



**HIGH POWER WIRELESS N MINI USB ADAPTER**

**K-300MWUN**

**USER'S MANUAL**

## **Introduction**

Thank you for your purchase of the Kozumi K-300MWUN High Power Wireless N Mini USB Adapter. 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.

## **FEATURES**

Support Microsoft 2000, XP, x64, Vista and Win7

Operating distance of up to 300 meters in free space.

300/270/240/180/120/90/60/54/48/36/30/24/22/18/12/11/6/5.5/2/1 Mbps selectable

Data Rate.

64/128-bit WEP , WPA (Wi-Fi Protected Access), WPA2, WPS

2.400GHz ~ 2.484GHz unlicensed ISM Frequency Band. Modulation Method :

IEEE 802.11b : DSSS (Direct Sequence Spread Spectrum).

IEEE 802.11g / 802.11n : OFDM (Orthogonal Frequency Division Multiplexing). Easy operation and setting up.

## **SYSTEM REQUIREMENTS**

Windows System : 2000, XP 32/64, Vista 32/64, Windows 7

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

## **BEFORE YOU START**

1. Confirm Box Contents
  - Wireless LAN Adapter
  - Resource CD
  - 2 dBi Antenna

## CONNECTING YOUR WLAN ADAPTER TO PC

2. Connect your WLAN adaptor to your PC. And Install driver.

## GETTING TO KNOW WIRELESS LAN ADAPTER

3. LEDs
  - LED turns on when WLAN link to WLAN adaptor or AP.
  - LED is blinking when WLAN Adapter is active.

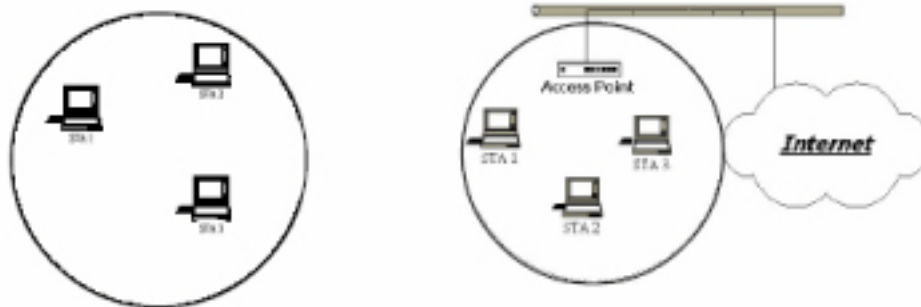
## Wireless LAN Basics

Wireless LAN network defined by IEEE 802.11b/g/n standard committee could be configured as :

**Ad Hoc wireless LAN.**

**Infrastructure wireless LAN.**

**Ad Hoc** network is a group of PCs installed with wireless LAN cards, this group of PCs is called a BSS (Basic Service Set). PCs in this group can use their wireless LAN cards to communicate with each other, but can not connect to the **Internet**.



**Ad Hoc** Wireless Network

**Infrastructure** Wireless Network

The most obvious difference between **Infrastructure** wireless network and **Ad Hoc** wireless network is that the PCs in **Infrastructure** wireless network can access the resource in the Internet through **Access Point**.

Depending on your requirement, you can easily set up your PC's network to be a "**Ad Hoc**" or "**Infrastructure**" wireless network. Generally speaking, if in your network, there is an **Access Point** in it, we recommend you to set your network as an "**Infrastructure**", so it can connect to the **Internet**.

## **IP ADDRESS**

To use the WLAN Adapter with a computing device, the WLAN Adapter must be equipped with a proper Interface. All drivers and supporting software for the WLAN Adapter must be installed and configured first.

Ask your system administrator for the following information, which you may need to provide during driver installation :

Your Wireless Client Name.

Your Wireless SSID.

Your computer's unique client name and workgroup name.

For your network account, your user name and password.

Your IP address, gateway address, and subnet mask if you're not using a DHCP client.

Any computer on a network is identified by a unique network address. There are two methods to assign a network address to a computer on a TCP/IP network :

Static IP addressing.

Dynamic IP addressing (DHCP Client).

In network with static IP addressing, 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. You may manually change the IP address in the [Network Properties dialog box](#). Network using static IP address is easy to set up and do not require additional network management software.

In network with dynamic IP addressing, a DHCP server in the network dynamically assigns IP addresses to all clients every time they log on to the network. Network using dynamic IP address requires setting up and running a DHCP Server.

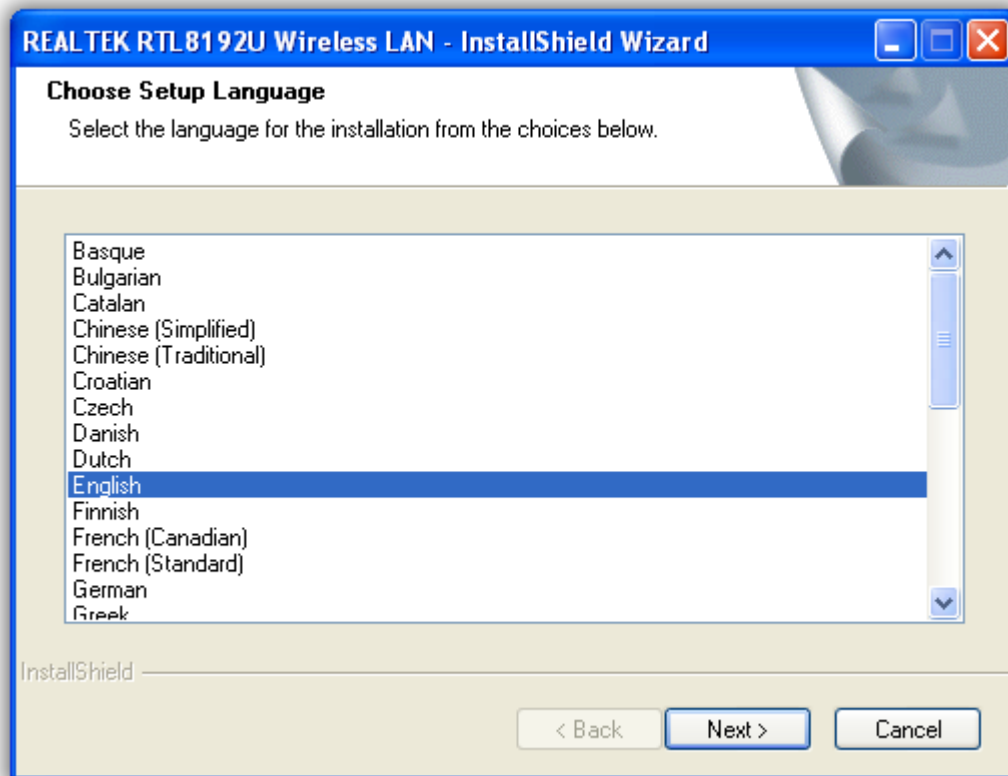
## Install Driver/Utility

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

## Windows XP/2K

### Step 1 :

Insert the installation CD into your CD-ROM. Installation program will prompt language setup. Choose the Setup Language you would like to use and click **Next** button.



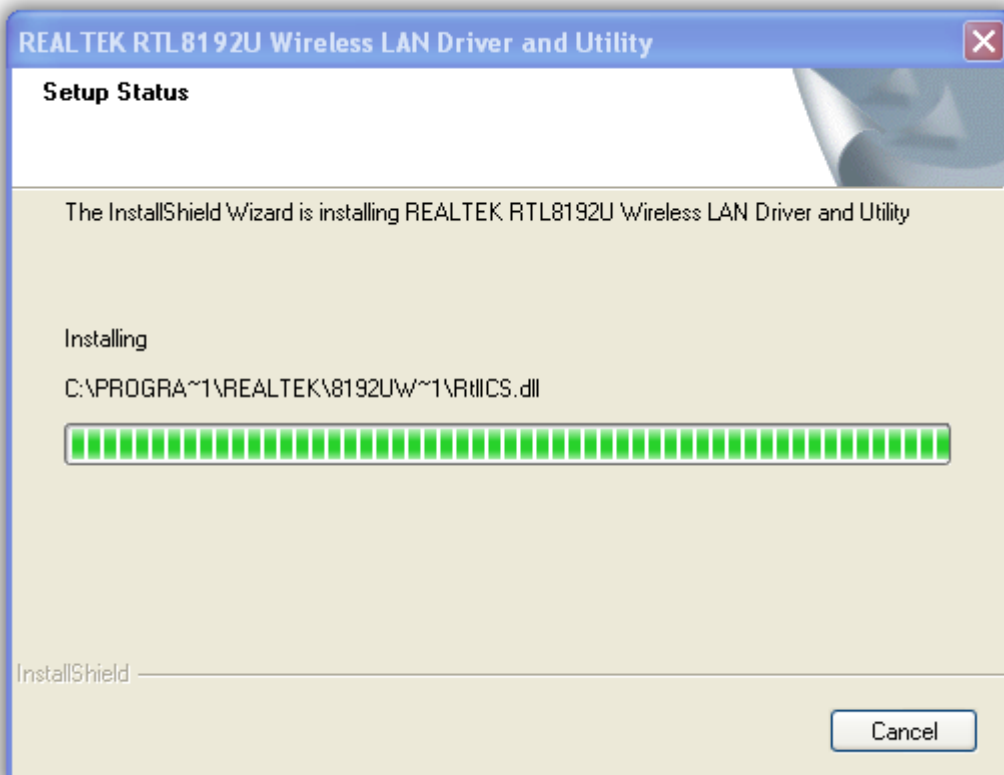
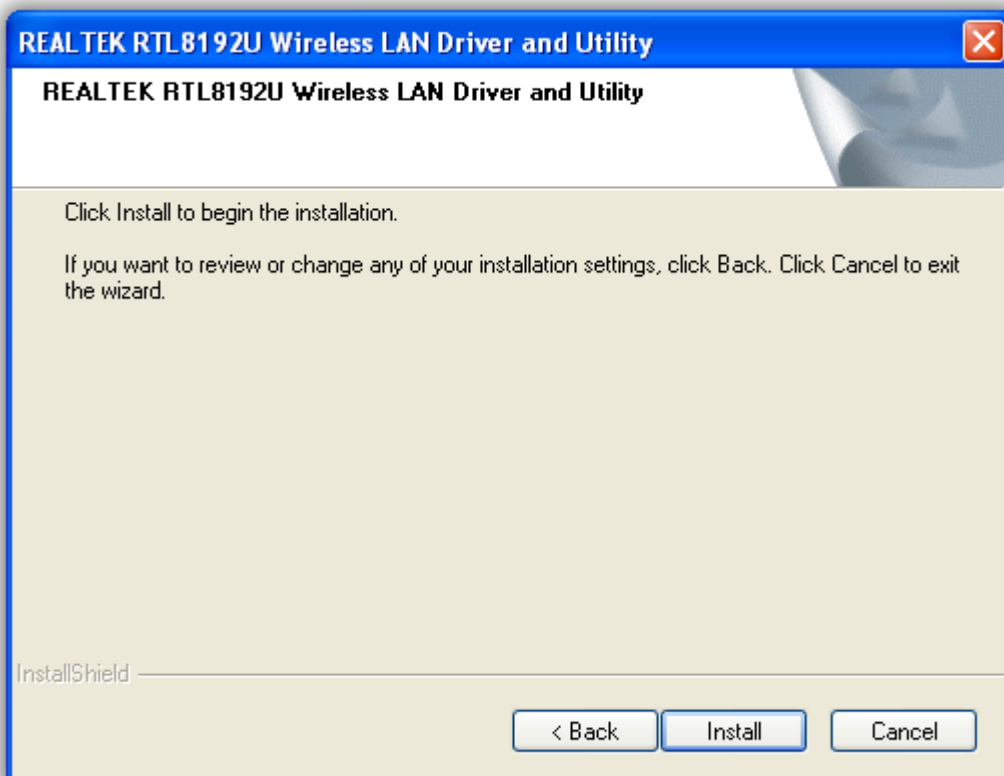
### Step 2 :

Welcome Installation dialog prompt shown. Click **Next** to continue. Click **Cancel** to close installation. Installing and configuring wlan utility.



Step3 :

Click Install.



Step4 :

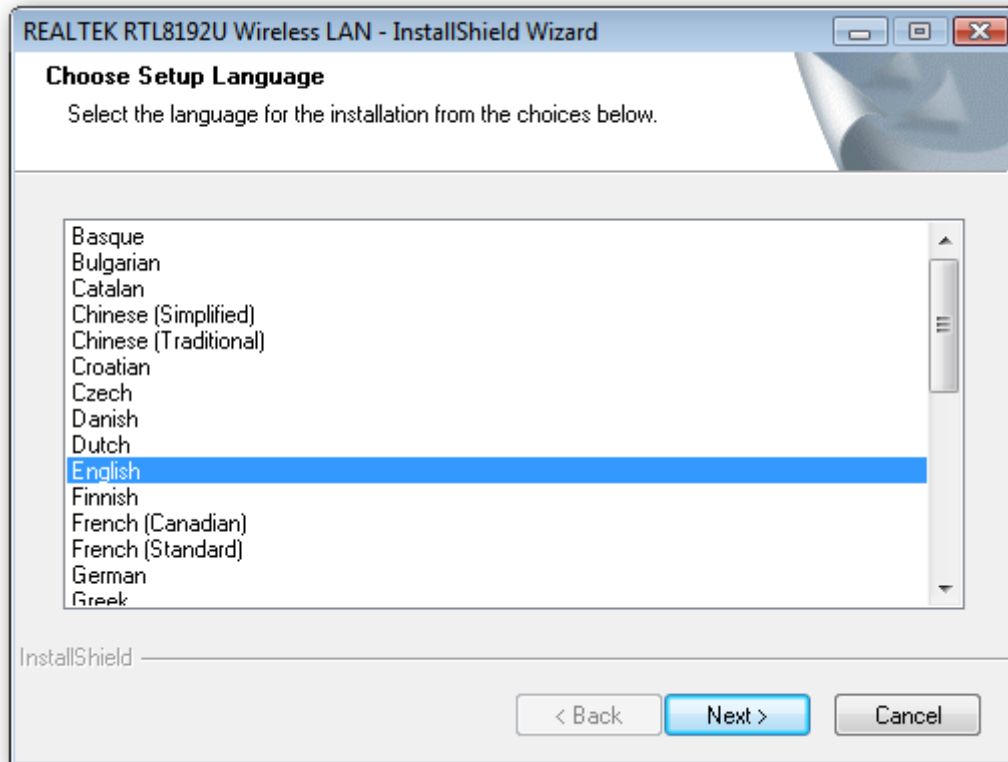
Click **Finish** to complete installation.

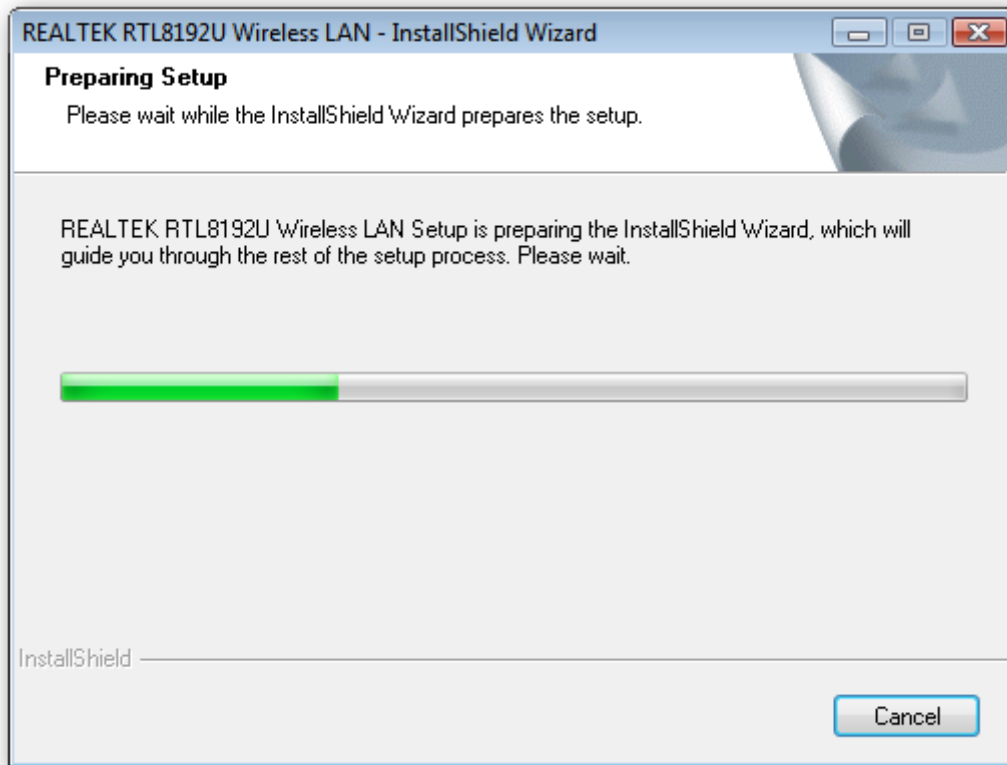


## Windows Vista

### Step 1 :

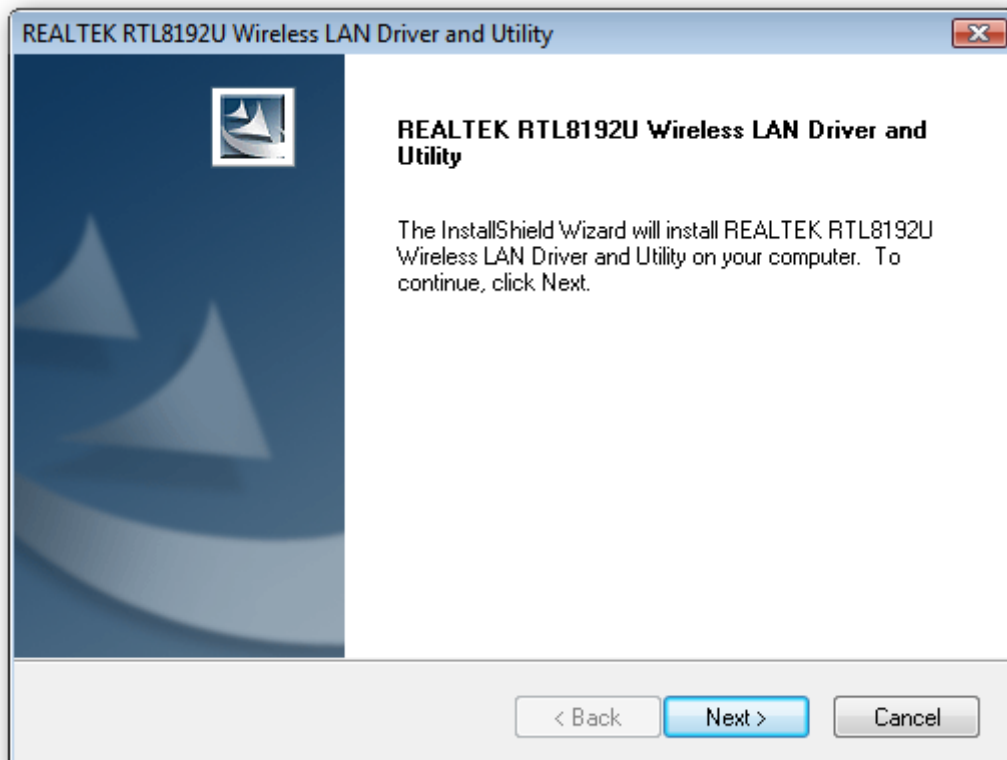
Insert the installation CD into your CD-ROM. Installation program will prompt language setup. Choose the Setup Language you would like to use and click [Next](#) button.





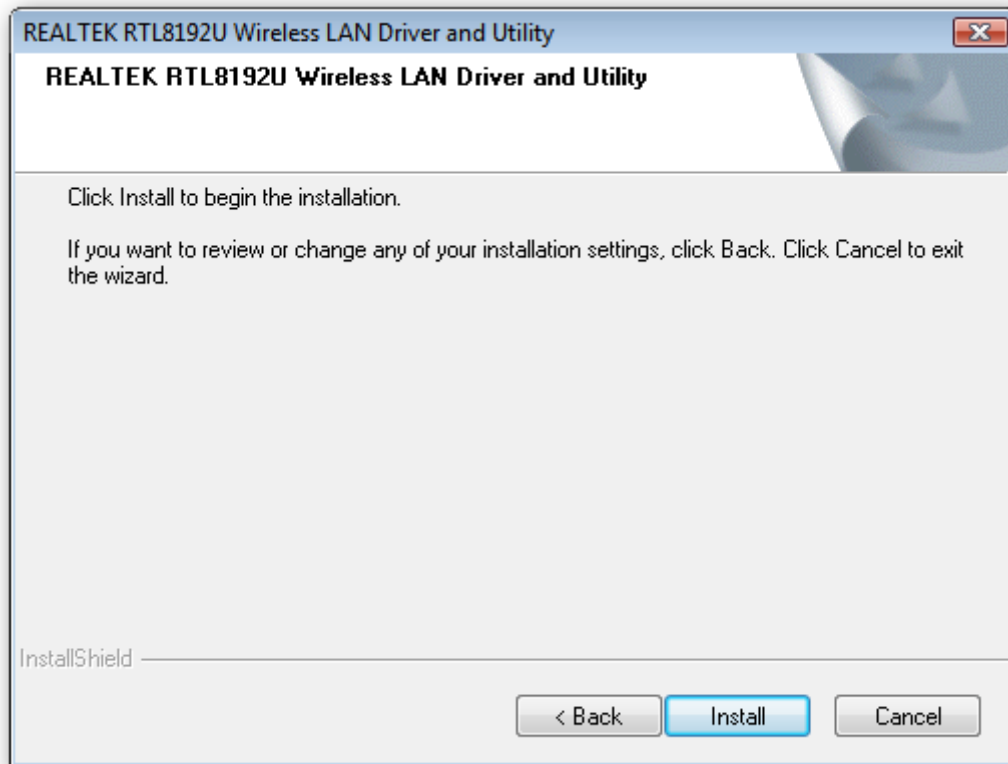
**Step 2 :**

Welcome Installation dialog prompt shown. Click [Next](#) to continue. Click [Cancel](#) to close installation. Installing and configuring wlan utility.



Step3 :

Click [Install](#).



Step4 :

Click [Finish](#) to complete installation.

REALTEK RTL8192U Wireless LAN Driver and Utility



**InstallShield Wizard Complete**

The InstallShield Wizard has successfully installed REALTEK RTL8192U Wireless LAN Driver and Utility. Click Finish to exit the wizard.

< Back

Finish

Cancel

## **Wireless Network Configuration**

WLAN adapter uses its own management software. All functions controlled by users are provided by this application. When you insert the WLAN Adapter into your laptop or desktop, a icon should appear in the Windows System Tray automatically.

### **Utility Icon**

Client mode utility running but no WLAN Adapter plugged.



Client mode utility running and WLAN Adapter scan available network.

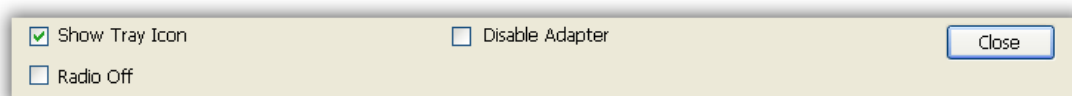


Client mode utility running and WLAN Adapter can not scan any AP.



## **Client Mode (Default Setting)**

### **Wireless Device Control**



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

Radio Off – Stop wireless signal.

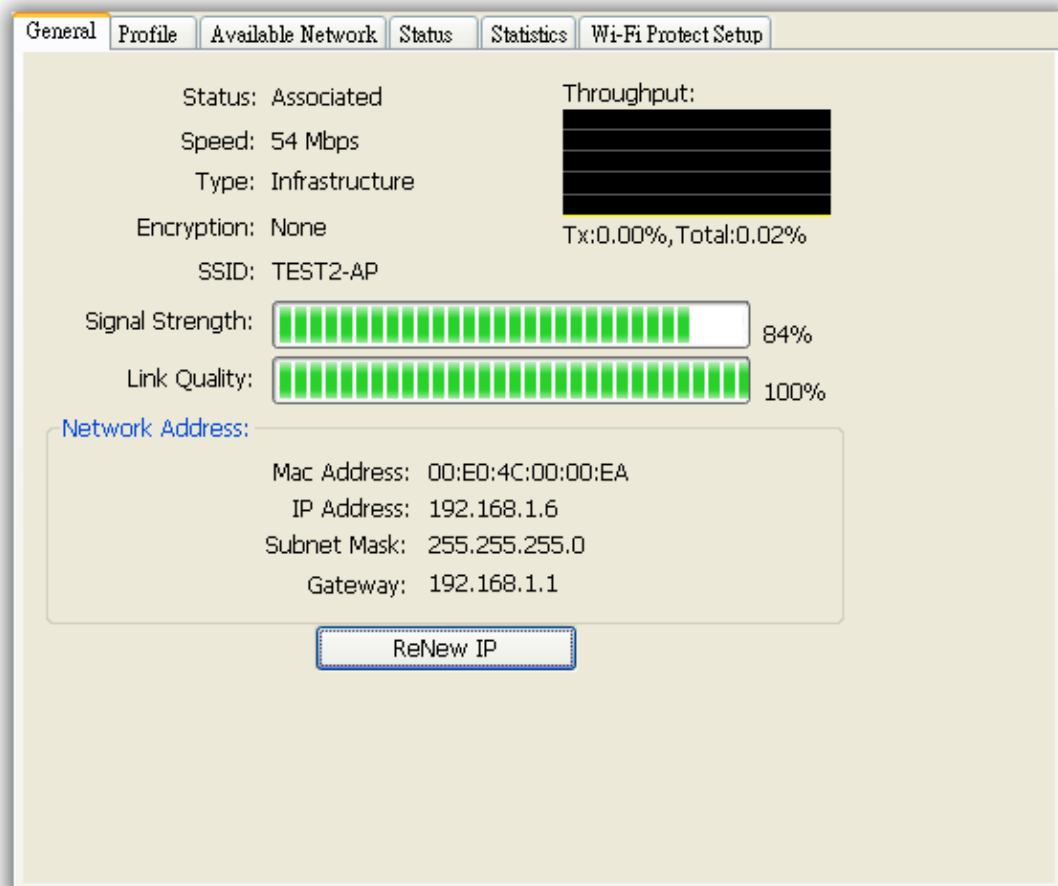
Disable Adapter – Stop wireless device.

## **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 displayed also. The bar graph displays the quality and strength of the link between the node

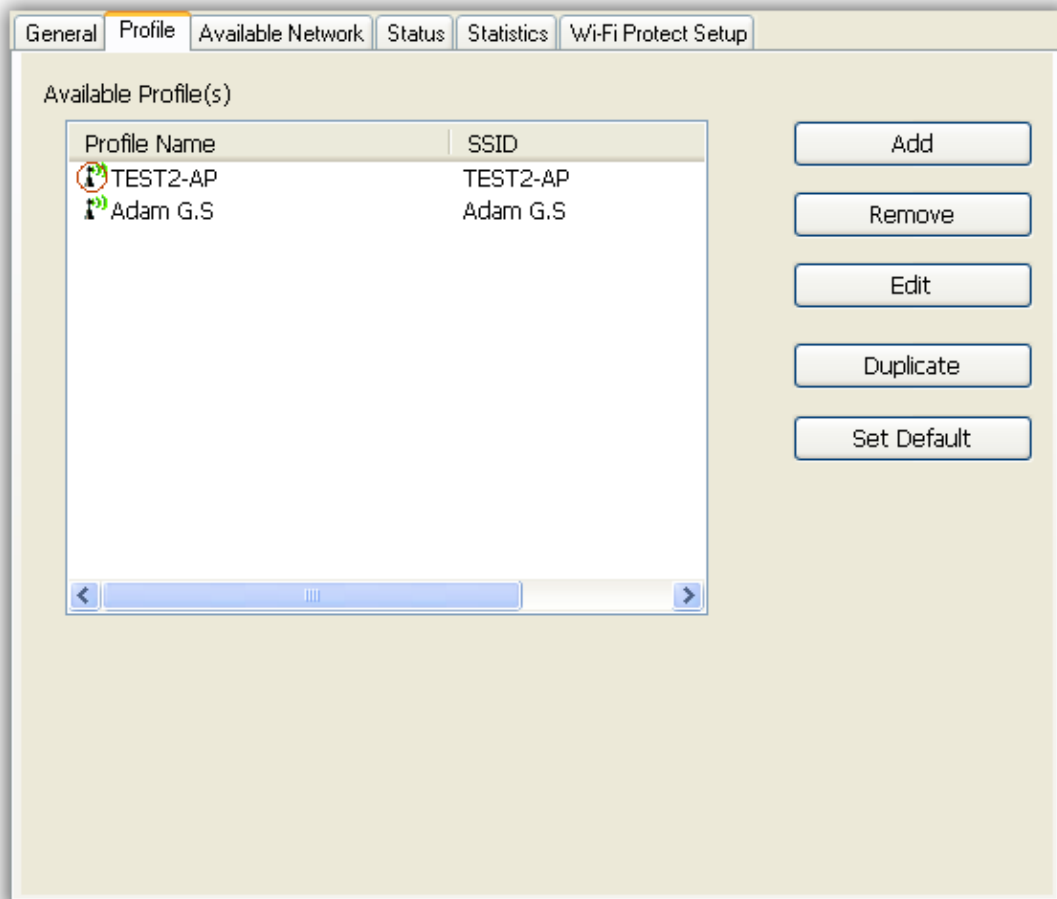
and its Access Point. Link Quality is a measurement of receiving and transmitting performances over the radio.

**Network Address** displays current MAC Address, IP Address, Subnet. and Gateway. Click **Renew IP** button to refresh IP address leased from wireless AP.



## **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**.



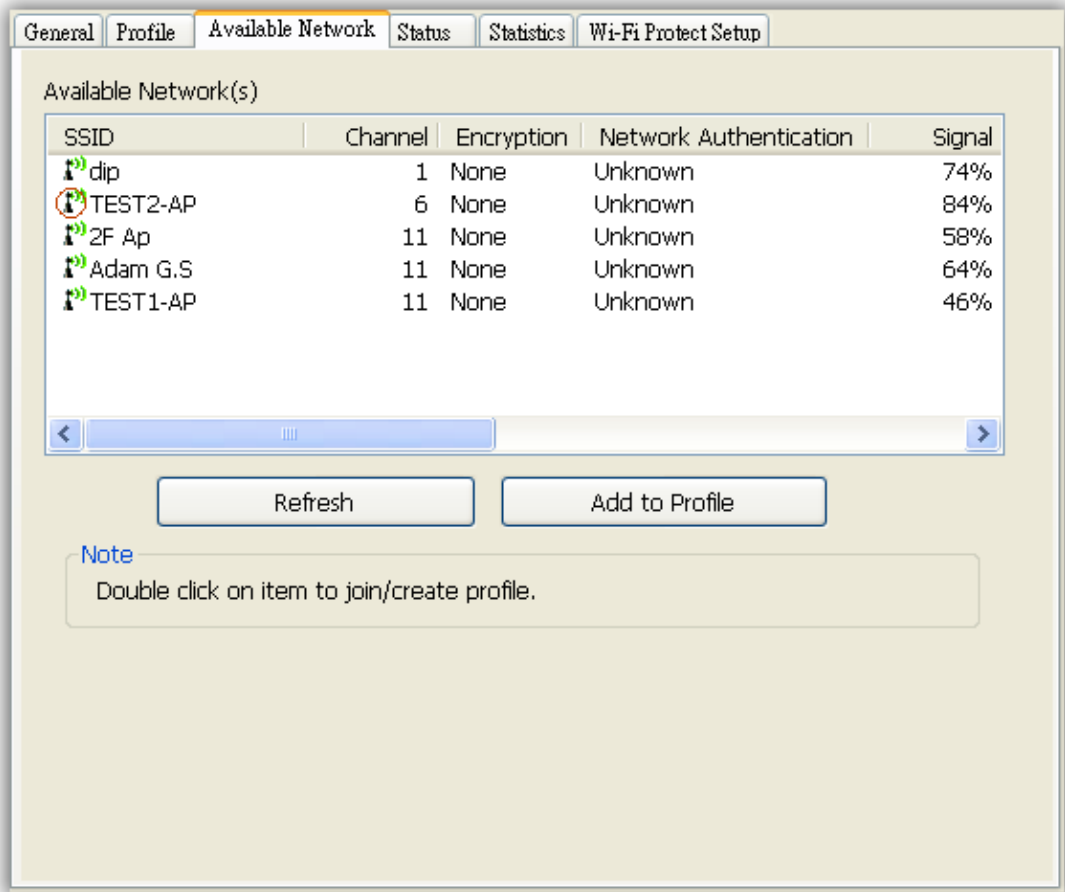
## **AVAILABLE NETWORK SETTING**

Click **Available Network** tab and it will show all available networks that radio can reach.

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.



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:**

Profile Name: TEST2-AP  
Network Name(SSID): TEST2-AP

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

Channel: 6 (2437MHz)

**Wireless network security**  
This network requires a key for the following:  
Network Authentication: Open System  
Data encryption: Disabled

ASCII  PASSPHRASE

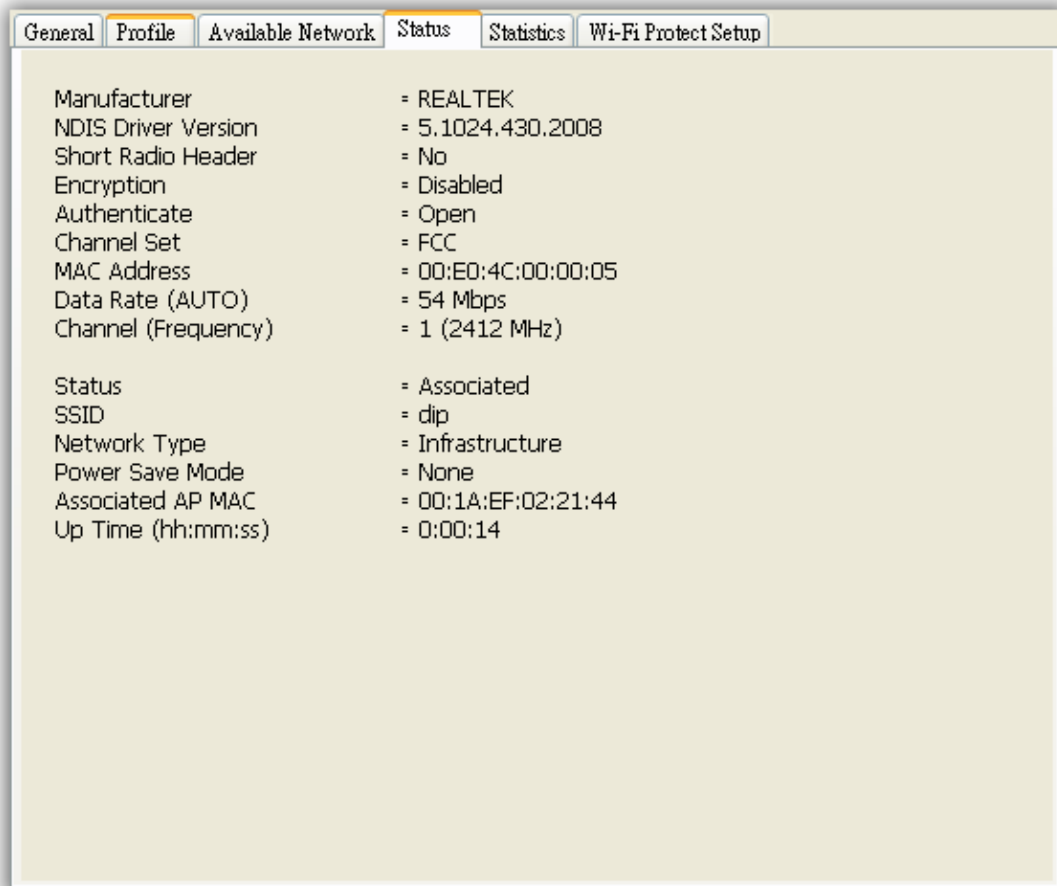
Key index (advanced): 1  
Network key:  
Confirm network key:

**802.1x configure**  
EAP TYPE : GTC  
Tunnel :  
Username :  
Identity :  
Password :  
Certificate :

OK Cancel

## **Status**

Status page tab, shows all wireless, networking and device driver version in details.



## **Statistics**

Statistics page tab will show real-time TX/RX relative counters to check or evaluate the wireless performance.

Click [Reset](#) button to set counter to zero.

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

Counter Name	Value
Tx OK	57
Tx Error	0
Tx Retry	0
Tx Beacon OK	0
Tx Beacon Error	0
Rx OK	115
Rx Packet Count	150
Rx Retry	0
Rx CRC Error(0-500)	0
Rx CRC Error(500-1000)	0
Rx CRC Error(>1000)	0
Rx ICV Error	0

Reset

**Wi-Fi Protected Setup**

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

### Pin Input Config (PIN)

After pushing the PIN button, Please enter the PIN code into your AP.

**PIN Code : 54287198**

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)

## **Technical Specifications**

Product Name	K-300MWUN
Chipset	Realtek RTL8192+RTL8256
Standard	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Frequency Band	2.4GHz ~ 2.484GHz unlicensed ISM band
Spread Spectrum	IEEE 802.11b : DSSS IEEE 802.11g : OFDM IEEE 802.11n : OFDM
Modulation	BPSK, QPSK, 16QAM, 64QAM
Data Rate	IEEE 802.11b : 1, 2, 5.5, 11Mbps IEEE 802.11g : 6, 11, 12, 18, 22, 24, 30, 36, 48, 54 , 60, 90Mbps IEEE 802.11n : Maximum of 300Mbps
Operation Mode	Ad hoc, Infrastructure
Transmitter Power	25(±1) dBm @11b,20(±1) dBm @11g,19(±1) dBm @11n
Receive Sensitivity	Operating at 11Mbps: < -80 dBm @8% FER, 54 Mbps: < -68 dBm @8% FER HT20(2RX/4RX): MCS=0 < -84dBm, MCS=15 < -69dBm HT40(2RX/4RX): MCS=0 < -84dBm, MCS=15 < -69dBm
Security	64-bit , 128-bit WEP, WPA / WPA2 (TKIP/AES)
LED	power
Operating System	Windows® 2000, XP 32/64, Vista 32/64, Windows 7
Operating Temperature	0 ~ 55 Celsius degree
Storage Temperature	-20 ~ 70 Celsius degree
Humidity	5 ~ 90% (non-condensing)
Size	49 (L) x 46 (W) x 10 (H) mm

## Troubleshooting

Symptom :	The LED is off.
Remedy :	Make sure the PC Card is inserted properly. Otherwise contact your vendor.
Symptom :	The LED is always on not blinking.
Remedy :	Make sure that you have installed the driver from attached CD. Otherwise contact your vendor.
Symptom :	The LED is blinking but the PC Card icon does not appear in your icon tray.
Remedy :	Make sure that you have installed the Utility from the attached CD.
Symptom :	The PC Card is linking, but can't share files with others.
Remedy :	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>
Symptom :	Slow or poor performance under AP mode
Remedy :	Try to select another channel for the communicating group or move your device closer to the Access Point.

## **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 application for mobile workers.

### **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 worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands 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 IEEE 802.11-1997 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.