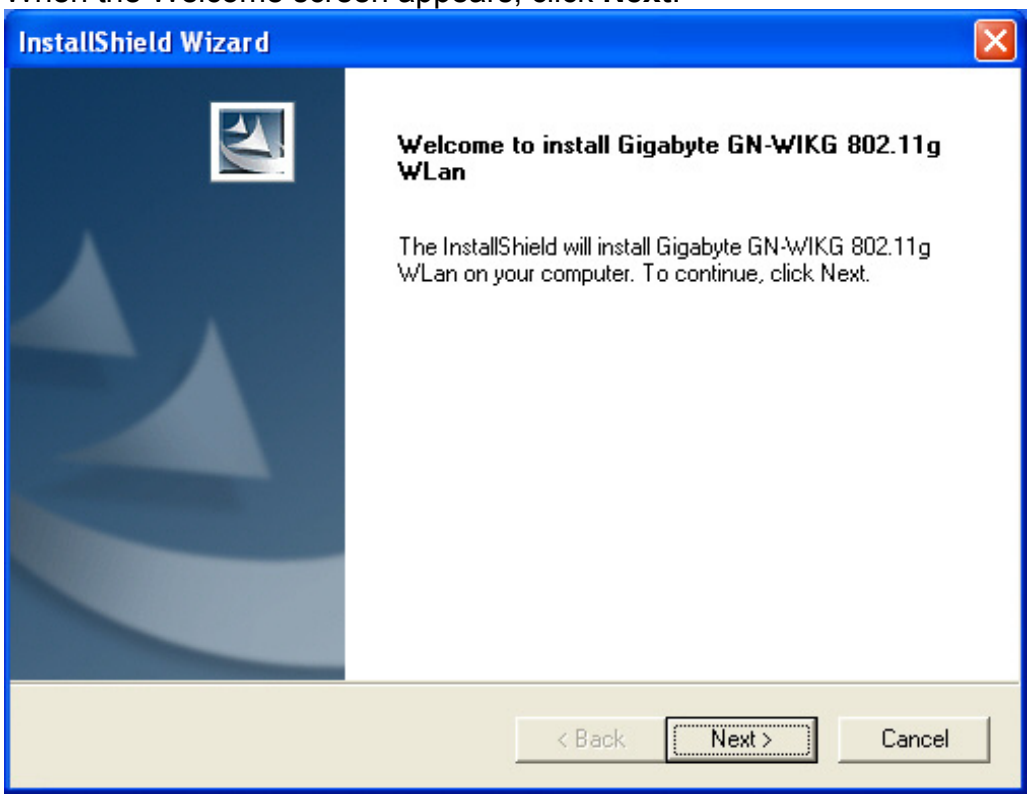
2-5. Driver & Utility Installation - Windows® XP

Step 1: When the **Found New Hardware Wizard** screen appears, click **Cancel** to exit.

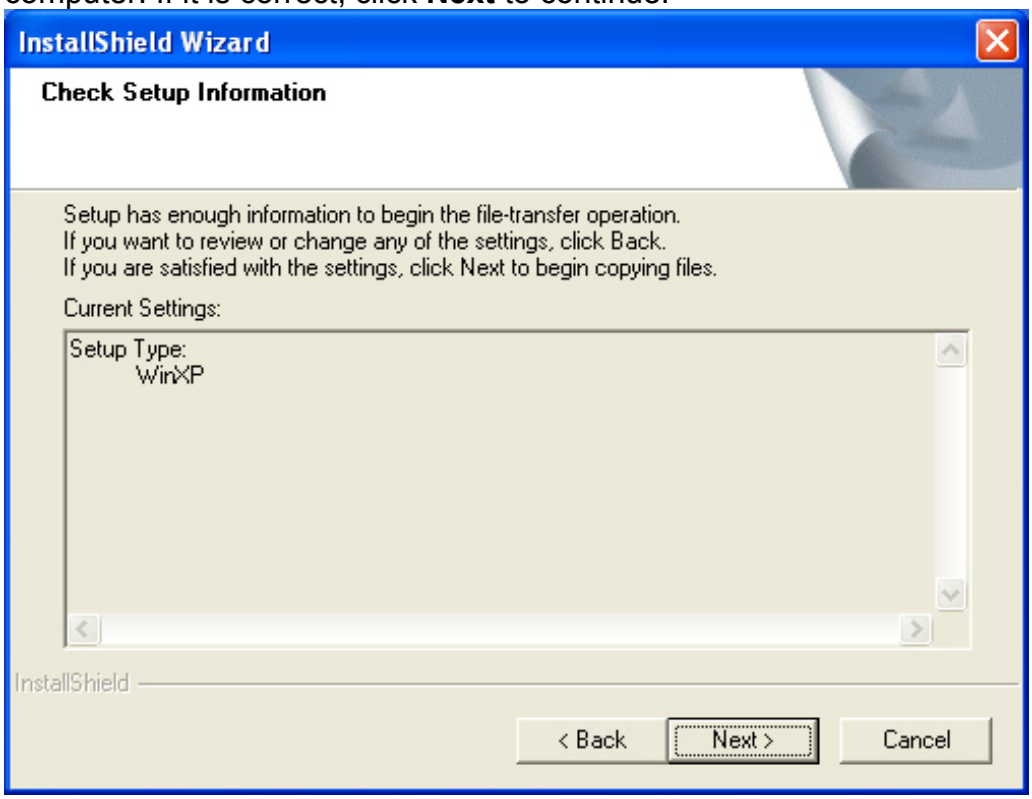
Step 2: Insert the GN-WIKG Installation CD into the CD-ROM drive. The GIGABTYE GN-WIKG Wireless Mini-PCI Adapter setup screen appears.

Step 3: Drag your mouse over **Install Wireless LAN Utility** and click on it to start the utility installation program.

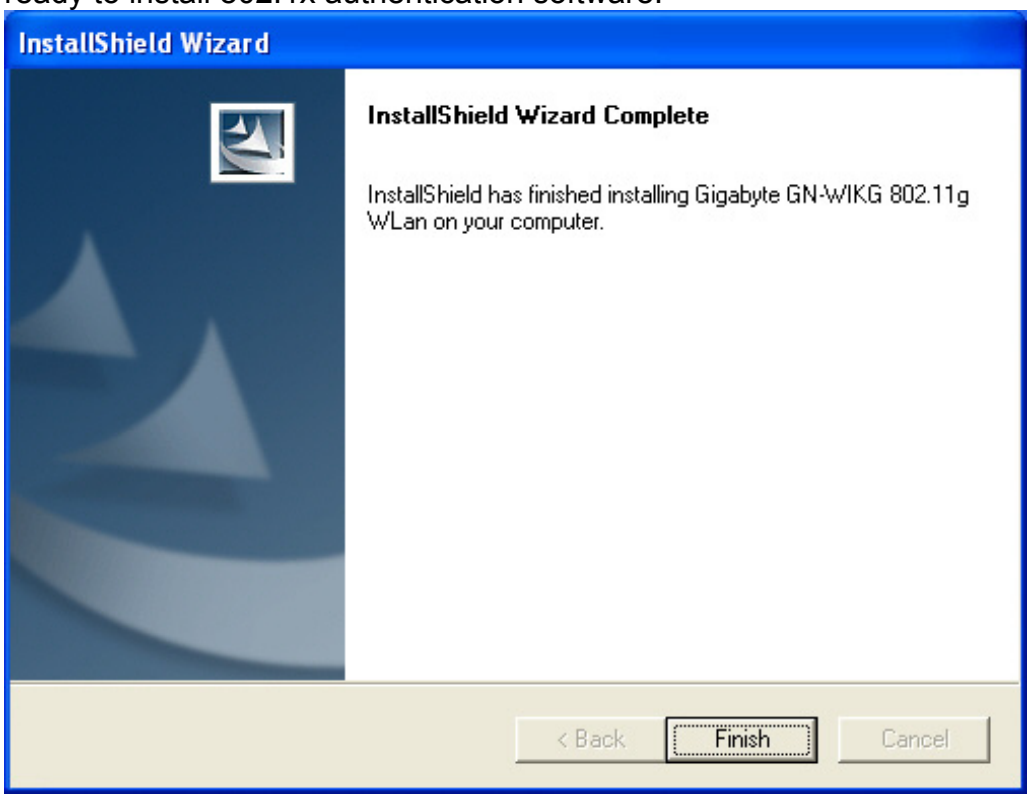
Step 4: When the Welcome screen appears, click **Next**.



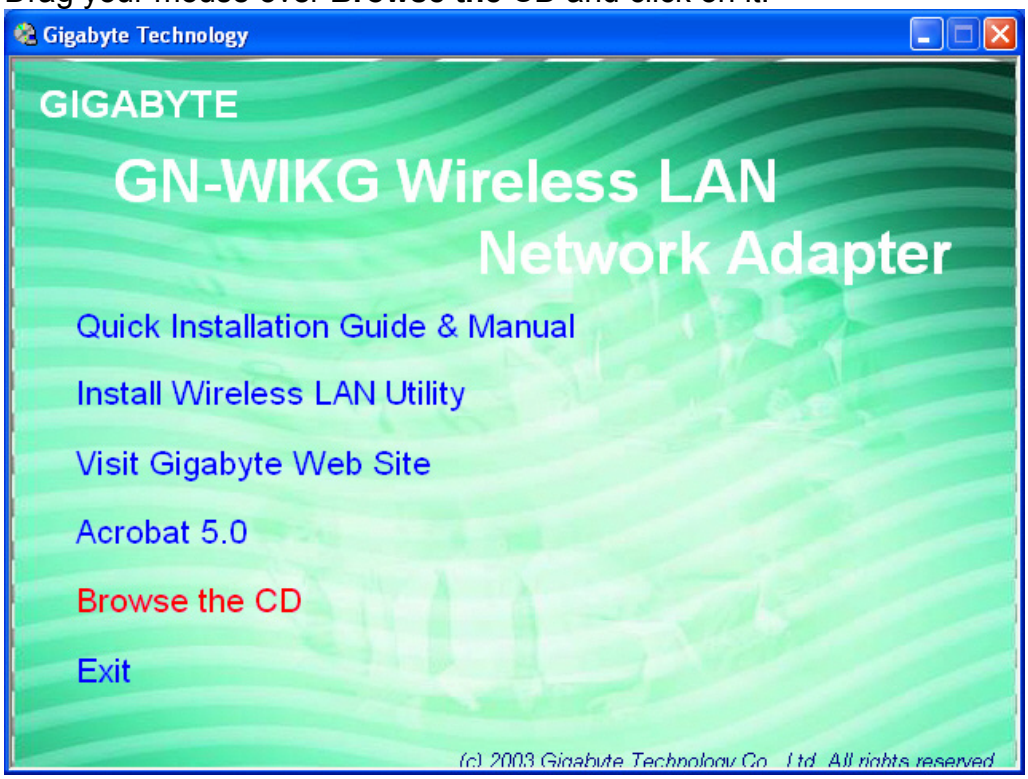
Step 5: The Check Setup Information screen displays the Operating System of your computer. If it is correct, click **Next** to continue.



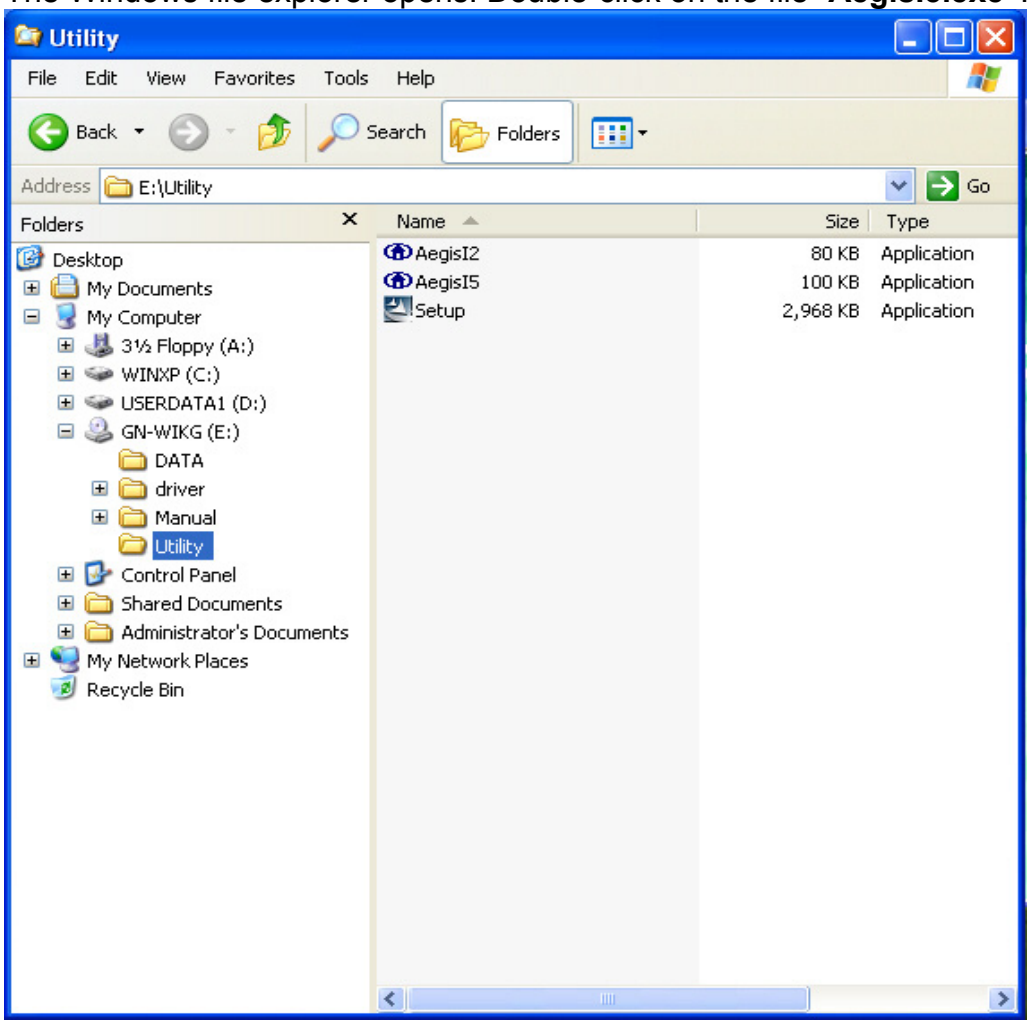
Step 6: After the software utility installation is complete, click **Finish**. You are now ready to install 802.1x authentication software.



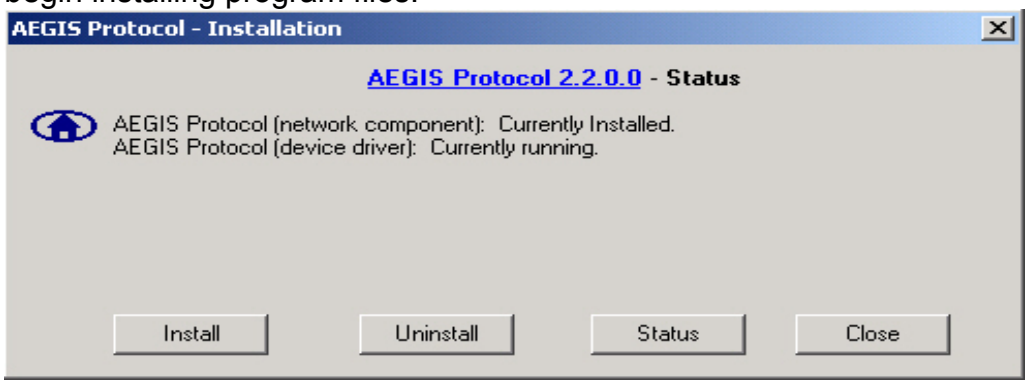
Step 7: Drag your mouse over **Browse the CD** and click on it.



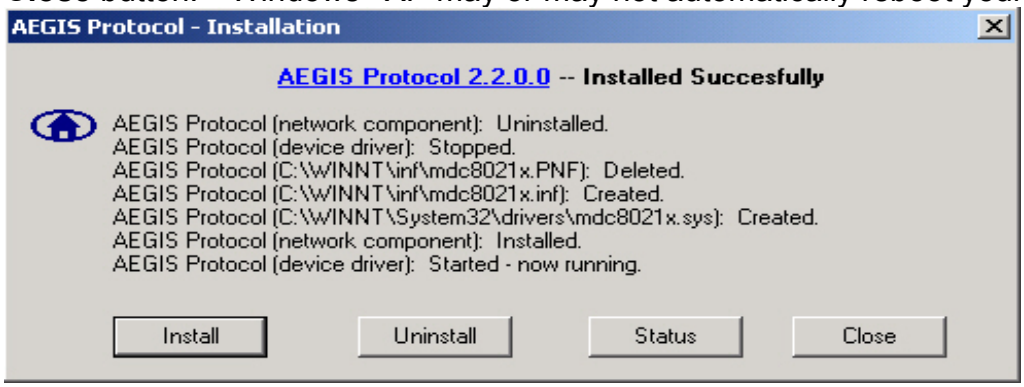
Step 8: The Windows file explorer opens. Double-click on the file "**AegisI5.exe"**.



Step 9: When the AEGIS Protocol Installation window appears click the **Install** button to begin installing program files.



Step 10: When the message **Installed Successfully** appears in the dialog box, click the **Close** button. Windows® XP may or may not automatically reboot your PC.



Chapter 3 Using the GIGABYTE WLAN Configuration Utility

The Gigabyte WLAN Utility is a powerful application that helps you to configure the GN-WIKG Wireless Mini-PCI Adapter as well as monitor the network status link. It automatically appears as an icon in the system tray at the bottom right corner of screen whenever the card is operating *(see **Figure 3-1**)*. The icon displays signal strength (one green box = weak signal, 4 green boxes = strong signal) and double-clicking on it launches the utility.

Figure 3-1 Gigabyte Configuration & Monitor Utility Icon

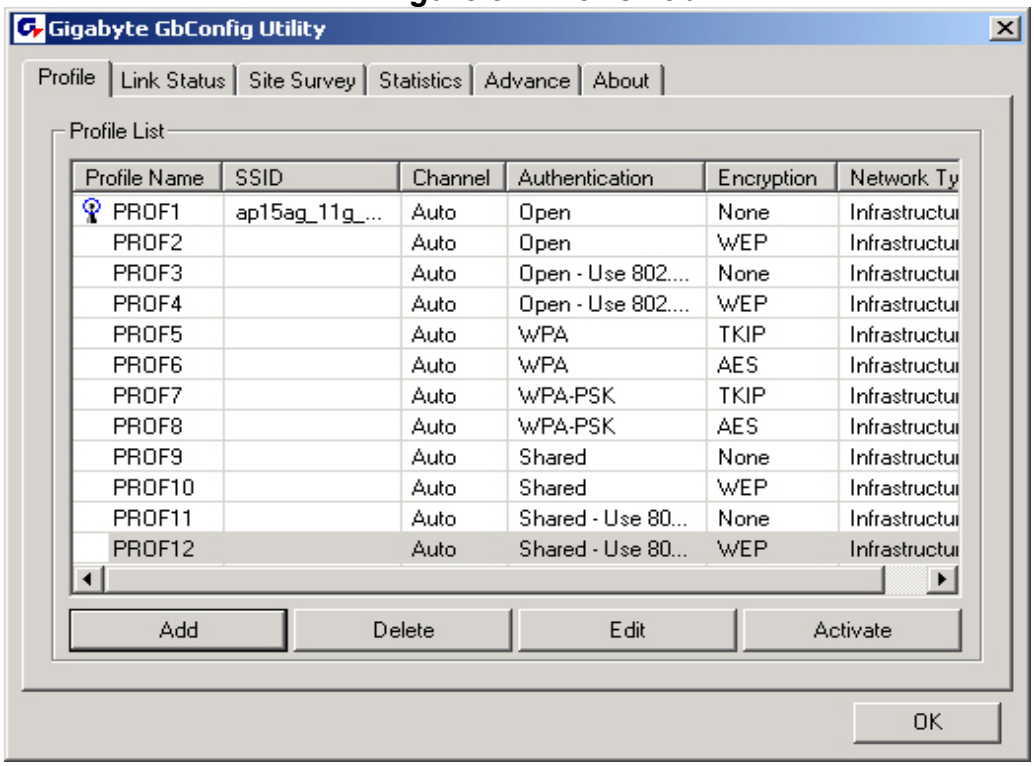
You may also open the Gigabyte WLAN Utility from the Windows **Start** menu, selecting **Programs** and then **Gigabyte WLAN Utility**.

Note: Modifications to WLAN configuration settings can be done when GN-WIKG is in use or through the network configuration tool provided by Windows® when it is inactive.

3-1. The Profile Tab

Click on the Profile tab in the Gigabyte WLAN Configuration Utility to view the values for each defined profile. Click the **Add** button to create a new profile (see section below for further details), the **Delete** button to delete a selected profile, the **Edit** button to modify a selected profile and click the **Activate** button to have a selected profile become active.

Figure 3-2 Profile Tab



Profile Name -
Name associated with specific wireless parameters and settings. The icon indicates the currently active profile.

SSID –
Displays the Service Set Identity (wireless network name) associated with active profile.

Channel –
Displays which channel the profile is operating on.

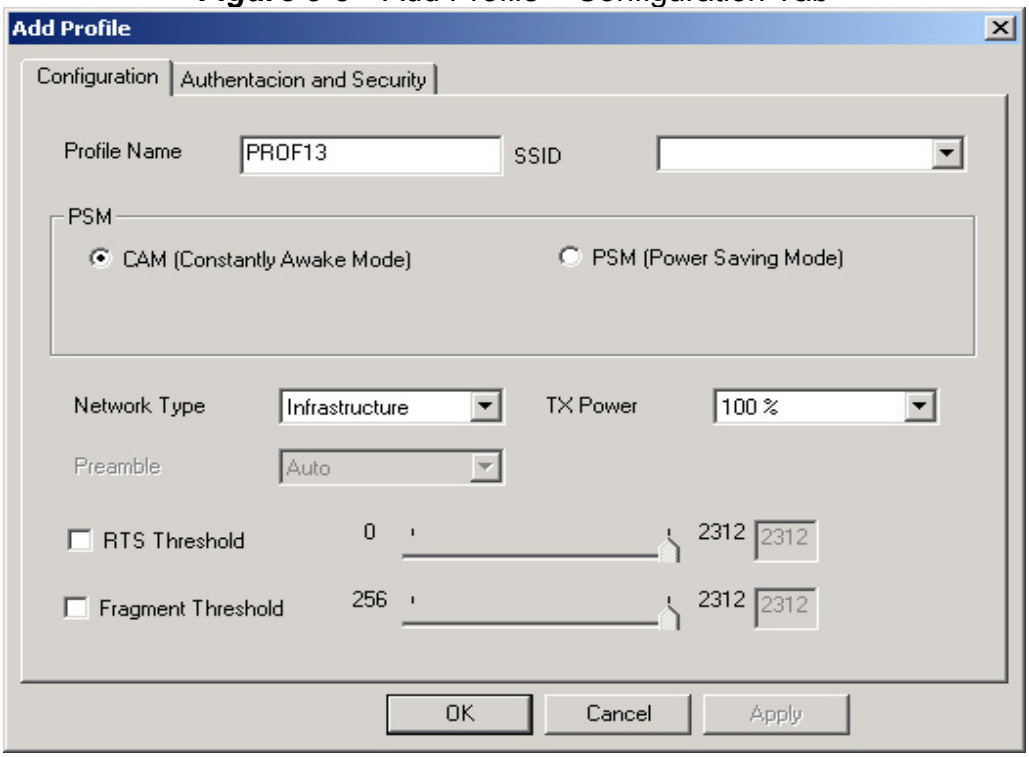
Authentication –
Displays authentication type associated with profile.

Encryption –
Four encryption types currently used in the profile include “None”, “WEP”, “AES” and “TKIP”.

Network Type –
Displays the wireless mode (Infrastructure or Ad-Hoc) associated with the profile.

3-1-1. Add Profile – Configuration Tab

Figure 3-3 Add Profile – Configuration Tab



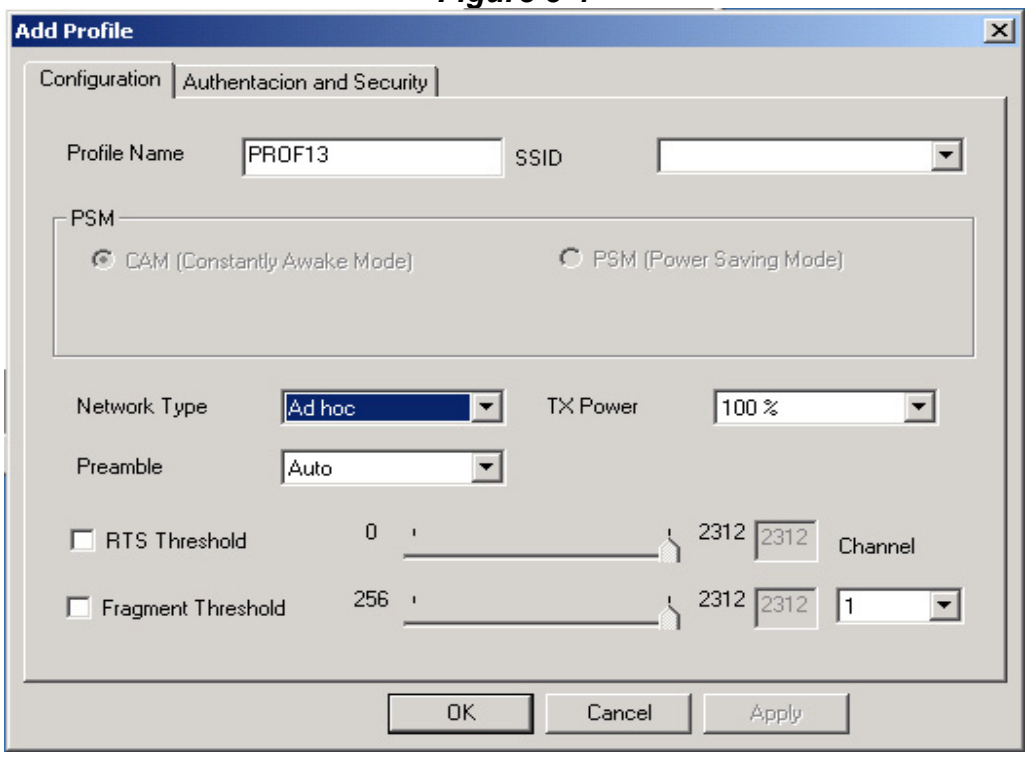
Profile Name –
Type in a unique profile name, set the corresponding parameters and click the **Apply** button to add profile.

SSID –
Select a defined Service Set Identity detected by the system from the drop-down list or input a new SSID (32-character maximum).

Power Saving Mode –
Select the PSM option to enable power saving feature (when no data will be transmitted) or the CAM option to have device always on.

Network Type –
Displays the current wireless mode (Infrastructure or Ad-Hoc) the Mini-PCI Adapter is operating in. Infrastructure is the most common and is used when connecting your PC to a wireless access point or wireless router. Ad-Hoc mode is used to connect to another computer without the use of a wireless access point or wireless router. In Ad-Hoc mode, the Preamble and Channel can be manually set *(see **Figure 3-4**)*.

Figure 3-4



TX Power –
Allows you to define the transmit power at various percentage levels with 100% being the default value.

RTS Threshold –
Define the packet size the wireless node uses to determine appropriate transmission mechanism.

Fragmentation Threshold –
Define the packet length used for fragmentation. Packets larger than value will be fragmented.

3-1-2. Add Profile - Authentication and Security

If an authentication or security setting is configured in a wireless access point or wireless router, it is necessary for the Wireless Mini-PCI Adapter profile to match the security parameters in order to obtain access and establish a connection. Both WEP Encryption and 802.1X Authentication protocols are supported.

Figure 3-5. Authentication and Security

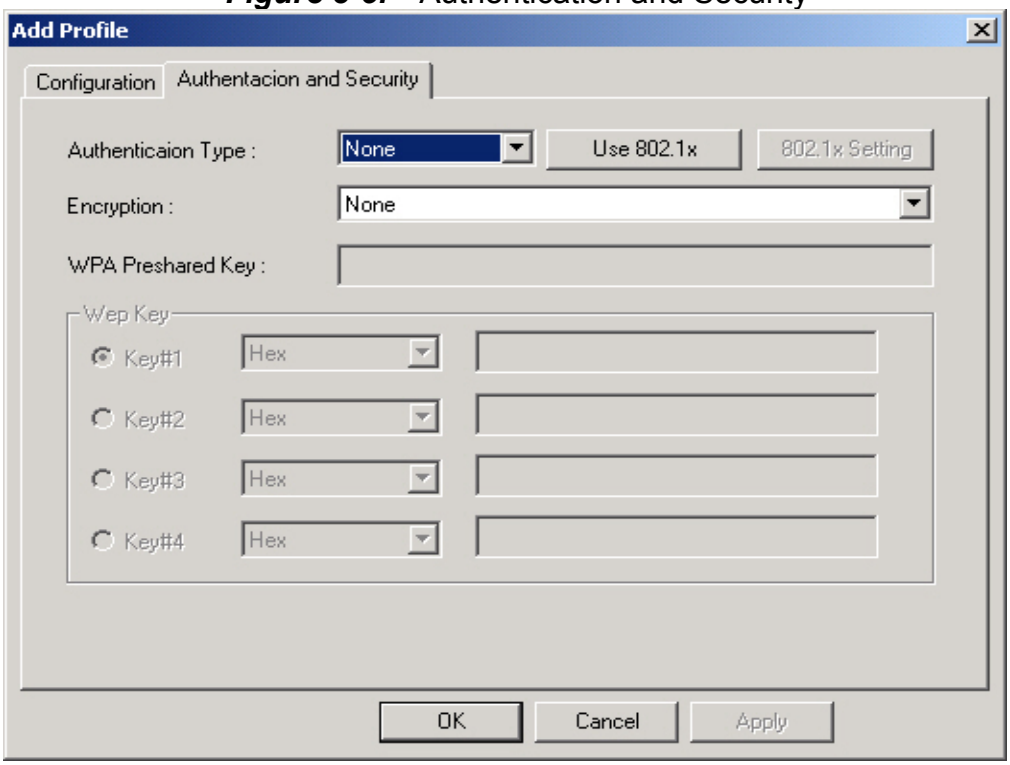


Table 3-1

Authentication Type	Security	Secure Key Setting	802.1X Enabled
None	None	None	YES
	WEP	Key Setting	
Shared	None	None	YES
	WEP	Key	
WPA	TKIP	None	YES
	AES	None	
WPA-PSK	TKIP	WPA-PSK Key	NO
	AES	WPA-PSK Key	

3-1-2-1. Authentication and Security

Authentication –
Before a station connects to a SSID, the authentication type used by the SSID must be known. Authentication types include OPEN SYSTEM, WAP, WAP-PSK and SHARED.

Security –
To prevent unauthorized access to data transmitted on the network, WLAN card provide a data encryption of high security. The access point must have the same password and encryption to connect with you. Different authentication types have different level of security. Please refer to ***Table 3-1***.

WEP Encryption –

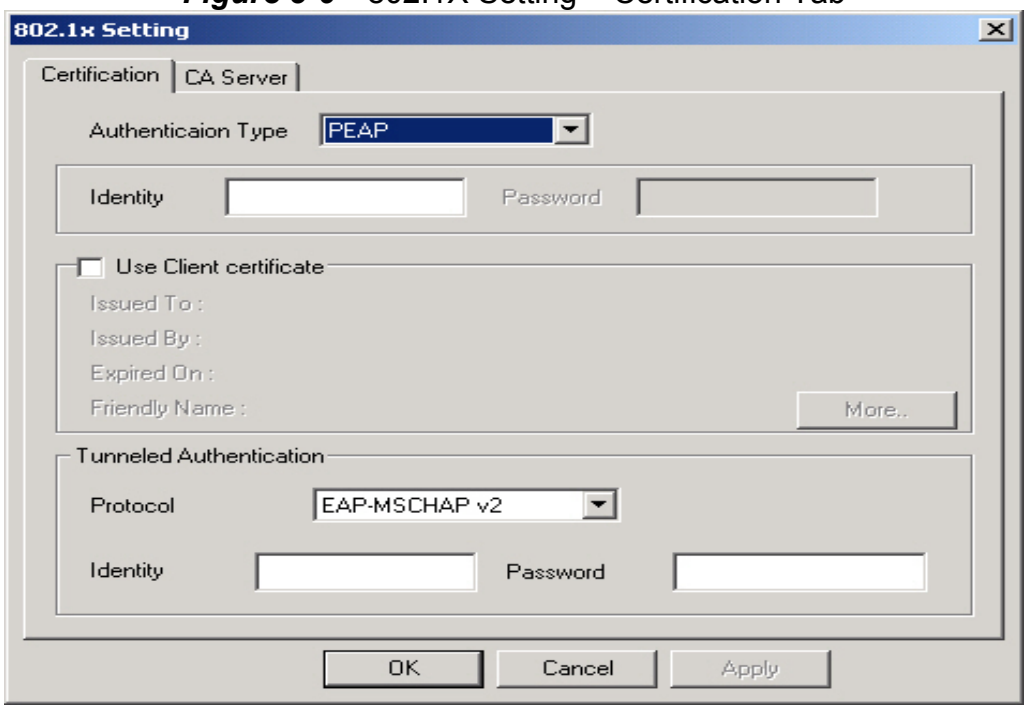
To activate the WEP Encryption, choose **WEP Encryption** from the drop-down menu in the Encryption field. Then follow instructions below:
1. Select a Key. (You may specify up to 4 Keys)
2. Select data type as either Hex or ASCII. (Hex = hexadecimal)
3. Enter a WEP key. [For 64-bit: 10 hexadecimal digits, 5 ASCII; For128-bit: 26 hexadecimal digits, 13 ASCII]
4. Click **OK** to save the settings.

WPA-PSK Encryption –
To activate WPA-PSK (Preshared Key) Encryption using TKIP or AES, choose WPA-PSK from the drop-down menu in the Encryption field. Then follow instructions below:
1. Enter a Preshared Key. [Key may be up to 64 hexadecimal digits or from 8 to 63 ASCII digits in length]
2. Click **OK** to save these settings.

3-1-2-2. 802.1X Setting

To enable 802.1X Authentication, click on the **Use 802.1x** button (see **Figure 3-5** above) and the **802.1X Setting** window will open. From the 802.1x Setting window you can configure authentication parameters such as Tunnel Protocol, ID and Password and Client Certificate or Certificate Chain.

Figure 3-6 802.1X Setting – Certification Tab



Authentication Type –
Choose authentication type from the drop-down menu. Authentication types supported include PEAP, TLS/Smart Card, TTLS, LEAP and MD5-Challenge.

Identity –
Enter the name of the user account.

Password –
The option to specify a password is only available when LEAP and MD5-Challenge are selected as the authentication types.

Use Client Certificate –
Check the **Use Client Certificate** box to confirm if the Client Certificate is correct in the authentication process. This applies only to TLS and TTLS authentication types.

Tunnel Authentication –
PEPA and TTLS use two-step authentication method. The first step is that Server sets up a Tunnel with its authentication. No option is need to be set for Station with WLAN card. The second step is to confirm the validity of Station with assigned authentication type in the Tunnel. Data needed for authentication includes Tunnel ID, Tunnel Password, Client Certificate or Server Authentication.

Protocol: Use assigned authentication type in the safe tunnel.

Tunnel Identity –
Enter name of user account.

Password –
Enter the user account password.

Figure 3-7. Client Certificate List

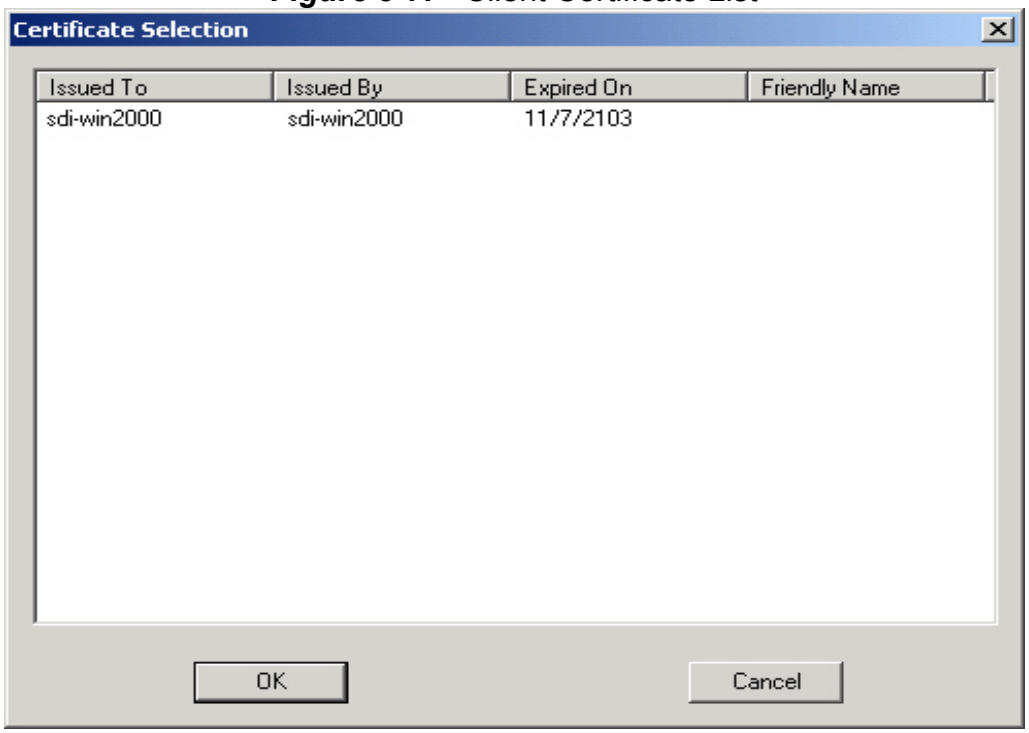
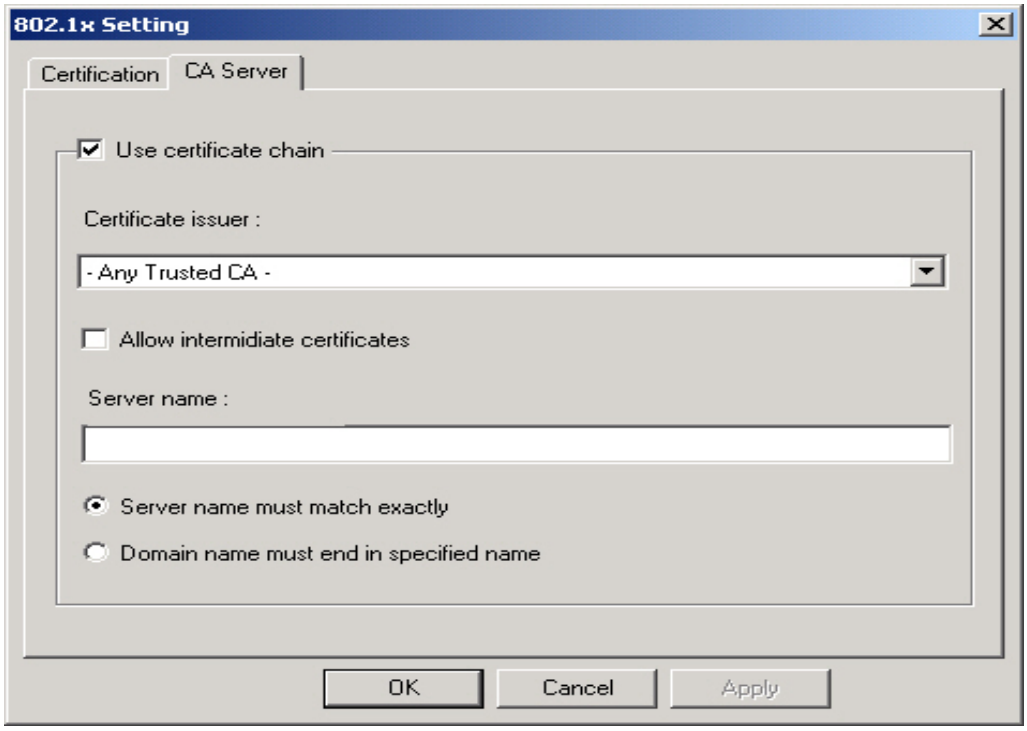


Figure 3-8. CA Server Setting



The CA Server is enabled only when TLS, TTLS or PEAP authentication is selected. The Client can verify if such server is reliable and then transmit Client Certificate after the verification is confirmed. (NOTE: Only available if **Use Client Certificate** is checked.)

Verify CA Server -

1. Confirm if the Server Certificate is issued by an assigned certificate issuer. If **Allow Intermediate Authentication** box is checked, the server certificate can be issued by one intermediate certificate issuer.

2. Check that the server name of server certificate matches the name entered by the user or belongs to the same domain.

Server Certificate –
Check the **Server Certificate** box to indicate that the Client will confirm whether the CA server is reliable.

Certificate issuer –
Specify the CA of a server certificate from the drop-down list.

Allow Intermediate Certificates –
When this option is checked, the certificate issuer can be an issuer recognized by a specific certificate issuer.

Server name –
This value can be a server name or the name of a domain where the server is located.

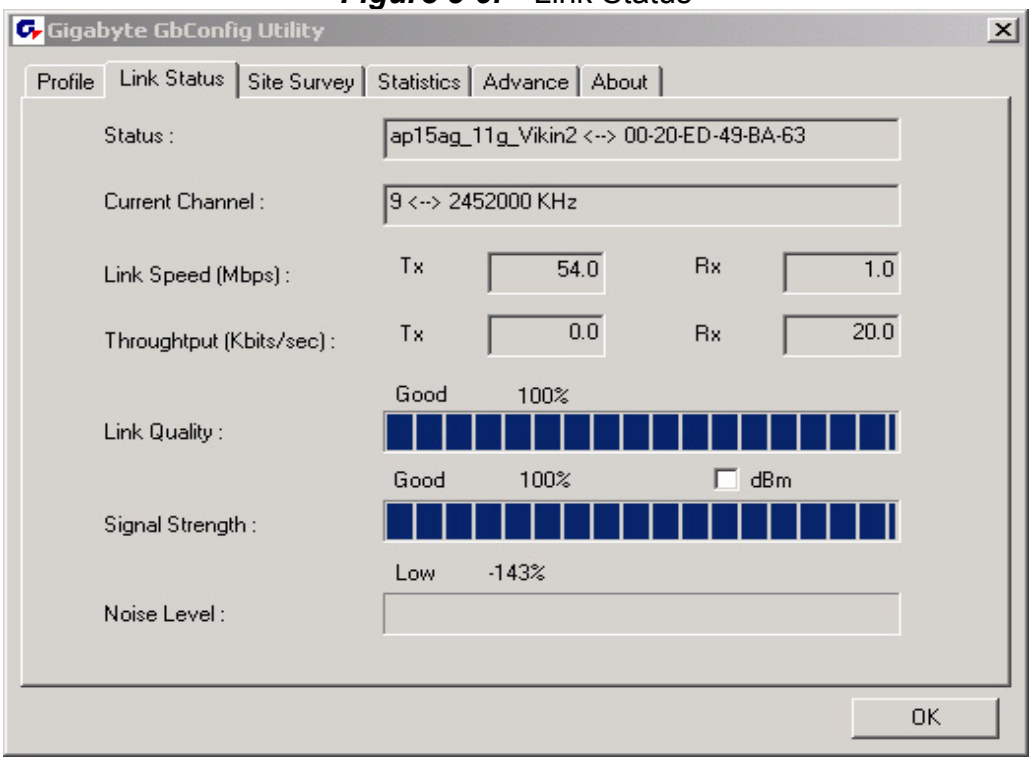
Server name must match exactly –
Select this option to specify that the server name of server certificate must be the same as **Server Name** or matches the name of domain where the server is located.

Domain name must end in specified name –
Select this option to specify that the certificate issuer must match the domain or secondary domain entered in **Server Name**.

3-2. The Link Status Tab

The **Link Status** tab displays information on the current wireless network connection.

Figure 3-9. Link Status



Status –
Displays the SSID and MAC address of the associated access point when GN-WIKG is configured in infrastructure mode.

Current Channel –
Displays the wireless channel currently in use ONLY when GN-WIKG is configured in Ad-Hoc mode.

Link Speed –
Indicates the transmission data rate between associated access point and the GN-WIKG

Throughput –
Indicates the number of successfully transmitted (Tx) and received (Rx) data (in bytes per second.

Link Quality –
Displays how well the GN-WIKG is communicating with wireless access point, wireless router or another wireless device.

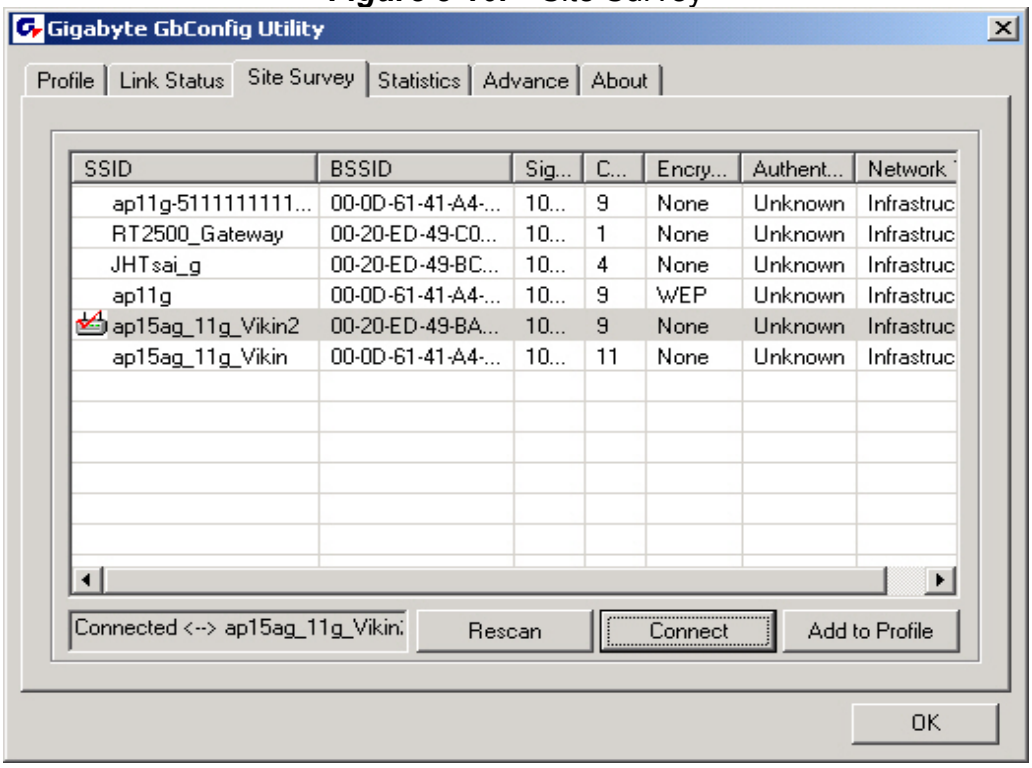
Signal Strength –
Displays the signal strength received by RF signal processor in dBm.

Noise Level –
Displays the noise level of connection.

3-3. The Site Survey Tab

The **Site Survey"** tab shows you the list of available access points and/or peer-to-peer stations. You can double click SSID that you want to connect or highlight the access point and click the **Connect** button.

Figure 3-10. Site Survey



BSSID –
Displays the MAC address of the access point.

Signal Strength –
Displays the access point signal strength.

Channel –
Displays the current broadcast channel used by the access point.

Encryption –
The security method used by the access point.

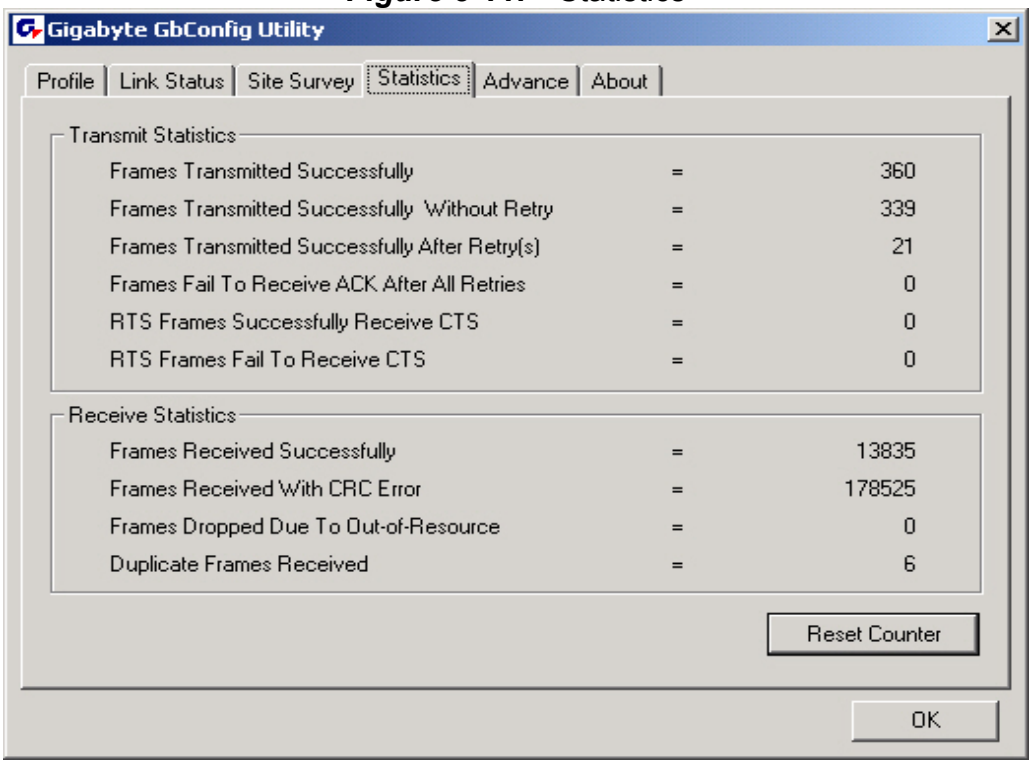
Authentication –
The authentication type used by the access point.

Network Type –
Informs you if an access point (infrastructure) or other wireless node (802.11 Ad Hoc) is connected.

3-4. "Statistics" Setting

The **Statistics** tab shows you the number of packets sent and received by the Wireless PCI Adapter.

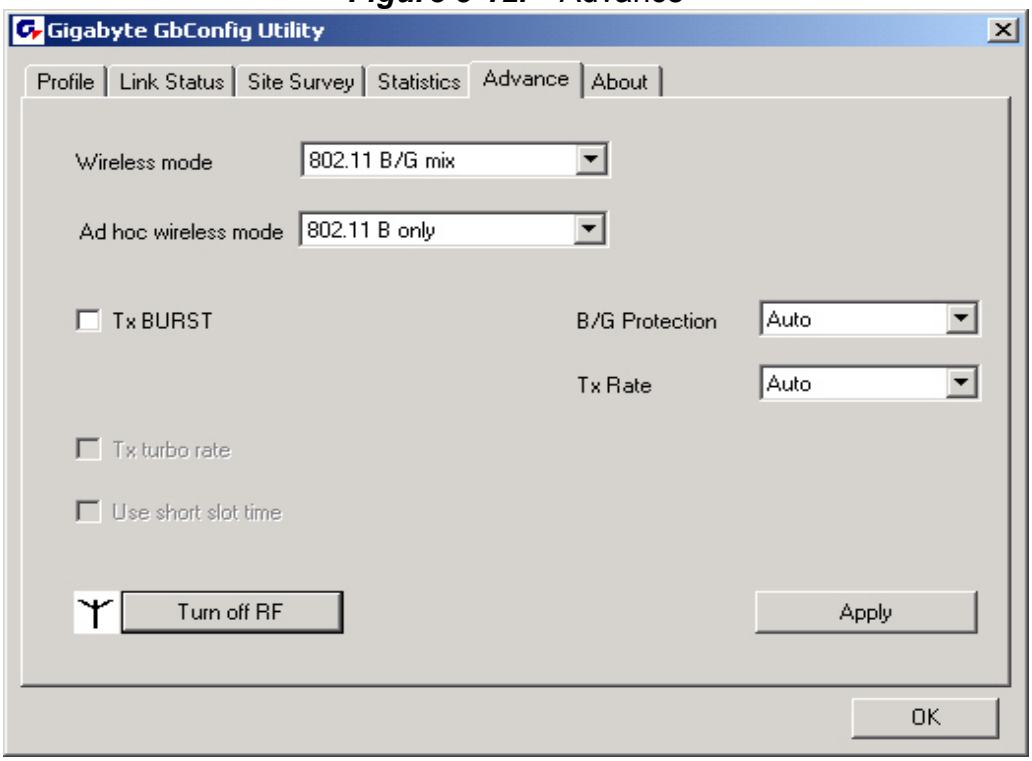
Figure 3-11. Statistics



3-5. The Advanced Tab

The **Advanced** tab includes fields of various parameters to review or change drivers. Just click “Apply” button to apply any parameter change to the driver in the tab. A reboot is not needed for the WLAN card *(see **Figure 3-12**)*

Figure 3-12. Advance



Wireless Mode: Sets infrastructure Protocols, including 802.11 B/G mix and 802.11 B Only.

Ad Hoc Wireless Mode: Sets Ad Hoc Wireless Protocols, including 802.11 B/G mix, 802.11 B Only and 802.11 G Only.

TX Burst: The longest interval between frames is normally one DIFS while frames are transmitted. When this setting is open, the longest interval between frames is one SIFS that means the system is allowed to transmit higher capacity of data in one interval.

B/G Protection: 802.11b uses CCK modulation. 802.11g uses OFDM while CCK modulation for 802.11b is compatible. To prevent data collision between two stations with 802.11b and 802.11g within range of the same Access Point, it is necessary to set 11B/G Protection. This setting only functions when 802.11 B/G mix is selected as Wireless Mode. Three setting are available: AUTO, EABLE and DISABLE.

This is a mechanism implemented to prevent the “Hidden Node” problem, “Hidden Note” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other and can not detect each other. This mechanism is a way to prevent data collision when WLAN equipments require transmission.

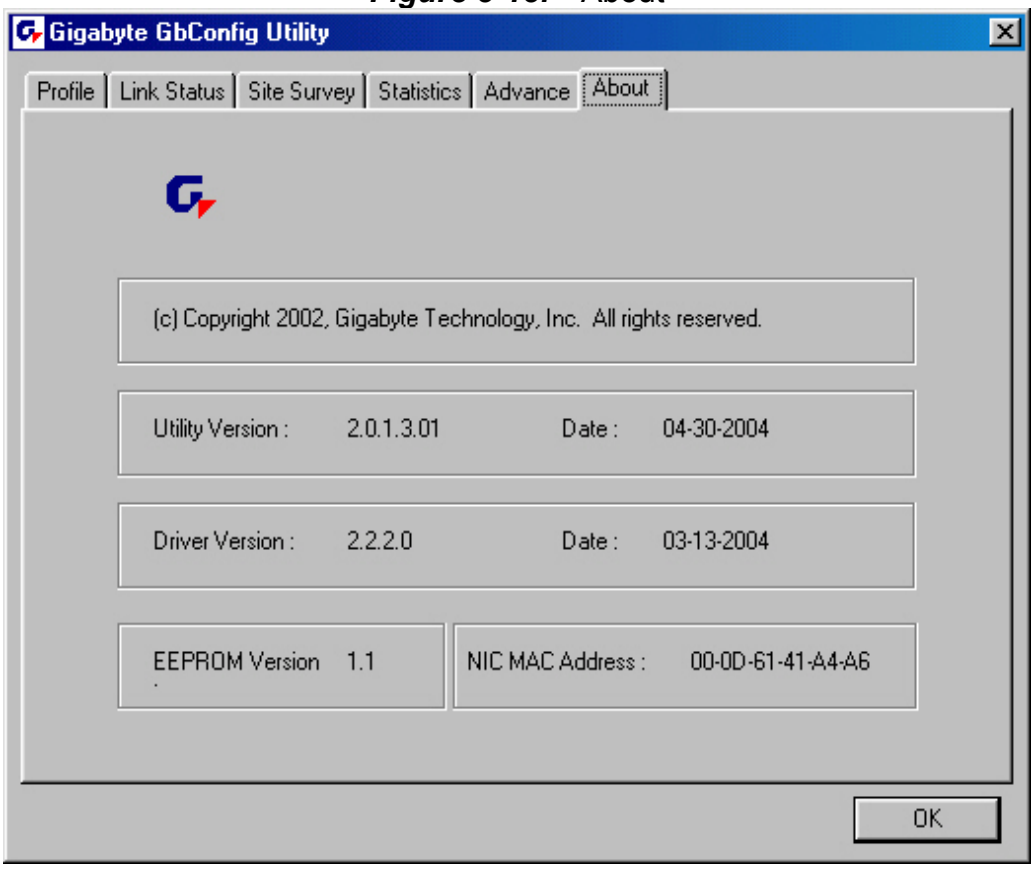
TX Rate: This option adjusts settings of TX Rate according to the setting of “Infrastructure Wireless Mode”.

Signal Control: To turn off transferring signals, click on **“Turn Off RF”** icon on the bottom right corner of the screen. Click **“Turn On RF”** to transfer signal again.
TX Turbo rate and Use short slot time: currently does not support.

3-6. The About Tab

The About tab displays information about current drivers and physical MAC address.

Figure 3-13. About



Chapter 4 Troubleshooting

This troubleshooting guide lists questions and possible solutions to some common problems which you may encounter while installing or using GIGABYTE Wireless Mini-PCI Adapter.

◆ Cannot Enable 802.1x, WPA or WPA-PSK

- Windows XP / 2000:

1. Run the **AegisI5.exe** file found on the GN-WIKG installation CD.
2. Click "**Install**".

- Windows 98SE / ME:

1. Run **AegisI2.exe** file found on the GN-WIKG installation CD.
2. Click "**Install**".

◆ Cannot Establish Connection to a Wireless Network

- Make sure the SSID for the Wireless Mini-PCI Adapter is the same as the wireless access point or wireless router.
- Make sure the security settings are the same as that of wireless access point / router. If WEP or WPA encryption is enabled, check if the WEP or WPA keys for the GN-WIKG match.
- Check that the MAC address of the Wireless Mini-PC Adapter is included in the access point/router's Authorization Table.

◆ Can Connect to an Access Point, but Cannot Access the Internet

- Make sure the security settings are the same as that of wireless access point / router. If WEP or WPA encryption is enabled, check if the WEP or WPA keys for the GN-WIKG match.
- Verify the network settings (IP address, subnet mask, gateway, and DNS) of your computer.
- Check that the proxy server of the WEB browser is correctly set.

◆ Poor Link Quality and Weak Signal Strength

- Keep the Wireless Mini-PCI Adapter away from microwave ovens and large metal objects to avoid radio interference.
- Locate the Wireless Mini-PC Adapter as near to the access point as possible.

Chapter 5 Hardware Specifications

1. System	
Host Interface	Mini-PCI Type III B
Operating Voltages	3.3V+-5%
2. RF Characteristics	
Frequency Bands	2412-2484 MHz (subject to local regulations)
Modulation Technology	OFDM and DSSS
Modulation Techniques	64QAM, 16QAM, QPSK, BPSK, CCK, DQPSK, DBPSK
Date Rates	54, 48, 36, 18,12, 9, 11, 6, 5.5, 2, and 1 Mbps, auto fallback
Typical Power	Receive:240 mA; Transmit:400 mA
Peak Output Power	Targeted at 20dBm @ Nominal Temp Range at antenna connector
Receive sensitivity	Targeted at -68dBm @54Mbps; -85dBm@11Mbps
Antenna connectors	Two antenna connectors for supporting antenna diversity
3.Safety Regulation and Operating Environment	
EMC certification	FCC Part 15 (USA)
Temperature Range	Operating: 0 ~ 55 deg C, Storing: -20 ~ 65 deg C
Humidity	10% ~ 90% Non-condensing
4. Software Support	
Driver	Windows 98SE/ME/2000/XP
Security	64/128 bit WEP; AES;802.1x client and WPA for Windows XP
Roaming	Seamless roaming among 802.11b/g access points.
Management Utility	Monitors the network situation.
5. Mechanical	
Dimensions	59mmx44mmx4mm
Weight	12± 1 g
Packaging	Packaging specially used by Gigabyte.

*This specification is subject to change without notice.