802.11n/b/g WLAN Module
WM5203

User's Manual

FCC Certification

Federal Communication Commission Interference Statement
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

CAUTION

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

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

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

USERS MANUAL OF THE END PRODUCT:
In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. If the size of the end product is smaller than 8x10cm, then additional FCC part 15.19 statement is required to be available in the users manual: This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

LABEL OF THE END PRODUCT:
The final end product must be labeled in a visible area with the following " Contains TX FCC ID: MQ4WM5203 ". If the size of the end product is larger than 8x10cm, then the following FCC part 15.19 statement has to also be available on the label: This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

IC Certification

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

IMPORTANT NOTE:
IC Radiation Exposure Statement:
This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
Declaración de exposición a la radiación de Canada:
Este equipo cumple con los límites de exposición a la radiación de la IC establecidos para un ambiente no controlado.
Este equipo se debe instalar y operar con una distancia mínima de 20 cm entre el radiador y su cuerpo.

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

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the IC RSS-102 radiation exposure limits set forth for an population/uncontrolled environment can be satisfied.

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

USERS MANUAL OF THE END PRODUCT:
In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the IC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. IC statement is required to be available in the users manual: This Class B digital apparatus complies with Canadian ICES-003. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

LABEL OF THE END PRODUCT:
The final end product must be labeled in a visible area with the following " Contains TX IC : 2826B-WM5203 ".

Table of Contents

CHAPTER 1: INTRODUCTION 1

FEATURES 1

PHYSICAL DETAILS 1

CHAPTER 2: INSTALLATION 1

FOR WINDOWS 2000/XP 1

Install Software 1

Install Hardware 4

Verification 4

FOR WINDOWS VISTA 5

Install Software 5

Install Hardware 7

Verification 7

FOR WINDOWS 7 8

Install Software 8

Install Hardware 10

Verification 10

CHAPTER 3: NETWORK CONNECTION 11

HOW TO MAKE A CONNECTION 11

HOW TO ADD A PROFILE 13

CHAPTER 4: UTILITY CONFIGURATION 14

FOR WINDOWS 2000/XP 14

Station Mode 14

Switch to AP Mode 23

Soft AP mode 24

FOR WINDOWS VISTA 29

Station Mode 29

Switch to AP Mode 38

Soft AP mode 39

FOR WINDOWS 7 44

Station Mode 44

Switch to AP Mode 53

Soft AP mode 54

CHAPTER 5: UNINSTALL 59

FOR WINDOWS 2000/XP 59

FOR WINDOWS VISTA 61

FOR WINDOWS 7 63

Chapter 1: Introduction

WM5203 measures just around 15 mm long and 15mm wide that make it hold the distinction of being the smallest USB dongle in the world at present. WM5203 give mobile workers the freedom of staying connected to the network while roaming around a building or multiple buildings maintaining access to the Internet, e-mail, networked applications with the best convenience in narrow or crowded space for it's ultra micro size.WM5203 is expected to be able to reach 150Mbps, which is relatively lower than normal, but still far more than sufficient to receive media streaming to the from access point.

Features

- 1T1R Mode with 150Mbps PHY Rate
- Complies with IEEE 802.11n and IEEE 802.11 b/g standards
- Supports WEP 64/128, WPA, WPA2
- Supports USB 2.0 interface

Chapter 2: Installation

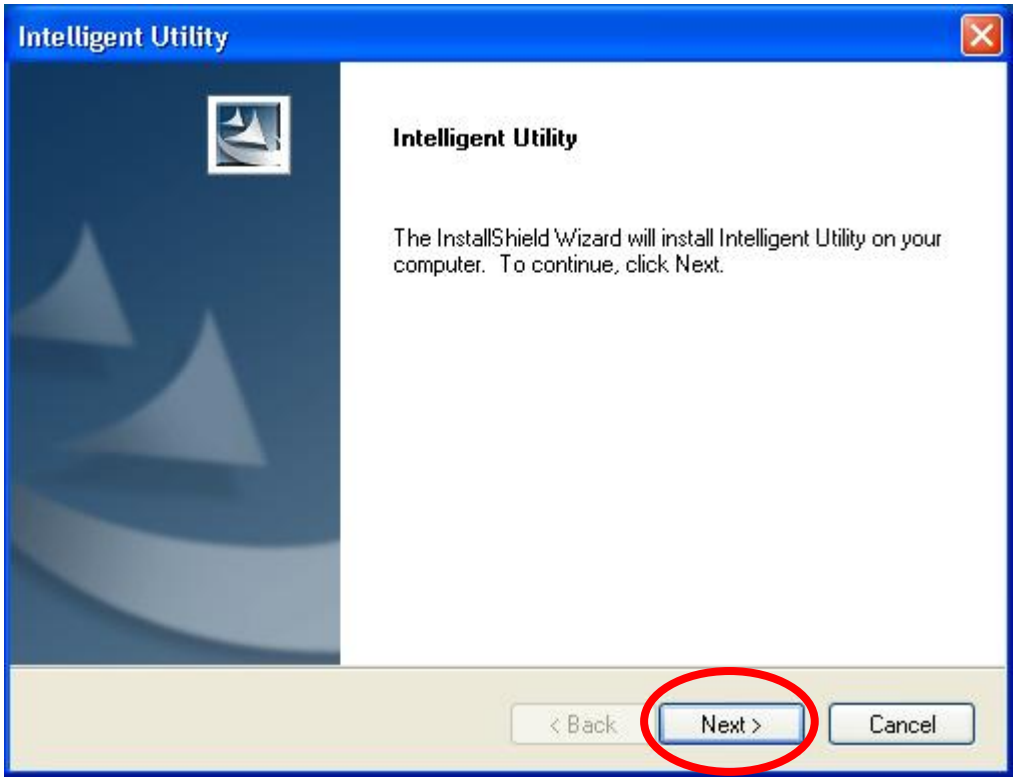
For Windows 2000/XP

Install Software

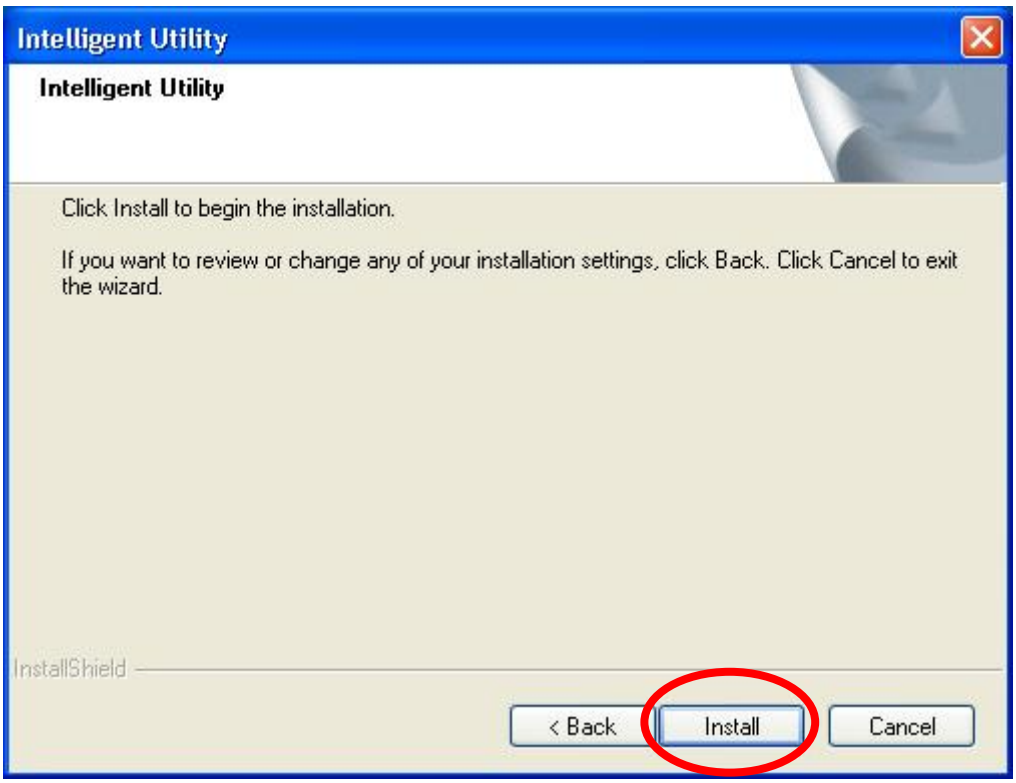
Note:

Do not insert the WLAN Module into the computer until the InstallShield Wizard finished installing.

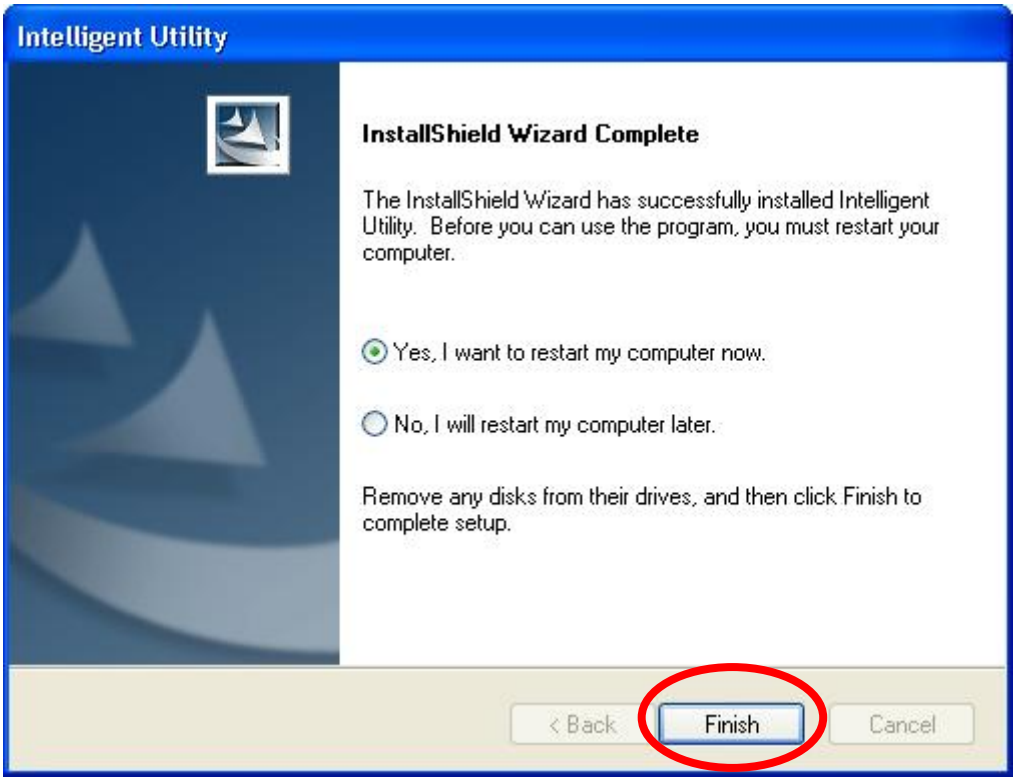
1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically. Please click **Next** to process the installation.



2. When prompt to the following message, please click **Install** to begin the installation.



3. When the following screen appears, click **Finish** to restart the computer to complete the software installation.



Install Hardware

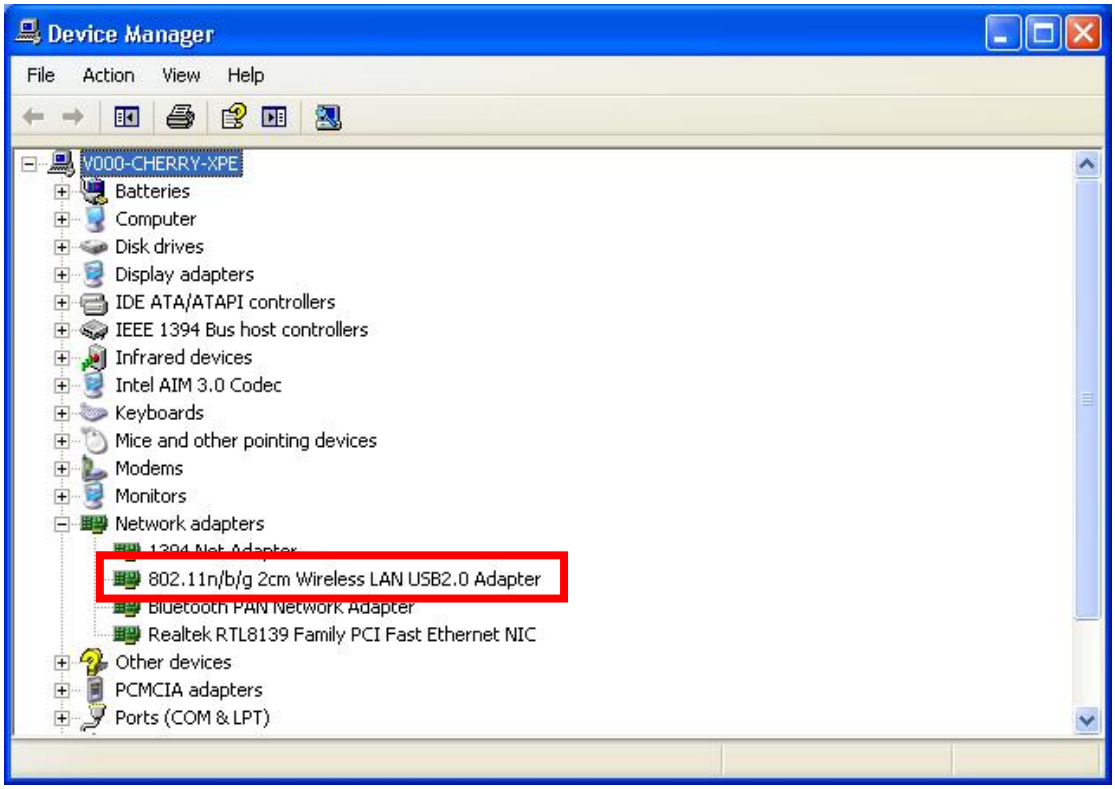
Note:

Insert the WLAN Module when finished software installation.

Insert the WLAN Module into the USB Port of the computer. The system will automatically detect the new hardware.

Verification

To verify the device is active in the computer. Go to **Start > Control Panel** > **System** > **Hardware**> **Device Manager**. Expand the **Network adapters** category. If the **802.11n/b/g 2cm Wireless LAN USB2.0 Adapter** is listed here, it means that the device is properly installed and enabled.



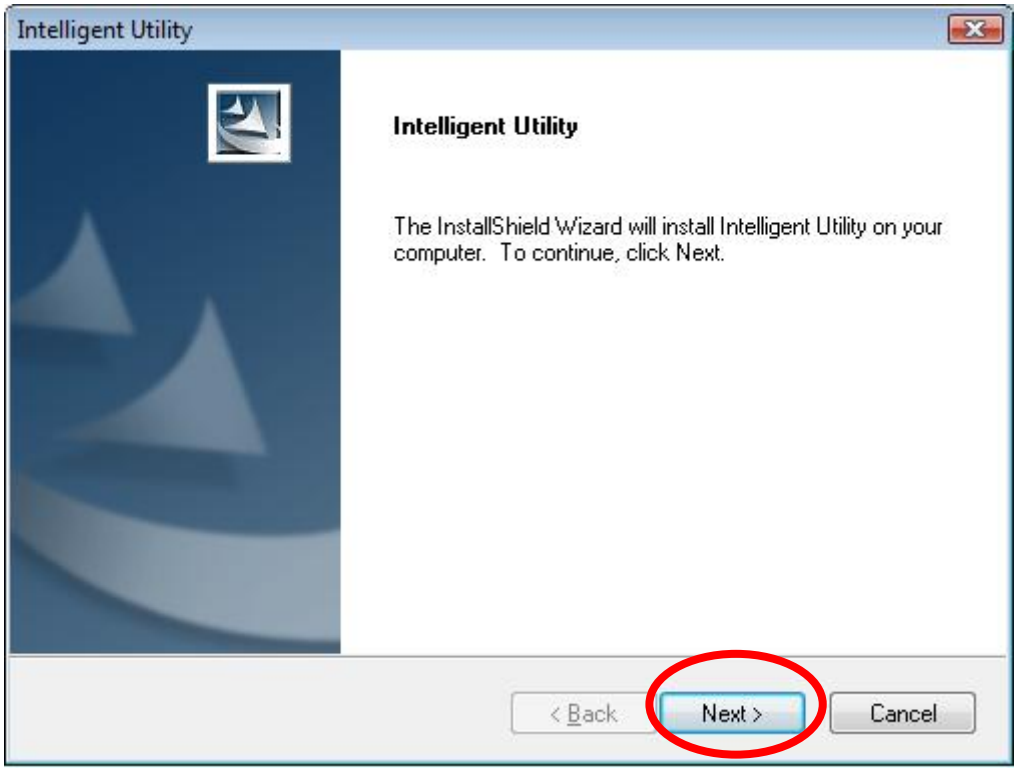
For Windows Vista

Install Software

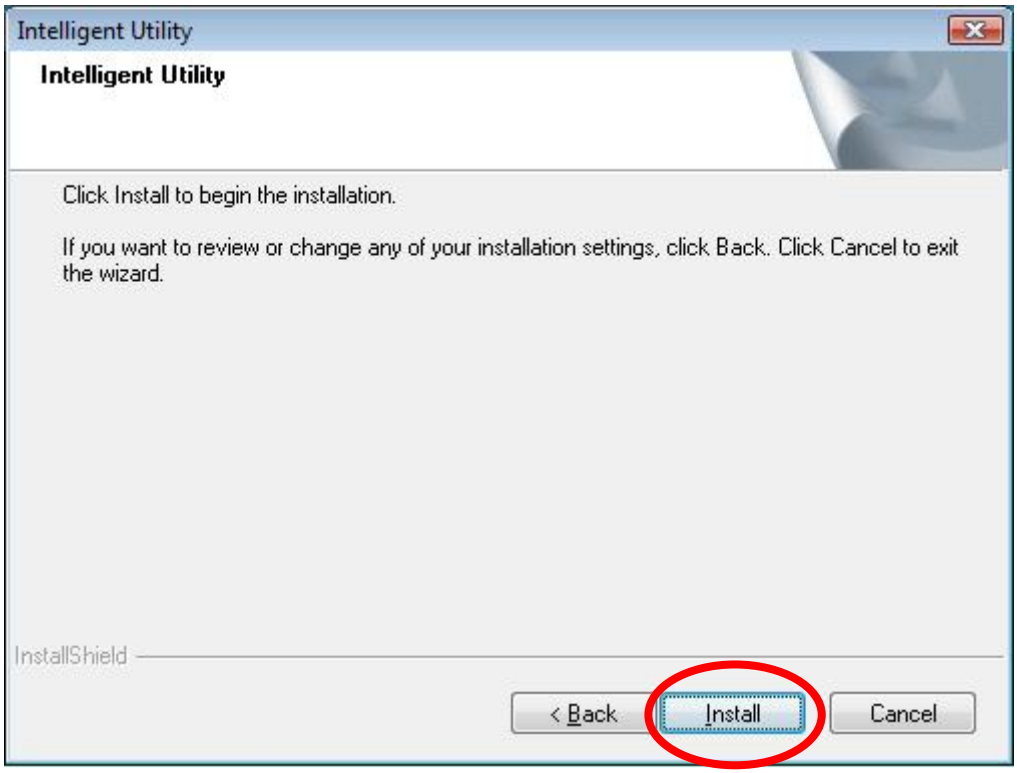
Note:

Do not insert the WLAN Module into the computer until the InstallShield Wizard finished installing.

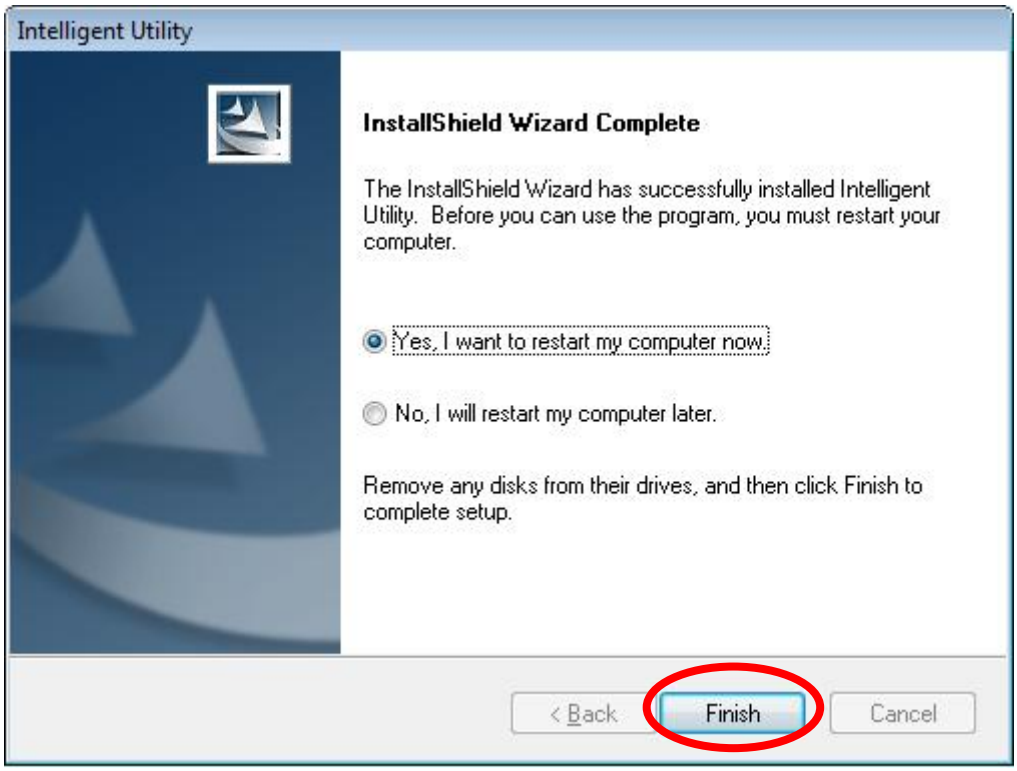
1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically. Please click **Next** to process the installation.



2. When prompt to the following message, please click **Install** to begin the installation.



3. When the following screen appears, click **Finish** to restart the computer to complete the software installation.



Install Hardware

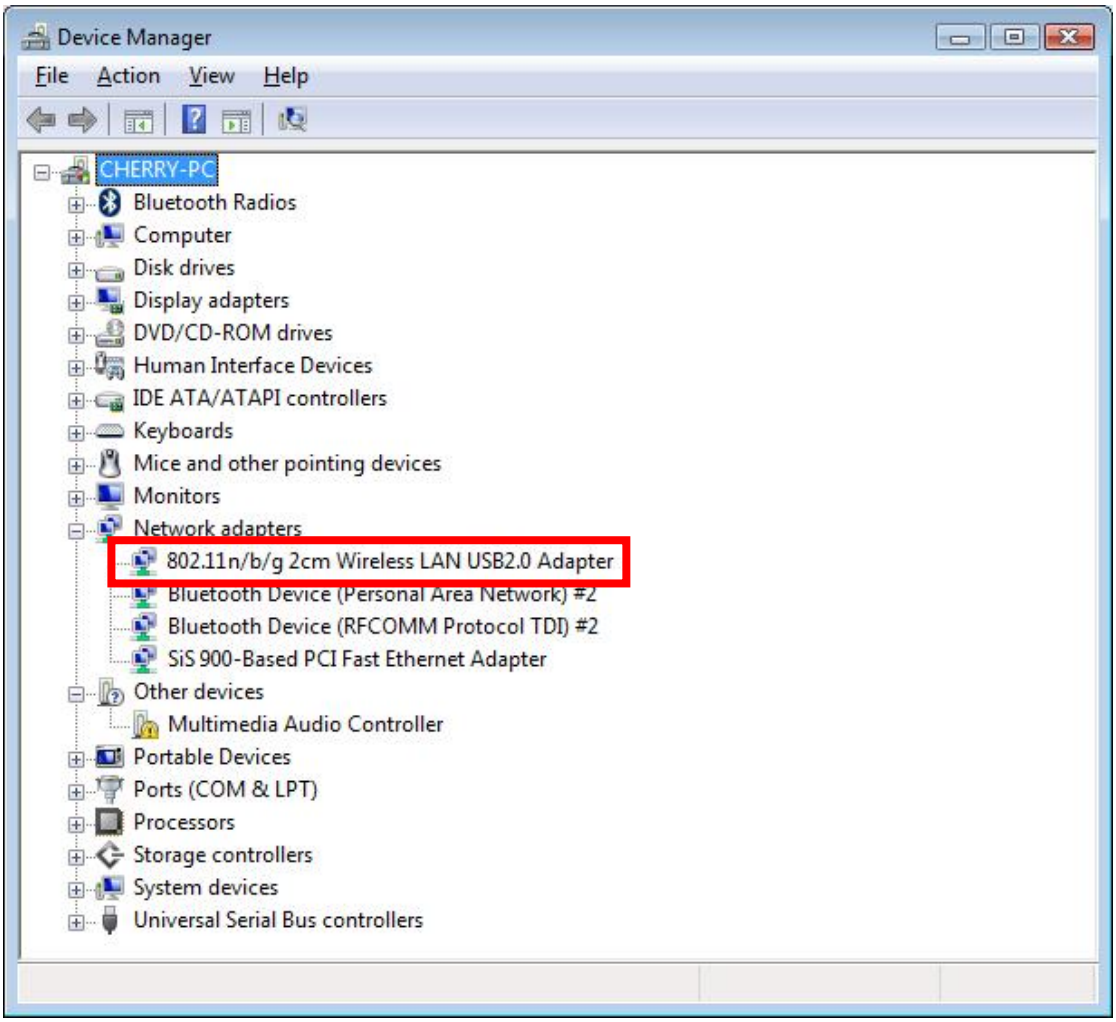
Note:

Insert the WLAN Module when finished software installation.

Insert the WLAN Module into the USB Port of the computer. The system will automatically detect the new hardware.

Verification

To verify the device is active in the computer. Go to **Start >Control Panel** > **Hardware and Sound** > **Device Manager**. Expand the **Network adapters** category. If the **802.11n/b/g 2cm Wireless LAN USB2.0 Adapter** is listed here, it means that the device is properly installed and enabled.



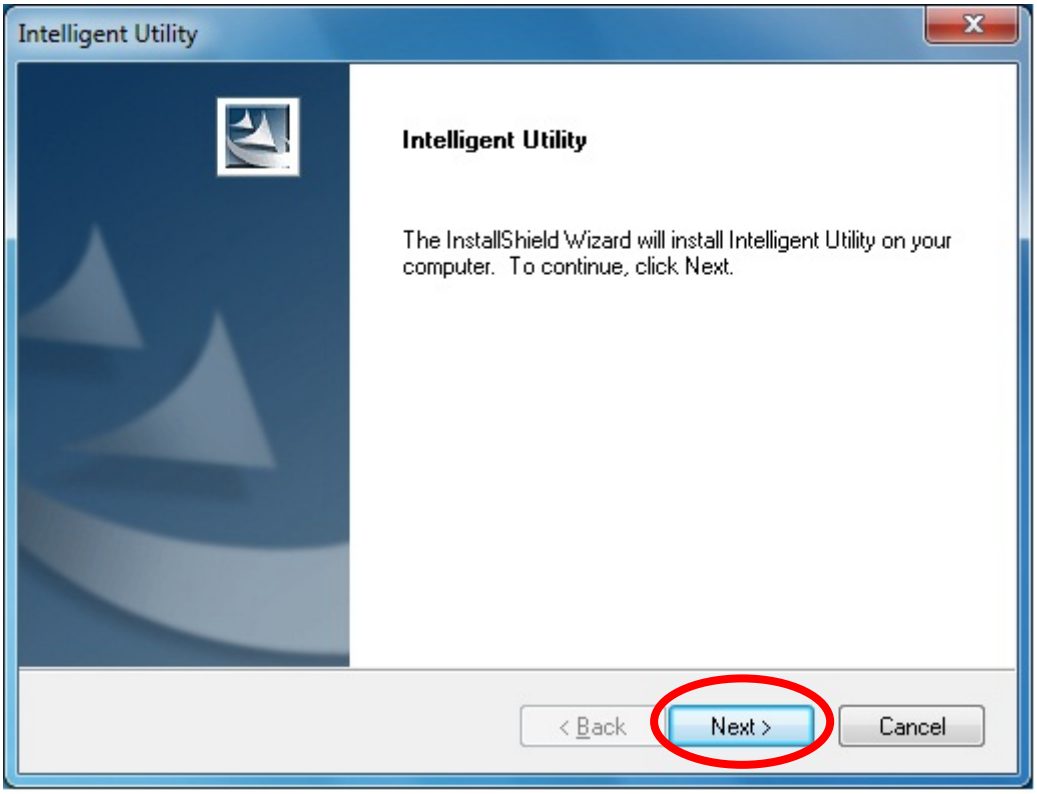
For Windows 7

Install Software

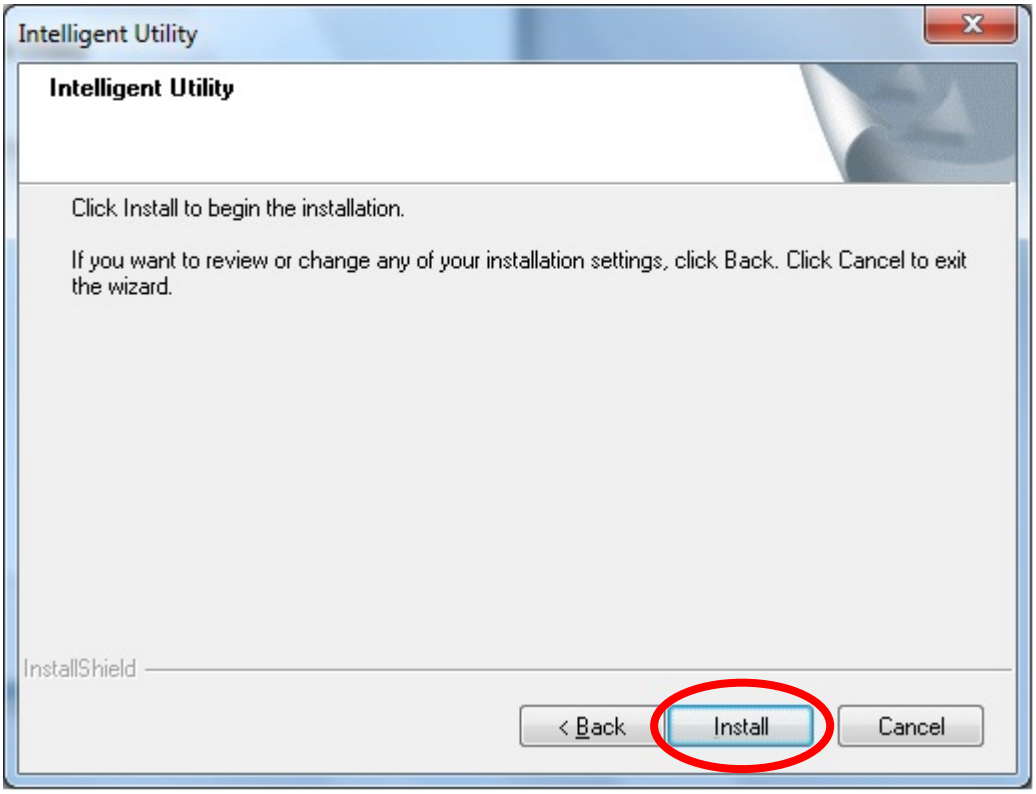
Note:

Do not insert the WLAN Module into the computer until the InstallShield Wizard finished installing.

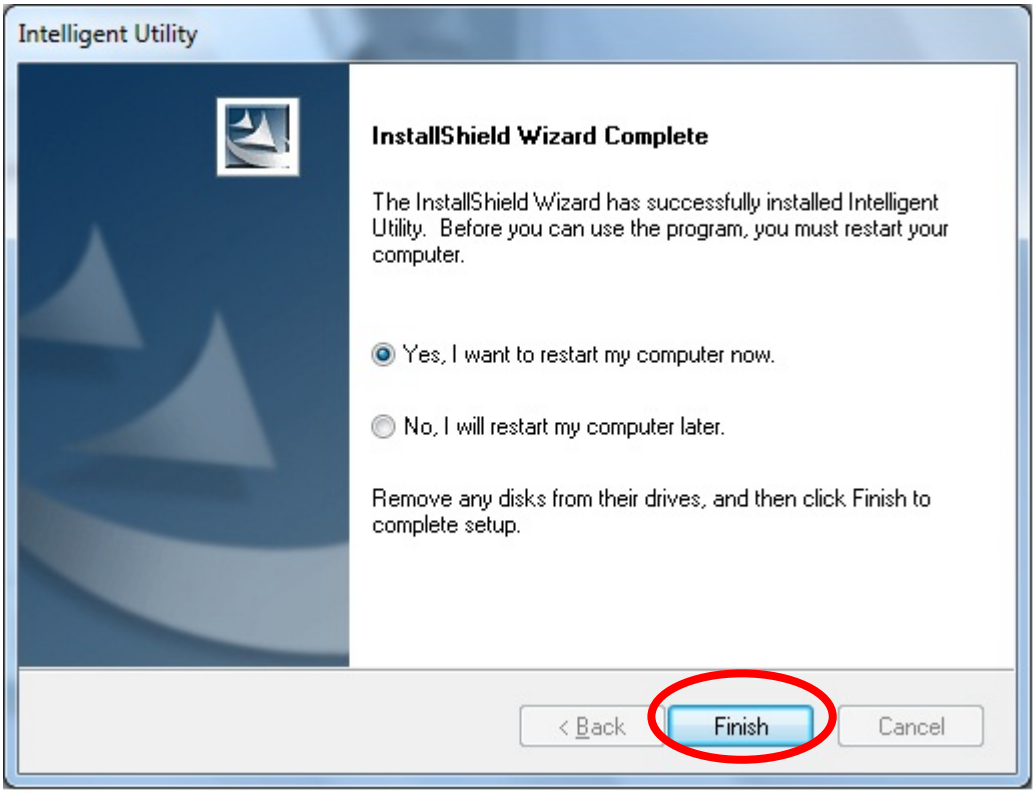
1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically. Please click **Next** to process the installation.



2. When prompt to the following message, please click **Install** to begin the installation



3. When the following screen appears, click **Finish** to restart the computer to complete the software installation.



Install Hardware

Note:

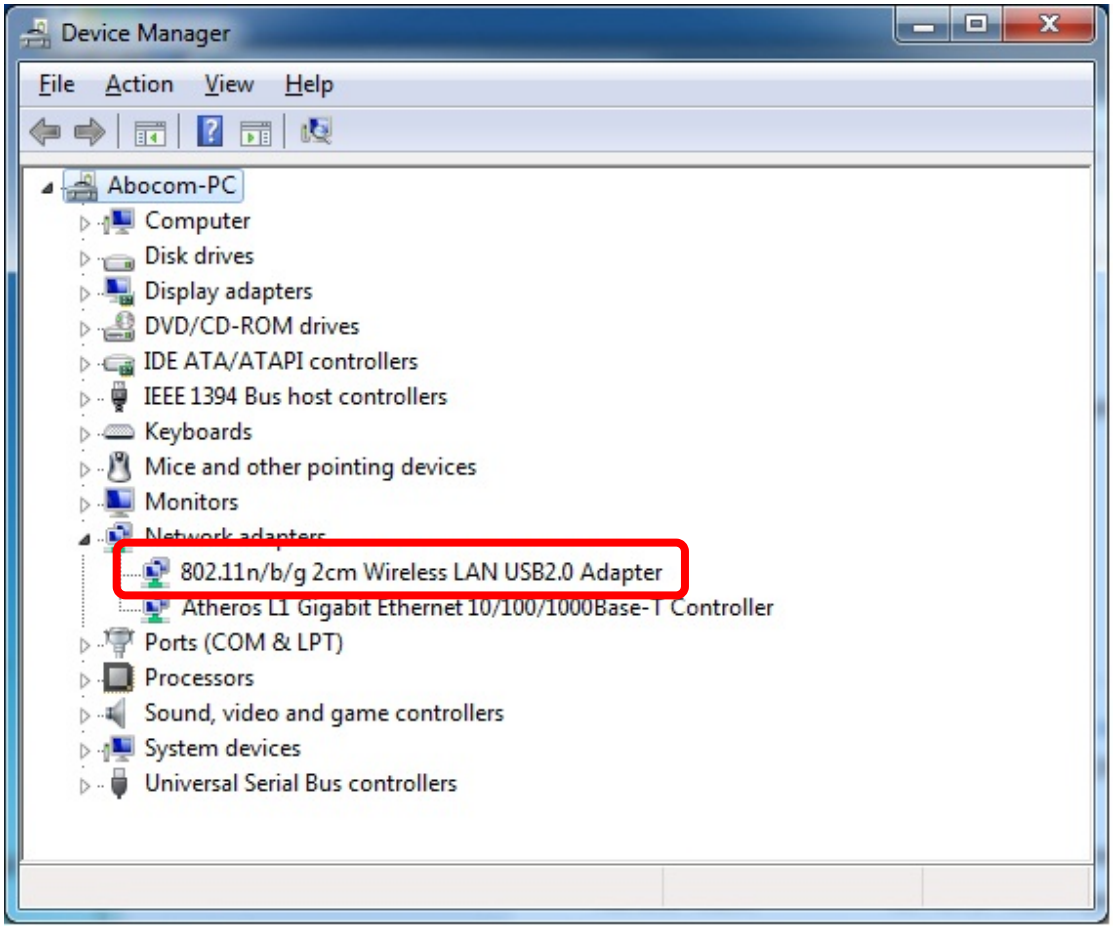
Insert the WLAN Module when finished software installation.

Insert the WLAN Module into the USB Port of the computer. The system will automatically detect the new hardware.

Verification

To verify the device is active in the computer. Go to **Start > Control Panel** > **Device Manager**.

Expand the **Network adapters** category. If the **802.11n/b/g 2cm Wireless LAN USB2.0 Adapter** is listed here, it means that the device is properly installed and enabled.



Chapter 3:
Network Connection

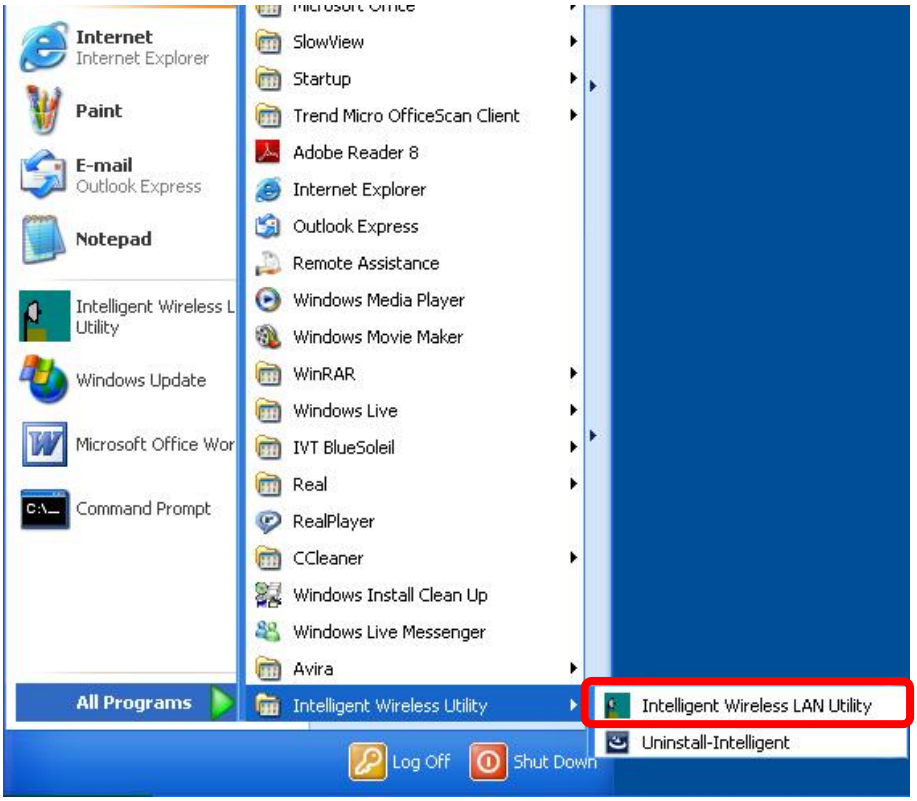
How to Make a Connection

To make a connection with an access point, please follow below steps. Here takes Windows XP OS for example.

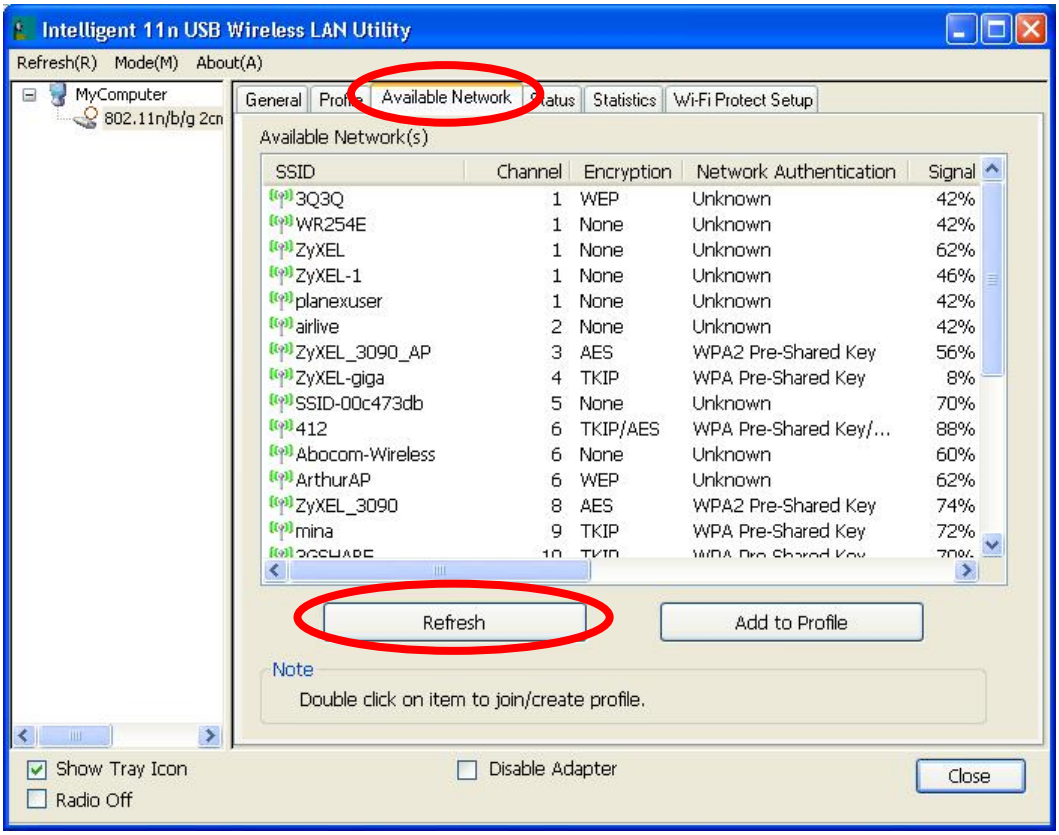
Step 1: After set up the WLAN Module successfully, please launch the Configuration Utility. There are two ways to launch the utility by:

(1) Double clicking the Intelligent Wireless LAN Utility icon on the desktop.

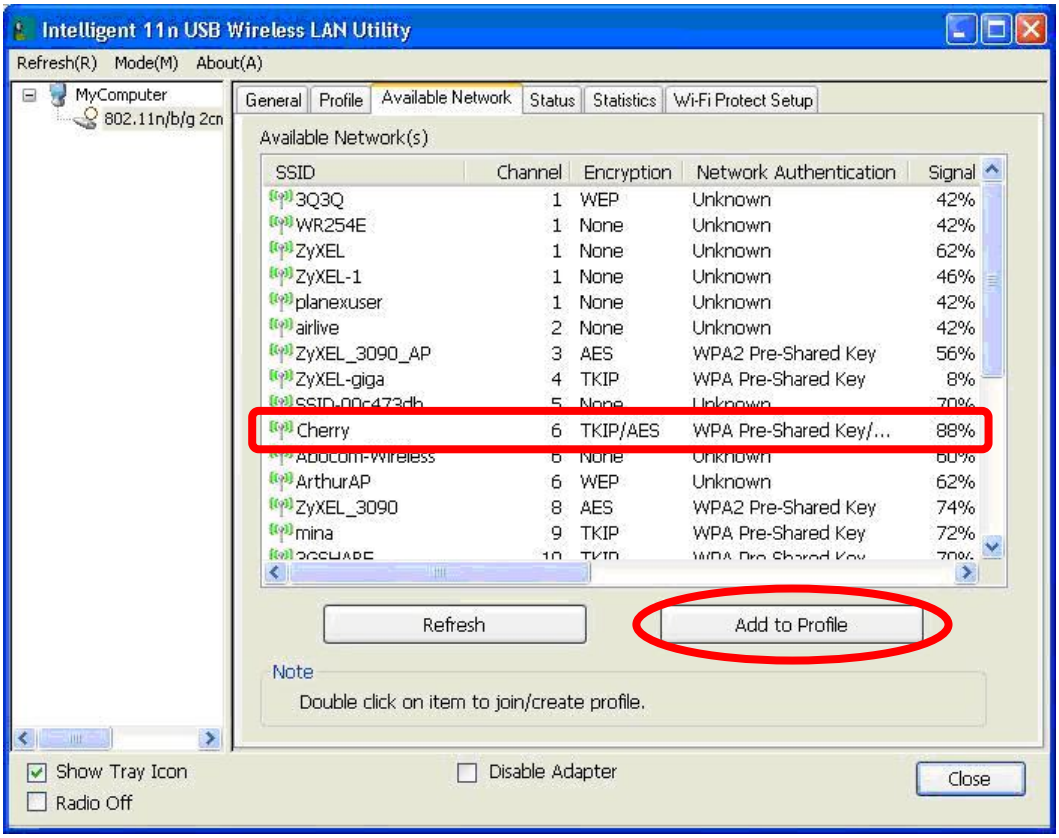
(2) Or go to **Start →All Programs →Intelligent Wireless Utility → Intelligent Wireless LAN Utility**.



Step 2: Please go to the **Available Network** tab, the system will automatically scan access points nearby, or click **Refresh** button to site survey again.

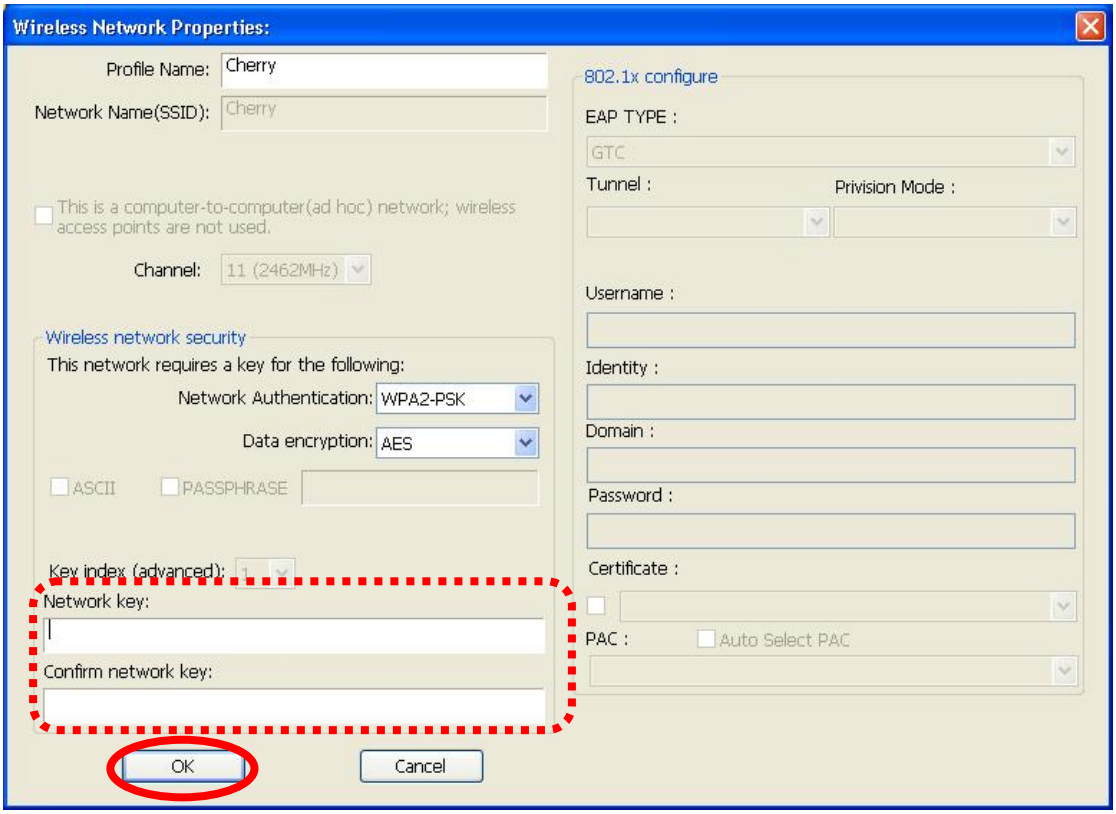


Step 3: Then, double click preferred access point or click **Add to Profile** button to make a connection (if the access point has been set up security, please enter passwords and then click **OK**.)

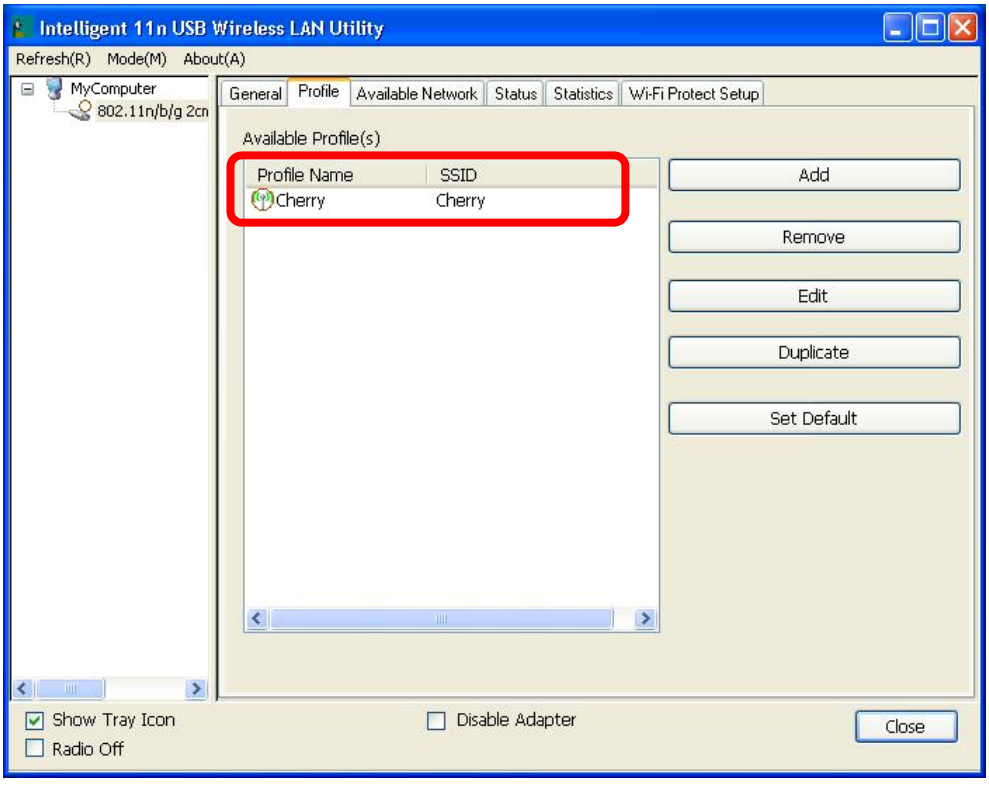


How to Add a Profile

After launched Wireless LAN Utility and selected preferred access point, please click **Add to Profile** button to enter **Wireless Network Properties** windows. If the access point has been set up security, please enter passwords, and then click **OK** to save profile settings.



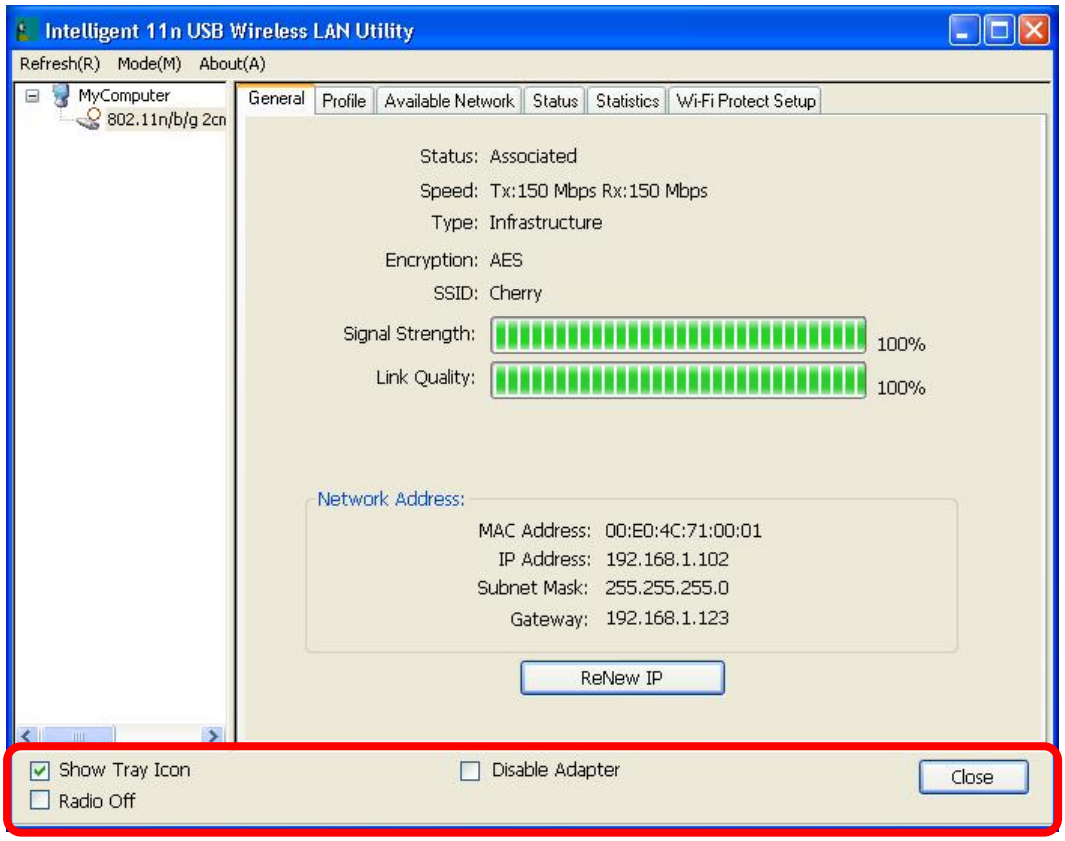
After finished above settings, please go to **Profile** tab to check the profile list (Available Profile(s)).



Chapter 4:
Utility Configuration

For Windows 2000 / XP

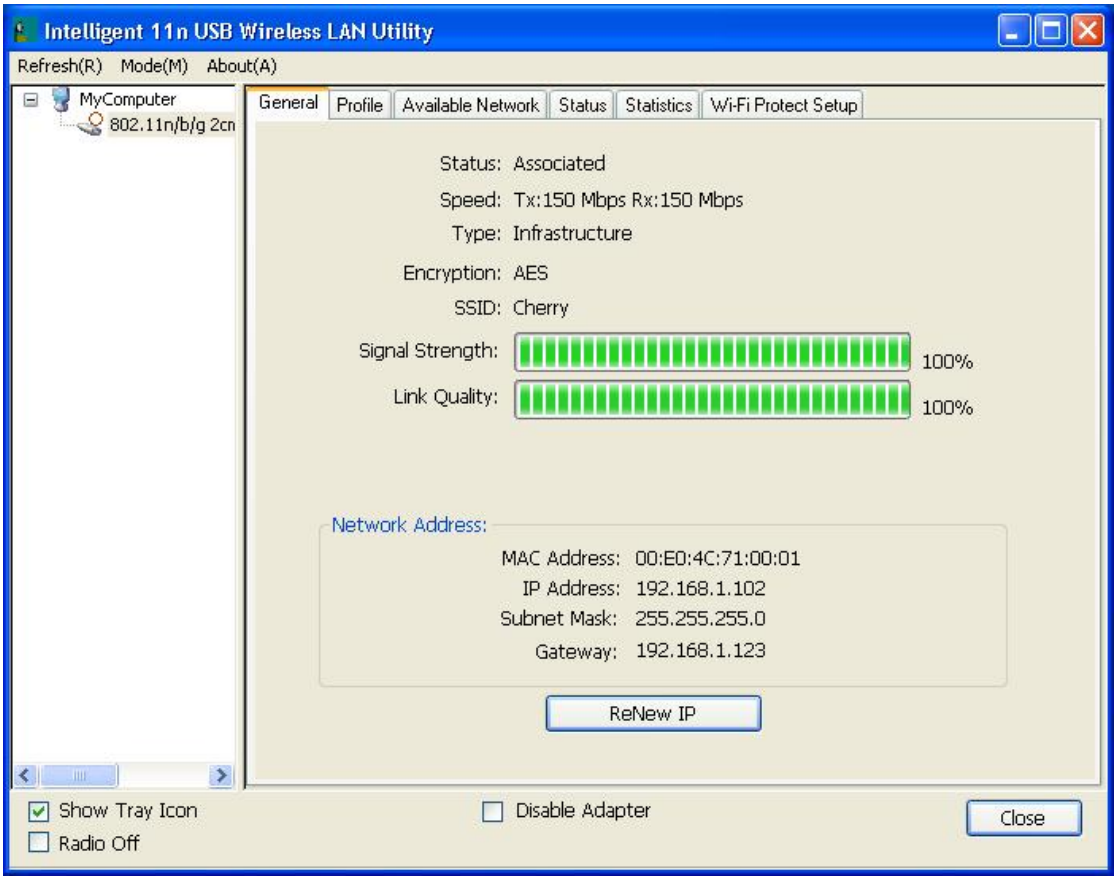
Station Mode



- **Show Tray Icon:** Check to show the wireless adapter icon at the tray.
- **Disable Adapter:** Check this to disable the wireless adapter.
- **Radio off:** Check this to turn OFF radio function.
- **Close:** Click to leave the Intelligent 11n USB Wireless LAN Utility.

General

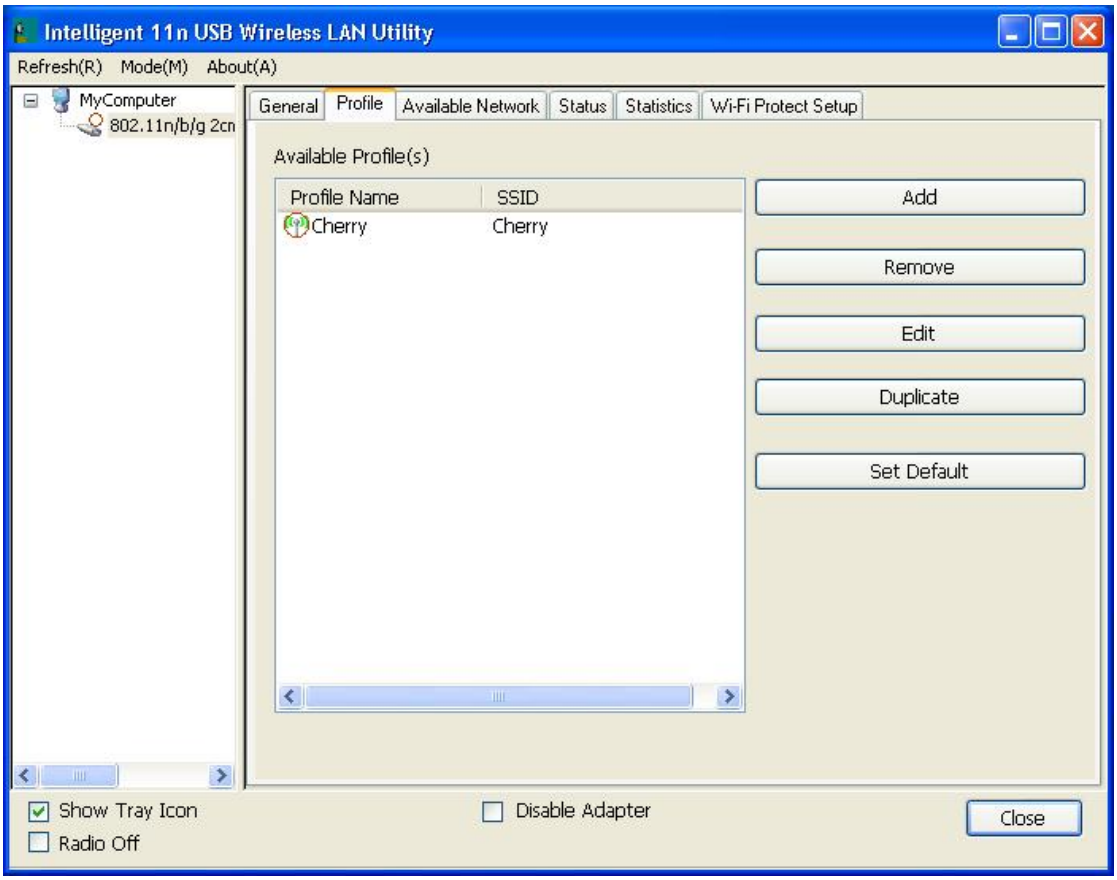
The General page displays the detail information of current connection.



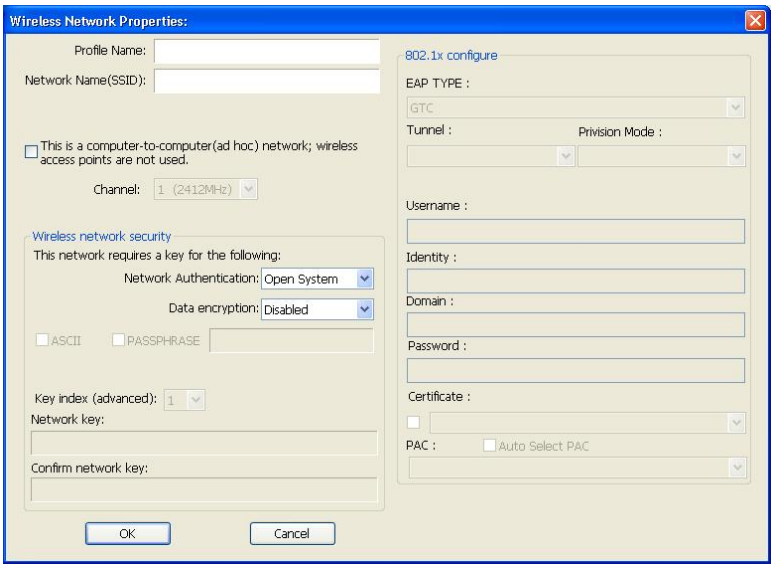
General Tab	
Status	Shows the current connected status. If there is no connection, it will show Not Associated. If been connected, the system will show Associated. When connecting, the system will show checking Status.
Speed	Shows the current transmitting rate and receiving rate.
Type	Network type in use, Infrastructure or Ad-Hoc.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
SSID	Shows the connected access point network name.
Signal Strength	Shows the receiving signal strength.
Link Quality	Shows the connection quality based on signal strength.
MAC Address	The physical address of the WLAN Module.
IP Address	Shows the IP address information.
Subnet Mask	Shows the Subnet Mask information.
Gateway	Shows the default gateway IP address.
Renew IP	Click the **Renew IP** button to obtain IP address form the connected gateway.

Profile

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add, Remove, Edit, Duplicate** and **Set Default** profiles.



Profile Tab	
Profile Name	Here shows a distinctive name of profile in this column.
SSID	The **SSID** is the unique name shared among all wireless access points in the wireless network.
Add	Click **Add** button to add a profile from the drop-down screen.



Profile Name: Users can enter profile name at will.

Network Name (SSID): The SSID is the unique network name (case-sensitive) shared among all wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network.

This is a computer-to-computer (ad hoc) network; wireless access points are not used: This function is selected to enable the ad hoc network type that computers should be setup at the same channel to communicate to each other directly without access point, users can share files and printers between each PC and laptop. User can select channels form the pull-down menu.

Wireless network security

Network Authentication: There are several types of authentication modes including Open System, Shared Key, WPA-PSK, WPA2-PSK, WPA 802.1X, WPA2 802.1X and WEP 802.1X.

Data encryption: For Open System, Shared Key and WEP 802.1X authentication mode, the selection of encryption type is WEP. For WPA-PSK, WPA2-PSK, WPA 802.1X and WPA2 802.1X authentication mode, the encryption type supports both TKIP and AES.

When encryption is set to WEP…

ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).

PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).

Key index (advanced): Select 1~4 key index form the pull-down menu, must match with the connected AP's key index.

When encryption is set to WPA-PSK/ WPA2-PSK…

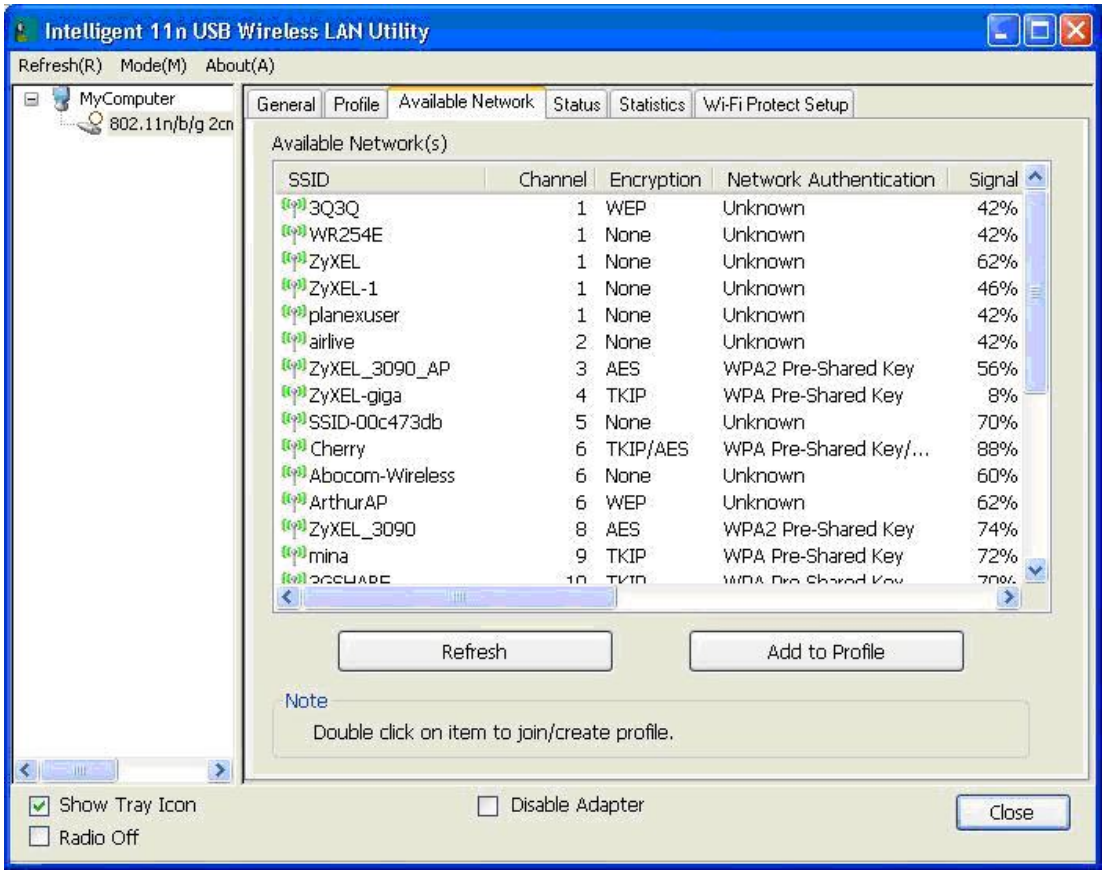
Network key: Enter network key at least 8 to 64 characters.

Confirm network key: Enter network key again to confirm.

	When encryption is set to WPA 802.1X/ WPA2 802.1X/ WEP 802.1X… When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge). **EAP TYPE:** • **TLS**: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point. • **LEAP:** Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication. • **TTLS**: Tunnelled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. • **PEAP**: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN. ⊙ **MD5**: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network. **Tunnel:** This is enabled under TTLS and PEAP type. For TTLS, the selections of tunnel are CHAP, MSCHAP, MSCHAP-V2, PAP. For PEAP, the selections of tunnel are MD5, GTC, TLS and MSCHAP-V2. **Username:** Enter the username for server. **Identity:** Enter the identity for server. **Domain:** Enter the domain of the network. **Password:** Enter the password for server. **Certificate:** Choose server that issuer of certificates.
Remove	Click **Remove** button to delete selected profile.
Edit	Click **Edit** button to edit selected profile.
Duplicate	Click **Duplicate** button to copy selected profile.
Set Default	Click **Set Default** button to set selected profile to be connected first.

Available Network

This page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Channel, Encryption, Network Authentication, Signal, Type, BSSID, Supported Rate (s), and Mode.

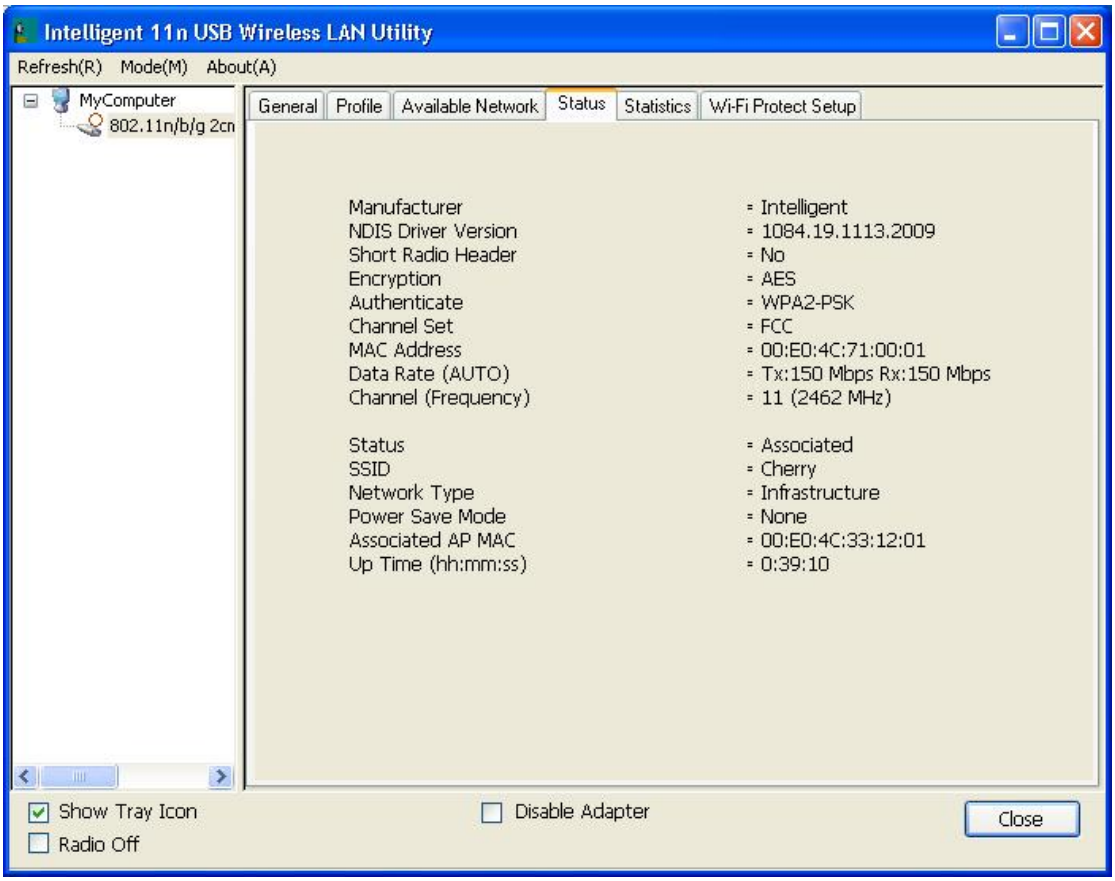


Network Tab	
SSID	Shows the network name of the access points.
Channel	Shows the currently channel in use.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, None and TKIP/AES.
Network Authentication	Show the device network authentication.
Signal	Shows transmit power, the amount of power used by a radio transceiver to send the signal out.
Type	Network type in use, Infrastructure or Ad-Hoc mode.
BSSID	Shows Wireless MAC address.
Supported Rate(s)	Shows the transmitting data rate.

Mode	Supported wireless mode. It may support 802.11b, 802.11g and 802.11n wireless mode.
Refresh	Click Refresh button to search and rescan the available network.
Add to Profile	Select an available network (SSID) on the list and then click Add to Profile button to add it into the profile list.
Note	Double click on item to join/create profile.

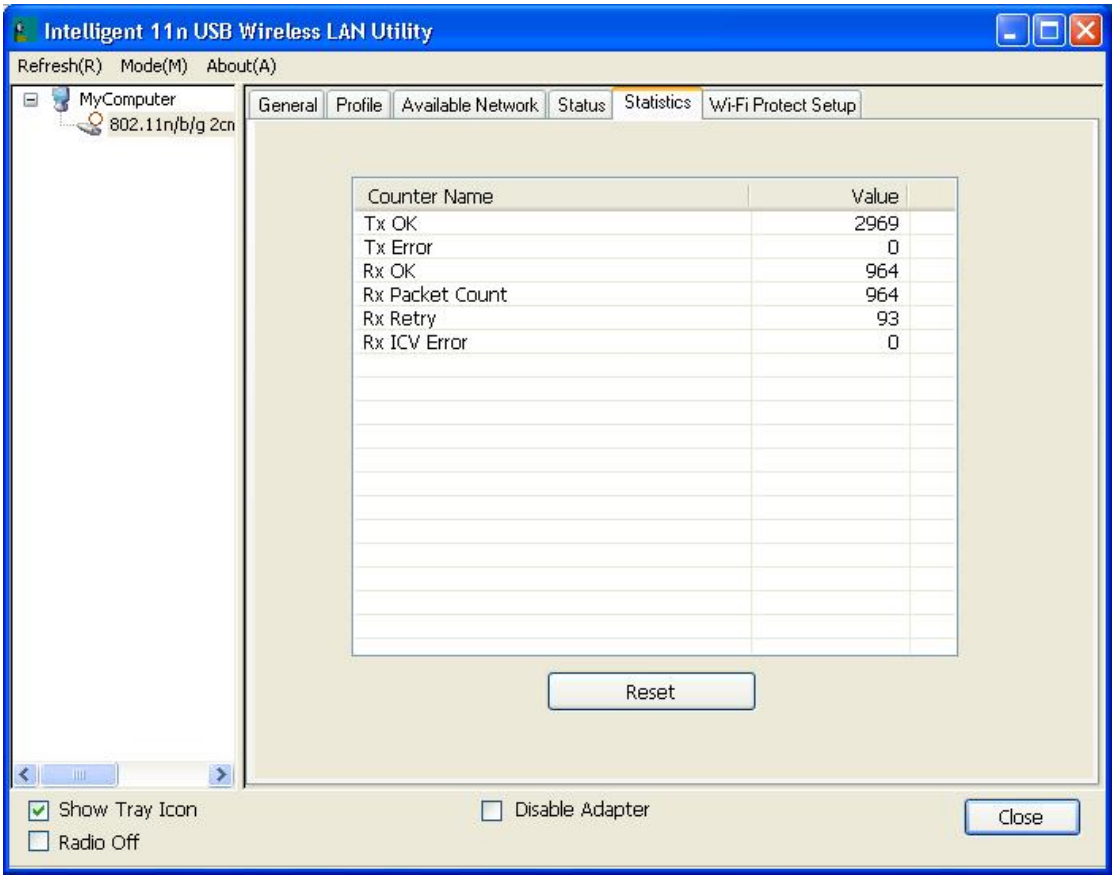
Status

This tab listed the information about the WLAN Module and connected access point.



Statistics

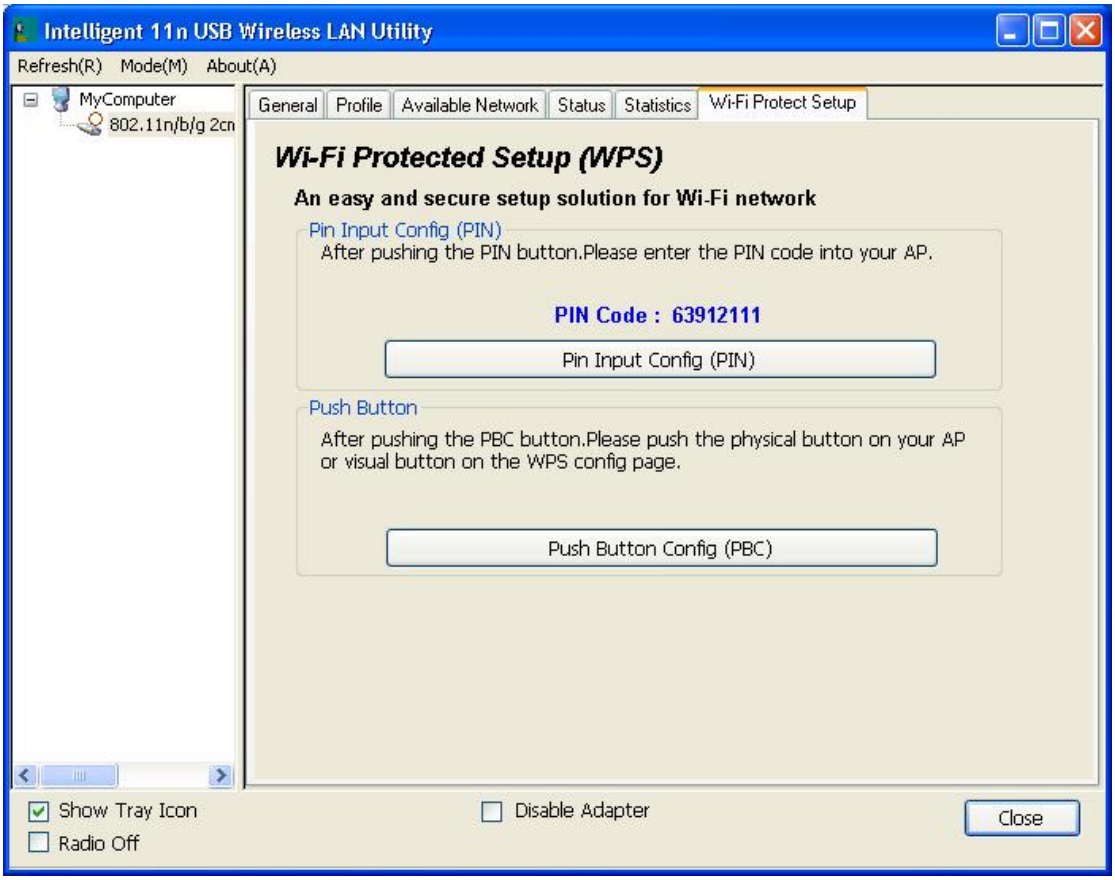
The Statistics screen displays the statistics on the current network settings.



Statistics	
Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

WPS

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.



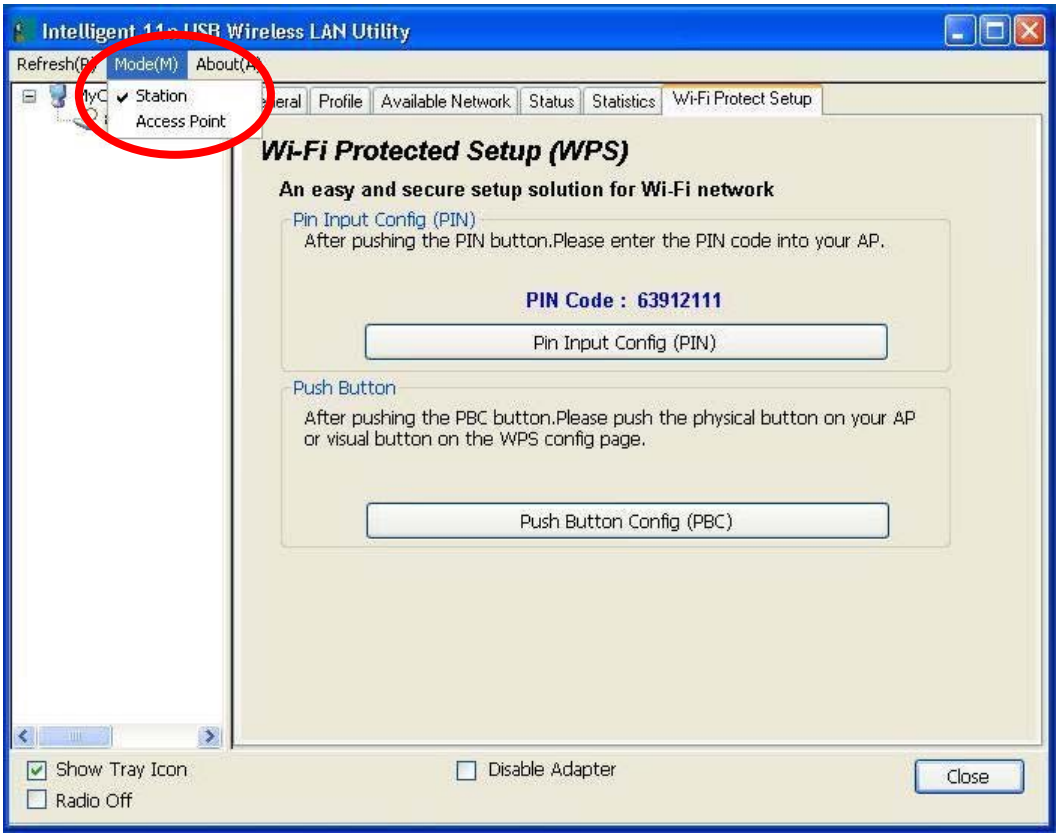
WPS Tab	
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use "**Renew**" button to re-generate new PIN Code.
Pin Input Config (PIN)	Click the **Pin Input Config (PIN)** button to select specific AP to process PIN Config.
Push Button Config (PBC)	Click this button to connect with AP that supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.

About

This page displays the information of the WLAN Module Version.

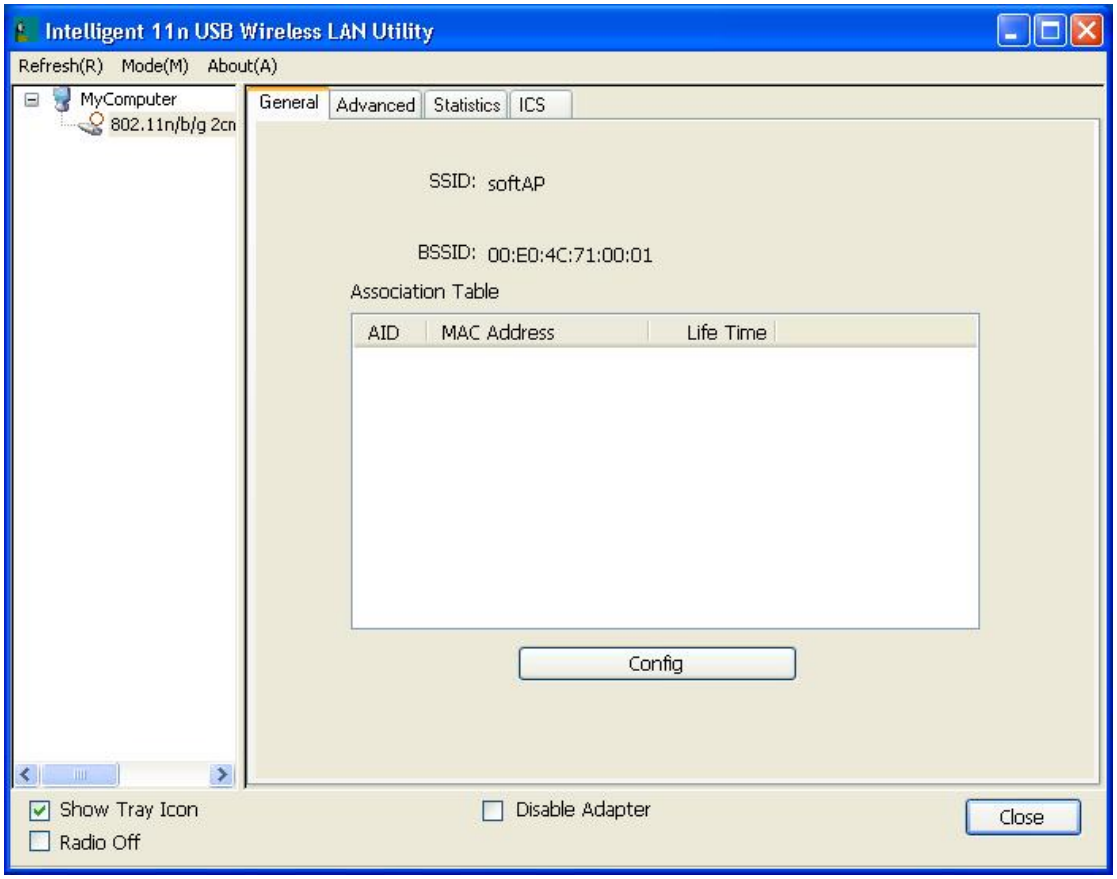
Switch to AP Mode

To access the soft AP mode, please select the **Mode** on the function list of the Utility to make the WLAN Module act as a wireless AP.

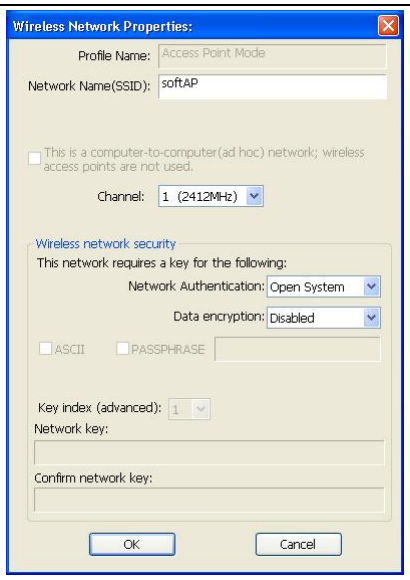


Soft AP mode

General



General	
SSID	Shows the network name of the AP.
BSSID	Shows the MAC address of the AP.
Association Table	This table shows the connected client here.
Config	Click the Config button to set up the Wireless Network Properties.



Network Name (SSID): User can change the network name of this access point.

Channel: User can select the channel form the pull-down list.

Wireless network security

Network Authentication: There are several types of authentication modes including Open System, Shared Key, WPA-PSK and WPA2-PSK.

Data encryption: For Open System and Shared Key authentication mode, the selection of encryption type is WEP. For WPA-PSK, WPA2-PSK, authentication mode, the encryption type supports both TKIP and AES.

When encryption is set to WEP…

ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).

PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).

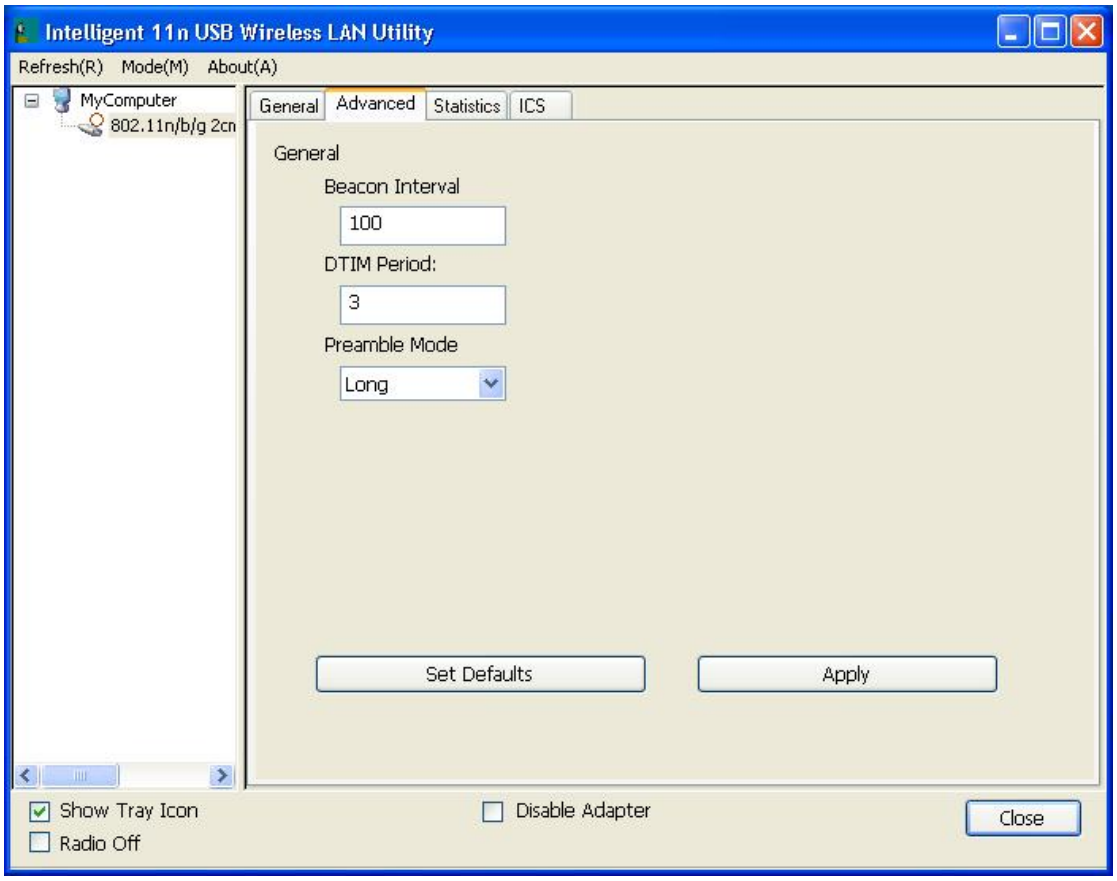
Key index (advanced): Select 1~4 key index form the pull-down menu, must match with the connected AP's key index.

When encryption is set to WPA-PSK/ WPA2-PSK…

Network key: Enter network key at least 8 to 64 characters.

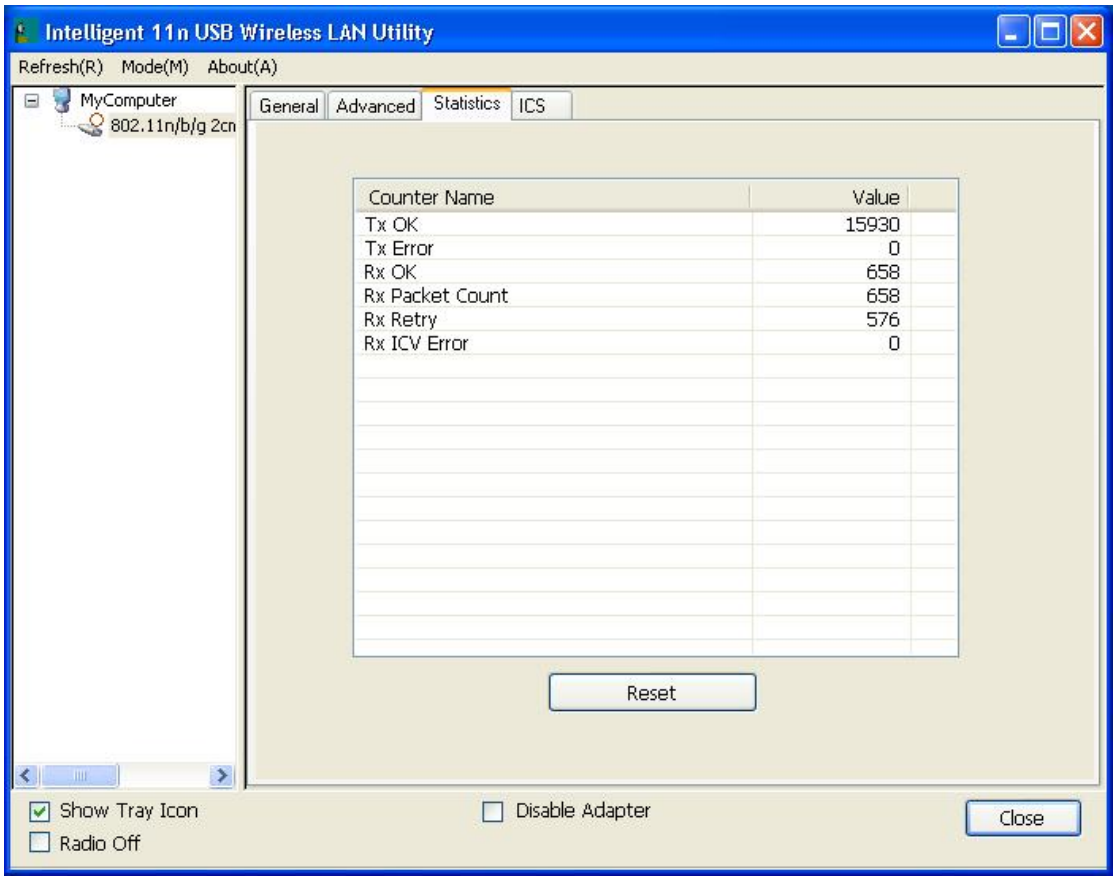
Confirm network key: Enter network key again to confirm.

Advanced



Advanced	
Beacon Interval	The time between two beacons. (The system default is 100 ms.)
DTIM Period	The delivery traffic indication message (DTIM) is an element included in some beacon frames. User can specify a value from 1 to 255 beacons.
Preamble	Select from the pull-down menu to change the Preamble type into **Short** or **Long**.
Set Defaults	Click to use the system default value.
Apply	Click to apply the above settings.

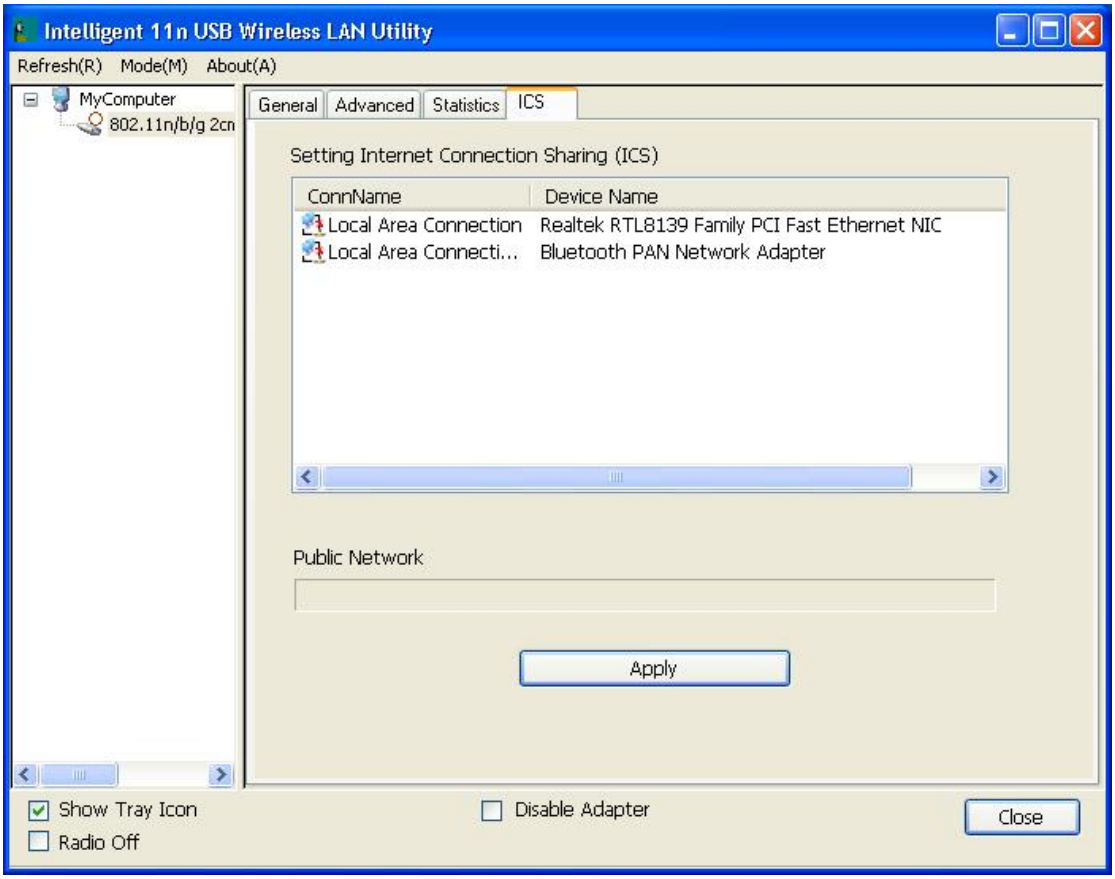
Statistics



Statistics	
Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

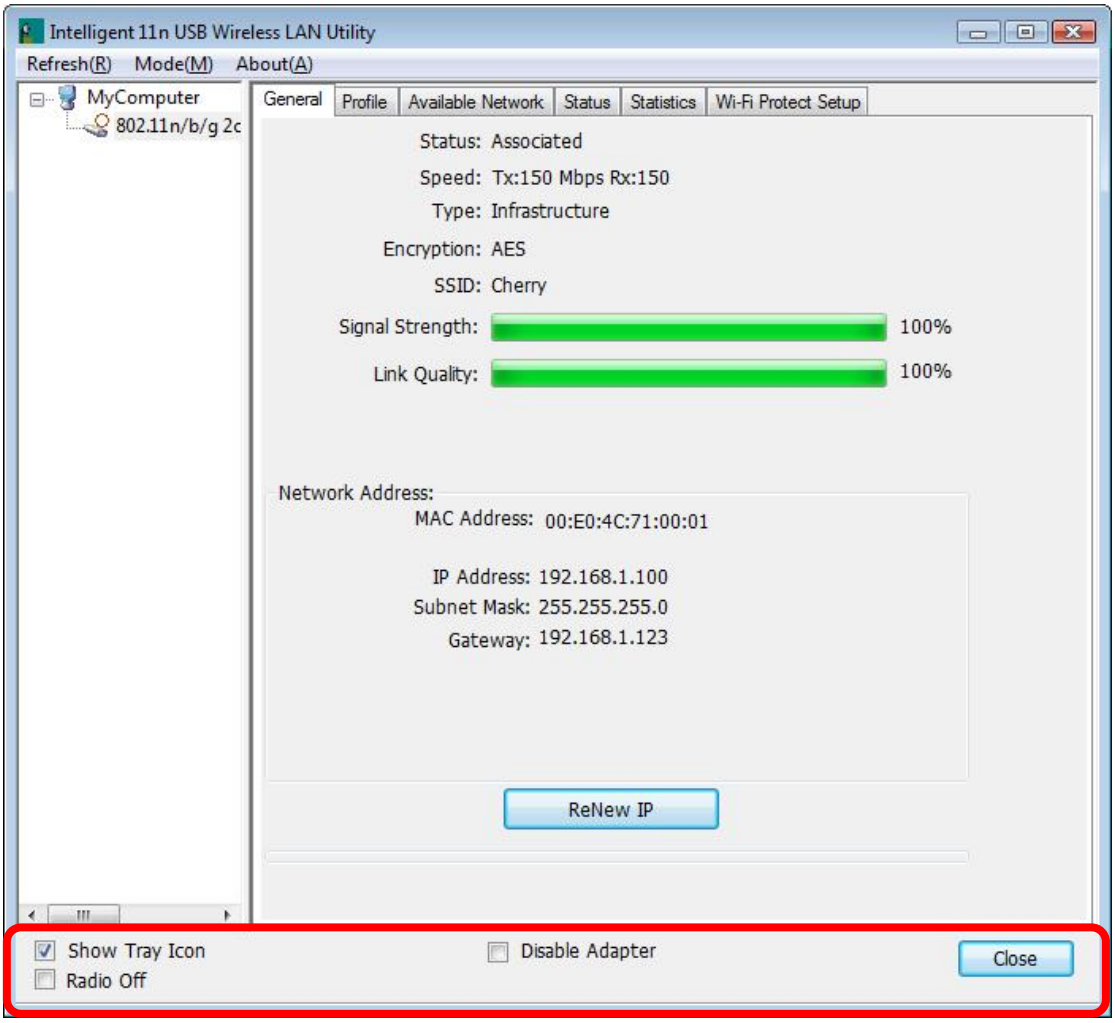
ICS

This page displays setting Internet connection sharing (ICS). Select a sharing public network and click Apply button to make a connection.



For Windows Vista

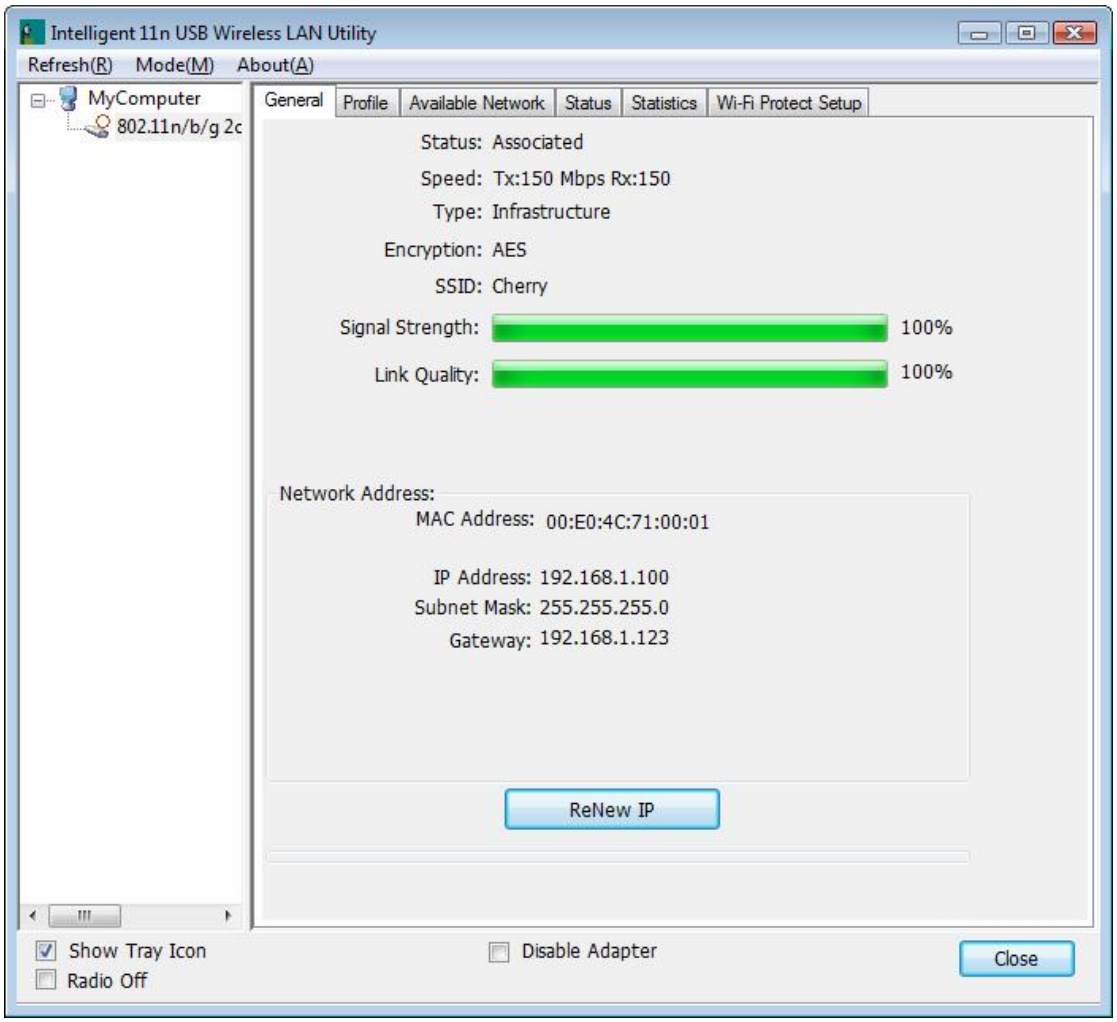
Station Mode



- **Show Tray Icon:** Check to show the wireless adapter icon at the tray.
- **Disable Adapter:** Check this to disable the wireless adapter.
- **Radio off:** Check this to turn OFF radio function.
- **Close:** Click to leave the Intelligent 11n USB Wireless LAN Utility.

General

The General page displays the detail information of current connection.

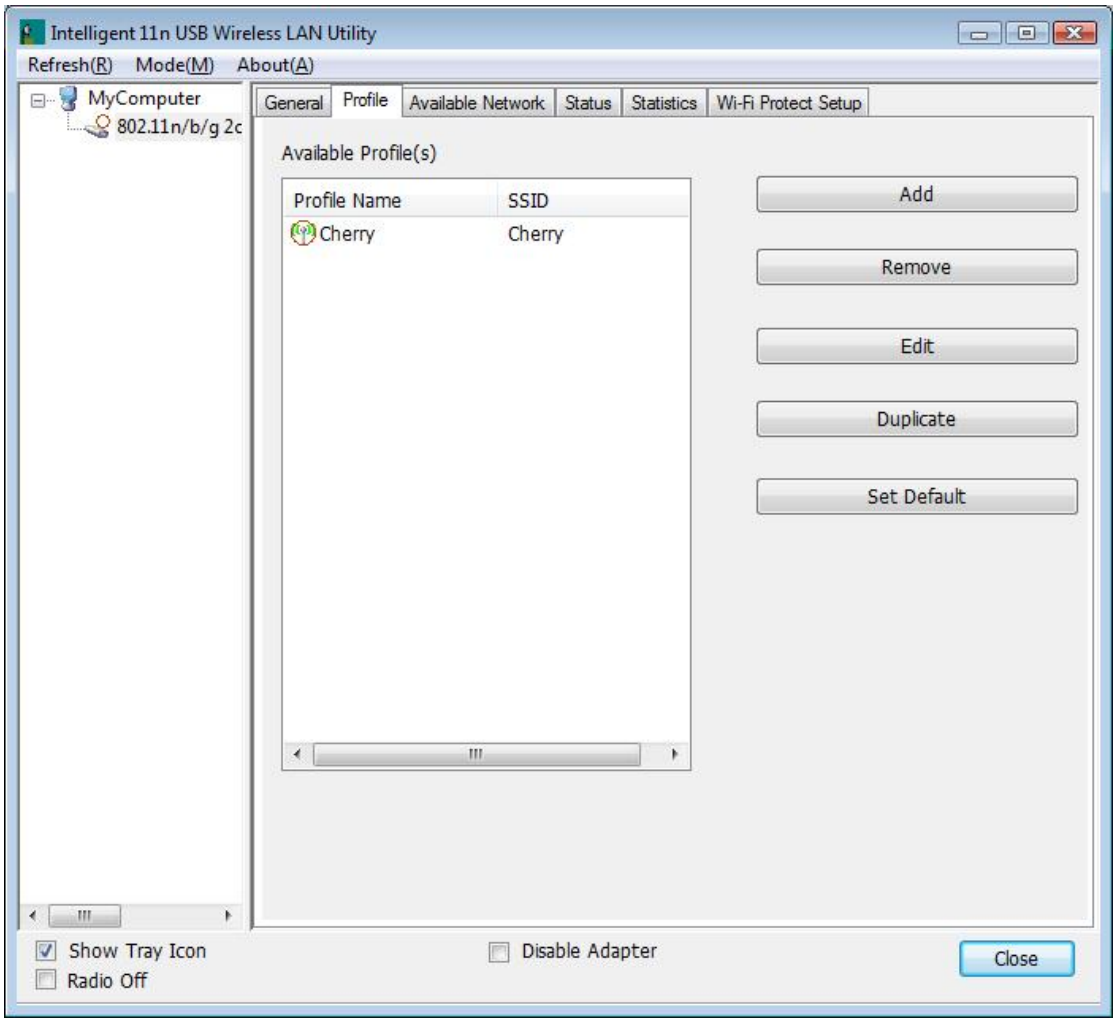


General Tab	
Status	Shows the current connected status. If there is no connection, it will show Not Associated. If been connected, the system will show Associated. When connecting, the system will show checking Status.
Speed	Shows the current transmitting rate and receiving rate.
Type	Network type in use, Infrastructure or Ad-Hoc.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
SSID	Shows the connected access point network name.
Signal Strength	Shows the receiving signal strength.
Link Quality	Shows the connection quality based on signal strength.
MAC Address	The physical address of the WLAN Module.
IP Address	Shows the IP address information.
Subnet Mask	Shows the Subnet Mask information.
Gateway	Shows the default gateway IP address.
Renew IP	Click the **Renew IP** button to obtain IP address form the connected

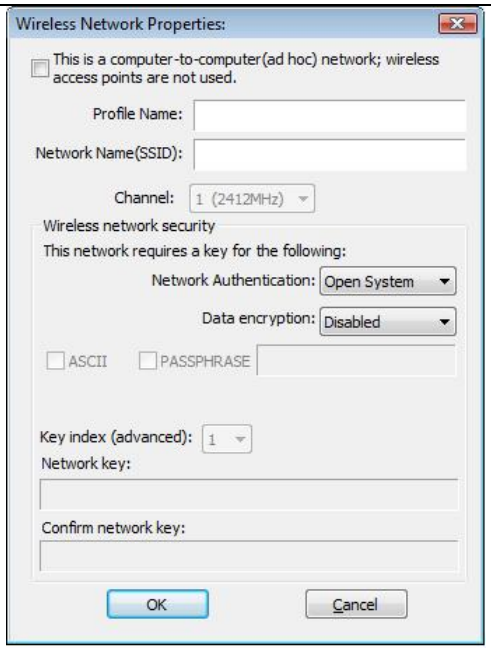
	gateway.

Profile

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add, Remove, Edit, Duplicate** and **Set Default** profiles.



Profile Tab	
Profile Name	Here shows a distinctive name of profile in this column.
SSID	The **SSID** is the unique name shared among all wireless access points in the wireless network.
Add	Click **Add** button to add a profile from the drop-down screen.



This is a computer-to-computer (ad hoc) network; wireless access points are not used: This function is selected to enable the ad hoc network type that computers should be setup at the same channel to communicate to each other directly without access point, users can share files and printers between each PC and laptop.

Profile Name: Users can enter profile name at will.

Network Name (SSID): The SSID is the unique network name (case-sensitive) shared among all wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network.

Channel: If set to ad hoc network type, user can select channels form the pull-down menu.

Wireless network security

Network Authentication: There are several types of authentication modes including Open System, Shared Key, WPA-PSK, WPA2-PSK, WPA 802.1X, WPA2 802.1X and WEP 802.1X.

Data encryption: For Open System, Shared Key and WEP 802.1X authentication mode, the selection of encryption type is WEP. For WPA-PSK, WPA2-PSK, WPA 802.1X and WPA2 802.1X authentication mode, the encryption type supports both TKIP and AES.

When encryption is set to WEP…

ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).

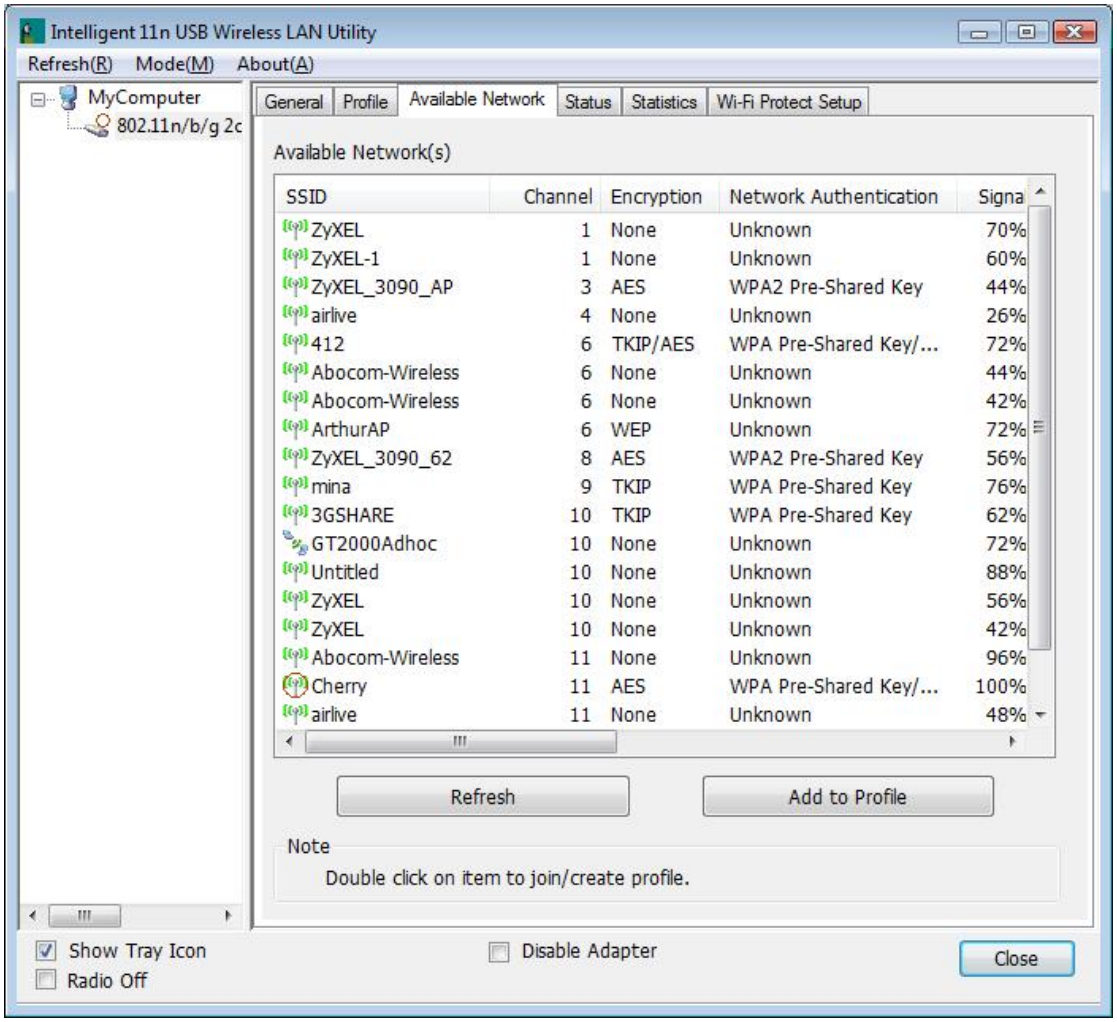
PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).

Key index (advanced): Select 1~4 key index form the pull-down menu, must match with the connected AP's key index.

	When encryption is set to WPA-PSK/ WPA2-PSK… **Network key:** Enter network key at least 8 to 64 characters. **Confirm network key:** Enter network key again to confirm. **When encryption is set to WPA 802.1X/ WPA2 802.1X/ WEP 802.1X…** When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge). **EAP TYPE:** • **TLS**: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point. • **LEAP:** Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication. • **TTLS**: Tunnelled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. • **PEAP**: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN. ⊙ **MD5**: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network. **Tunnel:** This is enabled under TTLS and PEAP type. For TTLS, the selections of tunnel are CHAP, MSCHAP, MSCHAP-V2, PAP. For PEAP, the selections of tunnel are MD5, GTC, TLS and MSCHAP-V2. **Username:** Enter the username for server. **Identity:** Enter the identity for server. **Domain:** Enter the domain of the network. **Password:** Enter the password for server. **Certificate:** Choose server that issuer of certificates.
Remove	Click **Remove** button to delete selected profile.
Edit	Click **Edit** button to edit selected profile.
Duplicate	Click **Duplicate** button to copy selected profile.
Set Default	Click **Set Default** button to set selected profile to be connected first.

Available Network

This page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Channel, Encryption, Network Authentication, Signal, Type, BSSID, Supported Rate(s), and Mode.

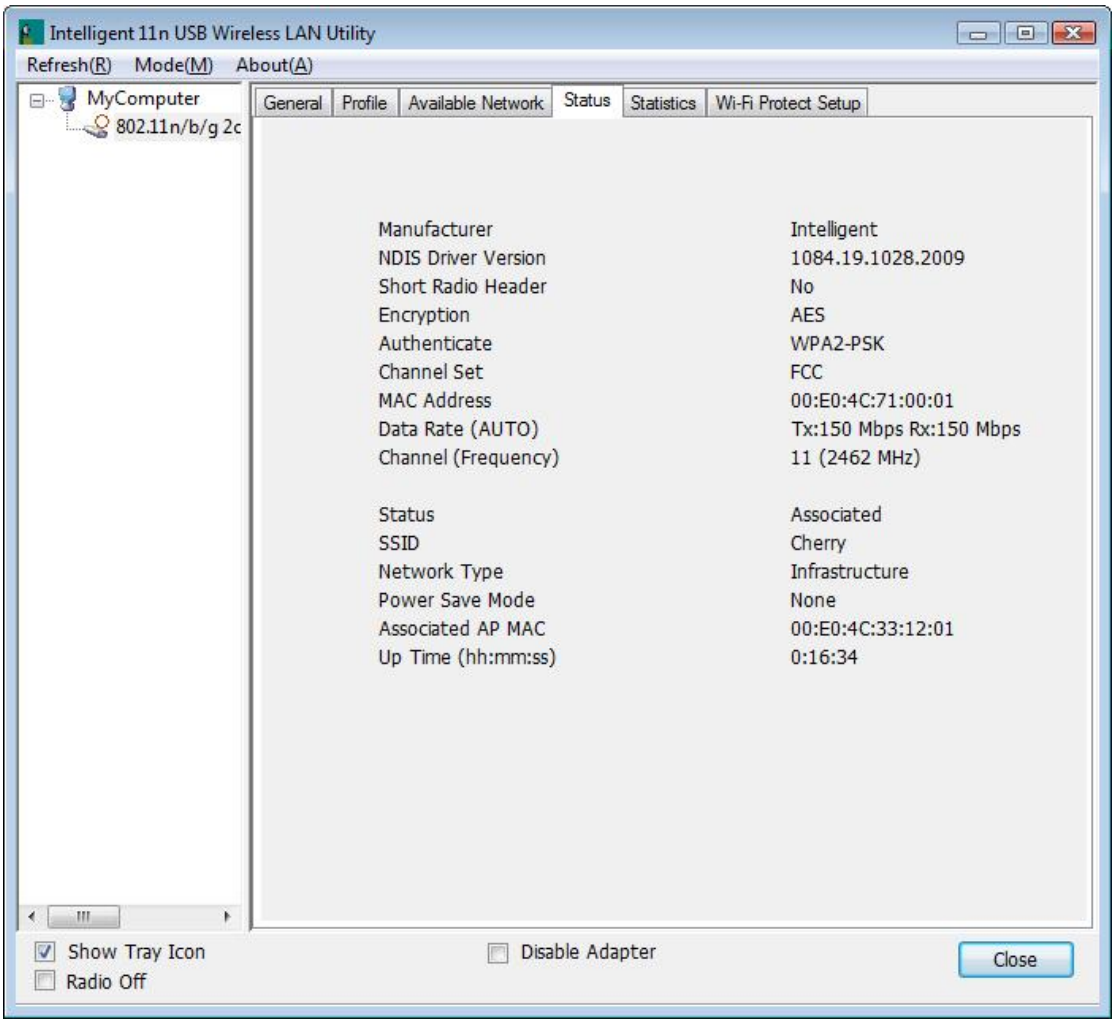


Network Tab	
SSID	Shows the network name of the access points.
Channel	Shows the currently channel in use.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, None and TKIP/AES.
Network Authentication	Show the device network authentication.
Signal	Shows transmit power, the amount of power used by a radio transceiver to send the signal out.
Type	Network type in use, Infrastructure or Ad-Hoc mode.

BSSID	Shows Wireless MAC address.
Supported Rate(s)	Shows the transmitting data rate.
Mode	Supported wireless mode. It may support 802.11b, 802.11g and 802.11n wireless mode.
Refresh	Click Refresh button to search and rescan the available network.
Add to Profile	Select an available network (SSID) on the list and then click **Add to Profile** button to add it into the profile list.
Note	Double click on item to join/create profile.

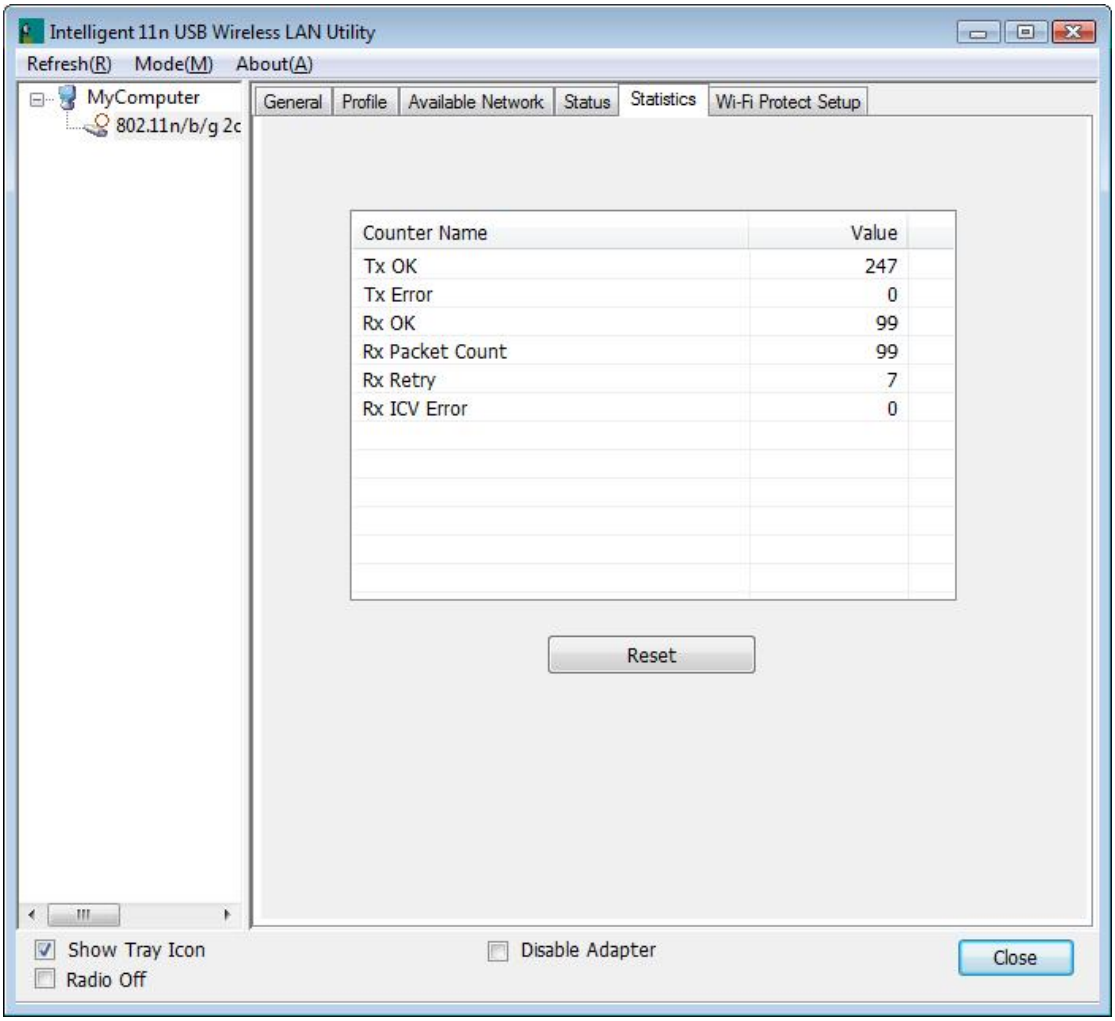
Status

This tab listed the information about the WLAN Module and connected access point.



Statistics

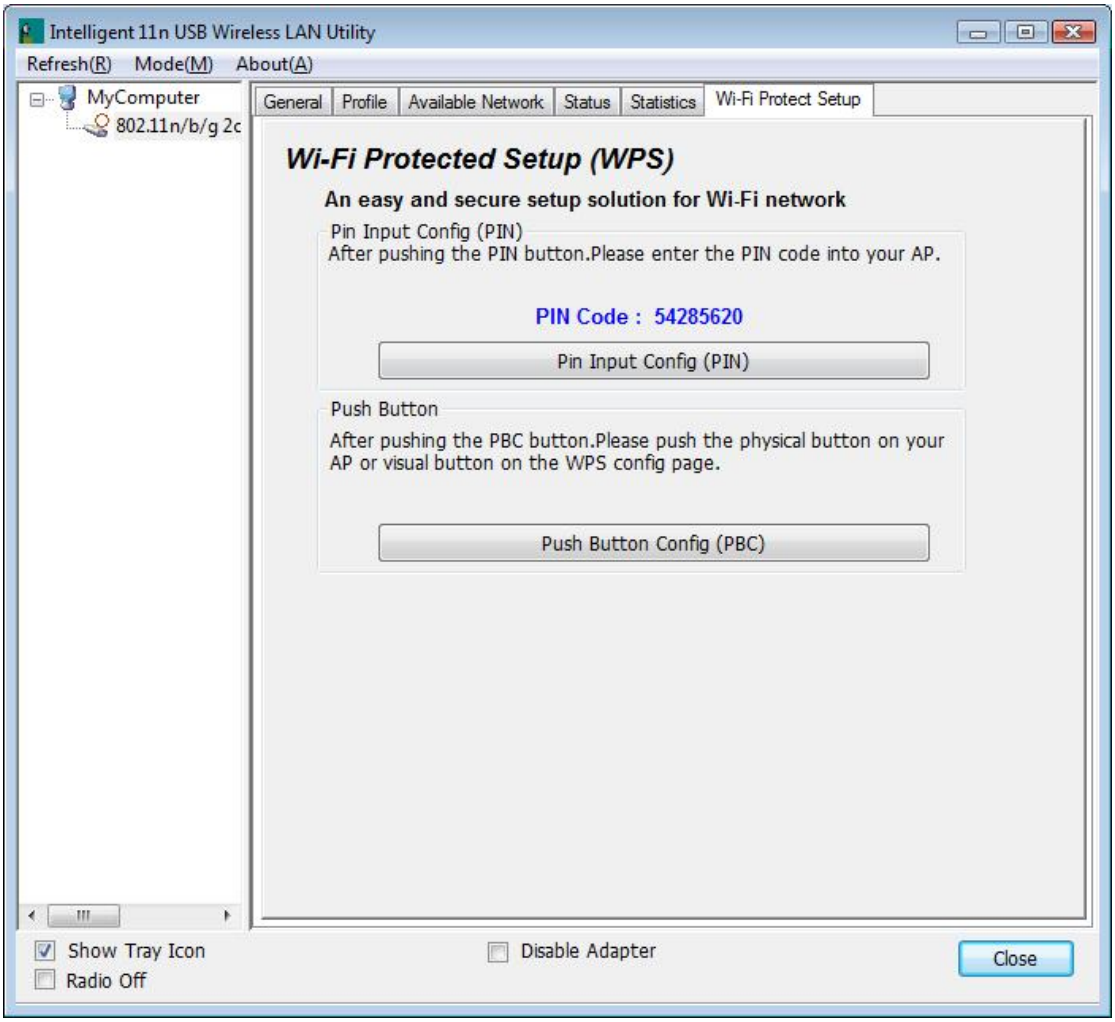
The Statistics screen displays the statistics on the current network settings.



Statistics	
Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

WPS

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.



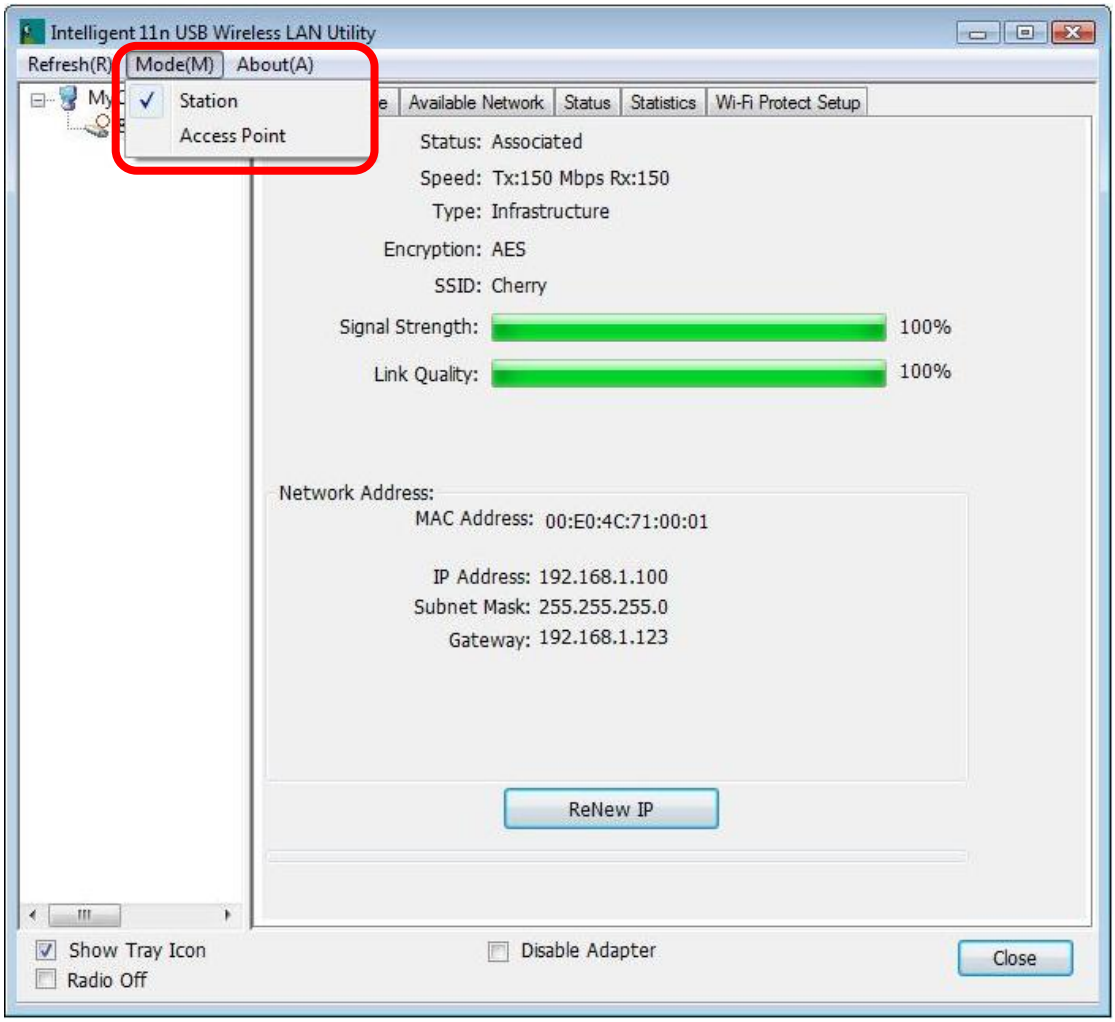
WPS Tab	
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use "**Renew**" button to re-generate new PIN Code.
Pin Input Config (PIN)	Click the **Pin Input Config (PIN)** button to select specific AP to process PIN Config.
Push Button Config (PBC)	Click this button to connect with AP that supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.

About

This page displays the information of the WLAN Module Version.

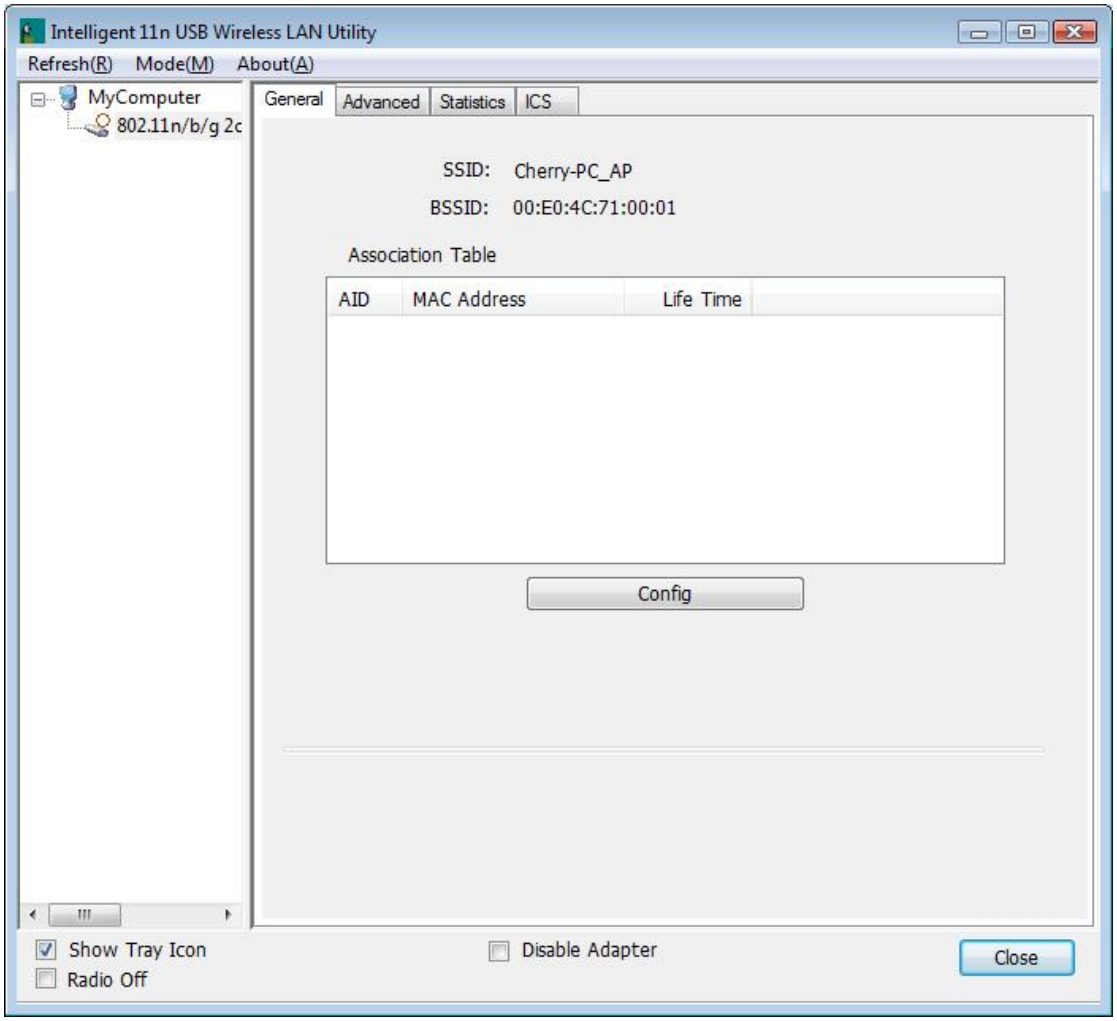
Switch to AP Mode

To access the soft AP mode, please select the **Mode** on the function list of the Utility to make the WLAN Module act as a wireless AP.

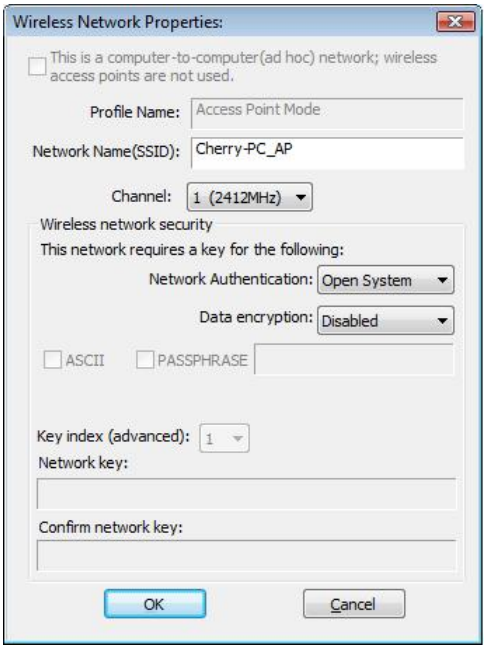


Soft AP mode

General



General	
SSID	Shows the network name of the AP.
BSSID	Shows the MAC address of the AP.
Association Table	This table shows the connected client here.
Config	Click the Config button to set up the Wireless Network Properties.



Network Name (SSID): User can change the network name of this access point.

Channel: User can select the channel form the pull-down list.

Wireless network security

Network Authentication: There are several types of authentication modes including Open System, Shared Key, WPA-PSK and WPA2-PSK.

Data encryption: For Open System and Shared Key authentication mode, the selection of encryption type is WEP. For WPA-PSK, WPA2-PSK, authentication mode, the encryption type supports both TKIP and AES.

When encryption is set to WEP…

ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).

PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).

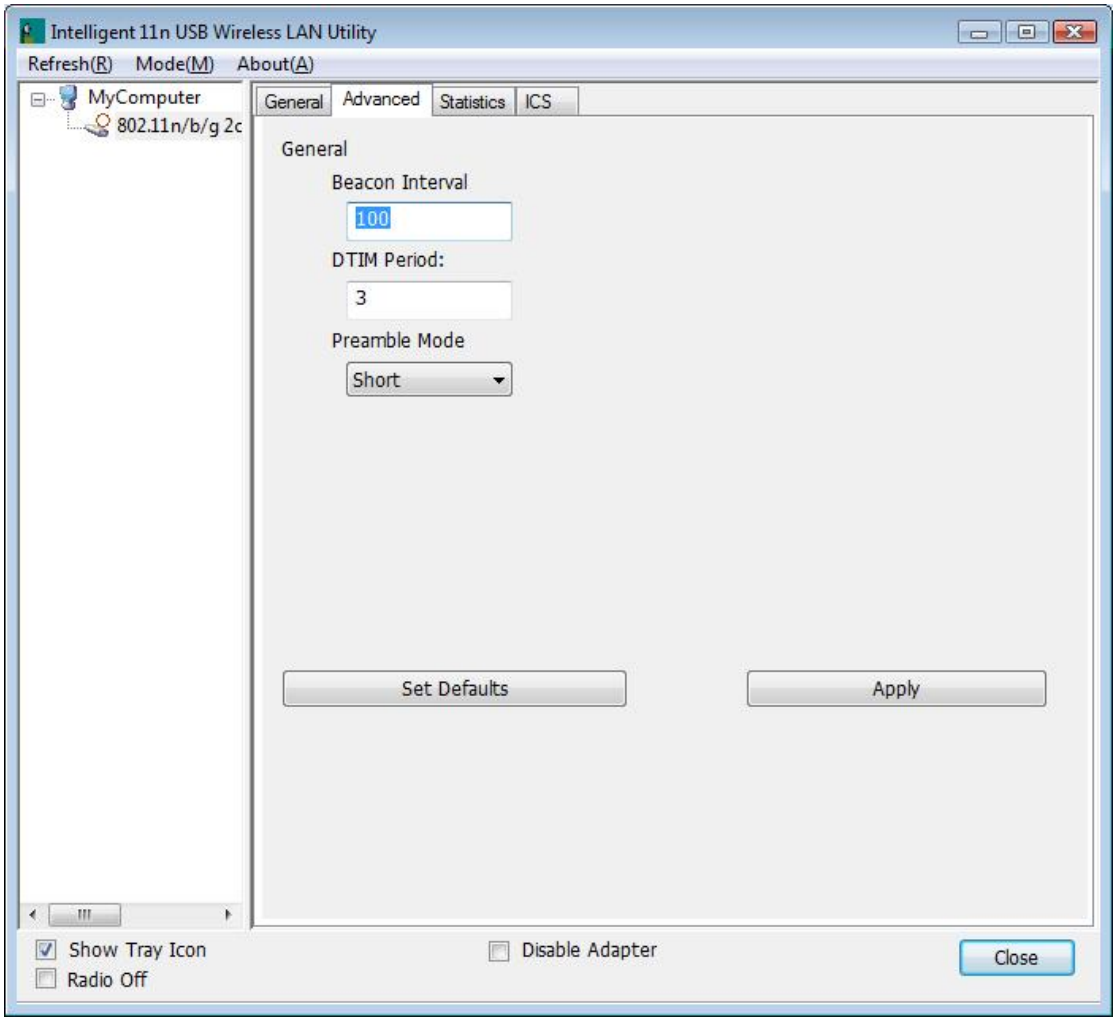
Key index (advanced): Select 1~4 key index form the pull-down menu, must match with the connected AP's key index.

When encryption is set to WPA-PSK/ WPA2-PSK…

Network key: Enter network key at least 8 to 64 characters.

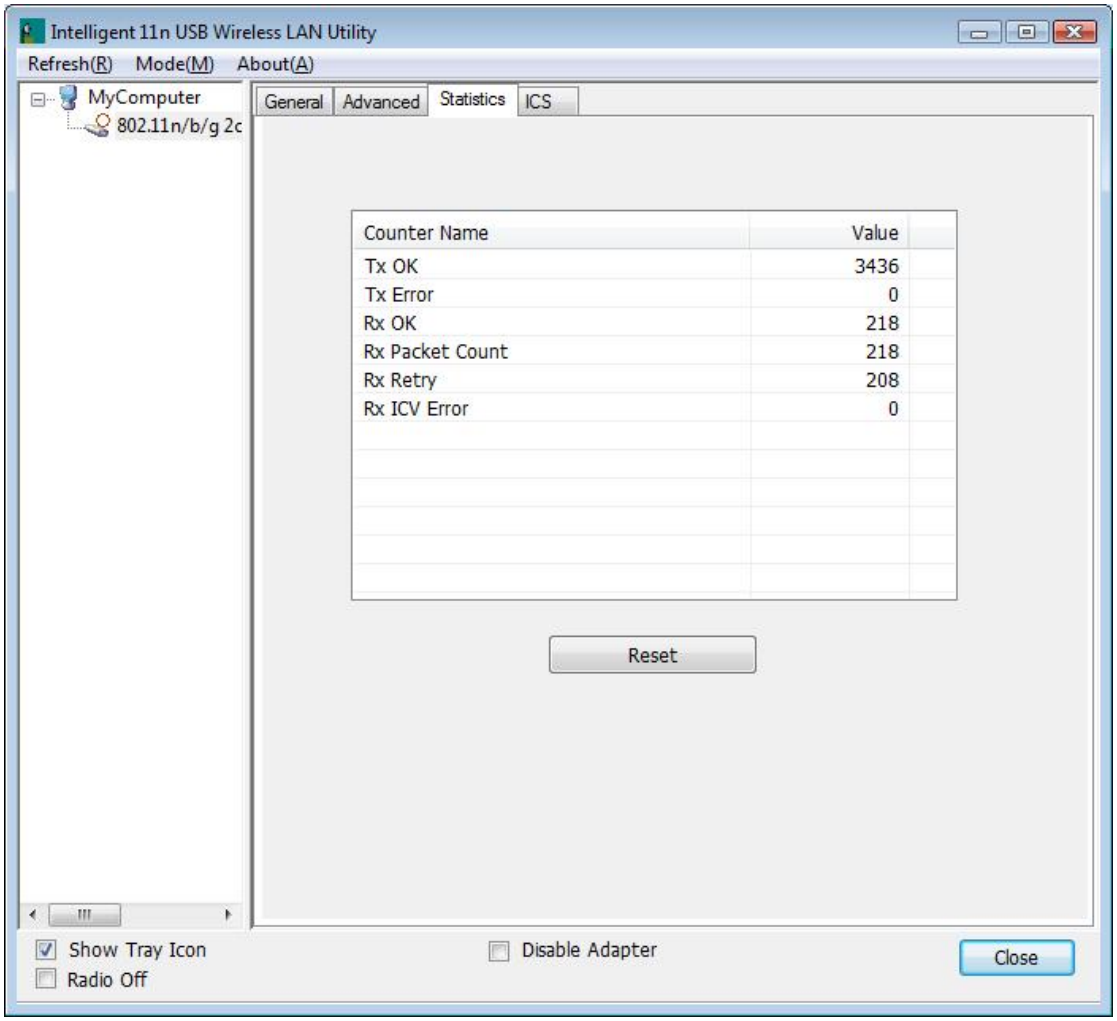
Confirm network key: Enter network key again to confirm.

Advanced



Advanced	
Beacon Interval	The time between two beacons. (The system default is 100 ms.)
DTIM Period	The delivery traffic indication message (DTIM) is an element included in some beacon frames. User can specify a value from 1 to 255 beacons.
Preamble	Select from the pull-down menu to change the Preamble type into **Short** or **Long**.
Set Defaults	Click to use the system default value.
Apply	Click to apply the above settings.

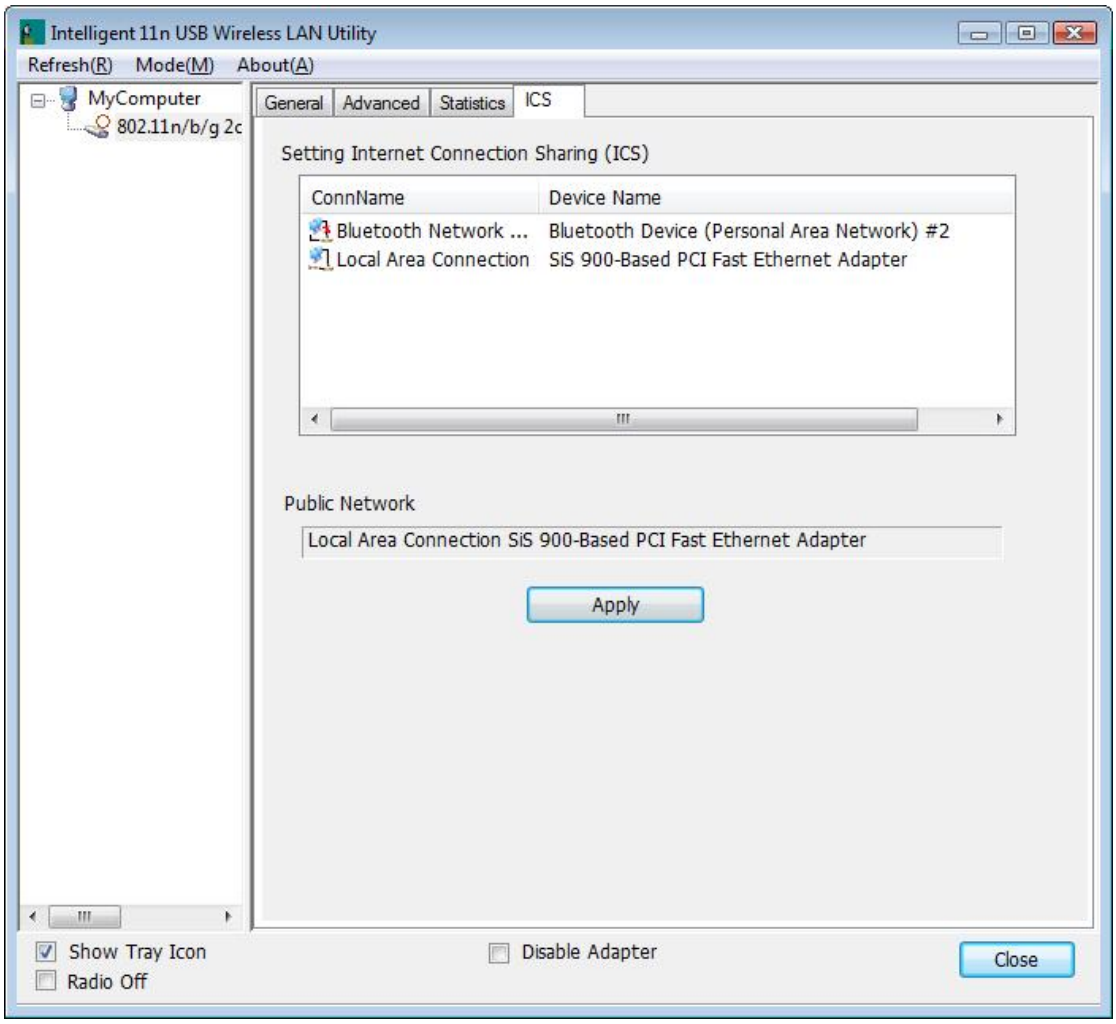
Statistics



Statistics	
Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

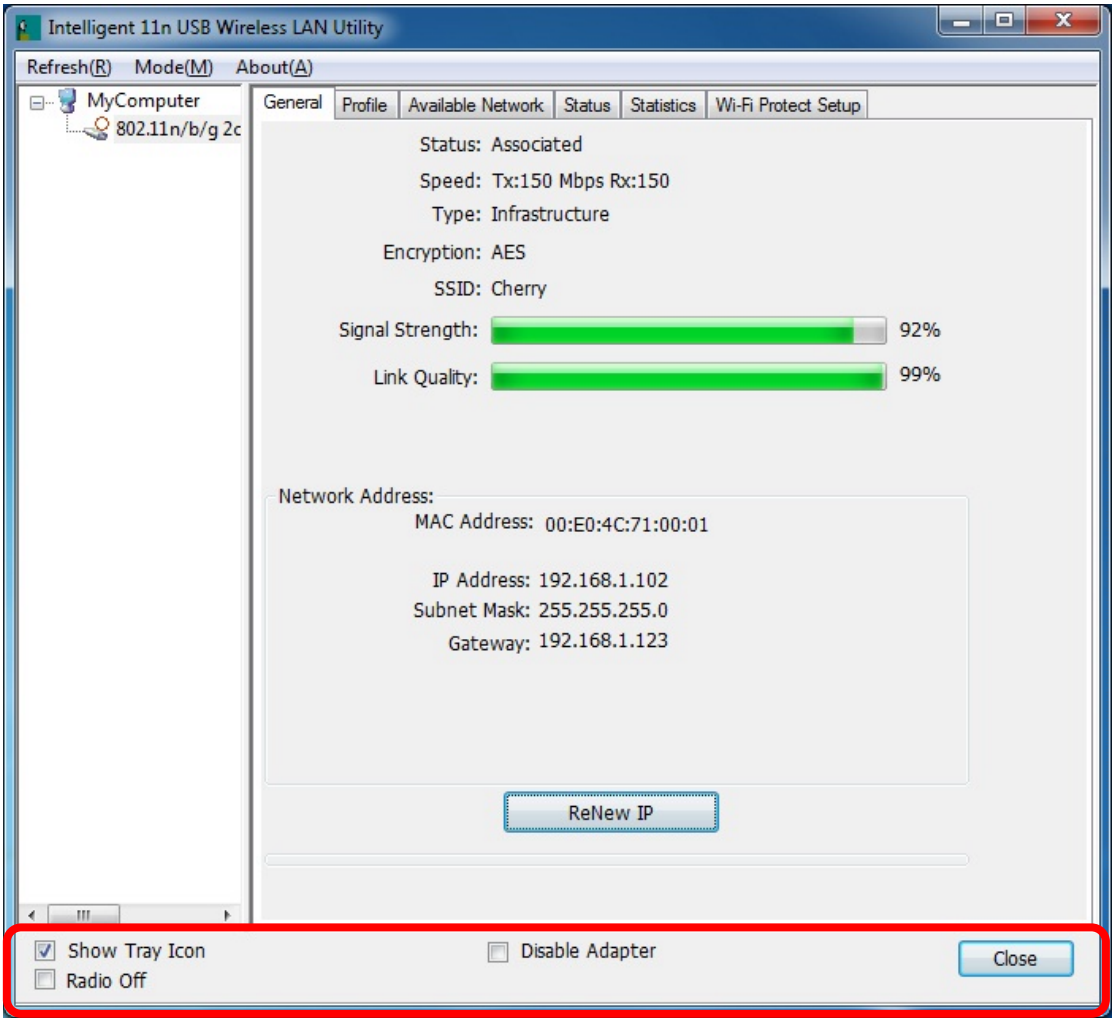
ICS

This page displays setting Internet connection sharing (ICS). Select a sharing public network and click Apply button to make a connection.



For Windows 7

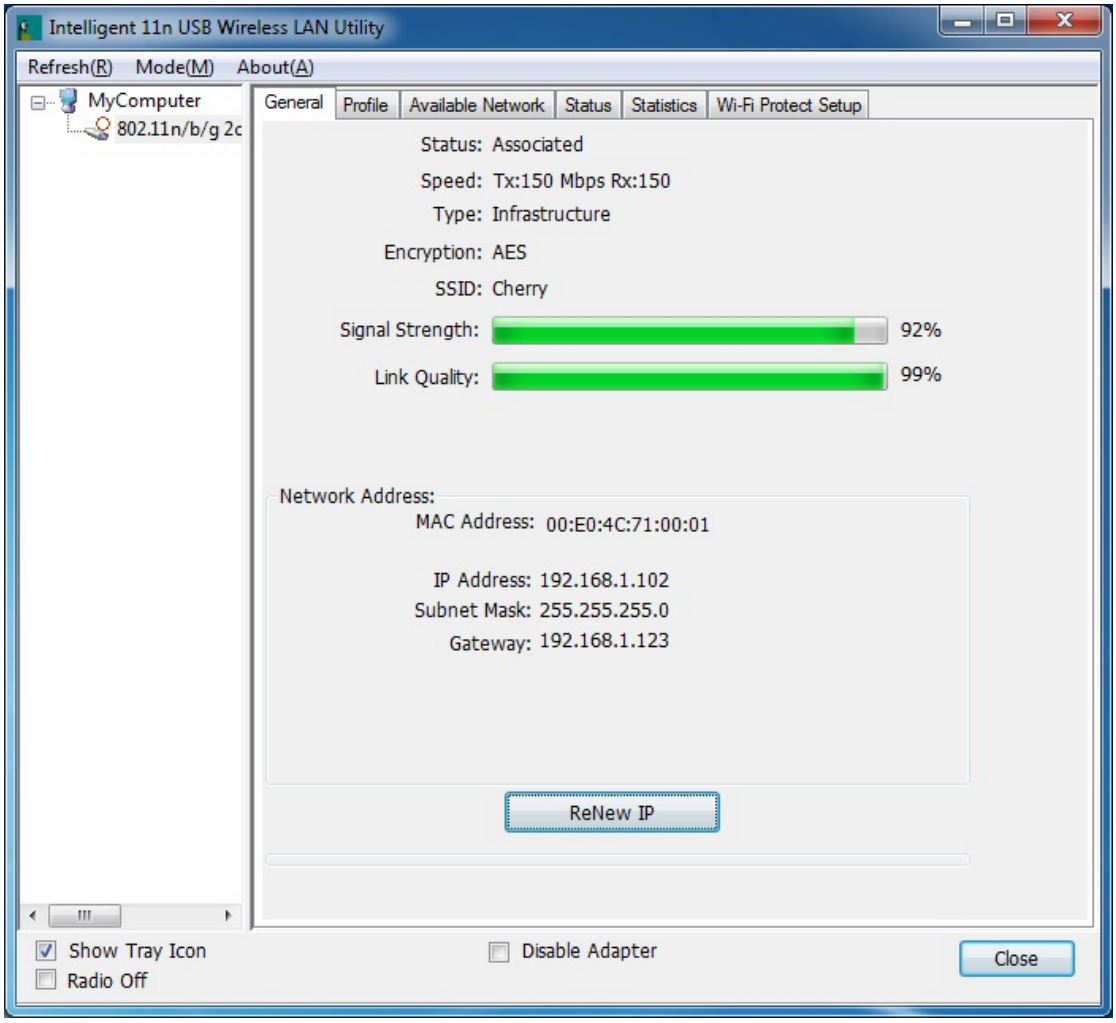
Station Mode



- **Show Tray Icon:** Check to show the wireless adapter icon at the tray.
- **Disable Adapter:** Check this to disable the wireless adapter.
- **Radio off:** Check this to turn OFF radio function.
- **Close:** Click to leave the Intelligent 11n USB Wireless LAN Utility.

General

The General page displays the detail information of current connection.

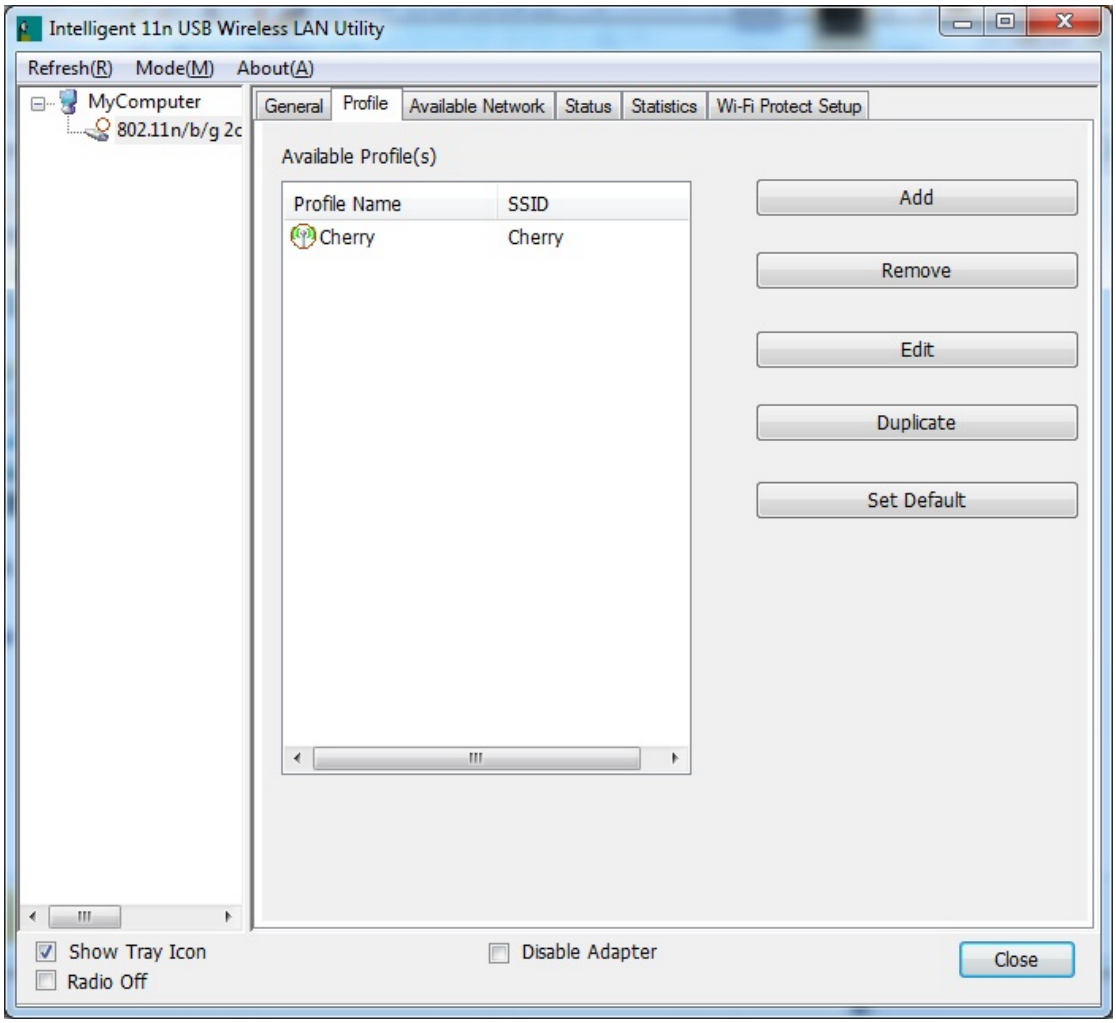


General Tab	
Status	Shows the current connected status. If there is no connection, it will show Not Associated. If been connected, the system will show Associated. When connecting, the system will show checking Status.
Speed	Shows the current transmitting rate and receiving rate.
Type	Network type in use, Infrastructure or Ad-Hoc.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
SSID	Shows the connected access point network name.
Signal Strength	Shows the receiving signal strength.
Link Quality	Shows the connection quality based on signal strength.
MAC Address	The physical address of the WLAN Module.
IP Address	Shows the IP address information.
Subnet Mask	Shows the Subnet Mask information.
Gateway	Shows the default gateway IP address.

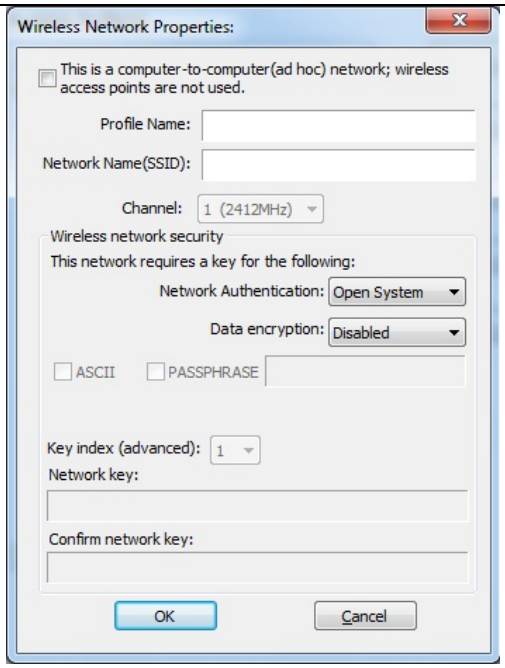
Renew IP	Click the **Renew IP** button to obtain IP address form the connected gateway.

Profile

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add, Remove, Edit, Duplicate** and **Set Default** profiles.



Profile Tab	
Profile Name	Here shows a distinctive name of profile in this column.
SSID	The **SSID** is the unique name shared among all wireless access points in the wireless network.
Add	Click **Add** button to add a profile from the drop-down screen.



This is a computer-to-computer (ad hoc) network; wireless access points are not used: This function is selected to enable the ad hoc network type that computers should be setup at the same channel to communicate to each other directly without access point, users can share files and printers between each PC and laptop.

Profile Name: Users can enter profile name at will.

Network Name (SSID): The SSID is the unique network name (case-sensitive) shared among all wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network.

Channel: If set to ad hoc network type, user can select channels form the pull-down menu.

Wireless network security

Network Authentication: There are several types of authentication modes including Open System, Shared Key, WPA-PSK, WPA2-PSK, WPA 802.1X, WPA2 802.1X and WEP 802.1X.

Data encryption: For Open System, Shared Key and WEP 802.1X authentication mode, the selection of encryption type is WEP. For WPA-PSK, WPA2-PSK, WPA 802.1X and WPA2 802.1X authentication mode, the encryption type supports both TKIP and AES.

When encryption is set to WEP…

ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).

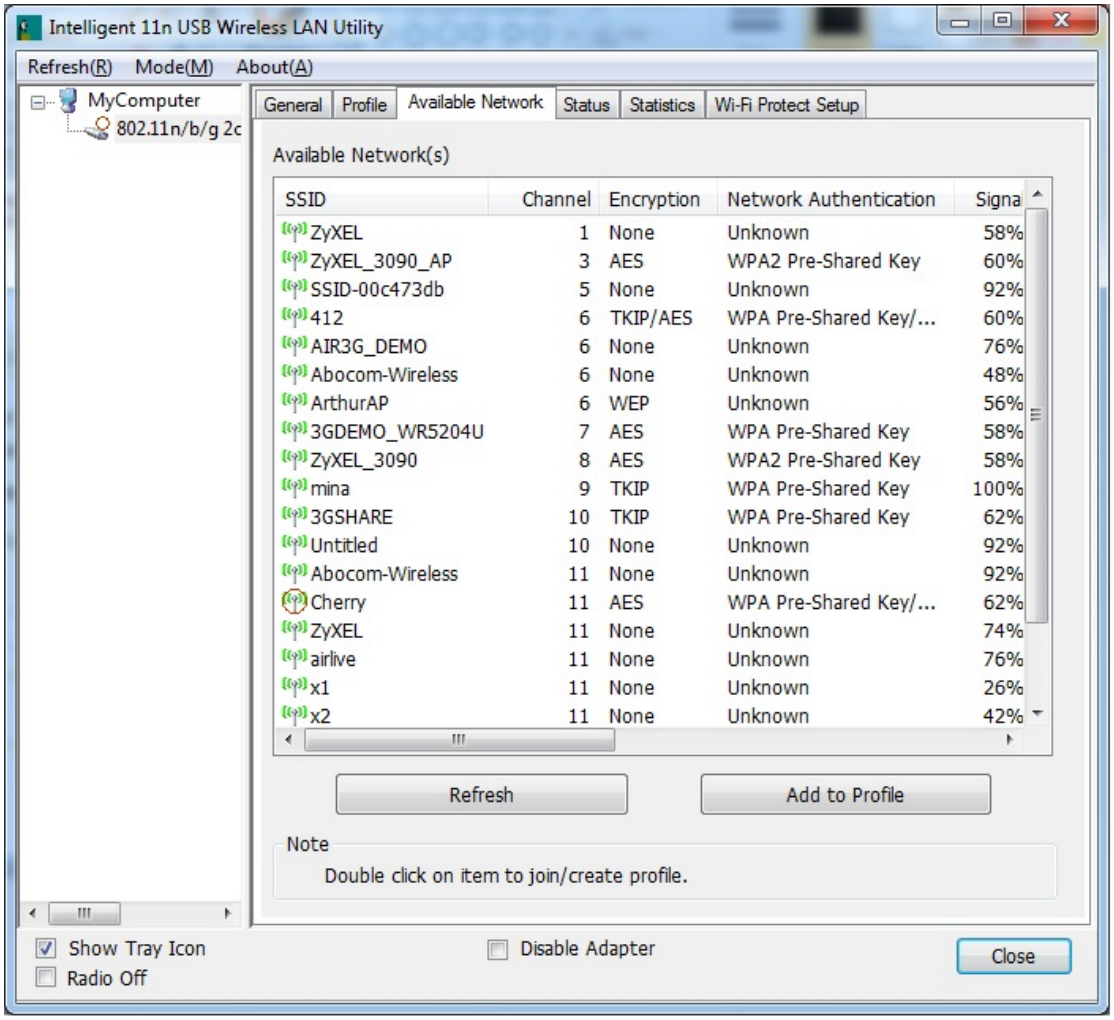
PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).

Key index (advanced): Select 1~4 key index form the pull-down menu, must match with the connected AP's key index.

	When encryption is set to WPA-PSK/ WPA2-PSK… **Network key:** Enter network key at least 8 to 64 characters. **Confirm network key:** Enter network key again to confirm. **When encryption is set to WPA 802.1X/ WPA2 802.1X/ WEP 802.1X…** When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge). **EAP TYPE:** • **TLS**: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point. • **LEAP:** Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication. • **TTLS**: Tunnelled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. • **PEAP**: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN. ⊙ **MD5**: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network. **Tunnel:** This is enabled under TTLS and PEAP type. For TTLS, the selections of tunnel are CHAP, MSCHAP, MSCHAP-V2, PAP. For PEAP, the selections of tunnel are MD5, GTC, TLS and MSCHAP-V2. **Username:** Enter the username for server. **Identity:** Enter the identity for server. **Domain:** Enter the domain of the network. **Password:** Enter the password for server. **Certificate:** Choose server that issuer of certificates.
Remove	Click **Remove** button to delete selected profile.
Edit	Click **Edit** button to edit selected profile.
Duplicate	Click **Duplicate** button to copy selected profile.
Set Default	Click **Set Default** button to set selected profile to be connected first.

Available Network

This page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Channel, Encryption, Network Authentication, Signal, Type, BSSID, Supported Rate(s), and Mode.

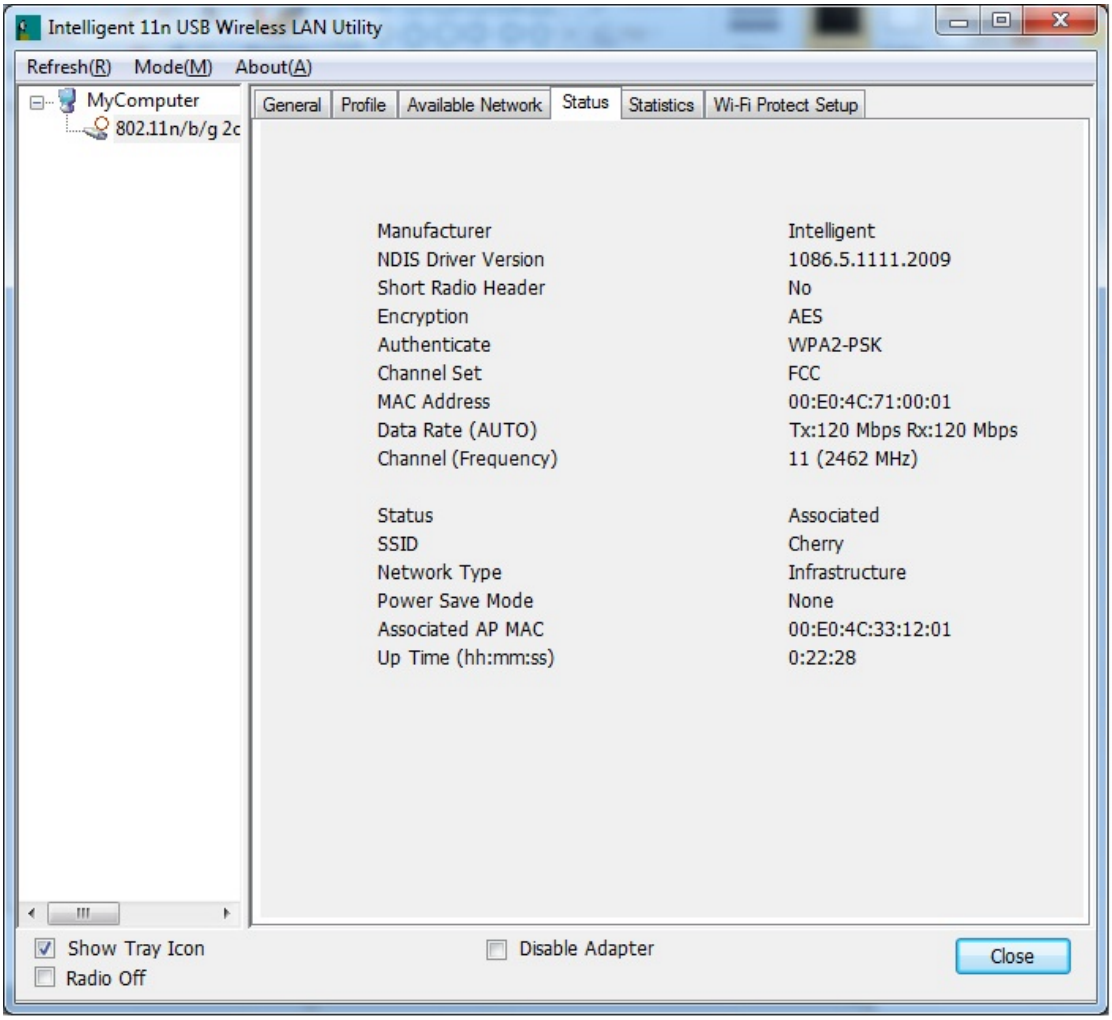


Network Tab	
SSID	Shows the network name of the access points.
Channel	Shows the currently channel in use.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, None and TKIP/AES.
Network Authentication	Show the device network authentication.
Signal	Shows transmit power, the amount of power used by a radio transceiver to send the signal out.
Type	Network type in use, Infrastructure or Ad-Hoc mode.

BSSID	Shows Wireless MAC address.
Supported Rate(s)	Shows the transmitting data rate.
Mode	Supported wireless mode. It may support 802.11b, 802.11g and 802.11n wireless mode.
Refresh	Click Refresh button to search and rescan the available network.
Add to Profile	Select an available network (SSID) on the list and then click **Add to Profile** button to add it into the profile list.
Note	Double click on item to join/create profile.

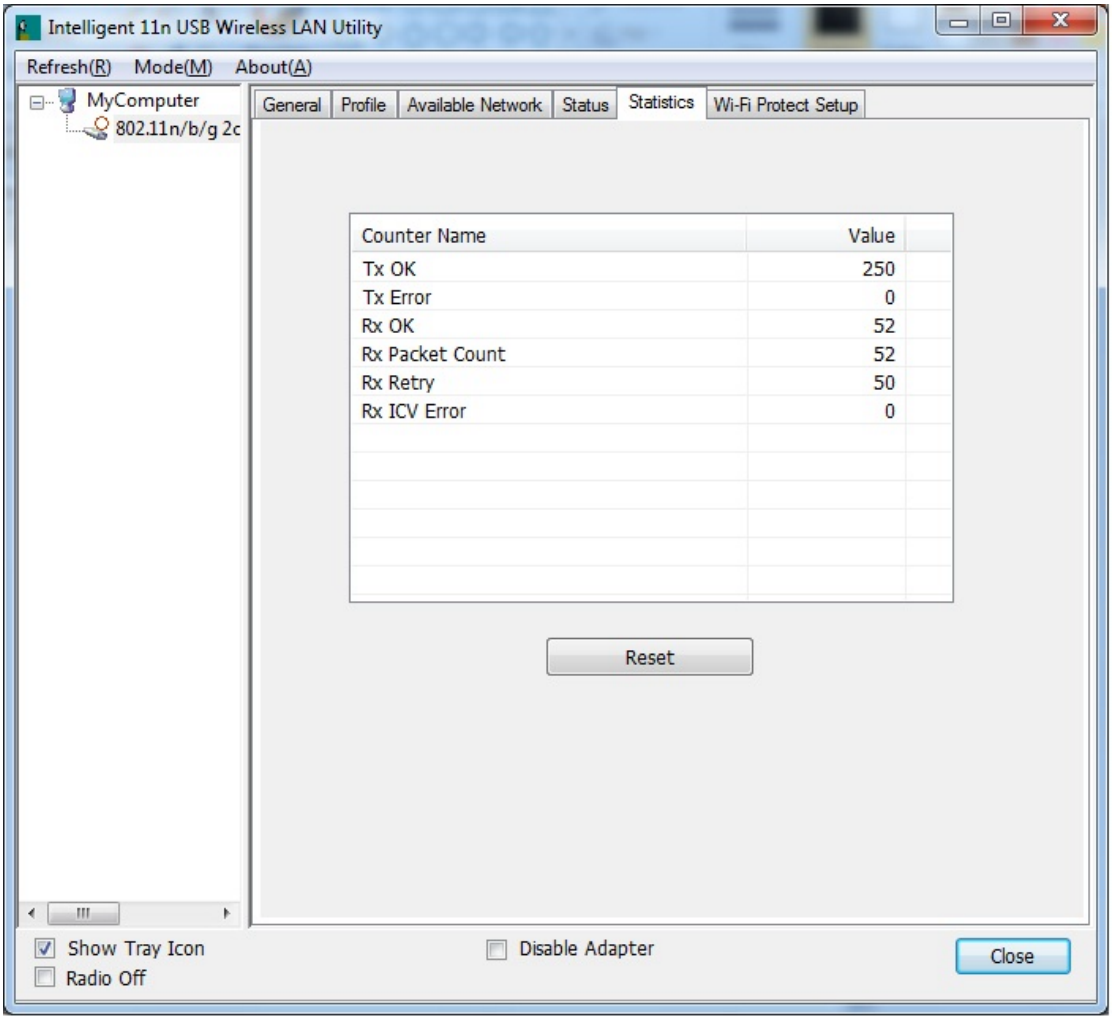
Status

This tab listed the information about the WLAN Module and connected access point.



Statistics

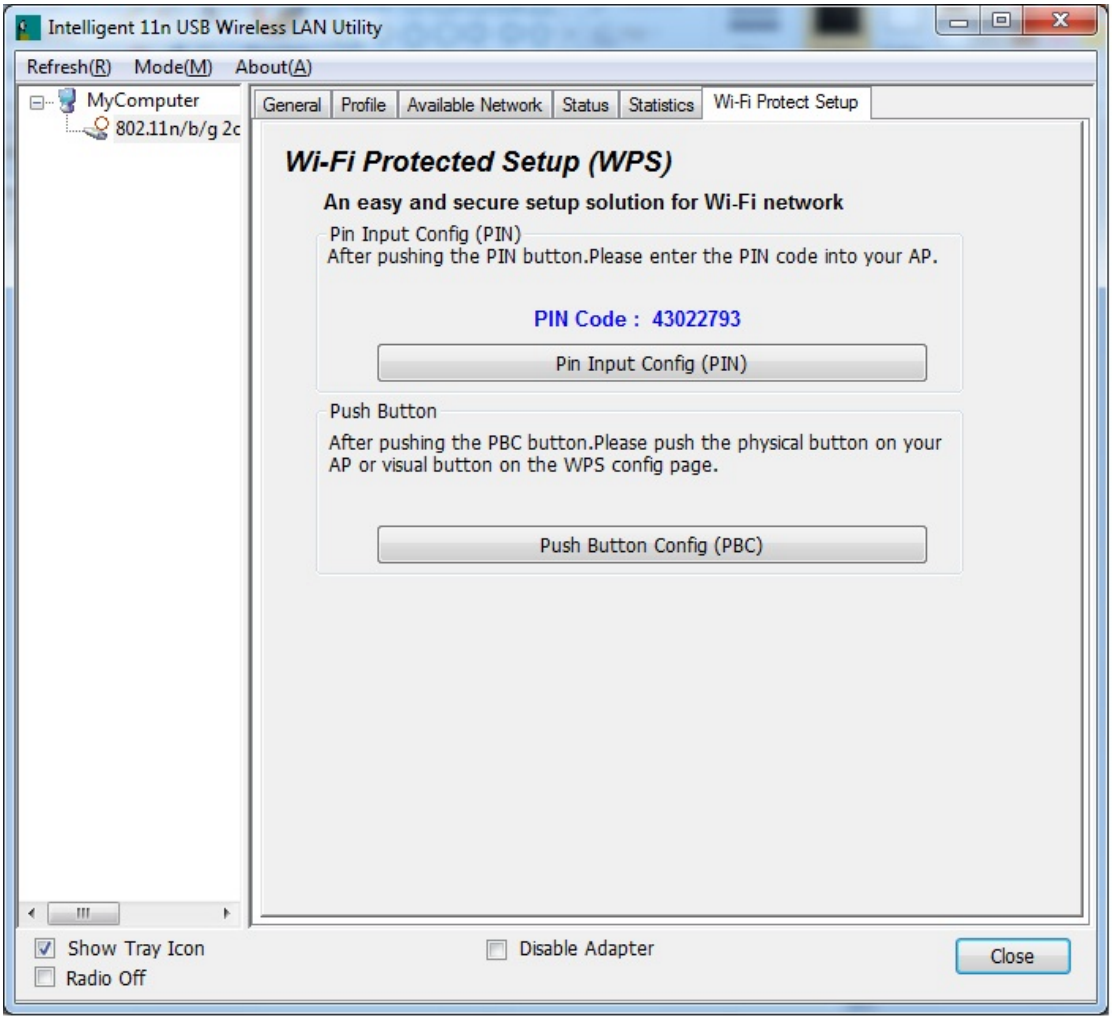
The Statistics screen displays the statistics on the current network settings.



Statistics	
Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

WPS

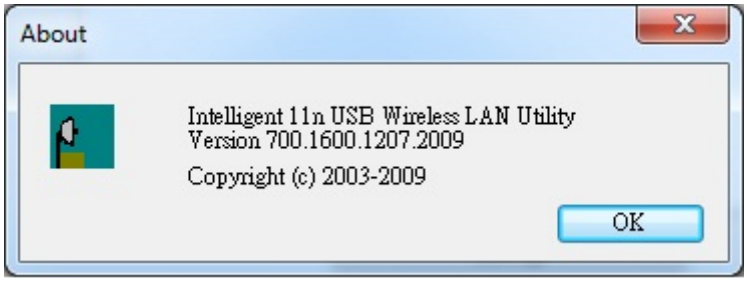
The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.



WPS Tab	
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use "**Renew**" button to re-generate new PIN Code.
Pin Input Config (PIN)	Click the **Pin Input Config (PIN)** button to select specific AP to process PIN Config.
Push Button Config (PBC)	Click this button to connect with AP that supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.

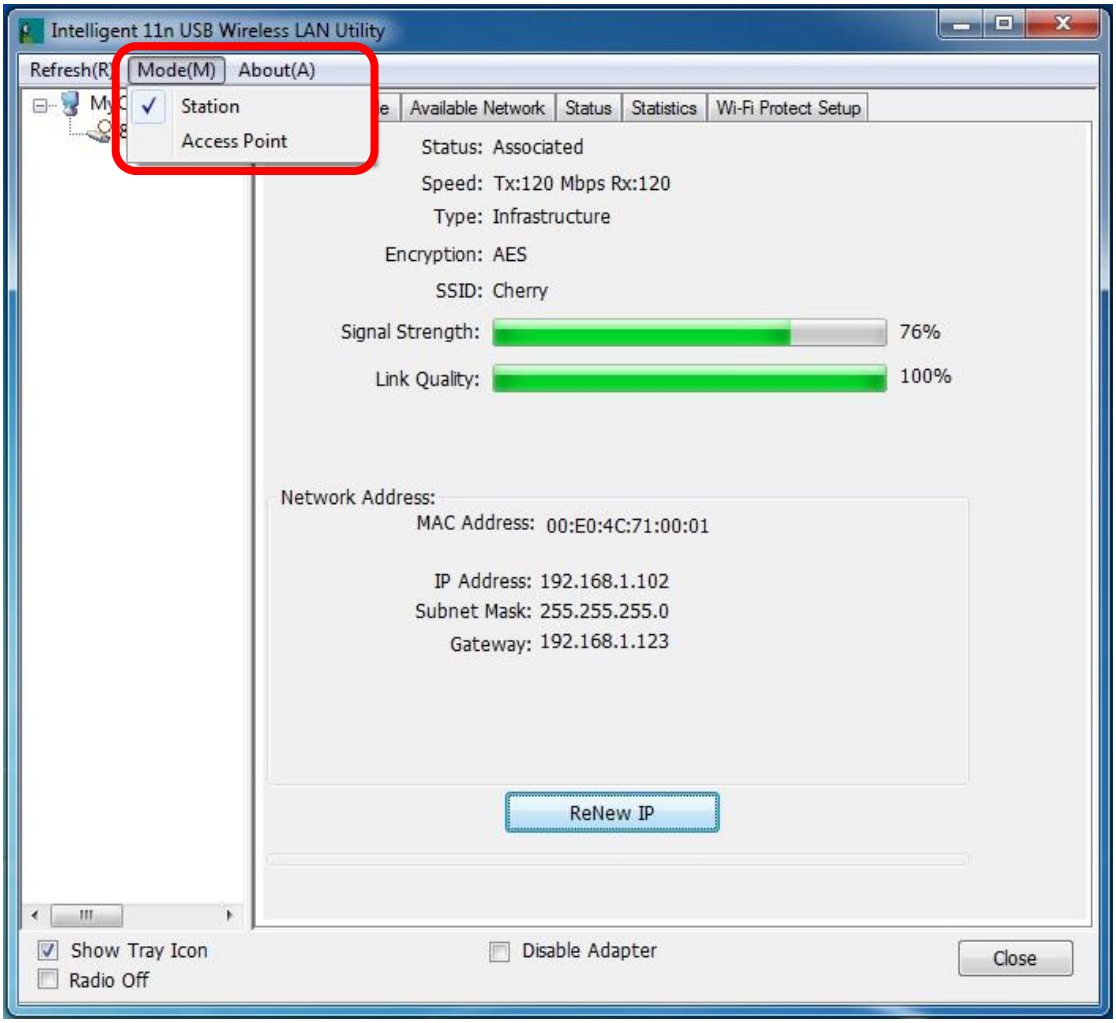
About

This page displays the information of the WLAN Module Version.



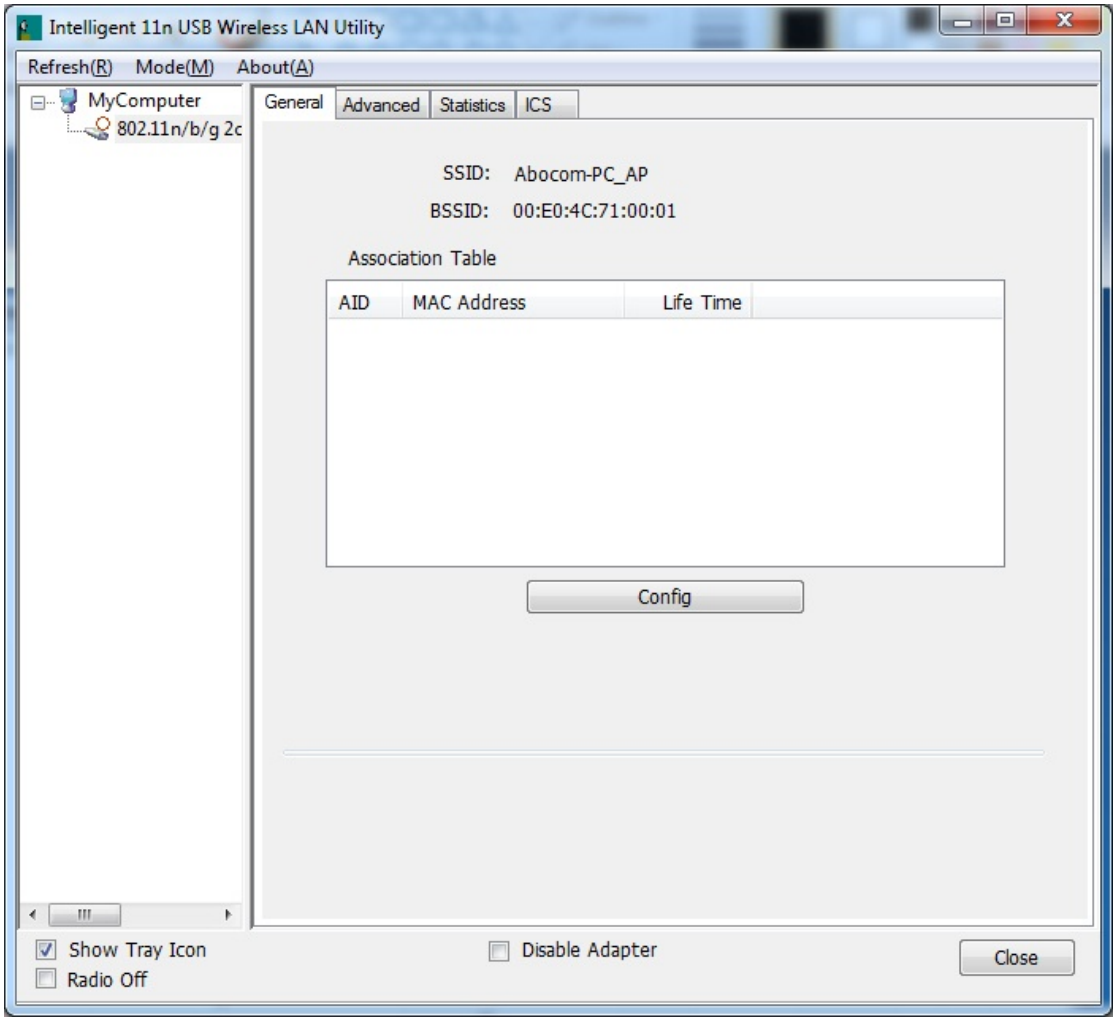
Switch to AP Mode

To access the soft AP mode, please select the **Mode** on the function list of the Utility to make the WLAN Module act as a wireless AP.

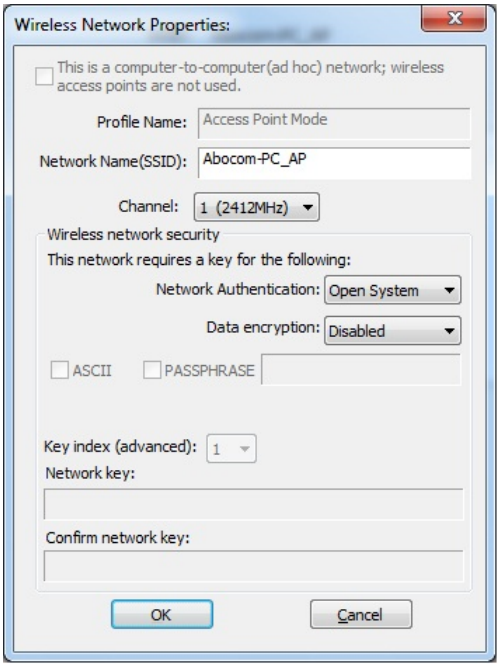


Soft AP mode

General



General	
SSID	Shows the network name of the AP.
BSSID	Shows the MAC address of the AP.
Association Table	This table shows the connected client here.
Config	Click the Config button to set up the Wireless Network Properties.



Network Name (SSID): User can change the network name of this access point.

Channel: User can select the channel form the pull-down list.

Wireless network security

Network Authentication: There are several types of authentication modes including Open System, Shared Key, WPA-PSK and WPA2-PSK.

Data encryption: For Open System and Shared Key authentication mode, the selection of encryption type is WEP. For WPA-PSK, WPA2-PSK, authentication mode, the encryption type supports both TKIP and AES.

When encryption is set to WEP…

ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).

PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).

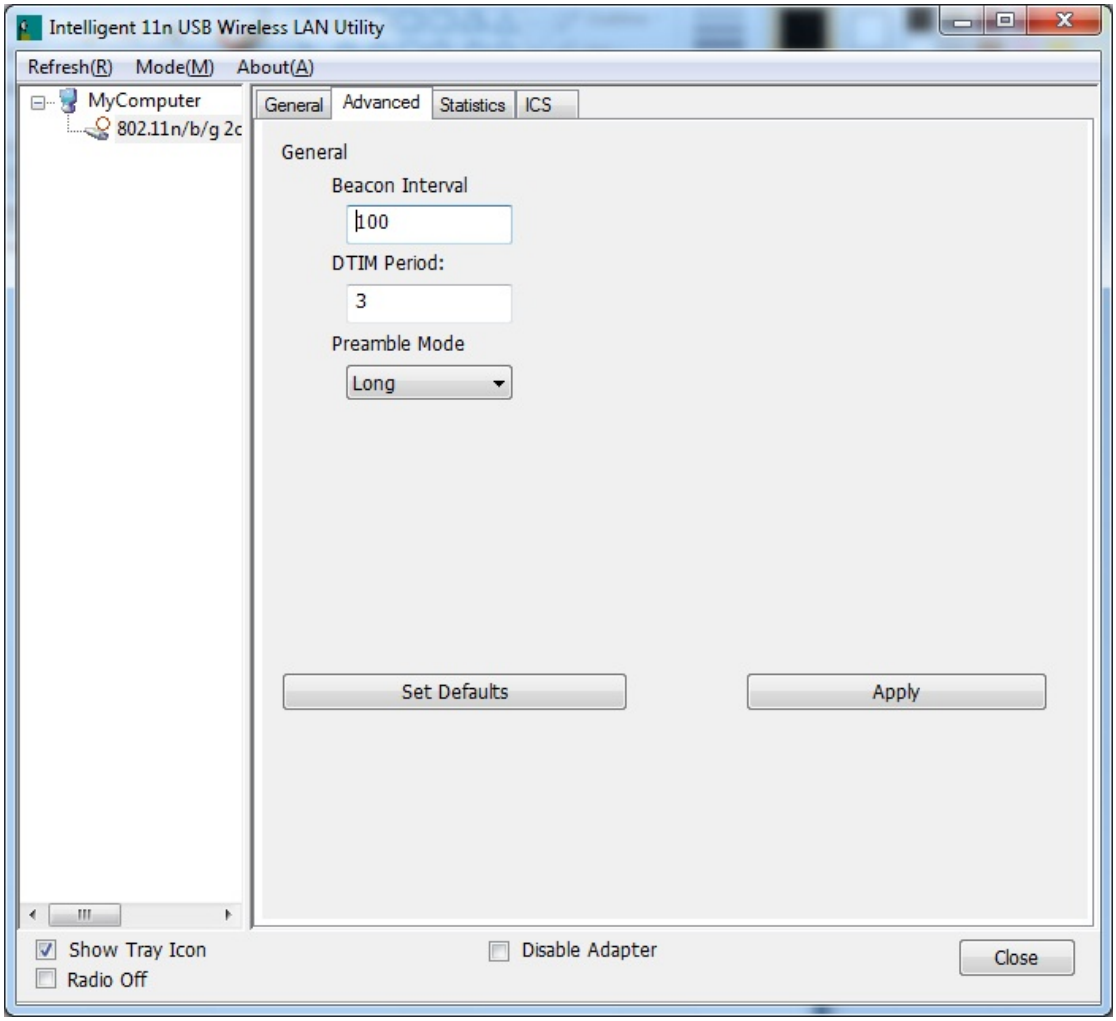
Key index (advanced): Select 1~4 key index form the pull-down menu, must match with the connected AP's key index.

When encryption is set to WPA-PSK/ WPA2-PSK…

Network key: Enter network key at least 8 to 64 characters.

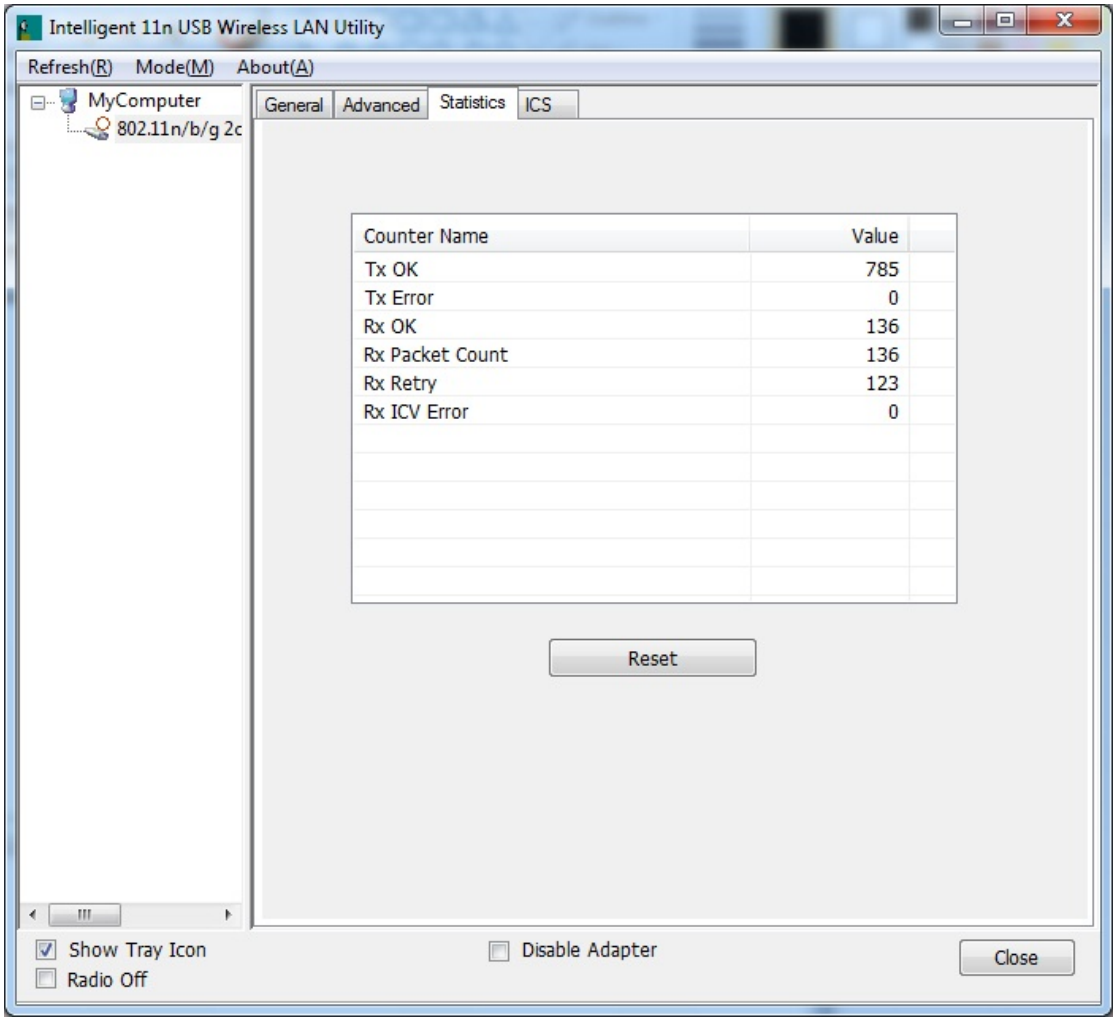
Confirm network key: Enter network key again to confirm.

Advanced



Advanced	
Beacon Interval	The time between two beacons. (The system default is 100 ms.)
DTIM Period	The delivery traffic indication message (DTIM) is an element included in some beacon frames. User can specify a value from 1 to 255 beacons.
Preamble	Select from the pull-down menu to change the Preamble type into **Short** or **Long**.
Set Defaults	Click to use the system default value.
Apply	Click to apply the above settings.

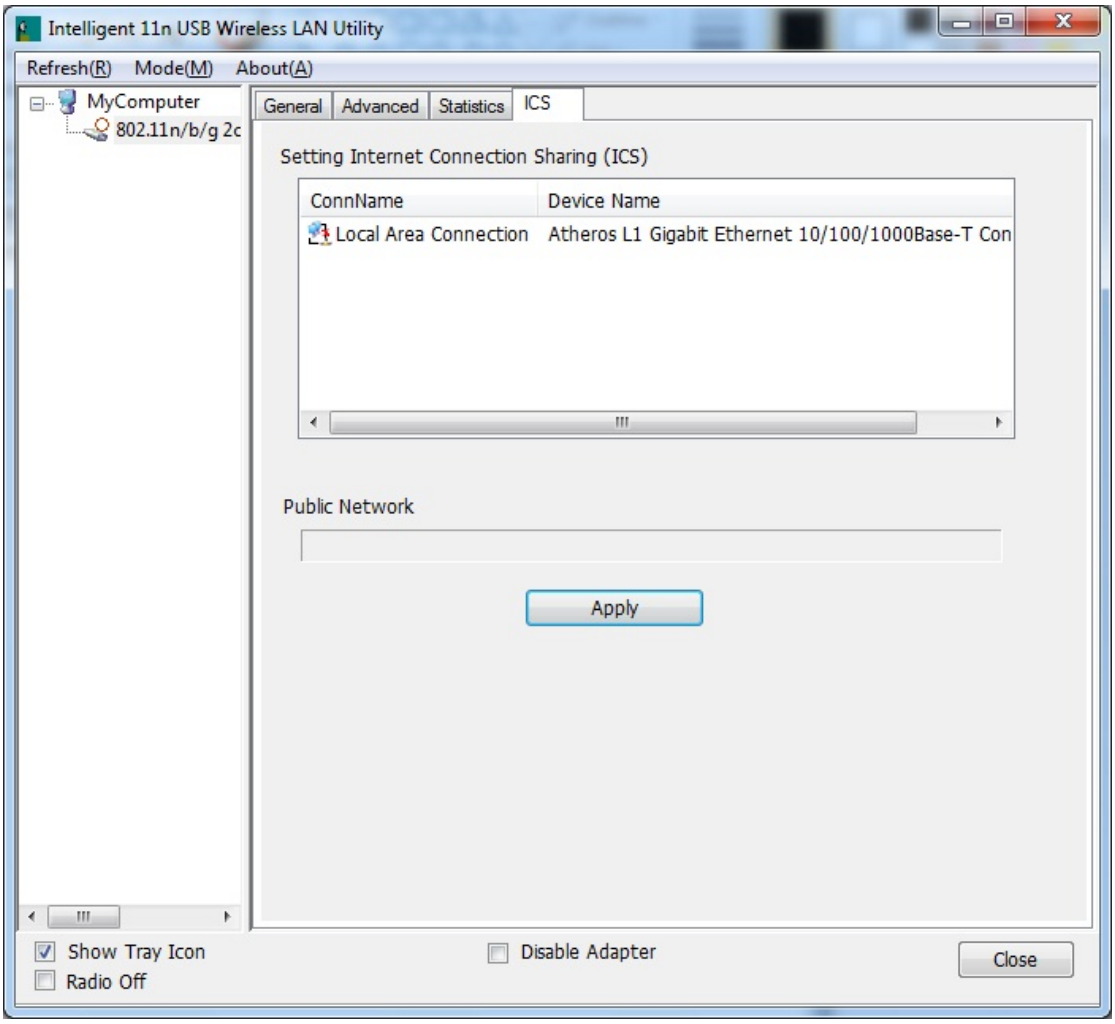
Statistics



Statistics	
Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

ICS

This page displays setting Internet connection sharing (ICS). Select a sharing public network and click Apply button to make a connection.

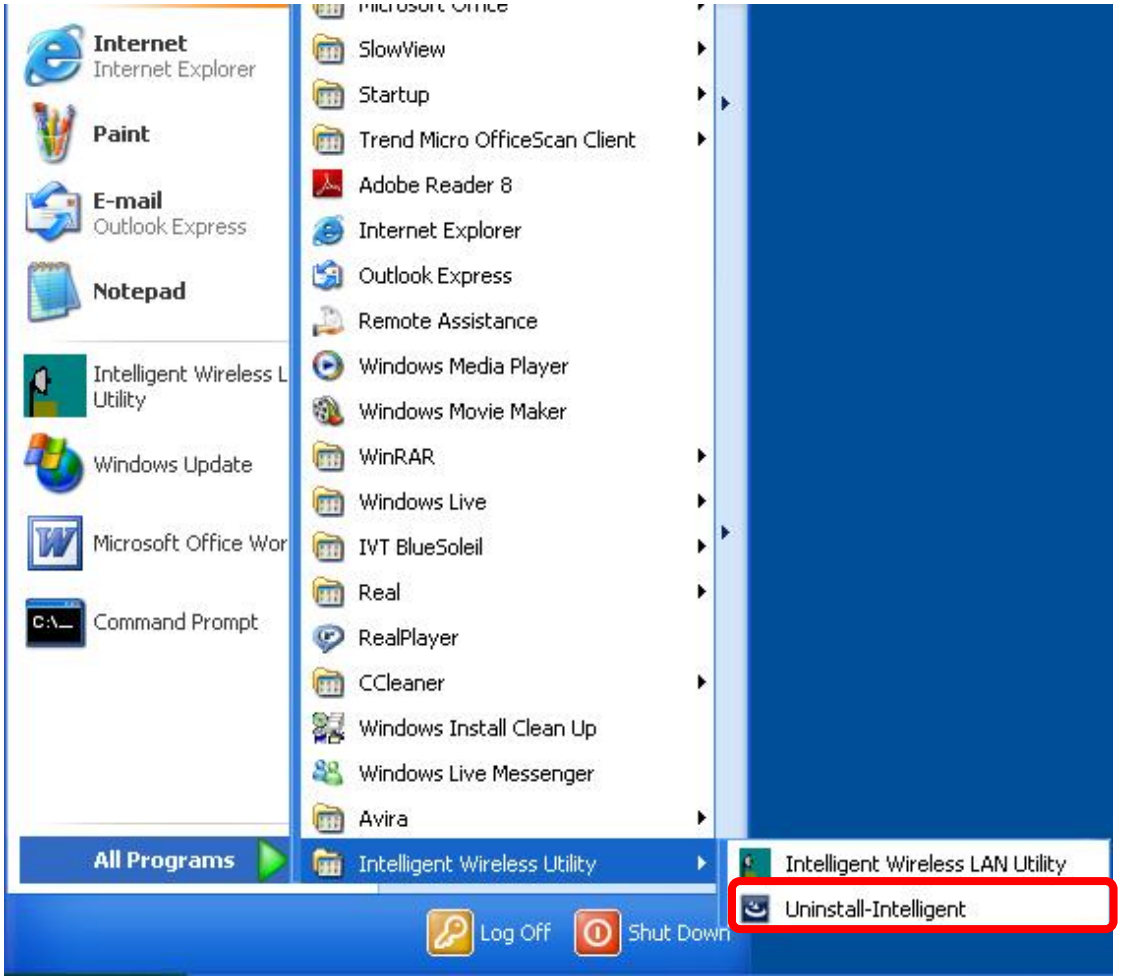


Chapter 5: Uninstall

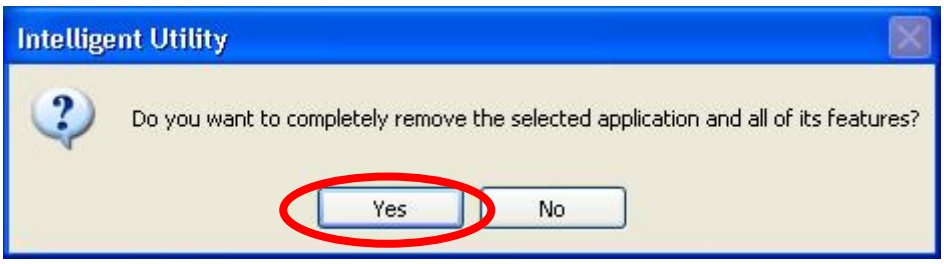
For Windows 2000 / XP

To remove the utility and driver, please refer to below steps. (When removing the utility, the driver will be removed as well.)

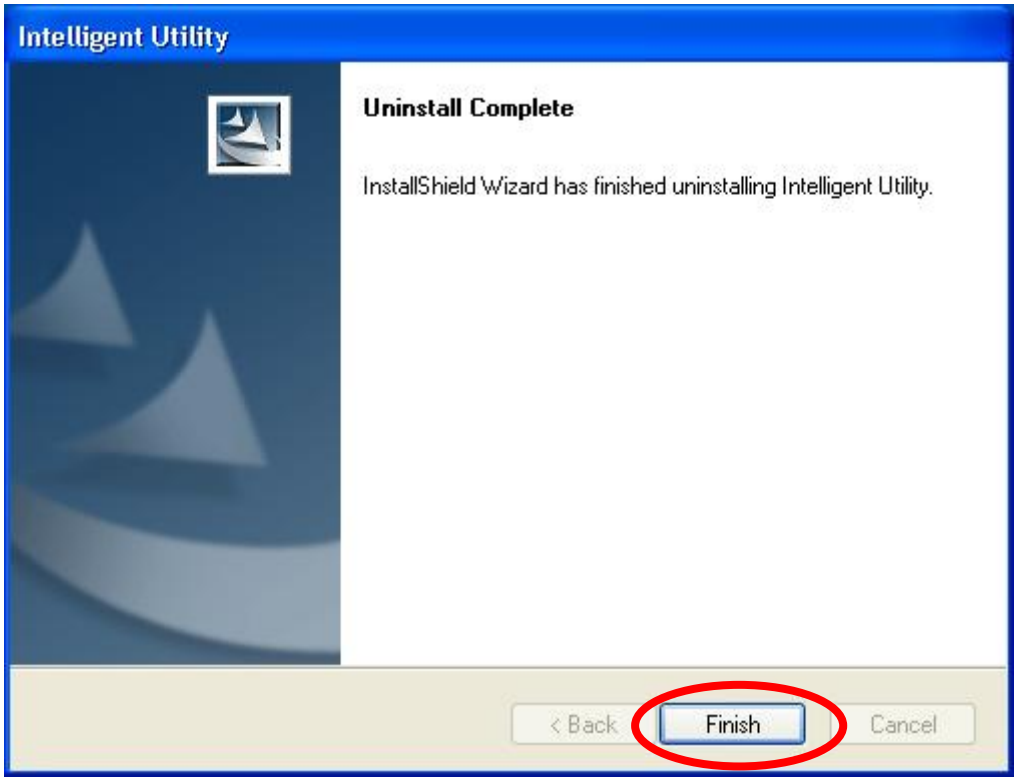
1. Go to **Start →All Programs →Intelligent Wireless Utility→ Uninstall –Intelligent.**



2. Click **Yes** to completely remove the selected application and all of its features.



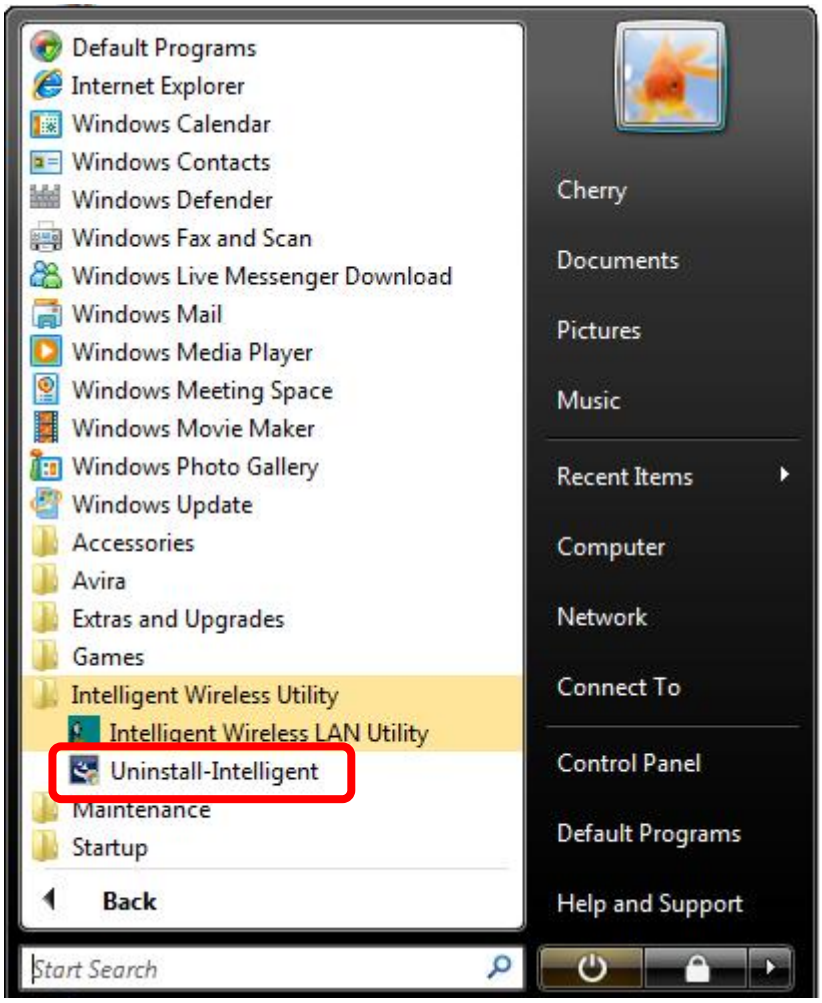
3. Then click **Finish** to complete uninstall.



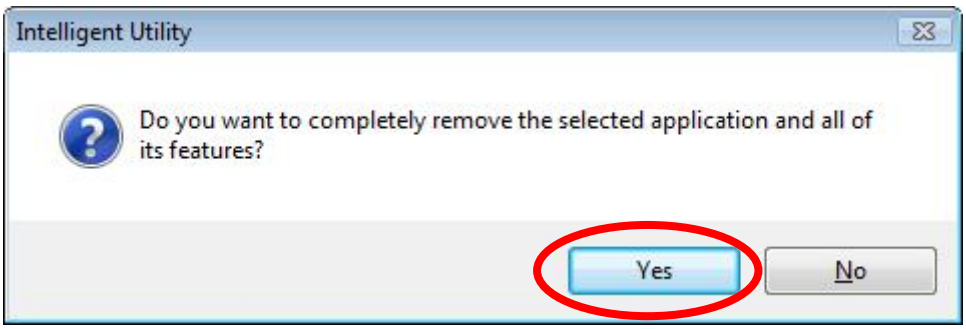
For Windows Vista

To remove the utility and driver, please refer to below steps. (When removing the utility, the driver will be removed as well.)

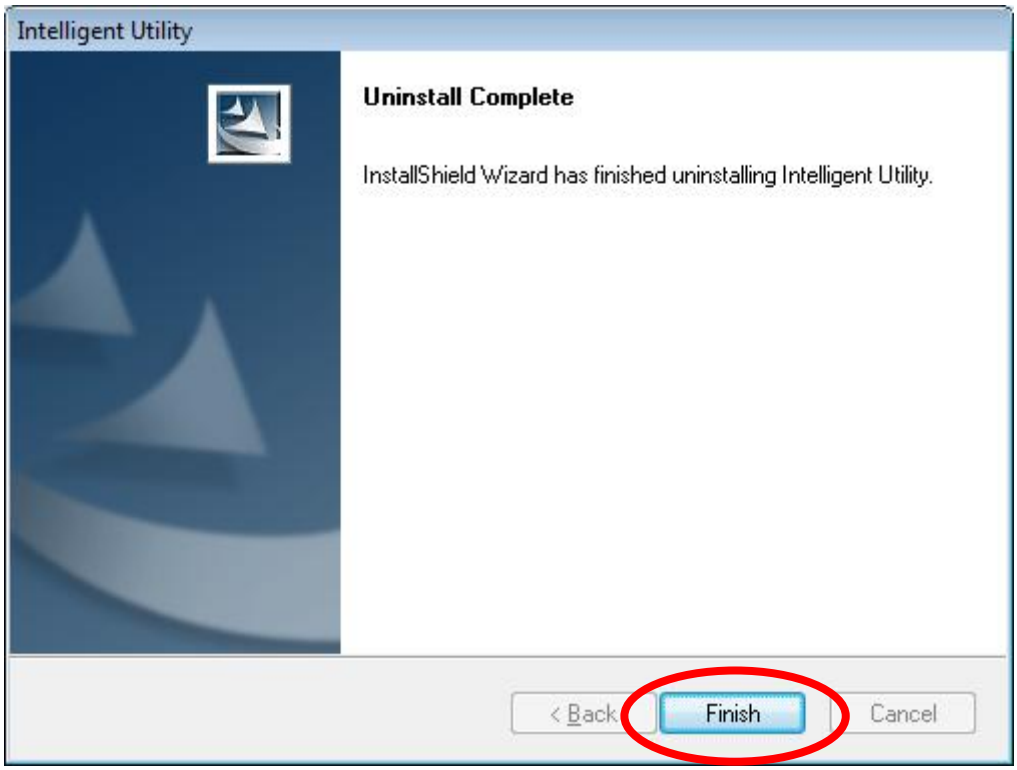
1. Go to **Start → Programs →Intelligent Wireless LAN Utility→ Uninstall –Intelligent**.



2. Click **Yes** to complete remove the selected application and all of its features.



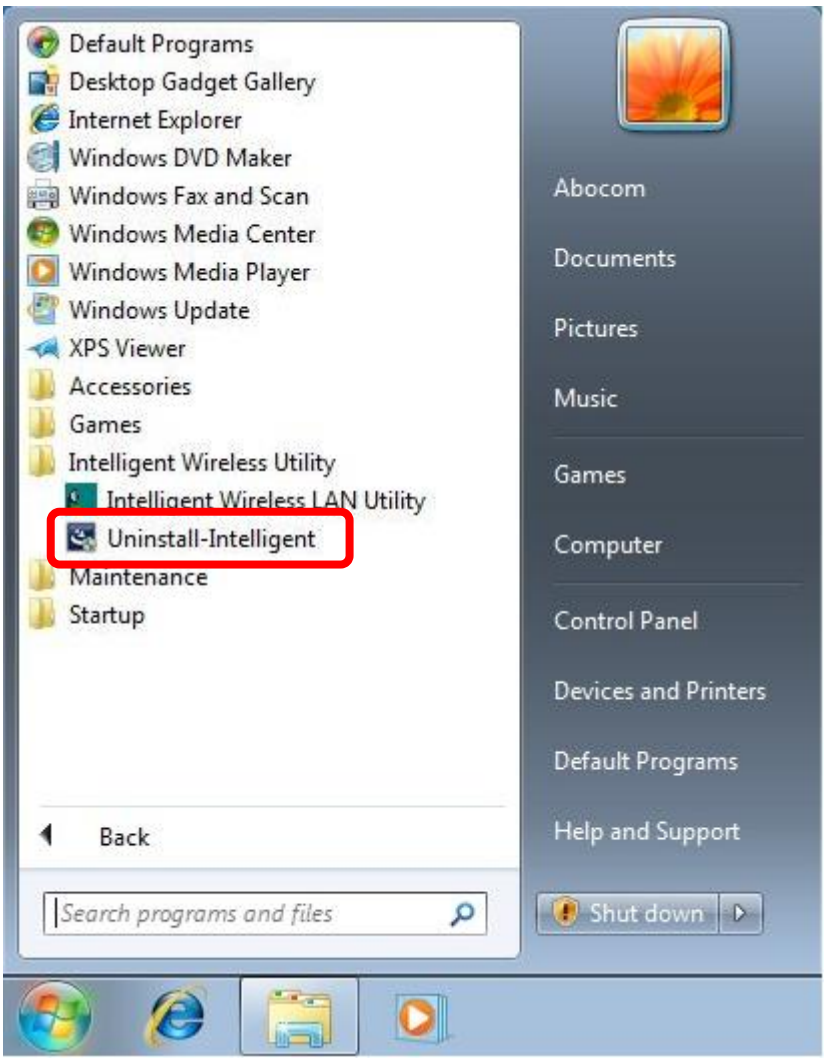
3. Finally, click **Finish** to complete uninstall.



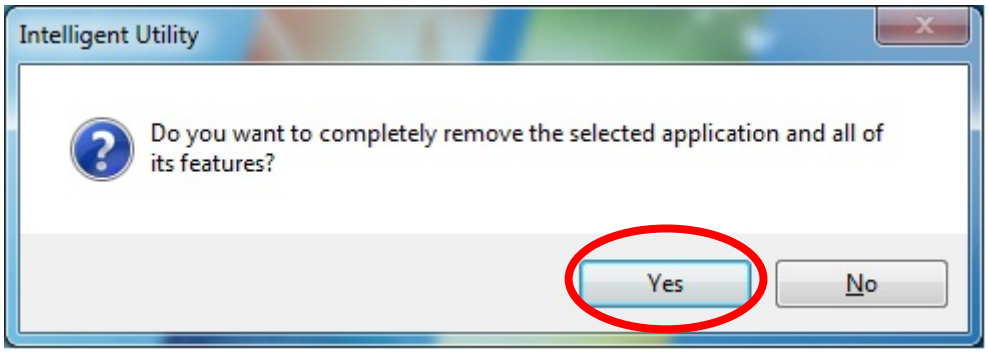
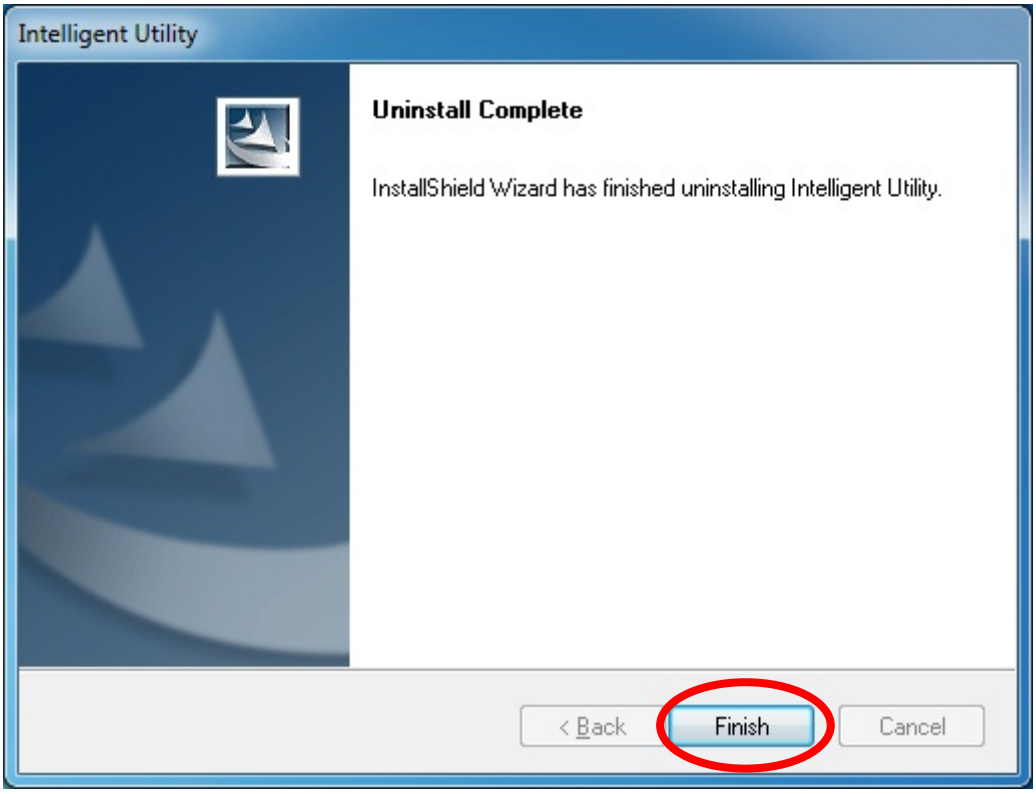
For Windows 7

To remove the utility and driver, please refer to below steps. (When removing the utility, the driver will be removed as well.)

1. Go to **Start → Programs →Intelligent Wireless Utility→ Uninstall –Intelligent**.



2. Click **Yes** to complete remove the selected application and all of its features.



3. Finally, click **Finish** to complete uninstall.