



# **802.11ac Wireless USB 3.0 Dongle**

## **USER MANUAL 1.0**

© 2013

# Contents

1.	Introduction.....	3
2.	Driver Installation .....	4
2.1	Windows 7 .....	4
3.	Wireless Network Configuration .....	6
3.1	Utility Icon.....	6
3.2	Client Mode .....	6
3.2.1	Wireless Device Control.....	6
3.2.2	General Setting .....	7
3.2.3	Profile Setting .....	8
3.2.4	Available Network Setting.....	9
3.2.5	Status .....	11
3.2.6	Statistics Page .....	13
3.2.7	Wi-Fi Protected Setup.....	14
4.	Access Point Mode .....	15
5.	Troubleshooting .....	19
6.	Glossary .....	20

# 1. Introduction

Thank you for your purchase of the WLAN Dongle. Featuring wireless technology, this wireless networking solution has been designed for both large and small businesses, and it is scalable so that you can easily add more users and new network features depending on your business scale.

## SYSTEM REQUIREMENTS

Windows System: XP 32/64, Vista 32/64, Win7 32/64, Win 8 32/64

PCs must have a device driver installed. It allows you to communicate with WLAN Dongle.

## BEFORE YOU START

### 1. Contents confirmation

Wireless LAN USB Dongle · Driver CD

## CONNECTING YOUR WLAN Dongle TO PC

2. Connect your WLAN USB dongle to your PC after the driver installation.

## GETTING TO KNOW WIRELESS LAN USB Dongle

### 3. LED

LED turns on when the WLAN dongle linking normally.

LED is blinking when WLAN Adapter is active.

*Warning! Do not cover or block the airflow to the adapter. The adapter will reach a high temperature during use.*

## 2. Driver Installation

### 2.1 Windows 7

*Notes: The following installation was operated under Windows 7. (Procedures are similar for Windows XP /vista)*

#### Step 1:

Insert the installation CD into your CD-ROM.

#### Step 2:

Welcome Installation dialog prompt shown.

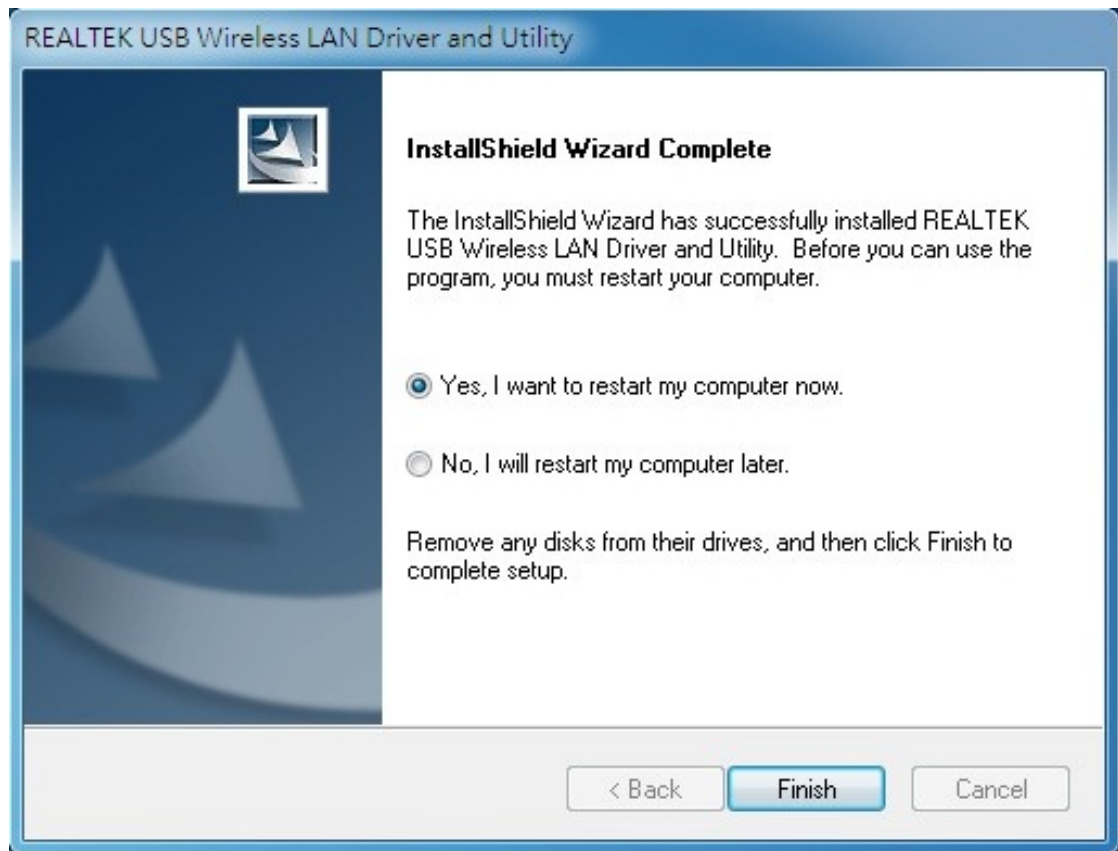
Click [Next](#) to continue.

Click [Cancel](#) to close installation. Installing and configuring WLAN utility.



**Step 3:**

Click Finish to complete installation.



### 3. Wireless Network Configuration

The management software is provided for the WLAN dongle.

When you insert the WLAN Adapter into your laptop or desktop, an icon should appear in the Windows System Tray automatically.

#### 3.1 Utility Icon

Client mode utility running but no WLAN Adapter plugged.



Client mode utility running and WLAN Adapter scan available network.

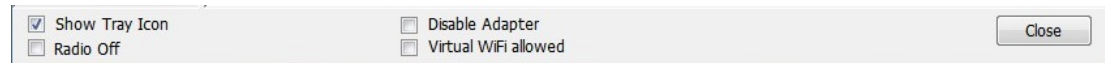


Client mode utility running and WLAN Adapter cannot scan any AP.



#### 3.2 Client Mode

##### 3.2.1 Wireless Device Control



Show Tray Icon – Show icon or not show icon in stray.

Radio Off – Stop wireless signal.

Disable Adapter – Stop wireless device.

Virtual WiFi allowed – Windows operating system control switch

### 3.2.2 General Setting

Once device is set, double click on that icon and the configuration window will pop up as shown. It shows the current connected network. The signal strength and link quality are also displayed. The bar graph displays the quality and strength of the link between the node and its Access Point. Link Quality is a measurement of receiving and transmitting performances over the radio.

[Network Address](#) displays current MAC Address, IP Address, and Subnet, and Gateway.

Click [Renew IP](#) button to refresh IP address leased from wireless AP.

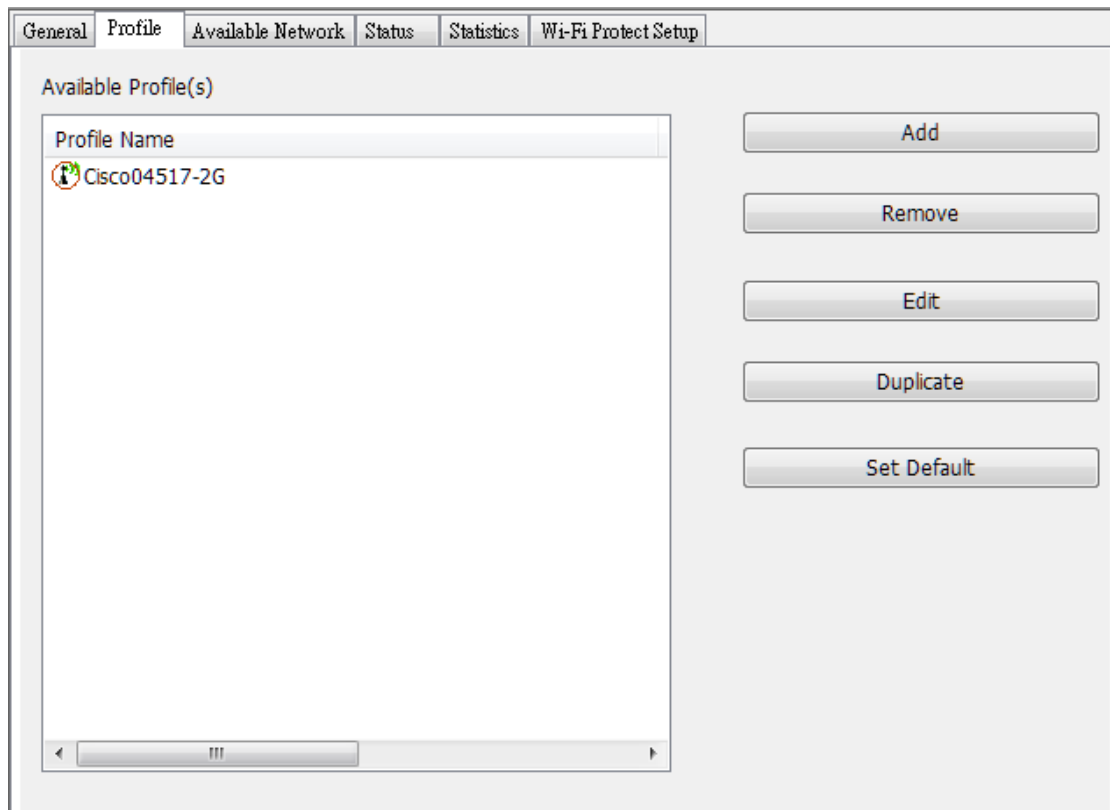
TX the POWER adjustable RF output power

The screenshot shows a network configuration window with the following details:

- General** (selected tab) | Profile | Available Network | Status | Statistics | Wi-Fi Protect Setup
- Status: Associated
- Speed: Tx:144 Mbps Rx:144.5 Mbps
- Type: Infrastructure
- Encryption: AES
- SSID: Cisco04517-2G
- Signal Strength: 92% (represented by a green bar)
- Link Quality: 100% (represented by a green bar)
- Network Address:**
  - MAC Address: 00:1A:EF:41:E2:D7
  - Realtek 8812AU Wireless LAN 802.11ac USB NIC
  - IP Address: 192.168.99.139
  - Subnet Mask: 255.255.255.0
  - Gateway: 192.168.99.1
- [ReNew IP](#) button

### 3.2.3 Profile Setting

In profile tab, you can [Add](#), [Remove](#), [Edit](#), [Duplicate](#) and [Set Default](#) to manipulate profile content manually. Strongly recommend to use profile after you do [Available Network](#).





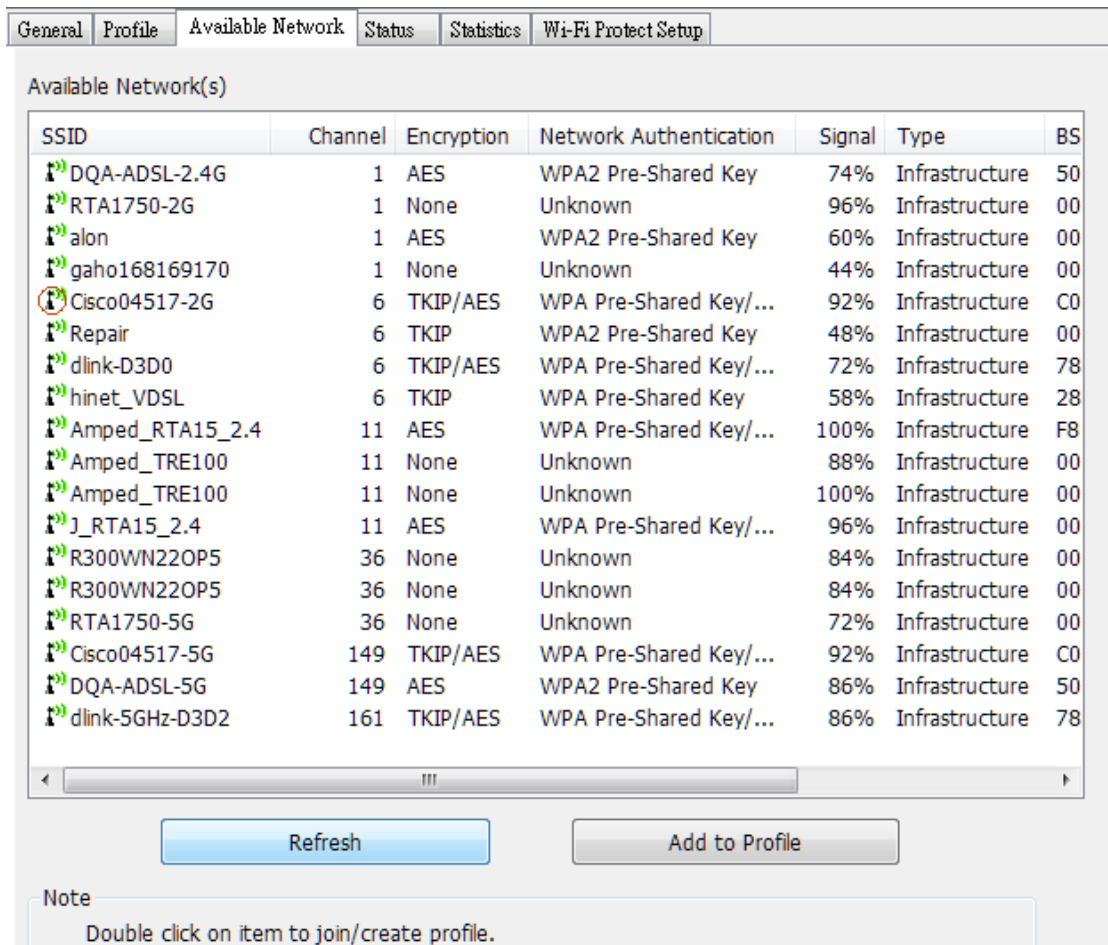
### 3.2.4 Available Network Setting

Click [Available Network](#) tab and it will show all available networks that radio can reaches. Select proper SSID & BSSID you want to connect.

Click [Refresh](#) button to force and rescan available networks currently.

Select one of SSIDs, and click [Add to Profile](#) to create profile that can be configured more wireless parameters.

**NOTE: Connect to the available router of 2.4GHz or 5GHz**



SSID	Channel	Encryption	Network Authentication	Signal	Type	BS
DQA-ADSL-2.4G	1	AES	WPA2 Pre-Shared Key	74%	Infrastructure	50
RTA1750-2G	1	None	Unknown	96%	Infrastructure	00
alon	1	AES	WPA2 Pre-Shared Key	60%	Infrastructure	00
gaho168169170	1	None	Unknown	44%	Infrastructure	00
Cisco04517-2G	6	TKIP/AES	WPA Pre-Shared Key/...	92%	Infrastructure	C0
Repair	6	TKIP	WPA2 Pre-Shared Key	48%	Infrastructure	00
dlink-D3D0	6	TKIP/AES	WPA Pre-Shared Key/...	72%	Infrastructure	78
hinet_VDSL	6	TKIP	WPA Pre-Shared Key	58%	Infrastructure	28
Amped_RTA15_2.4	11	AES	WPA Pre-Shared Key/...	100%	Infrastructure	F8
Amped_TRE100	11	None	Unknown	88%	Infrastructure	00
Amped_TRE100	11	None	Unknown	100%	Infrastructure	00
J_RTA15_2.4	11	AES	WPA Pre-Shared Key/...	96%	Infrastructure	00
R300WN22OP5	36	None	Unknown	84%	Infrastructure	00
R300WN22OP5	36	None	Unknown	84%	Infrastructure	00
RTA1750-5G	36	None	Unknown	72%	Infrastructure	00
Cisco04517-5G	149	TKIP/AES	WPA Pre-Shared Key/...	92%	Infrastructure	C0
DQA-ADSL-5G	149	AES	WPA2 Pre-Shared Key	86%	Infrastructure	50
dlink-5GHz-D3D2	161	TKIP/AES	WPA Pre-Shared Key/...	86%	Infrastructure	78

Refresh Add to Profile

Note Double click on item to join/create profile.

In this page, you can edit your profile name; configure wireless security like WEP, WPA, WPA2, 802.1x ...etc. After finishing setup, click **OK** button to save configuration.

**Wireless Network Properties:**

This is a computer-to-computer (ad hoc) network; wireless access points are not used.

Profile Name: Cisco04517-2G

Network Name (SSID): Cisco04517-2G

Channel: 6 (2437MHz)

Wireless network security

This network requires a key for the following:

Network Authentication: WPA2-PSK

Data encryption: AES

ASCII  PASSPHRASE

Key index (advanced): 1

Network key:

Confirm network key:

OK Cancel

### 3.2.5 Status

In this page, it shows all wireless, networking and device driver version of 2.4GHz in detail.

General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup
Manufacturer				REALTEK	
NDIS Driver Version				1026.12.606.2014	
Short Radio Header				Yes	
Encryption				AES	
Authenticate				WPA2-PSK	
Channel Set				2.4G FCC1, 5G FCC2	
MAC Address				00:1A:EF:41:E2:D7	
Data Rate (AUTO)				Tx:144 Mbps Rx:144.5 Mbps	
Channel (Frequency)				6 (2437 MHz)	
Status				Associated	
SSID				Cisco04517-2G	
Network Type				Infrastructure	
Power Save Mode				None	
Associated AP MAC				C0:C1:C0:62:3C:12	
Up Time (hh:mm:ss)				0:25:57	
USB HUB				USB2.0	
USB Mode				USB2.0	

In this page, it shows all wireless, networking and device driver version of 802.11n 5GHz in detail

General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup
Manufacturer				REALTEK	
NDIS Driver Version				1026.12.606.2014	
Short Radio Header				No	
Encryption				Disabled	
Authenticate				Open System	
Channel Set				2.4G FCC1, 5G FCC2	
MAC Address				00:1A:EF:41:E2:D7	
Data Rate (AUTO)				Tx:270 Mbps Rx:270 Mbps	
Channel (Frequency)				36 (5180 MHz)	
Status				Associated	
SSID				R300WN22OP5	
Network Type				Infrastructure	
Power Save Mode				None	
Associated AP MAC				00:1A:EF:AB:00:03	
Up Time (hh:mm:ss)				0:01:55	
USB HUB				USB2.0	
USB Mode				USB2.1	

In this page, it shows all wireless, networking and device driver version of 802.11ac 5GHz in detail.

General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup	
Manufacturer				REALTEK		
NDIS Driver Version				1026.12.606.2014		
Short Radio Header				No		
Encryption				AES		
Authenticate				WPA2-PSK		
Channel Set				2.4G FCC1, 5G FCC2		
MAC Address				00:1A:EF:41:E2:D7		
Data Rate (AUTO)				Tx:585 Mbps Rx:585 Mbps		
Channel (Frequency)				161 (5805 MHz)		
Status				Associated		
SSID				dlink-5GHz-D3D2		
Network Type				Infrastructure		
Power Save Mode				None		
Associated AP MAC				78:54:2E:FA:D3:D2		
Up Time (hh:mm:ss)				0:01:08		
USB HUB				USB2.0		
USB Mode				USB2.1		

### 3.2.6 Statistics Page

The Tx/Rx status of current wireless connection is shown. A statistic analysis of packet transition is listed.

Counter Name	Value
Tx OK	1876
Tx Error	0
Rx OK	4104
Rx Packet Count	4104
Rx Retry	105
Rx ICV Error	0

Reset

### 3.2.7 Wi-Fi Protected Setup

There is an easy and secure setup solution for Wi-Fi network. You can choose PIN Code or Push Button method to connect to an AP.

General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup
---------	---------	-------------------	--------	------------	---------------------

### Wi-Fi Protected Setup (WPS)

An easy and secure setup solution for Wi-Fi network

Role Selection

As WPS Device

Pin Input Config (PIN)  
After pushing the PIN button. Please enter the PIN code

**PIN Code : 10015544**

Pin Input Config (PIN)

Push Button  
After pushing the PBC button. Please push the physical button on your AP or visual button on the WPS config page.

Push Button Config (PBC)

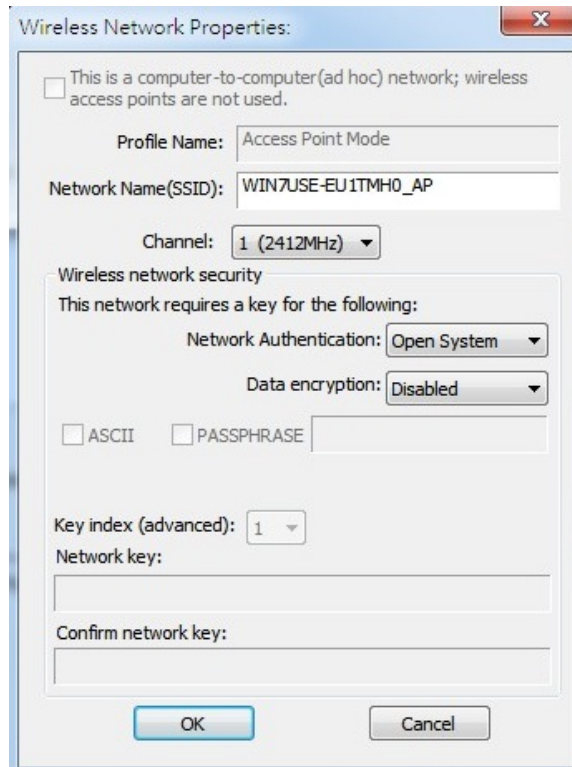
## 4. Access Point Mode

### 4.1 General Page

This page provides general information of this AP, including name, MAC address and list of joined stations.

The screenshot shows the 'General' tab of an AP configuration page. At the top, there are three tabs: 'General', 'Advanced', and 'Statistics'. Below the tabs, the SSID is 'RD-1213-PC\_AP' and the BSSID is '00:1A:EF:41:E2:D7'. An 'Association Table' is displayed as a table with columns for 'AID', 'MAC Address', and 'Life Time', but it is currently empty. Below the table is a 'Config' button. Further down, there is a section for 'Soft AP Use the following IP address:' with an 'IP Address' field containing '192 . 168 . 159 . 1' and an 'Apply' button. Below this, there are checkboxes for 'Setting Internet Connection Sharing (ICS)' (checked) and 'Auto Select Public Network' (unchecked). A 'Shared network:' dropdown menu is set to 'Realtek PCIe GBE Family Controller', with 'Refresh' and 'Apply' buttons below it.

1. SSID: The name of this AP.
2. BSSID: Six two-digital numbers of the MAC address of this AP.
3. Association Table: It is the list of joined stations to this AP.
4. AID (Association ID):  
The AID field is a value assigned by an AP during association that represents 16-bit ID of a station. It is a unique value assigned by AP.
5. MAC address:  
It is the six two-digit numbers that assemble the MAC address of respected joined station.
6. Life Time:  
It is the timer that counts down from 10 minutes whenever the AP connects the station successfully. If an STA associated to SW AP does not have any interaction with the AP in 10 minutes, it will be disassociated from the Infra-structure BSS.
7. Config: A dialog of this AP is shown for configuration modification.
8. ICS: Internet Connection Sharing.  
It enables this AP to create the domain to share this internet/intranet network connection.

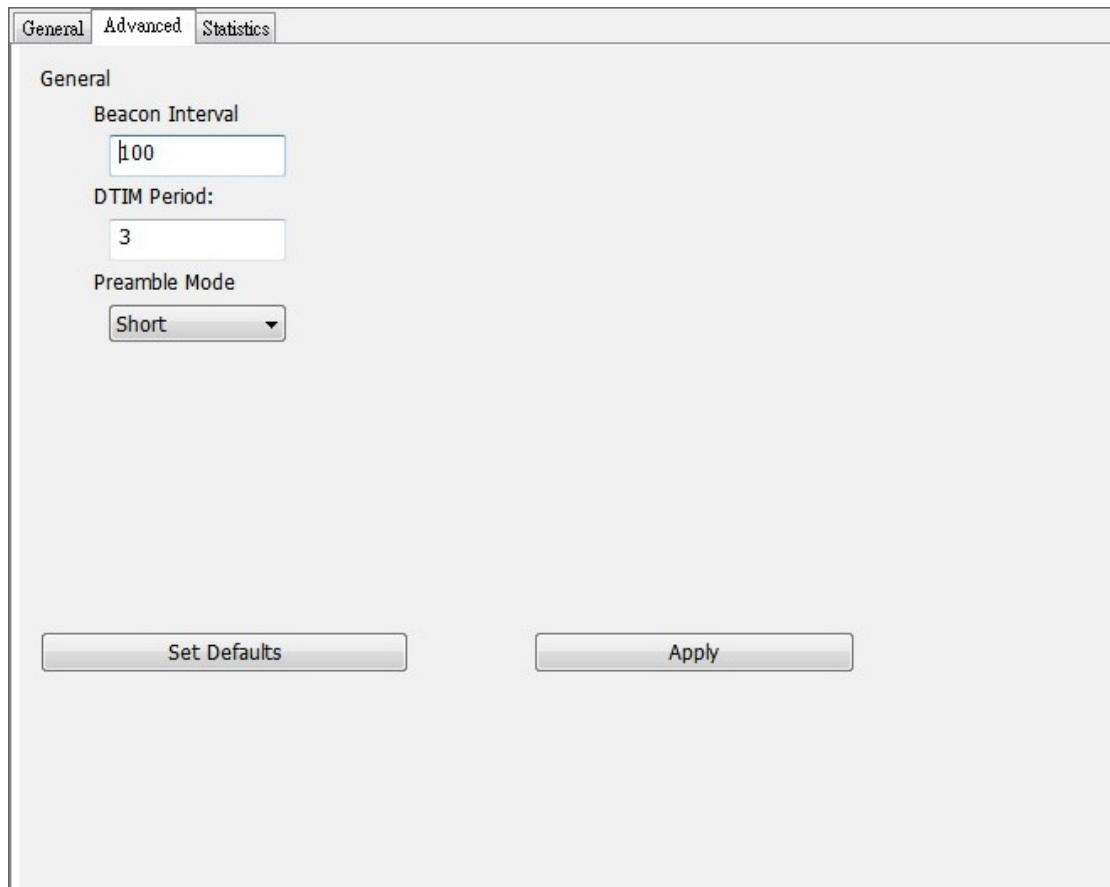


- a. Network Name (SSID):  
The name of the AP is searchable by other wireless nodes. The length of SSID should be shorter than 32 characters.
- b. Channel: Select the wireless channel within current channel plan.
- c. Network Authentication & Data Encryption :
  - Open System:  
It is combined with data encryption type to be WEP or to be disabled. Disabled: you decide to open this AP to every one without network authentication. WEP: you decide to setup the basic data encryption with a defined network key.
  - Shared Key + WEP:  
You decide to apply both authentication and data encryption to prevent unauthorized login.
  - WPA-PSK + TKIP & WPA2-PSK + TKIP:  
The most advanced authentication and data encryption that provide the best security protection.
- d. ASCII / PASSPHRASE:
  - ASCII:  
You should provide either 5 or 13 ASCII characters on Network key edit box.
  - PASSPHRASE: You could input words on Network
  - Key edit box:  
64 bits: The generated pass key is 64-bit to be complied with data packets. 128 bits: The generated pass key is 128-bit to be complied with data packets.
  - Hexadecimal:  
While both ASCII and PASSPHRASE are not checked, you should input hexadecimal number in the network key box. For example, 10 digits hex number for 64-bit WEP or 26 digits hex number for 128-bit WEP.
- e. Key index (advanced) (1 ~4):  
At most four key index to represent the opposite network key.



## 4.2 Advanced Page

Users could setup the advanced characteristics of network packet for transmission on this page.



The screenshot shows a web interface for configuring network settings. At the top, there are three tabs: 'General', 'Advanced', and 'Statistics'. The 'General' tab is selected. Below the tabs, the word 'General' is displayed. There are three main configuration fields: 'Beacon Interval' with a text input box containing '100', 'DTIM Period:' with a text input box containing '3', and 'Preamble Mode' with a dropdown menu showing 'Short'. At the bottom of the configuration area, there are two buttons: 'Set Defaults' and 'Apply'.

1. **Beacon Interval:**  
This field indicates the interval between each beacon that this AP sends out in unit of TU (1024 micro-seconds).
2. **DTIM Period:**  
The DTIM Period field is the number of Beacon intervals between successive DTIMs.
3. **Preamble Mode:**
  - Long: higher quality but with lower performance than preamble short mode.
  - Short: Normal quality but with higher performance than preamble long mode.
  - Auto: select the proper preamble mode by current signal frame information.

### 4.3 Statistics Page

The Tx/Rx status of current wireless connection is shown. A statistic analysis of packet transition is listed.

Counter Name	Value
Tx OK	146
Tx Error	0
Rx OK	0
Rx Packet Count	0
Rx Retry	0
Rx ICV Error	0

Reset

## 5. Troubleshooting

<b>Symptom :</b>	The LED is off.
<b>Remedy :</b>	Make sure the PC Card is inserted properly. Otherwise contact your vendor.
<b>Symptom :</b>	The LED is always on not blinking.
<b>Remedy :</b>	Make sure that you have installed the driver from attached CD. Otherwise contact your vendor.
<b>Symptom :</b>	The LED is blinking but the PC Card icon does not appear in your icon tray.
<b>Remedy :</b>	Make sure that you have installed the Utility from the attached CD.
<b>Symptom :</b>	The PC Card is linking, but can't share files with others.
<b>Remedy :</b>	Make sure the <b>file and printer sharing</b> function is enabled. You can enable the function by checking the icon of <b>My Computer -&gt; Control Panel -&gt; Network -&gt; file and printer sharing -&gt; I want to be able to give others to access to my files.</b>
<b>Symptom :</b>	Slow or poor performance under AP mode
<b>Remedy :</b>	Try to select another channel for the communicating group or move your device closer to the Access Point.

## 6. Glossary

### 1. IEEE 802.11 Standard

The IEEE 802.11 Wireless LAN standards subcommittee, which is formulating a standard for the industry.

### 2. Access Point

An internetworking device that seamlessly connects wired and wireless networks together.

### 3. Ad Hoc

An Ad Hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN

Ad Hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

### 4. BSSID

A specific Ad Hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSSID.

### 5. DHCP

Dynamic Host Configuration Protocol - a method in which IP addresses are assigned by server dynamically to clients on the network. DHCP is used for Dynamic IP Addressing and requires a dedicated DHCP server on the network.

### 6. Direct Sequence Spread Spectrum

This is the method the wireless cards use to transmit data over the frequency spectrum. The other method is frequency hopping. Direct sequence spreads the data over one frequency range (channel) while frequency hopping jumps from one narrow frequency band to another many times per second.

### 7. ESSID

An Infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS could roam freely between BSSs while served as a continuous connection to the network wireless stations and Access Points within an ESS must be configured with the same ESSID and the same radio channel.

### 8. Ethernet

Ethernet is a 10/100Mbps network that runs over dedicated home/office wiring. Users must be wired to the network at all times to gain access.

### 9. Gateway

A gateway is a hardware and software device that connects two dissimilar systems, such as a LAN and a mainframe. In Internet terminology, a gateway is another name for a router. Generally a gateway is used as a funnel for all traffic to the Internet

### 10. IEEE

Institute of Electrical and Electronics Engineers Infrastructure. An integrated wireless and

wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless

## 11. ISM Band

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the so-called ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available of users around the globe.

## 12. Local Area Network (LAN)

A LAN is a group of computers, each equipped with the appropriate network adapter card connected by cable/air, that share applications, data, and peripherals. All connections are made via cable or wireless media, but a LAN does not use telephone services. It typically spans a single building or campus.

## 13. Network

A network is a system of computers that is connected. Data, files, and messages can be transmitted over this network. Networks may be local or wide area networks.

## 14. Protocol

A protocol is a standardized set of rules that specify how a conversation is to take place, including the format, timing, sequencing and/ or error checking.

## 15. SSID

A Network ID unique to a network. Only clients and Access Points that share the same SSID are able to communicate with each other. This string is case-sensitive.

## 16. Static IP Addressing

A method of assigning IP addresses to clients on the network. In networks with Static IP address, the network administrator manually assigns an IP address to each computer. Once a Static IP address is assigned, a computer uses the same IP address every time it reboots and logs on to the network, unless it is manually changed.

## 17. Temporal Key Integrity Protocol (TKIP)

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

## 18. Transmission Control Protocol / Internet Protocol (TCP/IP)

TCP/IP is the protocol suite developed by the Advanced Research Projects Agency (ARPA). It is widely used in corporate Internet works, because of its superior design for WANs. TCP governs how packet is sequenced for transmission the network. The term "TCP/IP" is often used generically to refer to the entire suite of related protocols.

## 19. Transmit / Receive

The wireless throughput in Bytes per second averaged over two seconds.

## 20. Wi-Fi Alliance

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability. The organization is formerly known as WECA.

## 21. Wi-Fi Protected Access (WPA)

The Wi-Fi Alliance put together WPA as a data encryption method for 802.11 wireless LANs. WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, including using dynamic keys.

## 22. Wide Area Network (WAN)

A WAN consists of multiple LANs that are tied together via telephone services and / or fiber optic cabling. WANs may span a city, a state, a country, or even the world

## 23. Wired Equivalent Privacy (WEP)

Now widely recognized as flawed, WEP was a data encryption method used to protect the transmission between 802.11 wireless clients and APs. However, it used the same key among all communicating devices. WEP's problems are well-known, including an insufficient key length and no automated method for distributing the keys. WEP can be easily cracked in a couple of hours with off-the-shelf tools.

## 24. Wireless LAN (WLAN)

A wireless LAN does not use cable to transmit signals, but rather uses radio or infrared to transmit packets through the air. Radio Frequency (RF) and infrared are the commonly used types of wireless transmission. Most wireless LANs use spread spectrum technology. It offers limited bandwidth, usually under 11Mbps, and users share the bandwidth with other devices in the spectrum; however, users can operate a spread spectrum device without licensing from the Federal Communications Commission (FCC).

## 25. Fragment Threshold

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large.

This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead. Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

## 26. RTS(Request To Send) Threshold

The RTS threshold is the packet size at which packet transmission is governed by the

RTS/CTS transaction. The IEEE802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

## 27. Beacon Interval

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion. Beacon Interval represents 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 (and learn whether there are buffered frames at the access point).

## 28. Preamble Type

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

## 29. WPA2

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

## 30. Temporal Key Integrity Protocol (TKIP)

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

## 31. 802.1x Authentication

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284. Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

## 32. Advanced Encryption Standard (AES)

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.