- 2. Select the profile to remove from the list of configuration profiles.
- 3. Click **Remove**.

4.3.3 Profile Auto Selection

- 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:
- 1. On the **Profile Management** tab, click **Order Profiles**.
- 2. The **Auto Profile Selection Management** window pops up, with a list of all created profiles in the **Available Profile** box.
- **3**. Highlight the profiles to add to Auto Profile selection, and then click **Add**. The profiles appear in the **Auto Selected Profiles** box.

Auto Profile Selection Management	? 🔀
Available Profiles:	Add
Auto Selected Profiles:	
	Move up
	Move down
	Remove
Ok	Cancel

- Ordering the auto selected profiles:
- 1. On the **Profile Management** tab, click **Order Profiles**.
- 2. Highlight a profile in the **Auto Selected Profiles** box.
- 3. Click **Move up** or **Move down** as appropriate.

Auto Profile Selection Management	? 🗙
Available Profiles:	Add
Auto Selected Profiles: NC53 WLAN	Move up Move down Remove
	Ok Cancel

- 4. Click OK.
- 5. Check the Auto Selected Profiles box.
- 6. Save the modified configuration file.
- 7. 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.
- *NOTE!* 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.

4.3.4 Switching Profiles

- 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 Activate.
- 4. 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.

4.4 Security

You may select WPA, WPA Passphrase, 802.1x, Pre-Shared Key or None.

4.4.1 Using EAP-TLS Security

To use **EAP-TLS** security in the Utility, access the **Security** tab in the **Profile Management** window.

- 1. On the Security tab, click **WPA/WPA2** or **802.1x**.
- 2. Select **EAP-TLS** from the drop-down menu.

Profile Management	? 🛛
General Security Advanced	
Set Security Options	
WPA/WPA2 WPA/WPA2 EAP Type:	EAP-TLS
○ WPA/WPA2 Passphrase	EAP-TLS EAP-TTLS
O 802.1x 802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)
Pre-Shared Key (Static WEP)	LEAP
◯ None	
Confirme	
Coninguie	Allow Association to Mixed Cells
	OK Cancel
Profile Management	? 🛛
Profile Management	28
Profile Management General Security Advanced	? 🗙
Profile Management General Security Advanced Set Security Options	
Profile Management General Security Advanced Set Security Options OWPA/WPA2 WPA/WPA2 EAP Type:	LEAP
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase	LEAP
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase WPA/WPA2 Passphrase 802.1x EAP Type:	LEAP EAP-TLS
Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase 802.1x EAP Type: Pre-Shared Key (Static WEP) Pre-Shared Key (Static WEP)	EAP-TLS
Security Advanced General Security Advanced Set Security WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: Pre-Shared Key (Static WEP) None	EAP-TLS
Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase 802.1x EAP Type: Pre-Shared Key (Static WEP) None	EAP-TLS EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP
Security Advanced General Security Advanced Set Security O WPA/WPA2 WPA/WPA2 WPA/WPA2 EAP Type: O WPA/WPA2 Passphrase Image: Security Image: Security Image: Security Options Image: Security Options Image: WPA/WPA2 WPA/WPA2 EAP Type: Image: Security Image: Security	EAP-TLS EAP-TLS EAP-TTLS EAP-TTLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells
Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase WPA/WPA2 Passphrase None None Configure Configure	EAP-TLS EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells
Security Advanced General Security Advanced Set Security WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Solar EAP Type: Pre-Shared Key (Static WEP) None Configure Configure	EAP-TLS EAP-TLS EAP-TTLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase Image: Set Security Options Image: WPA/WPA2 Passphrase Image: Set Security Options Image: WPA/WPA2 Passphrase Image: Set Security Options Image: Set Security Options Image: WPA/WPA2 Passphrase Image: Set Security Options Image: Set Security Options	EAP-TLS EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells

4.4.2 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.

1. Click Configure.

Define	e Certificate		? 🛛
	Select a Certificate		
	aga [Issued: 2004/9/24]	~	
	Server Properties		
	<any></any>	×	
	Server/Domain Name		
	JR32.com		
	Login Name		
	aga		
		Ok Cancel]

- 2. Select the appropriate certificate authority. Select Server Properties. The Server/Domain Name and the Login Name are filled in automatically from the certificate information.
- 3. Click OK again.
- 4. Activate the profile.

4.4.3 Using EAP-TTLS Security

To use **EAP-TTLS** security in the WLAN 802.11a/b/g Utility, access the **Security** tab in the **Profile Management** window.

- 1. On the Security tab, click **WPA/WPA2** or **802.1x**.
- 2. Select **EAP-TTLS** from the drop-down menu.

Profile Management	? 🗙
General Security Advanced	
Set Security Options	
WPA/WPA2 WPA/WPA2 EAP Type:	EAP-TTLS 👻
O WPA/WPA2 Passphrase	EAP-TLS EAP-TTLS
○ 802.1x 802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)
Pre-Shared Key (Static WEP)	
◯ None	
Configure	Allow Association to Mixed Cells
Profile Management	2
Profile Management General Security Advanced	? 🛛
Profile Management General Security Advanced	
Profile Management General Security Advanced Set Security Options	? X
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type:	
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase	LEAP
Security Advanced Set Security Options Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase WPA/WPA2 Passphrase WPA/WPA2 Passphrase WPA/WPA2 Passphrase	LEAP EAP-TTLS
Set Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Sold 1x EAP Type: Pre-Shared Key (Static WEP) Image: Constraint of the second s	EAP-TILS EAP-TILS EAP-TILS EAP-TILS PEAP (FAP-GIC)
Security Advanced General Security Advanced VPA/WPA2 WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Sold 1x B02.1x 802.1x EAP Type: Pre-Shared Key (Static WEP) None	EAP-TTLS EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) IFAP
Set Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase WPA/WPA2 Passphrase OPre-Shared Key (Static WEP) None Configure Configure	EAP-TTLS EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells
Security Advanced General Security Advanced Set Security WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 WPA/WPA2 EAP Type: Pre-Shared Key (Static WEP) None Configure Configure	EAP-TTLS EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells
Set Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase 0 802.1x 802.1x 802.1x EAP Type: 0 Pre-Shared Key (Static WEP) 0 None Configure Configure	EAP-TTLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase 0 802.1x 802.1x EAP Type: 0 Pre-Shared Key (Static WEP) None Configure	EAP-TTLS EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells

4.4.4 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.

1. Click Configure.

Define EAP-TTLS Configura	tion	? 🗙
Trusted Root Certification A	uthorities	
<any></any>		~
User Information for EAP-	TTLS Authentication	- 1
User Name: C	0200	
Password:		
Confirm Password:		
		-
	Advanced OK C	ancel

- 2. Select the appropriate certificate from the drop-down list and click **OK**.
- 3. Specify a user name for EAP authentication:
 - ✓ Enter an EAP user name in the User Name field to use a separate user name and password and start the EAP authentication process.
- 4. Click **Advanced** and:

Advanced Configuration		?×
Specific Server or Domain: Login Name:	0200	
	OK Cancel	

- ✓ Enter the Specific Server or Domain name of the server from which the client will accept a certificate.
- \checkmark Change the login name if needed.
- 5. Click OK.

6. Enable the profile.

4.4.5 Using PEAP(EAP-GTC) Security

To use **PEAP-GTC** security in the WLAN 802.11a/b/g Utility, access the **Security** tab in the **Profile Management** window.

- 1. On the Security tab, click **WPA/WPA2** or **802.1x**.
- 2. Select **PEAP(EAP-GTC)** from the drop-down menu.

		2
General Security Advanced		
Set Security Options WPA/WPA2 WPA/WPA2 Passphrase 802.1x Pre-Shared Key (Static W None Configure	WPA/WPA2 EAP Type: 802.1x EAP Type: /EP)	PEAP (EAP-GTC)
Profile Management		OK Cancel
Lieneral Security Advanced		
Set Security Options WPA/WPA2 WPA/WPA2 Passphrase	WPA/WPA2 EAP Type:	LEAP
Set Security Options WPA/WPA2 WPA/WPA2 Passphrase 0 802.1x Pre-Shared Key (Static W None Configure	WPA/WPA2 EAP Type: 802:1x EAP Type: /EP)	LEAP PEAP (EAP-GTC) EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells

4.4.6 Enabling PEAP(EAP-GTC) Security

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

- 1. Click Configure.
- 2. Select the appropriate network certificate authority from the drop-down list.

<any></any>		~
User Name:	0200	
Set Passw	ord	
🔵 Tok	en	
💽 Stat	ic Password	

- 3. Specify a user name for inner PEAP tunnel authentication:
 - ✓ Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
- 4. Select **Token** or **Static Password**, depending on the user database.

NOTE! 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.

5. Click Advanced and:

Advanced Configuration		? 🛛
Specific Server or Domain: Login Name:	PEAP-00037F056001	
	DK Cancel	

 ✓ Enter the Specific Server or Domain name of the server from which the client will accept a certificate.

- ✓ The login name used for PEAP tunnel authentication, fills in automatically as PEAP-XXXXXXXXX, where XXXXXXXXX is the computer's MAC address. Change the login name if needed.
- 6. Click **OK**.
- 7. Enable the profile.

4.4.7 Using PEAP-MSCHAP V2 Security

To use **PEAP-MSCHAP V2** security in the WLAN 802.11a/b/g Utility, access the **Security** tab in the **Profile Management** window.

- 1. On the Security tab, click **WPA/WPA2** or **802.1x**.
- 2. Select **PEAP- MSCHAP V2** from the drop-down menu.

Profile Management	? 🛛
General Security Advanced	
CSet Security Options	
	E PEAP (EAP-MSCHAP V2)
	EAP-TLS
	PEAP (EAP-GTC)
◯ 802.1x 802.1x E AP T	E PEAP (EAP-MSCHAP V2)
Pre-Shared Key (Static WEP)	
◯ None	
Configure	Allow Association to Mixed Cells
	Allow Association to mixed colo
	OK Cancel
Drefile Management	
Profile Management	?×
Profile Management General Security Advanced	? 🗙
General Security Advanced	? 🗙
Profile Management General Security Advanced Set Security Options	? X
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type	2. LEAP
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 Passphrase	2. LEAP
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 Passphrase WPA/WPA2 Passphrase R02 1x EAP Type R02 1x EA	? ▼ * LEAP * PEAP (EAP-MSCHAP V2) ▼
Security Advanced General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 Security EAP Type Security Security Charles Security Security Charles Security Security Charles	
Set Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type Pre-Shared Key (Static WEP) WPA/WPA2	EAP-TLS EAP-ICS EAP-ICS EAP-TLS PEAP (EAP-GTC)
Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type Pre-Shared Key (Static WEP) None	
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 Passphrase Set Security Options WPA/WPA2 Passphrase Set Security Options WPA/WPA2 Passphrase None Configure	
General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type Pre-Shared Key (Static WEP) None Configure Configure	
General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 Passphrase 802.1x 802.1x EAP Type Pre-Shared Key (Static WEP) None Configure	
General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 Passphrase 9 802.1x Pre-Shared Key (Static WEP) None Configure	EAP (EAP-MSCHAP V2) EAP-TLS EAP-TLS PEAP (EAP-MSCHAP V2) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells
General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type WPA/WPA2 WPA/WPA2 EAP Type Pre-Shared Key (Static WEP) None Configure Configure	EAP-TLS EAP-TLS PEAP (EAP-MSCHAP V2) EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells

4.4.8 Enabling PEAP- MSCHAP V2 Security

To use PEAP-MSCHAP V2 security, the server must have the PEAP-MSCHAP V2 certificates, and the server properties must already be set. Check with the IT manager.

- 1. Click Configure.
- 2. Select the appropriate network certificate authority from the drop-down list.

rusted Root Certification	n Authorities	
<any></any>		
User Information for PE	AP (EAP-MSCHAP V2) Authentication	
User Name:	0200	
Password:		
Password: Confirm Password:		

- 3. Specify a user name for inner PEAP tunnel authentication:
 - Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
- 4. Click Advanced and:

Advanced Configuration		? 🔀
Specific Server or Domain: Login Name:	0200	
	JK Cancel	

- ✓ Enter the Specific Server or Domain name of the server from which the client will accept a certificate.
- \checkmark Change the login name if needed.
- 5. Click OK.
- 6. Enable the profile.

4.4.9 Using LEAP Security

To use **LEAP** security in the WLAN 802.11a/b/g Utility, access the **Security** tab in the **Profile Management** window.

- 1. On the Security tab, click **WPA/WPA2** or **802.1x**.
- 2. Select **LEAP** from the drop-down menu.

Profile Management		?	×
General Security Advanced			
Set Security Options • WPA/WPA2 • WPA/WPA2 Passpl • 802.1x • Pre-Shared Key (Sta • None Configure	WPA/WPA2 EAP Type: nrase 802.1x EAP Type: tic WEP)	LEAP EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP	
		OK Cancel	
Profile Management		?	×
Profile Management General Security Advanced		?	
Profile Management General Security Advanced Set Security Options		?	
Profile Management General Security Advanced Set Security Options WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 Passpl	WPA/WPA2 EAP Type: trase	LEAP	
Profile Management General Security Advanced Set Security Options WPA/WPA2 WPA/WPA2 Passpl 0 802.1x Pre-Shared Key (Sta None Configure	WPA/WPA2 EAP Type: wase 802.1x EAP Type: ttic WEP)	LEAP EAP-TLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP Allow Association to Mixed Cells	×

4.4.10 Configuring LEAP

- 1. Click Configure.
- 2. Specify a user name and password:

LEAP Settings	? 🛛
LEAP username and passwo	rd settings
Use Temporary Use	r Name and Password
O Manually F	Prompt for LEAP User Name and Password
OUse Saved User Nar	ne and Password
User Name:	
Password:	
Confirm Password:	
Domain:	
✓ Include W ✓ No Netwo LEAP Authen	indows Logon Domain with User Name rk Connection Unless User Is Logged In tication Timeout Value (in seconds) OK Cancel



- (1) Manually Prompt for Leap User Name and Password is checked automatically.
- **Option 2:** Select to **Use Saved User Name and Password** by choosing the radio button:
 - (1) Enter the user name and password.
 - (2) Confirm the password.
 - (3) Enter a specific domain name.
- 3. Check the **Include Windows Logon Domain with User Name** setting to pass the Windows login domain and user name to the RADIUS server (default).
- 4. Check **No Network Connection Unless User Is Logged In** to force the wireless adapter to disassociate after logging off (default).
- 5. 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.
- 6. Click **OK**.

7. Enable the profile.

4.4.11 Using WPA Passphrase Security

To use **WEAP Passphrase** security in the WLAN 802.11a/b/g Utility, access the **Security** tab in the **Profile Management** window.

Profile Management	? 🗙
General Security Advanced	
Set Security Options	
O WPA/WPA2 WPA/WPA2 EAP Type: LEAP ✓	
WPA/WPA2 Passphrase	
○ 802.1x 802.1x EAP Type: LEAP	
O Pre-Shared Key (Static WEP)	
◯ None	
Configure Allow Association to Mixed Cells	
OK L	Cancel

- 1. On the Security tab, click **WPA/WPA2 Passphrase**.
- 2. Click Configure.
- 3. Fill in the WPA Passphrase.

Define WPA Pre-Shared Key		? 🛛
Enter a WPA Passphrase between 8 and 64 characters long	ı.	
	ОК	Cancel

4. Click OK.

4.4.12 Using Pre-Shared Key (Static WEP) Security

To use **Pre-Shared Key (Static Web)** security in the WLAN 802.11a/b/g Utility, access the **Security** tab in the **Profile Management** window.

Profile Management		?×
General Security Advanced		
Set Security Options WPA/WPA2 WPA/WPA2 EAP Type: WPA/WPA2 Passphrase	LEAP	
802.1x 802.1x EAP Type: Pre-Shared Key (Static WEP)	LEAP	
Configure	Allow Association to Mixed Cells	
	ок с.	ancel

- 1. On the Security tab, click **Pre-Shared Key** (Static WEP).
- 2. Click Configure.
- 3. Choose Hexadecimal or ASCII Text and then fill in the value of each WEP Key.

0	Hexadecimal (0-9, A-F)	ASCII Text (all keyboard characters)
Encryption Keys		
Tran K	smit ev	WEP Key Size:
WEP Key 1: 🧕		● 0 0
WEP Key 2:		
WEP Key 3:		000
WEP Key 4:		000

4.5 Display Setting

To change the display settings, choose $\underline{Options} \rightarrow \underline{Display Settings}$ from the menu. The Display Settings dialog box contains tools to set the Signal Strength Display Units, Refresh Interval and Data Display.

Display Settings	? 🛛
Signal Strength Display Units:	O% ⊙dBm
Refresh Interval (seconds):	3 📚
Data Display:	○ Relative ⊙ Cumulative
	OK Cancel

- Signal Strength Display Units: Sets the units used when displaying signal strength: percentage (%) or dBm.
- Refresh Interval: Use the up/down arrows to set the display refresh interval in seconds.
- Data Display: Sets the display to cumulative or relative. Relative displays the change in statistical data since the last update. Cumulative displays statistical data collected since opening the profile.

4.6 Actions Tools

Click **Action** from the menu to access the tools.

- **Enable/Disable Radio:** Enable or disable the RF Signal.
- Enable/Disable Tray Icon: Enable or disable the tray icon.



- Manual LEAP Login: Log in to LEAP manually, if LEAP is set to manually prompt for user name and password on each login. See Chapter 4 Security for enabling LEAP.
- **Reauthenticate:** Reauthenticate to a LEAP-configured access point.
- **Exit:** Exit the Utility application.

5. Right clicking the tray icon

Right-click on the tray icon to access the following options:

Show Connection Status	
Select Profile	۲
Reauthenticate	
Manual LEAP Login	
Disable Radio	
Preferences	
Open Adapter Utility	
Help Exit	

- **Help:** Open the online help.
- **Exit:** Exit the Utility application.
- **Open Adapter Utility:** Launch the Utility.
- Preferences: Set the startup options and menu options for the Utility. 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. See Chapter 4 Security for enabling LEAP.
- **Reauthenticate:** Reauthenticate to a LEAP-configured access point.
- Select Profile: Click a configuration profile name to switch to it. If no configuration profile exists for a connection, see Chapter 3 Profile Management to add a profile first.
- **Show Connection Status:** Display the Connection Status window.

Connection Status		
Active Profile: Auto Profile Selection: Connection Status: Link Quality:	Default Disabled Associated Good	Total 802.11
SSID: Access Point Name: Access Point IP Address: Link Speed:	wlan Unavailable Unavailable 1.0 Mbps	
Client Adapter IP Address:	169.254.54.161	OK

6. Network Application

This section consists of the network applications of 802.11a/b/g USB 2.0 Adapter, including:

- 1. To survey the network neighborhood
- 2. To share your folder with your network member(s)
- 3. To share your printer with your network member(s)
- 4. To access the shared folder(s)/file(s) of your network members(s)
- 5. To use the shared printer(s) of your network member(s)

In fact, the network applications of WLAN 802.11a/b/g USB 2.0 Adapter are the same as they are in a wired network environment. You may refer to the following 3 examples of Surveying the Network Neighborhood, File Sharing and Using the Shared Folder.

6.1 Surveying the Network Neighborhood

When multiple base stations are up and running in your wireless network, you can use the procedure described below to display the other computers:

- 1. **Double-click My Network Places** to display all stations in your Microsoft Windows Network Group.
- 2. To display other workgroups in the network environment, **double-click Entire Network**.
- 3. If there is a **second network operating system** running in your network environment (for example a Novell NetWare network), the "Entire Network" window will also display available servers running under the second network operating system. If you click on these servers, you may be asked to **enter your user name and password** that applies to the other network operating system. If you cannot find it, verify whether the other wireless computers are:
 - Powered up and logged on to the network.
 - Configured to operate with identical Microsoft Network settings concerning:
 - ✓ Networking Protocol.
 - ✓ Wireless Network Name.

To enable the sharing of **Internet access**, you should set your WLAN mode as **"Infrastructure"** and connect to the access point.

6.2 File Sharing

802.11a/b/g USB 2.0 Adapter allows the sharing of files between computers that are logged onto the same wireless network. If you want to share your folder "My Documents" with other computers of the wireless network, please **highlight the folder "My Documents" and drag it to Shared Documents folder**.





Sharing files in the IEEE802.11a/b/g wireless network will be like sharing files on a wired LAN.

6.3 Using the Shared Folder

If you would like to access a shared folder stored in other stations of same network, please follow the process below:

- 1. Double-click the "My Network Places" icon, and then double-click the computer where the shared folder is located.
- 2. Double-click the folder you want to connect to.
- 3. Now you may open the needed file(s).
- **NOTE!** If a password is required, the Windows will prompt a password column to you. Then you need to enter the password that had been assigned to this shared folder.