIENTS32OTHER UNIX SYSTEMS32WIRELESS STATION CONFIGURATION33
APPENDIX A: TROUBLESHOOTING
OVERVIEW34GENERAL PROBLEMS34INTERNET ACCESS34WIRELESS ACCESS35
APPENDIX B: ABOUT WIRELESS LANS
BSS

# **Chapter 1: Introduction**

For easy configure and achieve stable wireless feature for household appliance and try to create a new application for Wi-Fi module. By MII interface, user could embed our module in projector, Set-Top BOX and Multimedia center etc.

# **Features**

- 1. Support the IEEE 802.11b/g/n standard, high speed date rate up to 300Mbps.
- High security with build-in Security: WEP 64/128 bits, WPA, WPA2, WPA Mixed, 802.1x Authenication.
- 3. Support AP, WDS and Client (Infrastructure) mode.
- 4. Advanced Quality of Service (QoS) 802.11e, WMM.
- 5. Easy configuration for home user setup.
- 6. MAC filtering for wireless.

# Chapter 2: About the Operation Modes

This device provides operational applications with **AP**, **WDS** and **Client** modes, which are mutually exclusive. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can use the web-based utility provided by the manufacturer as described in the following sections.

## **Access Point Mode**

When acting as an access point, this device connects all the stations (PC/notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the Access Point has the Internet connection.



## WDS Mode

The WDS (Wireless Distributed System) function lets this access point act as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools and so on. This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.



# **Client Mode**

If set to Client (Infrastructure) mode, this device can work like a wireless station when it's connected to a computer so that the computer can send packets from wired end to wireless interface.



# **Chapter 3: Configuration**

# Login

- 1. Start your computer. Connect an Ethernet cable between your computer and the device.
- 2. Make sure your wired station is set to the same subnet as the device, i.e. 198.245.80.123
- 3. Start your WEB browser. In the Address box, enter the following: http:// 198.245.80.211



4. Please enter the username "admin" and password "admin" for login.

<b>?</b>	This secure \	Web Site (at 198.245.80.211) i	equires you to log on.
20	Please type t	he User Name and Password.	
	<u>U</u> ser Name	admin	
	<u>P</u> assword	XXXXX	
	∏ <u>S</u> ave thi	s password in your password li:	st

The configuration menu is divided into three folders: Internet Settings, Wireless Settings, and Administration. Click on the desired setup item to expand the folder in the main navigation page. The setup pages covered in this utility are described below.

open all   close all Status Operation Mode Comparison Mode Comparison Operation Operation Operation Operation	Status		
	System Info		
	Firmware Version	5.5.1.6.1_B1_en_JP (Jun 20 2008)	
	System Up Time	Oday:3h:21m:16s	
	Operation Mode	Access Point Mode	٦.
	Local Network		
	Physical Address	00:E0:98:28:AA:DD	
	Local IP Address	198.245.80.211	
	Local Netmask	255.255.255.0	

# **Common Connection Types**

### **Cable Modems**

Туре	Details	ISP Data required
Dynamic IP	Your IP Address is	Usually, none.
Address	allocated automatically,	However, some ISP's may
	when you connect to you	require you to use a particular
	ISP.	Hostname, Domain name, or
		MAC (physical) address.
Static (Fixed) IP	Your ISP allocates a	IP Address allocated to you.
Address	permanent IP Address to	Some ISP's may also require
	you.	you to use a particular
		Hostname, Domain name, or
		MAC (physical) address.

## **DSL Modems**

Туре	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	<ul> <li>PPTP Server IP Address.</li> <li>User name and password.</li> <li>IP Address allocated to you, if Static (Fixed).</li> </ul>

# Other Modems (e.g. Broadband Wireless)

Туре	Details	ISP Data required
Dynamic	Your IP Address is allocated	None.
IP Address	automatically, when you	
	connect to you ISP.	
Static (Fixed)	Your ISP allocates a permanent	IP Address allocated to you.
IP Address	IP Address to you.	

# **Configuration via Web**

## **Operation Mode**

Select an operation mode then click **Apply** to enable the mode you preferred or click **Reset** button to discard current settings. Default operation mode is AP mode.

### **Operation Mode Configuration**

You can setup different modes to LAN and WLAN interface for bridging function.

Un Alsia una	k La stratt EAN anno aktiva ada tara direta ala indanafa sati ana taristana dika bakka ana aktiva dika 100 a. J
function is	s disabled. All the WAN related function and firewall are not supported. The
wireless r	mode is AP mode.
🔘 Adapter Mode	e:
In this mo	de, all Ethernet ports are bridged together and the wireless client will conne
to other ac	ccess point.
	Apply Beset

Operation Mode	
Access Point	When acting as an access point, this device connects all the stations (PC/notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the Access Point has the Internet connection.
Adapter Mode	If set to Client (Infrastructure) mode, this device can work like a wireless station when it's connected to a computer so that the computer can send packets from wired end to wireless interface.

# **Internet Settings**

# LAN (Local Area Network) Settings

### Local Area Network (LAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

IP Address	198.245.80.211	
Subnet Mask	255.255.255.0	
DHCP Type	Server 💌	
DHCP Start IP	198.245.80.100	
DHCP End IP	198.245.80.200	
DHCP Subnet Mask	255.255.255.0	
DHCP Lease Time	86400	

LAN Interface Setup		
IP Address	Shows the IP address of the device.	
Subnet Mask	Shows the subnet mask of the device.	
DHCP Type	<b>Disable</b> : Select to disable this device to distribute IP addresses.	
	<b>Server</b> : Select to enable this device to distribute IP Addresses (DHCP Server). And the following field will be activated for you to enter the starting IP Address.	
DHCP Start IP	The starting address of this local IP network address pool.	
DHCP End IP	The ending address of this local IP network address pool.	
<b>DHCP Subnet Mask</b>	Shows the DHCP subnet mask.	
<b>DHCP Lease Time</b>	Default settings are 86400 seconds.	
Apply	Click to save and apply the current settings.	
Refresh	Click to get the latest information.	

# **DHCP Clients**

### **DHCP Client List**

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

DHCP Clients		
MAC Address	IP Address	Expires in
00:E0:18:86:91:BF	198.245.80.100	22:31:02

DHCP Clients	
MAC Address	Shows the client MAC address information.
IP Address	Shows the client IP address information.
Expires in	Shows the expired time of the client.

# Wireless Settings Basic

### **Basic Wireless Settings**

This page is used to configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode 💌
Network Name(SSID)	0007406A0638
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Broadcast Network Name (SSID)	● Enable ○ Disable
BSSID	00E09828AADD
Frequency (Channel)	2472MHz (Channel 13) 👻
Wireless Distribution System(WDS	)
WDS Mode	Disable
HT Physical Mode	
Operating Mode	
Channel BandWidth	○ 20
Guard Interval	O long   Auto
MCS	Auto 💌
Reverse Direction Grant(RDG)	O Disable 💿 Enable
Extension Channel	2452MHz (Channel 9) 🖌
Aggregation MSDU(A-MSDU)	Disable      Enable
Auto Block ACK	O Disable O Enable
Auto Block ACK Decline BA Request	Disable      Enable     OEnable
Auto Block ACK Decline BA Request Other	Disable     Enable     Disable     Disable
Auto Block ACK Decline BA Request <b>Other</b> HT TxStream	O Disable      Enable

Wireless Network	
Radio On/Off	Click <b>Radio OFF</b> button to turn off the radio function.
Network Mode	Select <b>11 b/g mixed mode</b> , <b>11b onl</b> y, <b>11g only</b> or <b>11 b/g/n</b> <b>mixed mode</b> from the pull-down menu. Default setting is <b>11</b> <b>b/g/n mixed mode</b> .

Network Name (SSID)	A SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Multiple SSID 1~6	A multiple SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Broadcast Network Name(SSID)	<b>Enable</b> : This wireless AP will broadcast its SSID to stations. <b>Disable</b> : This wireless AP will NOT broadcast its SSID to stations. If stations want to connect to this wireless AP, this AP's SSID should be known in advance to make a connection.
BSSID	Shows the MAC address of the device.
Frequency (Channel)	Select Channel 1~13 or Auto Select from the pull-down menu.
Wireless Distribution	System(WDS)
WDS Mode	Select the mode from the pull-down menu, <b>Disable</b> , <b>Lazy Mode</b> , <b>Bridge Mode</b> or <b>Repeater Mode</b> .
HT Physical Mode	
Operating Mode	Select <b>Mixed Mode</b> or <b>Green Field</b> . Default setting is <b>Mixed</b> <b>Mode</b> .
<b>Channel Band Width</b>	Select <b>20</b> or <b>20/40</b> , default setting is <b>20/40</b> .
Guard Interval	Select Long or Auto, default setting is Auto.
MCS	Default setting is Auto. Or select form the pull-down menu 0~15, 32 or Auto.
<b>Reverse Direction</b> <b>Grant(RDG)</b>	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Enable</b> .
<b>Extension Channel</b>	Default setting is 2452MHz (Channel 9).
Aggregation MSDU (A-MSDU)	Select <b>Disable</b> or <b>Enable</b> , default setting is <b>Disable</b> .
Auto Block ACK	Select <b>Disable</b> or <b>Enable</b> , default setting is <b>Enable</b> .
<b>Decline BA Request</b>	Select <b>Disable</b> or <b>Enable</b> , default setting is <b>Disable</b> .
Other	
HT Tx Stream	Select 1 or 2 form the pull-down menu.
HT Rx Stream	Select 1 or 2 form the pull-down menu.
Apply	Click to save and apply the current settings.
Cancel	Click to discard the current settings.

# Advanced

# **Advanced Wireless Settings**

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

BG Protection Mode	Auto 💌
Basic Data Rates	Default(1-2-5.5-11 Mbps)
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
Short Preamble	O Enable 💿 Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ◯ Disable
Pkt_Aggregate	● Enable ○ Disable
IGMP Snooping	O Enable ③ Disable
Wi-Fi Multimedia	
VVMM Capable	💿 Enable 🔘 Disable
APSD Capable	O Enable 💿 Disable
WMM Parameters	WMM Configuration

Advanced Wirele	SS
BG Protection Mode	Select Auto, On or Off from the pull-down menu.
Basic Data Rates	By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: <b>1-2Mbps</b> , <b>Default (1-2-5.5-11Mbps)</b> , or <b>All(1-2-5,5-6-11-12-24Mbps.)</b>
Beacon Interval	Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon. Range 20- 999, default is <b>100</b> .
Data Beacon Rate (DTIM)	Range from 1 to 255, default setting is 1.
Fragment Threshold	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If the 802.11g MIMO Wireless Device often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is <b>2346</b> .

RTS Threshold	RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. If the "Hidden Node" problem is an issue, please specify the packet size. <u>The RTS mechanism will be activated if the data size exceeds the value you set.</u> The default value is 2347.
	<b>Warning:</b> Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.
	This value should remain at its default setting of <b>2347</b> . Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Short Preamble	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Disable</b> . A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter.
Short Slot	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Enable</b> .
Tx Burst	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Enable</b> .
Pkt_Aggregate	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Enable</b> .
IGMP Snooping	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Disable</b> .
Wi-Fi Multimedia	
WMM Capable	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Enable</b> .
APSD Capable	Select <b>Disable</b> or <b>Enable</b> this function, default setting is <b>Disable</b> .
WMM Parameters	Click the <b>WMM Configuration</b> button to go further settings.
Apply	Click to save and apply the current settings.
Cancel	Click to discard the current settings.

# Security

## **Wireless Security Settings**

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID choice	0007406A0638 🕶	
Security Mode "000740	6A0638"	
Security Mode	Disable	

Select SSID				
SSID choice	Select the SS	SID form the pull-	-down menu for secu	rity settings.
Security Mode	There are set Open, Shar PSK, WPA-	veral types of auti ed, WEP Auto, V ·PSK/WPA2-PSI	hentication modes ind VPA, WPA-PSK, W K, WPA/WPA2 and	cluding <b>Disable</b> , /PA2, WPA2- 802.1X.
	Disable			
	Wireless This page allows Keys could preve	Security Setting s you to setup the wireless ent any unauthorized acces	S security. Turn on WEP or WPA I ss to your wireless network.	by using Encryption
	Select SSID			
	SSID choice	000	07406A0638 💌	
	Security Mode	"0007406A0638"		
	Security Mode	Dis	sable 💌	
		Apply	Cancel	
	<b>Disable:</b> En	cryption is set to	<b>Disable</b> by default. T	There is no security
	be set when		.d.	
	ODEN GU		TO	
	OPEN, SHA	ARED, WEP AU	10	
	Security Mode	"0007406A0638"		
	Security Mode		EN 💌	
	Wire Equivalence	Protection (WEP)		
	Default Key		Key1 💌	
		WEP Key 1 :		Hex 💌
	WEP Keys	WEP Key 2 :		Hex 💌
		WEP Key 3 :		Hex 💌
		WEP Key 4 :		Hex 💌
		Apply	Cancel	
	<b>Open</b> : If you the wireless	ır wireless device adapter will need	is using " <b>Open</b> " aut to be set to the same	hentication, then authentication
	type.			
	Shared: Sha secret key.	red key is when b	both the sender and th	ne recipient share a
	WEP Auto: WEP keys e make the RA	If <b>WEP</b> encrypti either manually or ADIUS server to is	on is selected, users we select to <b>Use 802.1x</b> ssue the WEP key dy	will have to <b>Set</b> Authentication to mamically.
	<b>Default Key</b> computers, a key when m	y: There are four laccess points, an aking a connection	keys 1~4 that you ca d wireless adapters = n.	n select at will. All must use the same

<b>WEP Key 1~4:</b> Enter the password in the encryption key field that the encryption key number must match the selected key.
• Hexadecimal (128bits): 26 Hex characters (0~9, a~f).

• ASCII (128bits): 13 ASCII characters.

## WPA

On a with Marda	
Security Mode	
WPA	
WPA Algorithms	⊙ TKIP ○ AES
32.	
Radius Server	
IP Address	
Port	1812
Shared Secret	
	Apply Cancel

security and provides stronger data protection and network access control than WEP. Most wireless networks should use either WEP or WPA security. If **WPA** is selected, please select **WPA Algorithms** for **TKIP** or **AES**. Then enter **Port**, **IP address** and **Shared Secret** for **Enterprise** (**RADIUS Server**) authentication mode. RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

**IP Address:** Enter the RADIUS Server's IP Address provided by your ISP.

**Port:** Enter the RADIUS Server's port number provided by your ISP. The default is **1812**.

**Shared Secret:** Enter the password that the device shares with the RADIUS Server.

### WPA-PSK

Security Mode	WPA-PSK
wpa	
WPA Algorithms	● TKIP ○ AES
Pass Phrase	

serves as a password. Users may key in 8 to u select Passphrase to set the passwords or he 802.1x Authentication will be activated. word is used on client's end.
WPA2
WPA2
WPA2     TKIP • AES   TKIP/AES   Disable • Enable     1812   1812   ply • Cancel   t TKIP, AES or TKIP/AES for the WPA
TKIP • AES   TKIP/AES   Disable • Enable     1812   1812   ply • Cancel   t TKIP, AES or TKIP/AES for the WPA
○ TKIP ⊙ AES         ○ TKIP/AES         ○ Disable ○ Enable         1812         1812         ply       Cancel         t TKIP, AES or TKIP/AES for the WPA
Disable O Enable   Image: Disable O Enable     1812     1812     ply     Cancel   t TKIP, AES or TKIP/AES for the WPA
1812    ply    Cancel   t TKIP, AES or TKIP/AES for the WPA
1812         1919         Cancel         t <b>TKIP, AES</b> or <b>TKIP/AES</b> for the WPA
1812         ply       Cancel         t TKIP, AES or TKIP/AES for the WPA
ply Cancel t <b>TKIP, AES</b> or <b>TKIP/AES</b> for the WPA
ply Cancel t <b>TKIP, AES</b> or <b>TKIP/AES</b> for the WPA
<ul> <li>aly valid under WAP2-RADIUS</li> <li>anost important features beyond WPA to</li> <li>bugh 802.11i/ WPA2 are: pre-authentication,</li> <li>croaming without noticeable signal latency.</li> <li>les a way to establish a PMK security</li> <li>t associates. The advantage is that the client</li> <li>disconnected to the network.</li> <li>S is an authentication, authorization and</li> <li>protocol. The client is a Network Access</li> <li>nenticate its links. The server is a server that</li> </ul>
ADIUS Server's IP Address provided by
Server's port number provided by your ISP.
password that the device shares with the

Security Mode "00	07406A0638"		
Security Mode	V	VPA2-PSK	*
WPA			
WPA Algorithms		) TKIP ③ AES ) TKIP/AES	
Pass Phrase			
WPA Algorith	Apply ms: Select TH	Cance Cance Cance	el <b>er</b> ' <b>KIP/AES</b> for
63 characters st leave it blank, i Make sure the s	ring if you set n which the 8 ame password	ect Passphrase 02.1x Authent 1 is used on cli	to set the pas ication will be ent's end.
WPA/WPA2 Security Mode "00	07406A0638"		
Security Mode	V	/PA/WPA2	*
NAME A			
WPA		) TKIP	
WPA WPA Algorithms Radius Server		) TKIP ③ AES ) TKIP/AES	
WPA Algorithms           Radius Server           IP Address		) TKIP ③ AES ) TKIPIAES	
WPA Algorithms           Radius Server           IP Address           Port		) TKIP ③ AES ) TKIP/AES	
WPA WPA Algorithms Radius Server IP Address Port Shared Secret		) TKIP ③ AES ) TKIP/AES 312	
WPA WPA Algorithms Radius Server IP Address Port Shared Secret	Apply	) TKIP   AES ) TKIPIAES	2
WPA WPA Algorithms Radius Server IP Address Port Shared Secret WPA Algorith Algorithms.	Apply ms: Select TH	TKIP • AES TKIPIAES	۶ <b>KIP/AES</b> for
WPA WPA Algorithms Radius Server IP Address Port Shared Secret WPA Algorithm Algorithms. Radius Server Server that desi has access to a t	Apply MR: Select TH RADIUS is a nt-server proto- res to authenti- user database	TKIP • AES TKIP/AES	T <b>KIP/AES</b> for on, authorizati t is a Network The server is a ation informat
WPA WPA Algorithms Radius Server IP Address Port Shared Secret WPA Algorithm Algorithms. Radius Server: accounting client Server that desi has access to a to IP Address: En your ISP.	Apply Apply ms: Select TH RADIUS is a at-server proto- res to authenti- user database atter the RADI	TKIP • AES TKIP/AES	<b>KIP/AES</b> for on, authorizati t is a Network The server is a ation informat Address prov
WPA WPA Algorithms Radius Server IP Address Port Shared Secret WPA Algorith Algorithms. Radius Server accounting clier Server that desi has access to a the IP Address: En your ISP. Port: Enter the The default is 1	Apply Apply ms: Select TI a RADIUS is a nt-server protocol res to authenti- user database atter the RADI RADIUS Ser 812.	TKIP • AES TKIP/AES	<b>KIP/AES</b> for on, authorizati t is a Network The server is a ation informat Address prov ber provided b

	802.1X	
	Coourth Mode "000740640620"	
	Security Mode	802.1×
	802.1x WEP	
	WEP	O Disable O Enable
	Radius Server	
	IP Address	
	Port	1812
	Shared Secret	
	Арр	ly Cancel
	802.1x WEP: Select Disa	ble or <b>Enable</b> to use 802.1x authentication
	to make the RADIUS serv	er to issue the WEP key dynamically.
	Radius Server: RADIUS accounting client-server pr	is an authentication, authorization and otocol. The client is a Network Access
	Server that desires to authors has access to a user databa	enticate its links. The server is a server that se with authentication information.
	<b>IP Address:</b> Enter the RA your ISP.	DIUS Server's IP Address provided by
	<b>Port:</b> Enter the RADIUS ST The default is <b>1812</b> .	Server's port number provided by your ISP.
	Shared Secret: Enter the RADIUS Server.	password that the device shares with the
Apply	Click to save and apply the	e current settings.
Cancel	Click to discard the curren	t settings.

# Wi-Fi Protected Setup

This page is used to setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

Apply         WPS Summary         WPS Current Status:       Idle         WPS Configured:       No         WPS SSID:       0007406A0638         WPS Auth Mode:       Open         WPS Lencrypt Type:       None         WPS Default Key Index:       1         WPS Key(ASCII)       AP PIN:         APP IN:       26651811         WPS mode       Image: PIN Image:	WPS:	Enable 💌	
WPS Summary         WPS Current Status:       Idle         WPS Configured:       No         WPS SSID:       0007406A0638         WPS Auth Mode:       Open         WPS Auth Mode:       Idle         WPS Encrypt Type:       None         WPS Default Key Index:       1         WPS Key(ASCII)       AP PIN:         AP PIN:       26651811         WPS mode       Image: PIN PBC         PIN       Image: PIN         Apply       Image: PIN PBC         WPS Status       Image: PIN PBC	Apply	1	
WPS Current Status:       Idle         WPS Configured:       No         WPS SSID:       0007406A0638         WPS Auth Mode:       Open         WPS Encrypt Type:       None         WPS Default Key Index:       1         WPS Key(ASCII)       AP PIN:         26651811       Reset OOB         WPS mode       Image: PIN         PIN       PBC         PIN       PIN         Apply       MPS Status	WPS Summary		
WPS Configured:       No         WPS SSID:       0007406A0638         WPS Auth Mode:       Open         WPS Encrypt Type:       None         WPS Default Key Index:       1         WPS Key(ASCII)       AP PIN:         AP PIN:       26651811         WPS mode       Image: PIN         PIN       PBC         PIN       PBC         PIN       PBC         PIN       WPS Status	WPS Current Status:	Idle	
WPS SSID:     0007406A0638       WPS Auth Mode:     Open       WPS Encrypt Type:     None       WPS Default Key Index:     1       WPS Key(ASCII)     AP PIN:       AP PIN:     26651811       WPS Progress     WPS mode       PIN     PBC       PIN     Apply	WPS Configured:	No	
WPS Auth Mode: Open WPS Encrypt Type: None WPS Default Key Index: 1 WPS Key(ASCII) AP PIN: 26651811 Reset OOB WPS Progress WPS mode	WPS SSID:	0007406A0638	
WPS Encrypt Type: None WPS Default Key Index: 1 WPS Key(ASCII) AP PIN: 26651811  Reset OOB  WPS Progress WPS mode PIN PIN PIN PIN PIN WPS Status	WPS Auth Mode:	Open	
WPS Default Key Index:       1         WPS Key(ASCII)	WPS Encrypt Type:	None	
WPS Key(ASCII) AP PIN: 26651811 Reset OOB WPS Progress WPS mode   PIN  PBC PIN Apply WPS Status	WPS Default Key Index:	1	
AP PIN: 26651811          Reset OOB         WPS Progress         WPS mode         Image: PIN         PIN         Apply         WPS Status	WPS Key(ASCII)		
Reset OOB         WPS Progress         WPS mode         Image: PIN         PIN         Apply         WPS Status	AP PIN:	26651811	
WPS mode   PIN O PBC  PIN  Apply  WPS Status	WPS Progress		
PIN	WPS mode	● PIN ○ PBC	
Apply WPS Status	PIN		
WPS Status	Apply		
wps status			
	WPS Status		

WPS Configuration		
WPS	Select Enable or Disable from the pull-down menu.	
Apply	Click to save and apply the current settings.	
WPS Summary	Here shows the WPS function status.	
Reset OOB	Click the button to reset the settings.	
WPS Process		
WPS mode	Select <b>PCB</b> or <b>PIN</b> WPS mode.	
PIN	Enter the <b>PIN</b> code form the registrar or enrollee to make a WPS connection with client.	
PBC	Select <b>PBC</b> then click <b>Apply</b> to make a WPS connection with client.	
Apply	Click to save and apply the current settings.	
WPS Status	Here shows the current status of the WPS function.	

# **Trusted Stations**

## **Trusted Stations Settings**

If you choose 'Rules for ACCEPT', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

Select SSID		
SSID choice		0007406A0638 💌
Trusted Stat	ions Policy "0007406Al	0638"
Trusted Stati	ons Policy	Disable
Station MAC /	Address	
	Reset	
Current Trus	ted Stations rules	2444
No.	Station Address	s Status
Delete S	elected Delete /	All Reset
Select SSID		
SSID choice	Select the SSID	from the pull-down menu.
Trusted Stations	Policy	
Trusted Stations Policy	Select <b>Disable</b> , <b>ACCEPT</b> form	Enable –Rules for DROP, or Enable –Rules for the pull-down menu.
Station MAC Address	Enter the MAC	address of the station.
Apply	Click to save an	d apply the current settings.
Reset	Press to discard	the current settings.
Current Trusted Stations rules	Here shows the	information of the trusted stations clients.
Delete Selected	Select the unwa Delete Selected	nted trusted station MAC addresses and then click the button to eliminate them.
Delete All	Click to delete a	Il the trusted station MAC addresses in the table.
Reset	Click to clear th	e current settings.

## **Station List**

Here shows the information of stations that connected with the AP.

#### Wireless Stations List

This page is used to monitor stations which associated to this AP here.

Active Clients	te	5 U		AU:	402 Q	
MAC Address	Tx Rate(Mbps)	MCS	BW	PhyMode	WMM	PSM

# **Administration**

### **User/ Password**

### System Account Management

You may configure administrator account and password here.

Administrator Settings			
Account	admin		
Password	••••		
	VlqqA	Cancel	

Administrator Settings		
Account	Enter the user name for managing this device. Maximum Input is 16 alphanumeric characters.	
Password	Enter the passwords for managing this device.	
Apply	Click to save and apply the current settings.	
Cancel	Click to discard the current settings.	

# System Log

You may Set or Show various system log messages here.		
_ Enable Log System all		
	Apply Changes	
Refrech Clear		

System Log Management		
Enable Log	nable Log         Check the box to enable this function.	
System all	Check to show all system related log files.	
Apply Changes	Click this button to save the settings.	
Refresh	Click to renew the current log message.	
Clear	Click to remove current log message.	

# **Upload Firmware**

# **Upgrade Firmware**

This page allows you to upgrade this device's firmware to new version.

If you want to keep the current configuration, remember to backup the config file before upgrading firmware, and restore the config file after upgrading firmware.

Please note,  $\ensuremath{\text{DO NOT}}$  power off the device during this process because it may crash the system.

Update Firmware		
Location:		Browse
Apply	Reset	

Update Firmware		
Location	Click the <b>Browse</b> button, find and open the firmware file (the browser will display to correct file path).	
Apply	Click the Apply button to perform.	
Reset	Click Reset to restore to default values.	

# **Settings Management**

## **Settings Management**

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Export Button	Exp	ort
mport Settings		
Settings file location		Browse
	Import	Cancel
Load Factory Defaults		
at massing and as		

Export Settings		
Export Button	Click the <b>Export</b> button to export the current device settings.	
Import Settings		
Settings file location	Click the <b>Browse</b> button, find and open the file that has been saved before. (The browser will display to correct file path).	
Import	Click the <b>Import</b> button to import the device settings.	
Cancel	Click to discard the current settings.	
Load Factory Defaults		
Load Default Button	Click to <b>Load Default</b> button to set the device back to factory default settings.	

# **Statistics**

This screen displays the transmission and reception statistics on your current networks.

### Statistic

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Memory	
Memory total:	12844 kB
Memory left:	2680 kB
LAN	
LAN Rx packets:	904
LAN Rx bytes:	111074
LAN Tx packets:	4765
LAN Tx bytes:	2046455
WLAN	
WLAN Rx packets:	66
WLAN Rx bytes:	3547
WLAN Tx packets:	0
WLAN Tx bytes:	3501216

# **Chapter 4: PC Configuration**

# **Overview**

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

## Windows Clients

- This section describes how to configure Windows clients for Internet access via the Wireless Device.
- The first step is to check the PC's TCP/IP settings.
- The Wireless Device uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

### **TCP/IP Settings - Overview**

# If using default Wireless Device settings, and default Windows TCP/IP settings, no changes need to be made.

- By default, the Wireless Device will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

# If using a Fixed (specified) IP address, the following changes are required:

- The Gateway must be set to the IP address of the Wireless Device.
- The *DNS* should be set to the address provided by your ISP.

### **Checking TCP/IP Settings - Windows 2000**

- 1. Select Control Panel Network and Dial-up Connection.
- 2. Right click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

Local Area Connection	Properties		? ×
General			
Connect using:			
SMC EZ Card 10	)/100 (SMC1211T	X)	
,			Configure
Components checked a	are used by this c	onnection:	
🗹 🔜 Client for Micro	soft Networks		
File and Printer	Sharing for Micro	soft Network:	s
🔍 🗹 🍹 Internet Protoci	ol (TCP/IP)	)	
Install	Uninstall	( P	roperties
Install	Uninstall		
Install Description Transmission Control wide area network p across diverse interc	Uninstall Protocol/Internet rotocol that provid connected network	Protocol. Th les communic ks.	roperties ne default cation
Install Description Transmission Control wide area network p across diverse interc Show icon in taskb	Uninstall I Protocol/Internet rotocol that provie connected network ar when connected	Protocol. Th des communic ks.	roperties le default cation

- 3. Select the *TCP/IP* protocol for your network card.
- 4. Click on the *Properties* button. You should then see a screen like the following.

nternet Protocol (TCP/IP) Prop	erties ?
You can get IP settings assigned a this capability. Otherwise, you nee the appropriate IP settings.	automatically if your network supports d to ask your network administrator for
Obtain an IP address automa	atically
Use the following IP address	
IP address:	and the second sec
Subnet mask:	
Default gateway:	
Obtain DNS server address     Use the following DNS server	automatically v addresses:
Preferred DNS server:	
Alternate DNS server:	
	Advanced
	OK Cancel

5. Ensure your TCP/IP settings are correct, as described below.

### Using DHCP

- To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the Wireless Device will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Device.

### Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the Wireless Device's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Device.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

#### **Checking TCP/IP Settings - Windows XP**

- 1. Select Control Panel Network Connection.
- 2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

🕹 Local Area Connection Properties	? 🗙
General Authentication Advanced	
Connect using:	
B D-Link DFE-530TX PCI Fast Ethernet Adapter (rev.B)	
This connection uses the following items:	
<ul> <li>Client for Microsoft Networks</li> <li>Elie and Printer Sharing for Microsoft Networks</li> <li>Guos Packet Scheduler</li> </ul>	
Internet Protocol (TCP/IP)	
Install Uninstall Properties	$\supset$
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	
OK Car	ncel

- 3. Select the *TCP/IP* protocol for your network card.
- 4. Click on the *Properties* button. You should then see a screen like the following.

Internet Protocol (TCP/IP) Properties		
General Alternate Configuration		
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.		
Dtain an IP address automatically		
O Use the fellowing IP address.		
IP address:		
Sybnet mask:		
Default gateway:		
Ohtain DNS server address automatically		
Use the following UNS server addresses:		
Preferred DNS server:		
Alternate DNS server:		
Ad <u>v</u> anced		
OK Cancel		

5. Ensure your TCP/IP settings are correct.

### **Using DHCP**

- To use DHCP, select *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the Wireless Device will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Device.

### Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the Wireless Device's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Device.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

#### **Internet Access**

To configure your PCs to use the Wireless Device for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

### For Windows 2000

- 1. Select Start Menu Settings Control Panel Internet Options.
- 2. Select the Connection tab, and click the *Setup* button.
- 3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
- 4. Select "I connect through a local area network (LAN)" and click Next.
- 5. Ensure all of the boxes on the following Local area network Internet Configuration screen are **unchecked**.
- 6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
- 7. Click Finish to close the Internet Connection Wizard. Setup is now completed.

### For Windows XP

- 1. Select Start Menu Control Panel Network and Internet Connections.
- 2. Select Set up or change your Internet Connection.
- 3. Select the *Connection* tab, and click the *Setup* button.
- 4. Cancel the pop-up "Location Information" screen.
- 5. Click Next on the "New Connection Wizard" screen.
- 6. Select "Connect to the Internet" and click *Next*.
- 7. Select "Set up my connection manually" and click Next.
- 8. Check "Connect using a broadband connection that is always on" and click Next.
- 9. Click *Finish* to close the New Connection Wizard. Setup is now completed.

### Accessing AOL

To access AOL (America On Line) through the Wireless Device, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- 1. Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- 2. Click the *Setup* button.
- 3. Select *Create Location*, and change the location name from "New Locality" to "Wireless Device."
- 4. Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- 5. Click *Save*, then *OK*. Configuration is now complete.
- 6. Before clicking "Sign On", always ensure that you are using the "Wireless Device" location.

## **Macintosh Clients**

From your Macintosh, you can access the Internet via the Wireless Device. The procedure is as follows.

- 1. Open the TCP/IP Control Panel.
- 2. Select *Ethernet* from the *Connect via* pop-up menu.
- 3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
- 4. Close the TCP/IP panel, saving your settings.

#### Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Device Address* field to the Wireless Device's IP Address.
- Ensure your DNS settings are correct.

### Linux Clients

To access the Internet via the Wireless Device, it is only necessary to set the Wireless Device as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

#### Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Device.
- Ensure your DNS (Name server) settings are correct.

### To act as a DHCP Client (Recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

- 1. Start your X Windows client.
- 2. Select Control Panel Network
- 3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
- 4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
- 5. To apply your changes:
  - Use the "Deactivate" and "Activate" buttons, if available.
  - OR, restart your system.

### Other Unix Systems

To access the Internet via the Wireless Device:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Device.
- Ensure your DNS (Name Server) settings are correct.

# Wireless Station Configuration

- This section applies to all Wireless stations wishing to use the Wireless Device's Access Point, regardless of the operating system that is used on the client.
- To use the Wireless Station with Wireless Device, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to <i>Infrastructure</i> .
SSID (ESSID)	This must match the value used on the Wireless Device. The default value is <b>Untitled</b> .
	Ry default the security setting on the Wireless Device is <b>Disabled</b>
WED	<ul> <li>If security setting remains disabled on the Wireless Device, all</li> </ul>
W LI	<ul><li>If security setting is enabled on the Wireless Device, each station</li></ul>
	must use the same settings as the Wireless Device.
WPA WPA2 (AES) WPA2 Mixed	WPA (TKIP/AES)/ WPA2 (AES)/ WPA2 Mixed: If one of these securities is enabled on the Wireless Device, each station must use the same settings as the Wireless Device. If there is no security is enabled on the Wireless Device, the security of each station should be disabled as well.

Note: By default, the Wireless Device will allow both 802.11b and 802.11g connections.

# Appendix A: Troubleshooting



# **Overview**

This chapter covers some common problems that may be encountered while using the Wireless Device and some possible solutions to them. If you follow the suggested steps and the Wireless Device still does not function properly, contact your dealer for further advice.

# **General Problems**

Problem 1:	Can't connect to the Wireless Device to configure it.	
Solution 1:	Check the following:	
	• The Wireless Device is properly installed, LAN connections are OK, and it is powered ON.	
	• Ensure that your PC and the Wireless Device are on the same network segment. (If you don't have a device, this must be the case.)	
	• If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.	
	<ul> <li>If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 10.10.10.1 to 10.10.10.253 and thus compatible with the Wireless Device's default IP Address of 10.10.10.254.</li> <li>Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Device.</li> <li>In Windows, you can check these settings by using <i>Control Panel-Network</i> to check the <i>Properties</i> for the TCP/IP protocol.</li> </ul>	

# **Internet Access**

Problem 1:	When I enter a URL or IP address I get a time out error.
Solution 1:	A number of things could be causing this. Try the following troubleshooting
	steps.
	<ul> <li>Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.</li> <li>If the PCs are configured correctly, but still not working, check the Wireless Device. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)</li> <li>If the Wireless Device is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.</li> </ul>
Problem 2:	Some applications do not run properly when using the Wireless Device.
Solution 2:	The Wireless Device processes the data passing through it, so it is not
	transparent.
	Use the Special Applications feature to allow the use of Internet
	applications, which do not function correctly. If this does solve the problem
	you can use the DMZ function. This should work with almost every
	application, but:
	• It is a security risk, since the firewall is disabled.

• Only one (1) PC can use this feature.

# Wireless Access

Problem 1:	My PC can't locate the Wireless Device.	
Solution 1:	Check the following:	
	• Your PC is set to <i>Infrastructure Mode</i> . (Access Points are always in <i>Infrastructure Mode</i> .)	
	• The SSID on your PC and the Wireless Device are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".	
	• Both your PC and the Wireless Device must have the same setting for security. The default setting for the Wireless Device is disabled, so your wireless station should also have security setting disabled.	
	• If security setting is enabled on the Wireless Device, your PC must have it enabled, and the password or key must match.	
	• If the Wireless Device's <i>Wireless</i> screen is set to <i>Allow LAN access to selected Wireless Stations only</i> , then each of your Wireless stations must have been selected, or access will be blocked.	
	• To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Device. Remember that the connection range can be as little as 100 feet in poor environments.	
Problem 2:	Wireless connection speed is very slow.	
Solution 2:	The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:	
	• Wireless Device location. Try adjusting the location and orientation of the Wireless Device.	
	• Wireless Channel. If interference is the problem, changing to another channel may show a marked improvement.	
	• Radio Interference. Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.	
	• <b>RF Shielding</b> . Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Device.	

# **Appendix B:**

# About Wireless LANs



# BSS

### BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

### Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

### Security

Authentication methods include **Disable**, **Open**, **Shared**, **WEP Auto**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**, **WPA2-PSK**, **WPA1/WPA2** and **802.1X**. Once you choose your authentication, you then need to select the **Data Encryption** methods which may includes **WEP** Key, **Pass Phrase** and **Radius** Server settings.

### **Encryption**

Enabling **WEP** can protect your data from eavesdroppers. There are two levels of WEP Encryption: 64 bits and 128 bits. 64 bits WEP encryption requires enter 10 Hex characters as a "secret key", whereas 128 bits WEP requires users to enter 26 Hex characters as "secret key". **PASS PHRASE** is applicable only when you select to use WPA-PSK authentication. You will need to enter an 8~63 characters password to kick off the encryption process, which will generate four WEP keys automatically.

**RADIUS** setup is used to set up additional parameters for authorizing wireless clients through RADIUS server. The **RADIUS** setup is required when you select to use **Open System with 802.1x** or **WPA/WPA2** authentication.

### **Open, Shared, WEP auto**

With **Shared Key or Open System**, the Wireless Device can automatically change its authentication method to **Shared Key** or **Open System** depending on its client's setting. WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data that is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit.
Кеу	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match.
WEP Authentication	Open System or Shared Key.

### WPA/WPA2

WPA/WPA2 (Wi-Fi Protected Access) is more secure than WEP. It uses a "Shared Key" which allows the encryption keys to be regenerated at a specified interval. There are four encryption options: **TKIP**, **AES**, **TKIP-AES** and additional setup for **RADIUS** is required in this method.

### WPA-PSK/WPA2-PSK

WPA/WPA2 (Wi-Fi Protected Access using Pre-Shared Key) is recommended for users who are not using a RADIUS server in a home environment and all their clients support WPA/WPA2. This method provides a better security.

Encryption	WEP Key 1~4	Passphrase
TKIP		
AES	NOT REQUIRED	8-63 characters

### 802.1x

With **802.1x** authentication, a wireless PC can join any network and receive any messages that are not encrypted, however, additional setup for **RADIUS** to issue the WEP key dynamically will be required.

# Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	On client Wireless Stations, the mode must be set to "Infrastructure." (The Access Point is always in "Infrastructure" mode.)	
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to, but the SSID can not set to be null (blank).	
WEP	The Wireless Stations and the Access Point must use the same settings for WEP (Off, 64 Bit, 128 Bit). <b>WEP Key:</b> If WEP is enabled, the Key must be the same on the Wireless Stations and the Access Point. <b>WEP Authentication:</b> If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").	

# **Regulatory Approvals**

### **CE Standards**

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

### **CE Marking Warning**

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.