IEEE 802.11n/b/g

WLAN 11n USB Adapter
WL-6200A

USER'S MANUAL

VERSION 1.0
2007/10/24

FC Tested To Comply
With FCC Standards
FOR HOME OR OFFICE USE

CE

This manual provides the necessary information for first-time users to successfully install the Atheros network driver interface specification (NDIS) driver, for the purpose of evaluating and / or operating the Atheros WLAN 11n USB Adapter STA Reference Design in a Microsoft Windows environment and the Atheros Client Utility (ACU) .

This guide describes the steps required to install NDIS drivers for the WLAN 11n USB Adapter in Windows 2000, Windows XP, Windows XP 64, Windows Vista, Windows Vista 64. This guide also includes the detailed instructions for configuring the network adapter to interact with an access point (AP) in infrastructure mode. Read this before installing the Atheros WLAN 11n USB Adapter and NDIS driver in the targeted operating system (OS) environment.

INFORMATION TO USER

Federal Communication Commission Interference Statement

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

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.

REGULATION INFORMATION

The WLAN 11n USB Adapter must be installed and used in strict accordance with the manufacturer's instructions. This device complies with the following radio frequency and safety standards.

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.

(2) This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

The users manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Europe- R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

CE Declaration of Conformity

For the following equipment:

WLAN 11n USB Adapter

(Product Name)

WL-6200A

(Model Designation)

is herewith confirmed to comply with the requirements set out in the Council (European parliament) Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility of Radio and Telecom device (1999/5/EC). For the evaluation regarding this Directive, the following standards were applied:

EN 300 328 V1.7.1

EN 301 489-1 V1.6.1 ; EN 301 489-17 V1.2.1

EN 60950-1:2001

EN 50371:2002

TABLE OF CONTENTS

1 INTRODUCTION

Thank you for your purchase of the WLAN 11n 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 Windows 2000, XP , Vista.
- Indoor up to 100 meters; Outdoor up to 280 meters.
- 270/240/180/120/90/60/54/48/36/30/24/22/18/12/11/6/5.5/2/1 Mbps selectable Data Rate and maximum of 300Mbps.
- Support USB 2.0 interface.
- 64-bit, 128-bit or WEP, TKIP, AES.
- 2.4GHz ISM Frequency Band.
- Modulation Method : BPSK/QPSK/16-QAM/64-QAM
- Spread Spectrum :
  IEEE 802.11b : DSSS (Direct Sequence Spread Spectrum).
  IEEE 802.11g / n: OFDM (Orthogonal Frequency Division Multiplexing).
- Easy operation and setting up.

SYSTEM REQUIREMENTS

- Windows System : Windows 2000, XP , Vista
- PCs must have a device driver installed. It allows you to communicate with WLAN 11n USB Adapter.

BEFORE YOU START

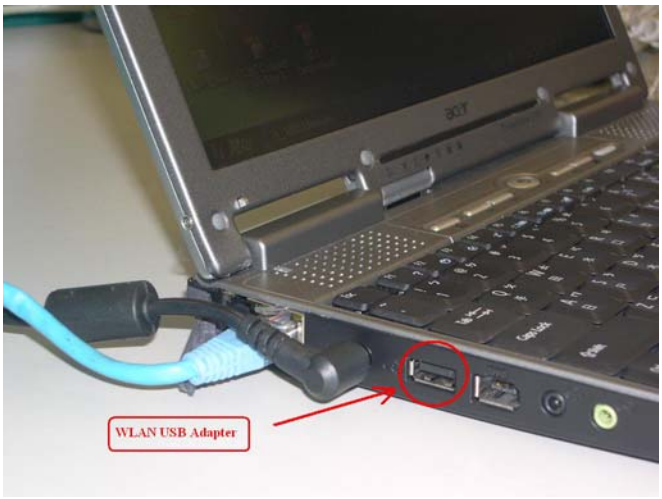
1. Confirm Box Contents

Wireless LAN Adapter

Quick Start Guide

Driver CD

CONNECTING YOUR WLAN USB ADAPTER TO PC



Quick Start Guide

- Connect your WLAN 11n USB Adapter to your PC.
- Install driver.

GETTING TO KNOW WLAN 11n USB ADAPTER

LED

- LED turns on when POWER is applied to the WLAN 11n USB Adapter.

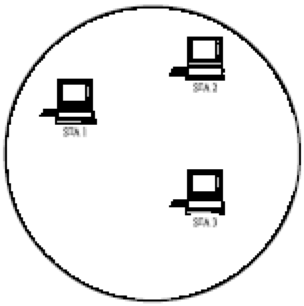
LED is blinking when PC is sending data through WLAN 11n USB Adapter.

2 WIRELESS LAN BASICS

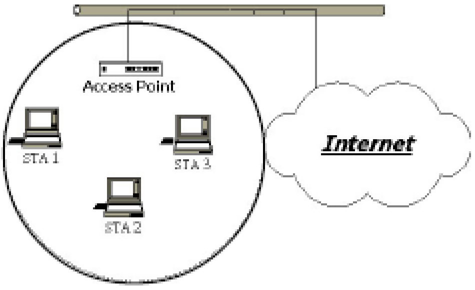
Wireless LAN network defined by IEEE 802.11n/b/g standard committee could be configured as :

- **Ad Hoc wireless LAN,** or
- **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**.

3 IP ADDRESS

To use the WLAN 11n USB Adapter with a computing device, the WLAN 11n USB Adapter must be equipped with an USB 1.1 or 2.0 Interface. All drivers and supporting software for the WLAN 11n USB 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 server.

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).

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.

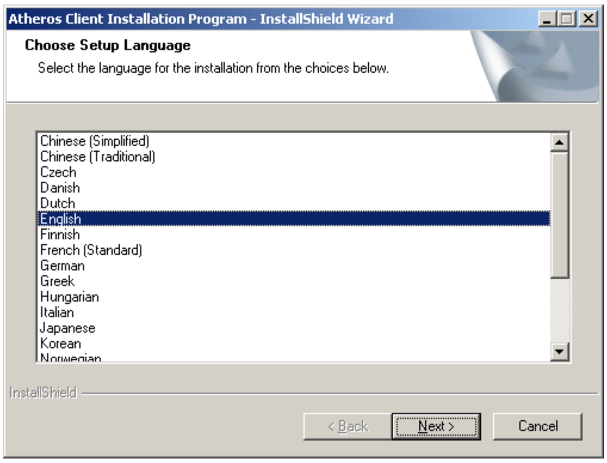
In network with dynamic IP addressing, a DHCP server in the network dynamically assigns IP addresses to all clients every time they log on to the network. Network using dynamic IP address requires setting up and running a DHCP Server.

4 INSTALL DRIVER / UTILITY

The installation & driver CD will automatically activate the autorun installation program after you insert the disk into your CD drive.

Step 1 :

Insert the installation & driver CD into your CD-ROM, chose your language and click **Next** to continue.



Atheros Client Installation Program - InstallShield Wizard

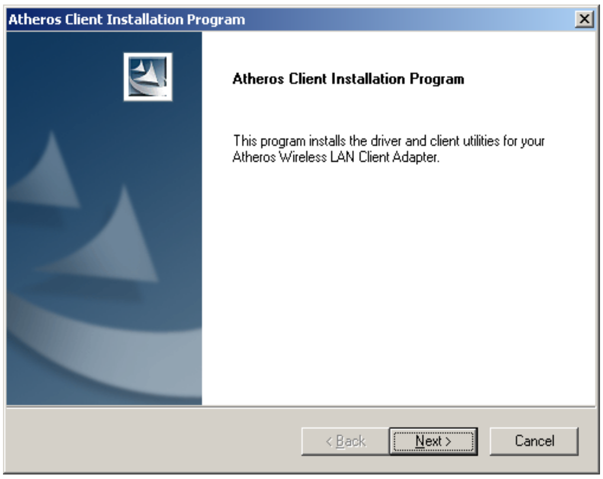
Choose Setup Language

Select the language for the installation from the choices below.

Chinese (Simplified)
Chinese (Traditional)
Czech
Danish
Dutch
English
Finnish
French (Standard)
German
Greek
Hungarian
Italian
Japanese
Korean
Norwegian

Step 2 :

Click **Next** to continue.



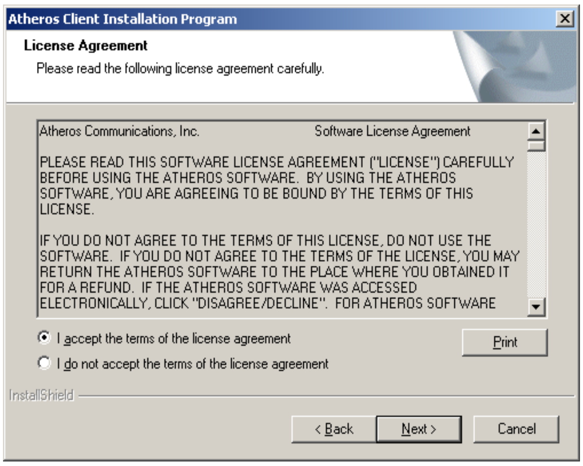
Atheros Client Installation Program

Atheros Client Installation Program

This program installs the driver and client utilities for your Atheros Wireless LAN Client Adapter.

Step 3 :

Choose accept and click **Next** to continue.



Atheros Client Installation Program

License Agreement

Please read the following license agreement carefully.

Atheros Communications, Inc. Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING THE ATHEROS SOFTWARE. BY USING THE ATHEROS SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE.

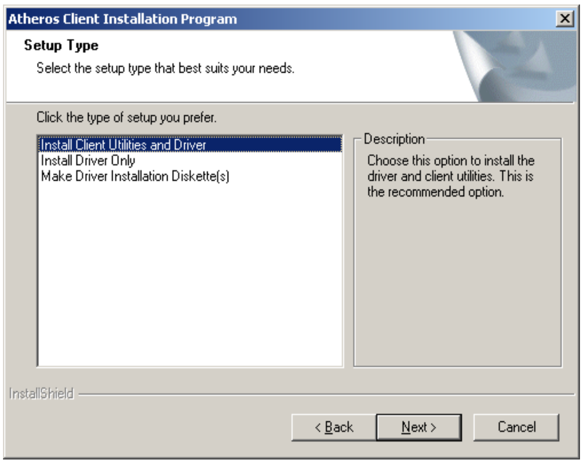
IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE ATHEROS SOFTWARE TO THE PLACE WHERE YOU OBTAINED IT FOR A REFUND. IF THE ATHEROS SOFTWARE WAS ACCESSED ELECTRONICALLY, CLICK "DISAGREE/DECLINE". FOR ATHEROS SOFTWARE

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Step 4 :

Choose the installation type. To install the client utilities and driver, select the appropriate button and click **Next**.



Atheros Client Installation Program

Setup Type

Select the setup type that best suits your needs.

Click the type of setup you prefer.

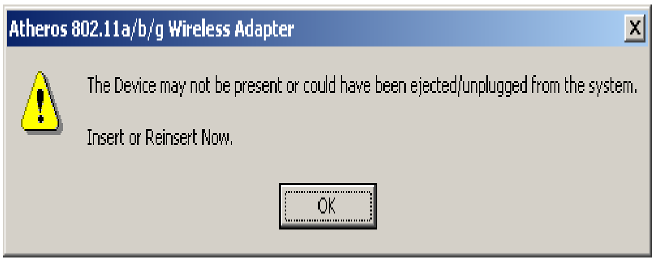
- Install Client Utilities and Driver
- Install Driver Only
- Make Driver Installation Diskette(s)

Description

Choose this option to install the driver and client utilities. This is the recommended option.

Step 5 :

Insert WLAN USB adapter into USB port and click OK to continue.



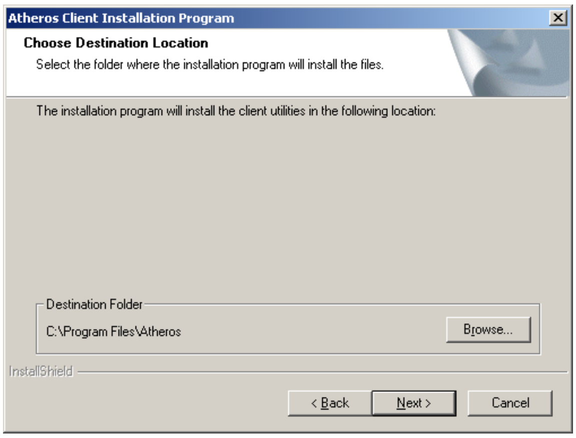
Atheros 802.11a/b/g Wireless Adapter

The Device may not be present or could have been ejected/unplugged from the system.

Insert or Reinsert Now.

Step 6 :

Click **Next** to install at the designated folder. Or, click “Browse” to select different folder.



Atheros Client Installation Program

Choose Destination Location

Select the folder where the installation program will install the files.

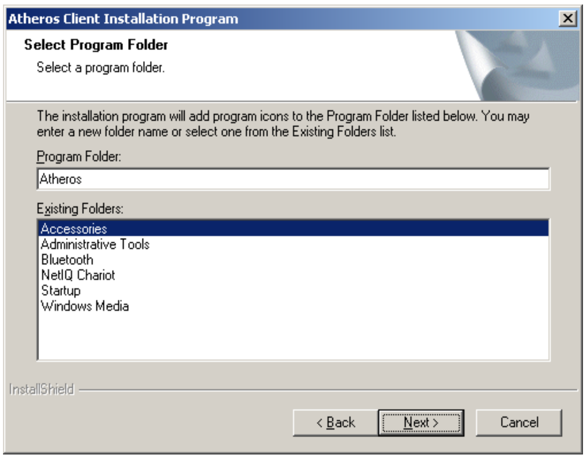
The installation program will install the client utilities in the following location:

Destination Folder

C:\Program Files\Atheros

Step 7 :

Click **Next** to continue.



Atheros Client Installation Program

Select Program Folder

Select a program folder.

The installation program will add program icons to the Program Folder listed below. You may enter a new folder name or select one from the Existing Folders list.

Program Folder:

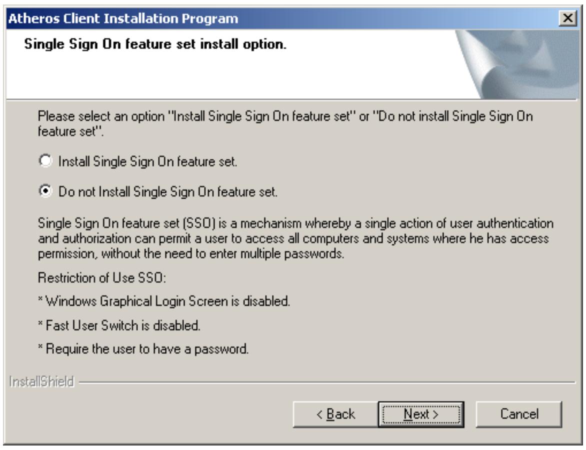
Atheros

Existing Folders:

- Accessories
- Administrative Tools
- Bluetooth
- NetIQ Chariot
- Startup
- Windows Media

Step 8 :

If you have multiple computers to access, choose SSO(Single sign on) feature set. Or you can choose “Do not install SSO feature set” and Click **Next** to continue.



Atheros Client Installation Program

Single Sign On feature set install option.

Please select an option "Install Single Sign On feature set" or "Do not install Single Sign On feature set".

○ Install Single Sign On feature set.

● Do not Install Single Sign On feature set.

Single Sign On feature set (SSO) is a mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords.

Restriction of Use SSO:

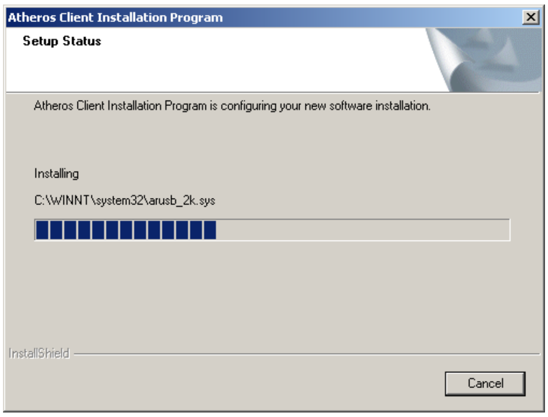
* Windows Graphical Login Screen is disabled.

* Fast User Switch is disabled.

* Require the user to have a password.

Step 9 :

Start copying files until it finishes the installation.



Atheros Client Installation Program

Setup Status

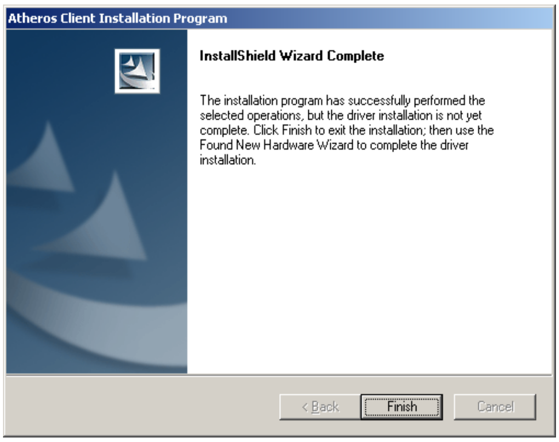
Atheros Client Installation Program is configuring your new software installation.

Installing

C:\WINNT\system32\arusb_2k.sys

Step 10 :

Click **Finish** to complete installation.



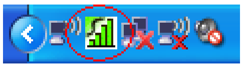
Atheros Client Installation Program

InstallShield Wizard Complete

The installation program has successfully performed the selected operations, but the driver installation is not yet complete. Click Finish to exit the installation; then use the Found New Hardware Wizard to complete the driver installation.

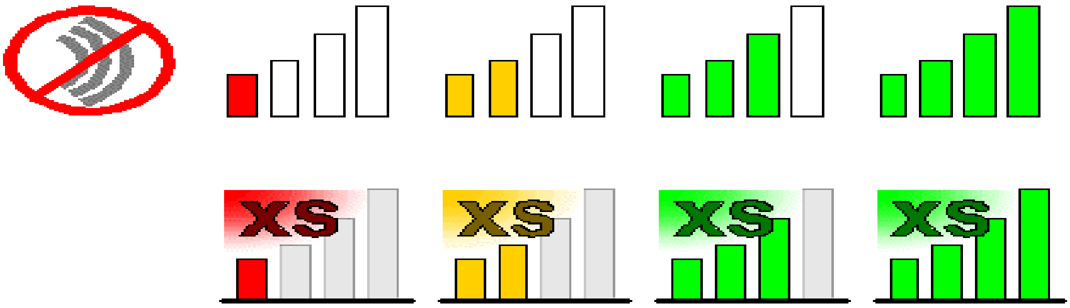
5 Wireless Network Configuration in Station mode

WLAN 11n USB Adapter uses its own management software. All functions controlled by users are provided by this application. When you insert the WLAN 11n USB Adapter into the USB port of your PC, a new icon should appear in the Windows System Tray automatically.



5.1 TRAY ICON

The tray icon appears at the bottom of the screen, and shows the signal strength using colors and the received signal strength indication (RSSI).



Hold the mouse cursor over the tray icon to display the current configuration profile name and association, as well as transmit and receive speed and the wireless adapter name and IP address.

Right-click on the tray icon to:

Help	Open the online help.
Open Atheros Client Utility	Launch the Atheros Client Utility (ACU). Use the ACU to configure the profile or view status and statistics information.
Client Managed Test	Run the Client Managed Test Utility.

Preferences Set the startup options and menu options for the ACU. Check whether the program should start automatically when Windows starts, and check the menu items that should appear on the popup menu.

Enable/Disable Radio Enable or disable the RF Signal.

Manual LEAP Login Log in to LEAP manually, if LEAP is set to manually prompt for user name and password on each login.

Reauthenticate Reauthenticate to the access point.

Select Profile Click a configuration profile name to switch to it. If no configuration profile exists for a connection, add a profile first.

Show Connection Status Display the Connection Status window. This window displays information about the connection:

Active Profile	Displays the name of the active configuration profile.
Auto Profile Selection	Shows whether auto profile selection is enabled.
Connection Status	Displays whether the adapter is connected to a wireless network.
Link Quality	Lists the quality of the link connection.
SSID	Displays the SSID of the associated network.
Access	Shows the name of the access point the

	wireless adapter is connected to.
Access Point IP Address	Shows the IP address of the access point the wireless adapter is connected to.
Current Receive Rate	Shows the current receive rate in Mbps.
Current Transmit Rate	Shows the current transmit rate in Mbps.
Client Adapter IP Address	Displays the IP address of the wireless adapter.

Exit Exit the Atheros Client Utility application.

The colors are defined as follows:

Color	Quality	RSSI*
Green	Excellent	20 dB +
Green	Good	10-20 dB +
Yellow	Poor	5-10 dB
Red	Poor	< 5 dB
Gray	No Connection	No Connection

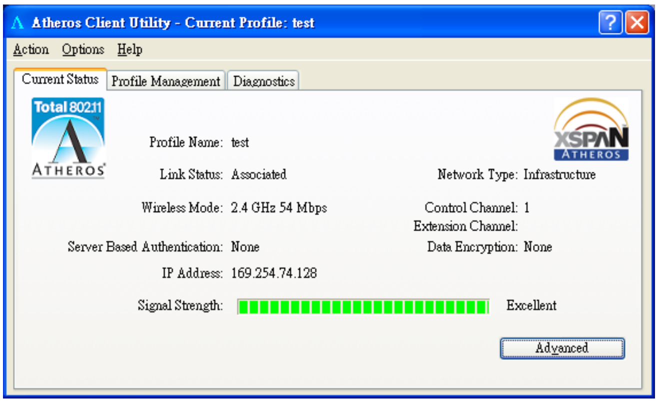
*Received signal strength indication RSSI. Displayed in dB or percentage.

Enable or disable the tray icon in the Action menu.

5.2 GENERAL CONNECTION SETTING

5.2.1 Current Status

The Current Status tab contains general information about the program and its operations. The Current Status tab does not require any configuration.



Profile Name: test

Link Status: Associated

Network Type: Infrastructure

Wireless Mode: 2.4 GHz 54 Mbps

Control Channel: 1

Extension Channel:

Server Based Authentication: None

Data Encryption: None

IP Address: 169.254.74.128

Signal Strength: Excellent

The following table describes the items found on the Current Status screen.

Profile Name	The name of the current selected configuration profile. Set up the configuration name on the General tab.
Link Status	Shows whether the station is associated to the wireless network.
Wireless Mode	Displays the wireless mode. Configure the wireless mode on the Advanced tab.
IP Address	Displays the computer's IP address.
Network Type	The type of network the station is connected to. The options include: • Infrastructure (access point) • Ad Hoc Configure the network type on the Advanced tab.
Current Channel	Shows the currently connected channel.
Control Channel	Shows the control channel. Available for 802.11n devices only.
Extension Channel	Shows the extension channel. Displayed only if the STA is connected in a 40 MHz channel. Available for 802.11n devices

	only.
Server Based Authentication	Shows whether server based authentication is used.
Data Encryption	Displays the encryption type the driver is using. Configure the encryption type on the Security tab.
Signal Strength	Shows the strength of the signal.

Click the Advanced button to see the advanced status diagnostics.

The following table describes the items found on the Advanced Status screen.

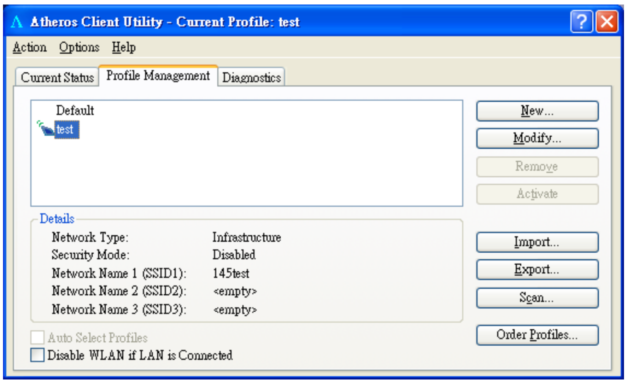
Network Name (SSID)	Displays the wireless network name. Configure the network name on the General tab.
Server Based Authentication	Shows whether server based authentication is used.
Data Encryption	Displays the encryption type the driver is using. Configure the encryption type on the Security tab.
Authentication Type	Displays the authentication mode. Configure the authentication mode on the General tab.
Message Integrity Check	Shows whether MIC is enabled. MIC prevents bit-flip attacks on encrypted packets.
Associated AP Name	Displays the name of the access point the wireless adapter is associated to.
Associated AP IP Address	Shows the IP address of the access point the wireless adapter is associated to.
Associated AP MAC Address	Displays the MAC address of the access point the wireless adapter is associated to.

11n MIMO Power Save	Shows the MIMO power save mode status. Available for 802.11n devices only.
Power Save Mode	Shows the power save mode. Power management is disabled in ad hoc mode. Configure the power save mode on the Advanced tab.
Current Power Level	Displays the transmit power level rate in mW. Configure the transmit power level on the Advanced tab.
Available Power Levels	Shows the 2.4 GHz available power levels.
Current Signal Strength	Shows the current signal strength in dBm.
Current Noise Level	Displays the current noise level in dBm.
Up Time	Shows how long the client adapter has been receiving power (in hours:minutes:seconds). If the adapter runs for more than 24 hours, the display shows in days:hours:minutes:seconds.
802.11b Preamble	Displays the 802.11b preamble format. Configure the preamble format on the Advanced tab.
Current Receive Rate	Shows the current receive rate in Mbps.
Current Transmit Rate	Displays the current transmit rate in Mbps.
Channel	Shows the currently connected channel.
Control Channel	Shows the current control channel. Available for 802.11n devices only.
Extension Channel	Shows the extension channel. Displayed only if the STA is connected in a 40 MHz channel. Available for 802.11n devices only.
Frequency	Displays frequency the station is using.

Control Frequency	Displays control frequency the station is using. Available for 802.11n devices only.
Extension Frequency	Displays extension frequency the station is using. Available for 802.11n devices only.
Channel Set	Shows the current channel set.
Channel Width	Shows the channel width. Available for 802.11n devices only.
QoS	The type of quality of service that is currently being used by your client adapter. QoS on wireless LANS (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification. A value of None represents that the WMM standard QoS is not enabled. A value of WMM represents that a component of the IEEE 802.11e WLAN standard for QoS is enabled.

5.2.2 Profile Management

Configure the wireless network adapter (wireless card) from the Profile Management tab of the Atheros Client Utility.



Details

Network Type: Infrastructure

Security Mode: Disabled

Network Name 1 (SSID1): 145test

Network Name 2 (SSID2): <empty>

Network Name 3 (SSID3): <empty>

□ Auto Select Profiles

□ Disable WLAN if LAN is Connected

a. Create or Modify a Configuration Profile

To add a new configuration profile, click New on the Profile Management tab. To modify a configuration profile, select the configuration from the Profile list and click the Modify button.

To configure a profile for ad hoc or access point (infrastructure) mode, edit the Network Type field on the Advanced tab.

Note that the ACU only allows the creation of 16 configuration profiles. After the creation of 16 profiles, clicking the New button displays an error message. Remove an old profile or modify an existing profile for a new use.

b. Remove a Configuration Profile

1. Go to the Profile Management tab.
2. Select the profile to remove from the list of configuration profiles.
3. Click the Remove button.

c. Activate a Configuration Profile

1. To switch to a different profile, go to the Profile Management tab.
2. Click on the profile name in the Profile List.
3. Click the Activate button.

The Profile List provides icons that specify the operational state for that profile. The list also provides icons that specify the signal strength for that profile.

d. Import and Export Profiles

Importing a Profile :

1. From the Profile Management tab, click the Import button. The Import Profile window appears.
2. Browse to the directory where the profile is located.
3. Highlight the profile name.
4. Click **Open**. The imported profile appears in the profiles list.

Exporting a Profile :

From the Profile Management tab, highlight the profile to export.
Click the **Export** button. The Export Profile window appears.
Browse to the directory to export the profile to.
Click **Save**. The profile is exported to the specified location.

e. Ordering Profiles

Including a profile in the auto selection feature allows the wireless adapter to automatically select that profile from the list of profiles and use it to connect to the network.
Including a profile in auto profile selection:
On the Profile Management tab, click the Order Profiles button.
The Auto Profile Selection Management window appears, with a list of all created profiles in the Available Profiles box.
Highlight the profiles to add to auto profile selection, then click Add. The profiles appear in the Auto Selected Profiles box.
Ordering the auto selected profiles:
Highlight a profile in the Auto Selected Profiles box.
Click Move Up, Move Down, or Remove as appropriate.
The first profile in the Auto Selected Profiles box has highest priority, and the last profile has lowest priority.
Click OK.
Check the Auto Select Profiles box.
Save the modified configuration file.
When auto profile selection is enabled by checking Auto Select Profiles on the Profile Management tab, the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID, and so on.

With auto profile selection enabled, the wireless adapter scans for available networks. The highest priority profile with the same SSID as a found network is used to connect to the network. On a failed connection, the client adapter tries with the next highest priority profile.

5.2.3 Diagnostics

The Diagnostics tab of the Atheros Client Utility provides buttons used to retrieve receive and transmit statistics. The Diagnostics tab does not require any configuration.

The Diagnostics tab lists the following receive and transmit diagnostics for frames received by or transmitted by the wireless network adapter:

Multicast packets transmitted and received

Broadcast packets transmitted and received

Unicast packets transmitted and received

Total bytes transmitted and received

Click the Adapter Information button for more general information about the the wireless network adapter and the network driver interface specification (NDIS) driver.

Click the Advanced Statistics button on the Diagnostics tab to also show receive and transmit statistical information for the following receive and transmit diagnostics for frames received by or transmitted to the wireless network adapter:

Transmitted Frames

Frames transmitted OK

Frames retried

Frames dropped

No ACK frames

ACK frames

RTS frames

Clear-to-send (CTS) frames

No CTS frames

Retried RTS frames

Retried data frames

Received Frames

Frames received OK

Beacons Received

Frames Received with errors

CRC errors

Encryption errors

Duplicate frames

AP mismatches

Data rate mismatches

Authentication time-out

Authentication rejects: the number of AP authentication failures received by the wireless network adapter

Association time-out

Association rejects: the number of access point authentication rejects received by the wireless network adapter

Standard MIC OK

Standard MIC errors

CKIP MIC OK

CKIP MIC errors

5.3 Security

In the Atheros Client Utility, access the Security tab by clicking New or Modify on the Profile Management tab. Click the Security tab in the Profile Management window.
Edit the fields in the Security tab of Profile Management to configure the profile. To define the security mode, select the radio button of the desired security mode. Make sure to also edit the General and Advanced tabs.
Note: If the Profile Locked checkbox is checked, Profile cannot be removed or modified. However the password fields can be edited. Contact your system administrator.

The type of security mode the station is using. The options include the following:

5.3.1 **WPA/WPA2**

Enables the use of Wi-Fi Protected Access (WPA).
Choosing WPA/WPA2 opens the WPA/WPA2 EAP drop-down menu. The options include:
EAP-FAST
To use EAP-FAST security, the machine must already support EAP-FAST. Check with the IT manager.
Click the Security tab from the Profile Editor window.
Click Configure. The Define EAP-FAST window appears.
Choose an EAP-FAST authentication method from the EAP-FAST Authentication Method drop-down list.
Click Configure.

If you chose GTC Token/Password from the EAP-FAST Authentication Method drop-down list and clicked Configure, the Define PEAP (EAP-GTC) Configuration window appears. To know more about this option refer Using PEAP (EAP-GTC) security.

If you chose MSCHAPv2 Username and Password from the EAP-FAST Authentication Method drop-down list and clicked Configure, the Configure Username and Password window appears. To know more about this option refer Using PEAP-MSCHAP V2 security.
If you chose TLS Client Certificate from the EAP-FAST Authentication Method drop-down list and clicked Configure, the Define Certificate window appears. When configuring EAP-TLS for EAP-FAST, you can check the Authenticate Server Identity check box to force the system to authenticate the identity of the server as an added level of security. This option is available only when configuring EAP-FAST. To know more about this option refer Using EAP-TLS security.

If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the No Network Connection Unless User is Logged In check box. The default setting is checked.
Perform one of the following:

If you want to enable automatic PAC provisioning, make sure the Allow Automatic PAC Provisioning for this Profile check box is checked. A protected access credentials (PAC) file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.). This is the default setting.
If you want to enable manual PAC provisioning, uncheck the Allow Automatic PAC Provisioning for this Profile check box. This option requires you to choose a PAC authority or manually import a PAC file.

From the Select one or more PAC Authority to use with this Profile list, highlight the PAC authorities associated with the network defined by the profile's SSID. The list contains the names of all the authentication servers from which you have previously provisioned a PAC.
Click Manage. The Select EAP-FAST PAC window appears.

This window lets you group PAC authorities to facilitate authentication while roaming. For example, if there are three PAC authorities at a certain site covering different areas of the site, you can create a group containing these authorities and select one of them in the PAC list. In this way, if you're roaming around the site, the other authorities in the group will allow you access to the network.

A group consists of one or more authorities. Each authority may have one or more PAC files. A PAC authority can belong to only one group.
To create a new group, click New Group. A group consists of one or more authority servers that the user trusts. To rename the group, right-click the group and choose Rename. You can also rename the group by clicking it and typing the new name.

When you create a new group, you can either import a PAC file into it using the Import button or you can move a PAC from another group to the new group.
To import a PAC, click Import. The PAC Import window appears. Do the following:
Click Browse and select a PAC file to import. The default location is C:/Program Files/Atheros.
Click the PAC file (*.pac) so that it appears in the File name box at the bottom of the window.
Click Open.
If the Enter Password window appears, enter the PAC file password, which can be obtained from your system administrator, and click OK.

Note: PAC file passwords are optional. The PAC authority determines whether to issue PAC files that require user-supplied passwords. Nevertheless, all PAC files (even those without passwords) are encrypted and protected. PAC file passwords are different from EAP-FAST passwords and need to be entered only once, at the time a PAC is imported.
If you try to import a PAC file with the same PAC ID as a previously imported PAC file, you are asked to update the existing PAC. If you click Yes, the existing PAC is replaced by the new one from the imported file.
If the PAC file was imported successfully, the following message appears: "EAP-FAST PAC file was imported and is ready for use." Click OK to return to the PAC Import window.
Click one of these PAC store options to determine where the imported PAC file will be stored and by whom it will be accessible:

Global - PACs that are stored in the global PAC store can be accessed and used by any user at any logon stage. Global PACs are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User is Logged In option.

Private - PACS that are stored in the private store can be accessed and used only by the user who provisioned them or the system administrator. They are not accessible until the user is logged onto the local system. This is the default option.
Click Import. The PAC file appears under the selected group.
To delete a group, select the group and click Delete. You can also delete the group by right-clicking the group and choosing Delete.
To close the Select EAP-FAST PAC window, click Close.
To automatically use PACs belonging to the same PAC authority group, check the Use Any PAC Belonging to the Same Group check box.
Check the Use Machine PAC for Domain Logon check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.
Click OK when done configuring EAP-FAST.

EAP-TLS

To use EAP-TLS security In the Atheros Client Utility, access the Security tab in the Profile Management window.
On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
Choose EAP-TLS from the drop-down menu.
Enabling EAP-TLS security:
To use EAP-TLS security, the machine must already have the EAP-TLS certificates downloaded onto it. Check with the IT manager.
If EAP-TLS is supported, choose EAP-TLS from the drop-down menu on the right, then click the Configure button.
Click Configure. The Define Certificate window appears.
Check the Use Machine Information for Domain Login check box if you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

Note: If you do not check the Use Machine Information for Domain Logon

check box, machine authentication is not performed. Authentication does not occur until you log on.
Check the Validate Server Identity check box to force the system to authenticate the identity of the server as an added level of security.
If you checked the Use Machine Information For Domain Logon check box in the previous step, the Always Do User Authentication check box at the bottom of the window becomes active. Perform one of the following:

Check the Always Do User Authentication check box if you want the client to switch from using machine authentication to using user authentication after you log on using your username and password. This is the default setting.
Uncheck the Always Do User Authentication check box if you want the client to continue to use machine authentication after the user's computer logs into the domain.

Choose your server certificate in the Select a Certificate drop-down list.
Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down list.
Perform one of the following:

Leave the Server/Domain Name field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down list (recommended).
In the Server/Domain Name field, enter the domain name of the server from which the client will accept a certificate.

If the Login Name is filled in automatically, enter your username in this format: username@domain.
Click OK to save your changes and return to the Profile Management (Security) window.
Click OK.
Activate the profile.

EAP-TTLS

To use EAP security In the Atheros Client Utility, access the Security tab in the Profile Management window.
On the Security tab, choose the WPA/WPA2 radio button.

OR: On the Security tab, choose the 802.1x radio button.

Choose EAP-TTLS from the drop-down menu.

Enabling EAP-TTLS security:

To use EAP-TTLS security, the machine must already have the EAP-TTLS certificates downloaded onto it. Check with the IT manager.

If EAP-TTLS is supported, choose EAP-TTLS from the drop-down menu on the right, then click the Configure button.

Select the appropriate certificate from the drop-down list and click OK.

Specify a user name for EAP authentication:

Check Use Windows User Name to use the Windows user name as the EAP user name.

OR: Enter a EAP user name in the User Name field to use a separate user name and password and start the EAP authentication process.

Click Settings and:

Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (recommended)

Enter the domain name of the server from which the client will accept a certificate.

Change the login name if needed.

Click OK.

Enable the profile.

PEAP (EAP-GTC)

To use PEAP (EAP-GTC) security In the Atheros Client Utility, access the Security tab in the Profile Management window.

On the Security tab, choose the WPA radio button.

OR: On the Security tab, choose the 802.1x radio button.

Choose PEAP (EAP-GTC) from the drop-down menu.

To use PEAP (EAP-GTC) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.

Click the Configure button.

To resume connection without providing credentials again after a temporary loss of connection, check Always Resume the Secure Session.

Select the appropriate network certificate authority from the drop-down list.

Specify a user name for inner PEAP tunnel authentication:

Check Use Windows User Name to use the Windows user name as the PEAP

user name.
OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
Check the Validate Server Identity check box to force the system to authenticate the identity of the server as an added level of security.
Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box.
Choose Token or Static Password, depending on the user database.

Note that Token uses a hardware token device or the Secure Computing SofToken program (version 1.3 or later) to obtain and enter a one-time password during authentication.
Click Settings and:
Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box on the Define PEAP (EAP-GTC) Configuration window (recommended) or enter the domain name of the server from which the client will accept a certificate.
If the Login Name field is not filled in automatically, enter your username.
Click OK to save your settings and return to the Profile Management (Security) window.
Click OK.
Enable the profile.

PEAP (EAP-MSCHAP V2)

To use PEAP-MSCHAP V2 security In the Atheros Client Utility, access the Security tab in the Profile Management window.
On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
Choose PEAP (EAP-MSCHAP V2) from the drop-down menu.
To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.
Click the Configure button.
Check the Validate Server Identity check box to force the system to authenticate the identity of the server as an added level of security.
Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box.

Perform one of the following to specify how you want to establish a network connection.

If you want to connect using a username and password, choose User Name and Password.
If you want to connect using a user certificate installed on your computer, choose Certificate, select a certificate from the drop-down box and go to Step 6.

Specify the username and password for inner PEAP tunnel authentication:

Check Use Windows User Name to use the Windows user name as the PEAP user name.
OR: Enter a PEAP user name in the User Name field to use a separate user name for the PEAP authentication process.

Click Settings. The Configuration Setting window appears.
Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box on the Define PEAP (EAP-MSCHAP V2) Configuration window (this is the recommended option) or enter the domain name of the server from which the client will accept a certificate.
If the Login Name field is not filled in automatically, enter your username with nothing after it.
Click OK.
Enable the profile.

LEAP
To use security In the Atheros Client Utility, access the Security tab in the Profile Management window.
LEAP security requires that all infrastructure devices (e.g. access points and servers) are configured for LEAP authentication. Check with the IT manager.
Configuring LEAP
Enabling LEAP

Configuring LEAP:

On the Security tab, choose the WPA radio button. Choose WPA-LEAP from the drop-down menu.

OR: On the Security tab, choose the 802.1x radio button. Choose LEAP from the drop-down menu.

Click the Configure button.

To resume connection without providing credentials again after a temporary loss of connection, check Always Resume the Secure Session.

Specify a user name and password:

Select to Use Temporary User Name and Password by choosing the radio button:

Check Use Windows User Name to use the Windows user name as the LEAP user name.

OR: Check Manually Prompt for LEAP User Name and Password to manually login and start the LEAP authentication process.

Select to Use Saved User Name and Password by choosing the radio button:

Specify the LEAP user name, password, and domain to save and use.

Enter the user name and password.

Confirm the password.

Specify a domain name:

Check the Include Windows Logon Domain with User Name setting to pass the Windows login domain and user name to the RADIUS server. (default)

OR: Enter a specific domain name.

If desired, check No Network Connection Unless User Is Logged In to force the wireless adapter to disassociate after logging off.

Enter the LEAP authentication timeout time (between 30 and 500 seconds) to specify how long LEAP should wait before declaring authentication failed, and sending an error message. The default is 90 seconds.

Click OK.

Enable the profile.

5.3.2 **802.1x**

Enables 802.1x security. This option requires IT administration.

Choosing 802.1x opens the 802.1x EAP type drop-down menu. The options include:

EAP-FAST
EAP-TLS
EAP-TTLS
PEAP (EAP-GTC)
PEAP (EAP-MSCHAP V2)
LEAP
Please refer to 5.3.1 WPA/WPA2
If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.

5.3.3 WPA Passphrase

To use WPA Passphrase security In the Atheros Client Utility, access the Security tab in the Profile Management window.
On the Security tab, choose the WPA Passphrase radio button.
Click on the Configure button.
Fill in the WPA Passphrase.
Click OK.

5.3.4 Pre-Shared Key (Static WEP)

Enables the use of pre-shared keys that are defined on both the access point and the station.

To define pre-shared encryption keys, choose the Pre-Shared Key radio button and click the Configure button to fill in the Define Pre-Shared Keys window.

If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.

5.3.5 None

No security (not recommended).

7 INSTALL VISTA DRIVER

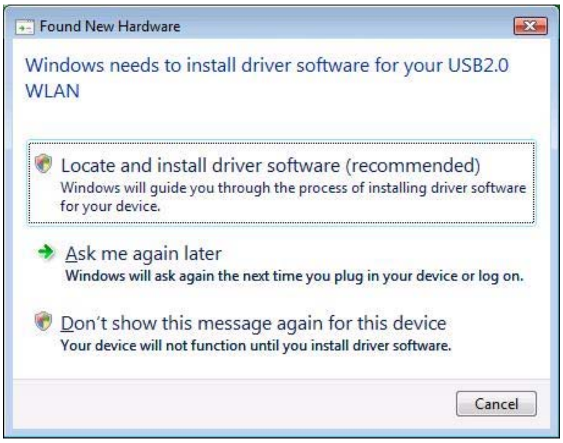
1. The installation & driver CD will automatically activate the autorun installation program after you insert the disk into your CD drive. Please refer to page 5 ”INSTALL DRIVER & UTILITY”

2. To install manually:

Plug your WLAN 11n USB Adapter into USB interface, windows Vista will search for compatible driver to install.

Step 1 :

Select “Locate and install the driver software”, Windows will guide you through the process of installing driver software for your device.



Windows needs to install driver software for your USB2.0 WLAN

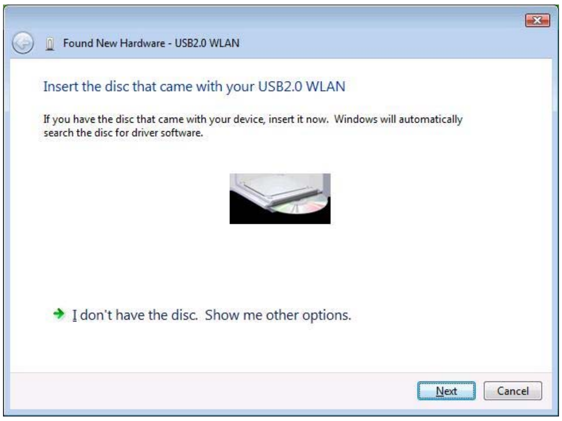
Locate and install driver software (recommended)
Windows will guide you through the process of installing driver software for your device.

Ask me again later
Windows will ask again the next time you plug in your device or log on.

Don't show this message again for this device
Your device will not function until you install driver software.

Step 2 :

Insert the installation disc into the CD-ROM and click “next” to continue installation.



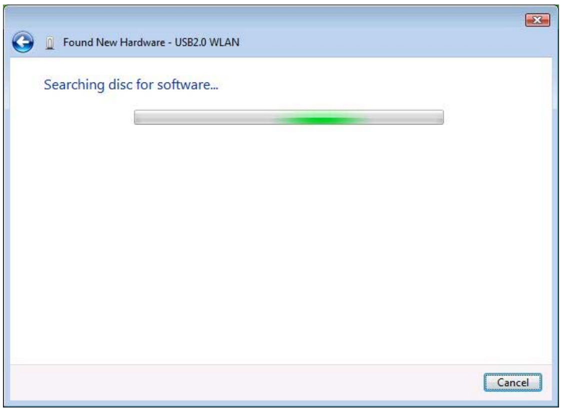
Insert the disc that came with your USB2.0 WLAN

If you have the disc that came with your device, insert it now. Windows will automatically search the disc for driver software.

I don't have the disc. Show me other options.

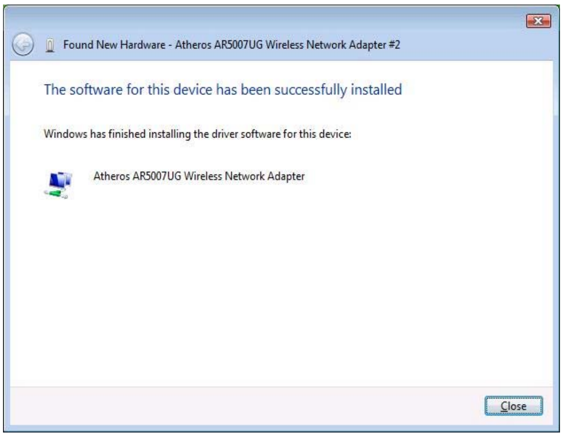
Step 3 :

Windows Vista search for the software and it will be installed successfully.



Found New Hardware - USB2.0 WLAN

Searching disc for software...



Found New Hardware - Atheros AR5007UG Wireless Network Adapter #2

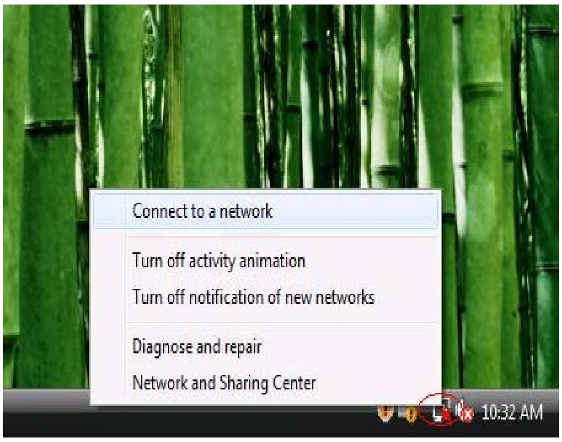
The software for this device has been successfully installed

Windows has finished installing the driver software for this device:

Atheros AR5007UG Wireless Network Adapter

Step 4 :

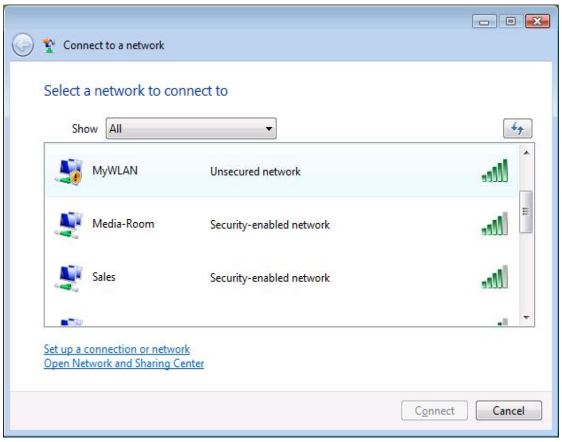
After installation, right click the network icon on the Windows Vista System Tray, and click “Connect to a network”.



Connect to a network
Turn off activity animation
Turn off notification of new networks
Diagnose and repair
Network and Sharing Center
10:32 AM

Step 5 :

Select a network to connect to and click “Connect”.



Connect to a network

Select a network to connect to

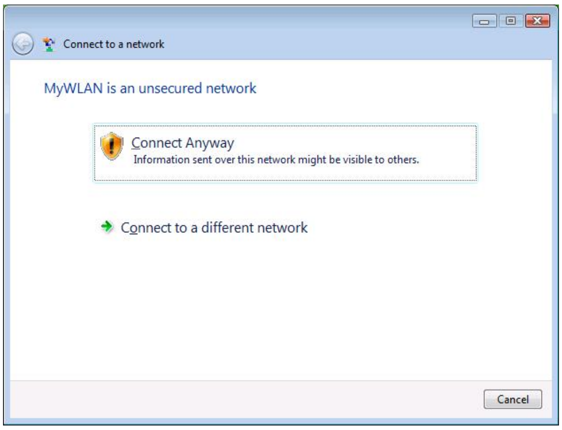
Show All

MyWLAN	Unsecured network	
Media-Room	Security-enabled network	
Sales	Security-enabled network	

Set up a connection or network
Open Network and Sharing Center

Step 6 :

Click “Connect Anyway” if the network is an unsecured network.

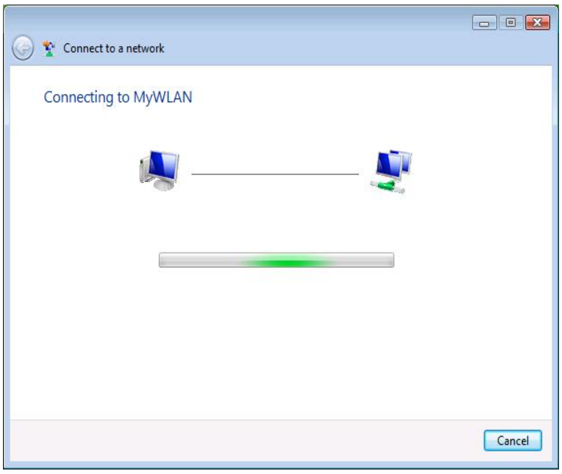


Connect to a network

MyWLAN is an unsecured network

Connect Anyway
Information sent over this network might be visible to others.

Connect to a different network

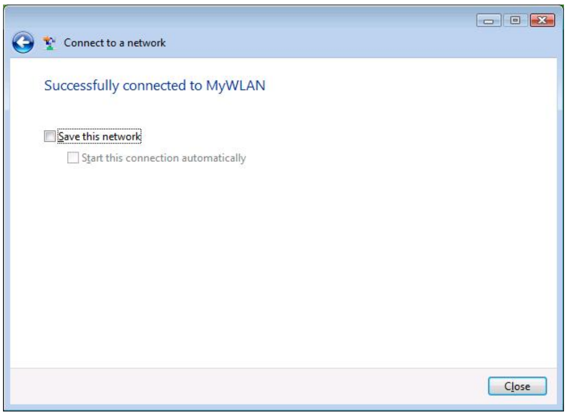


Connect to a network

Connecting to MyWLAN

Step 7:

USB Adapter successfully connected to network, Click “Close”



Connect to a network

Successfully connected to MyWLAN

□ Save this network

□ Start this connection automatically

8 TECHNICAL SPECIFICATIONS

Product Name	WLAN 11n USB Adapter
Standard	IEEE802.11n/b/g
Frequency Band	2.4GHz ISM band
Modulation method	BPSK/QPSK/16-QAM/64-QAM
Spread Spectrum	802.11b : DSSS (Direct Sequence Spread Spectrum)
	802.11g/n : OFDM (Orthogonal Frequency Division Multiplexing)
Data Rate	270/240/180/120/90/60/54/48/36/30/24/22/18/12/11/6/5.5/2/1Mbps and Maximum of 300Mbps.
Operation mode	Ad hoc
	Infrastructure (Access Points is needed)
Transmitter Output Power	< 13.5 dBm@11n, < 13.5 dBm@11b, < 13.5 dBm@11g
Receiver Sensitivity	Operating at 11Mbps: @ –80dBm
	Operating at 54Mbps: @ –70dBm
	Operating at 300Mbps: @ –64dBm
Operating Range	Indoor Up to 100 m, Outdoor Up to 280 m
Security	64-bit, 128-bit or WEP (Wired Equivalent Privacy); TKIP, AES
I/O Interface	USB 2.0
LED	Link/Active
Operating system supported	Windows 2000, XP and Vista
Management	Windows-based configuration utility and status monitoring
Regulation	FCC for North America
	CE/ETSI for European
Dimension	90 x 26 x 10.95 mm

Operating Temperature	-20 ~ 55 ℃
Storage Temperature	-10 ~ 70 ℃
Humidity	5 ~ 90% maximum (non-condensing)

9 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 **file and printer sharing** function is enabled. You can enable the function by checking the icon of **My Computer** -> **Control Panel** -> **Network** -> **file and printer sharing** -> **I want to be able to give others to access to my files**.

Symptom :
Slow or poor performance.
Remedy :
Try to select another channel for the communicating group or move your device closer to the Access Point.

10 GLOSSARY

IEEE 802.11 Standard

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

Access Point

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

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.

BSSID

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Roaming

In an infrastructure network, this is when a wireless PC moves out of range of the previously connected access point and connects to a newly connected access point. Throughout the network environment where access point is deployed, PCs can always be connected regardless of where they are located or roam.

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.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol is the network management protocol of TCP/IP. In SNMP, agents-which can be hardware as well as software-monitor the activity in the various devices on the network and report to the network console workstation. Control information about each device is maintained in a structure known as a management information block.

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.

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.

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.

Transmit / Receive

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

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.

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.

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.

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.

One Year Limited Warranty

- This device is guaranteed against manufacturing defects for one full year from the original date of purchase.
- This warranty is valid at the time of purchase and is non-transferable.
- This warranty must be presented to the service facility before any repair can be made.
- Sales slip or other authentic evidence is required to validate warranty.
- Damage caused by accident, misuse, abuse, improper storage, and/or uncertified repairs is not covered by this warranty.
- All mail or transportation costs including insurance are at the expense of the owner.
- Do not send any product to service center for warranty without a RMA (Return Merchandise Authorization) and proof of purchase. Ensure a trackable method of delivery is used (keep tracking number).
- Warranty is valid only in the country of purchase.
- We assumes no liability that may result directly or indirectly from the use or misuse of these products.

IMPORTANT

" This warranty will be voided if the device is tampered with, improperly serviced, or the security seals are broken or removed"