

Atheros Client Utility Help

Model AR5BMB6 (802.11a/b/g radio)

PRELIMINARY



ATHEROS[®]
COMMUNICATIONS

PRELIMINARY

Introduction

- System Requirements

Profile Management

- Create or Modify a Profile
- Remove a Profile
- Profile Auto Selection
- Switch Profiles
- Configure TCP/IP
- Configuring Win XP

Security

- EAP-TLS
- EAP-TTLS
- PEAP (EAP-GTC)
- PEAP (EAP-MSCHAP V2)
- LEAP
- WPA Passphrase

Check Status or Diagnostics

- Check Current Status
- Check Driver Information
- Check Statistics

Connect to Another Network

Settings

- Signal Strength Display
- Data Display
- Display Refresh Interval

Tools

- Tray Icon
- Troubleshooting Utility
- Enable/ Disable the Radio

Compliance

Introduction

The Atheros Client Utility (ACU) is a user-mode utility designed to edit and add configuration profiles, as well as display diagnostics pertaining to a selected Atheros network interface card (wireless adapter).

System Requirements

- Laptop/ PC containing:
 - 32-bit CardBus slot (or Desktop PC with PC Card-PCI adapter)
 - Mini PCI
 - 32 MB memory or greater
 - 300 MHz processor or higher

Microsoft Windows 2000, Windows Millennium Edition, Windows 98 Second Edition, Windows XP, or Windows NT 4.0 (with Service Pack 6)

Profile Management

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

- [Add a profile](#)
- [Edit a profile](#)
- [Import a Profile](#)
- [Export a Profile](#)
- [Order profiles](#)
- [Switch to a different profile](#)
- [Remove a profile](#)
- [Connect to a Different Network](#)

The wireless network adapter works in either [infrastructure mode](#) (which uses an access point) or [ad hoc mode](#) (a group of stations participating in the wireless LAN).

Create or Modify a Configuration Profile

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

The Profile Management dialog box displays the [General tab](#).

Profile Management:

- [Edit the General tab](#).
- [Edit the Security tab](#).
- [Edit the Advanced tab](#).

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

Remove a Configuration Profile

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

Auto Profile Selection Management

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 the [Order Profiles](#) button.
2. The Auto Profile Selection Management window appears, with a list of all created profiles in the [Available Profiles](#) box.
3. Highlight the profiles to add to auto profile selection, then click [Add](#). The profiles appear in the [Auto Selected Profiles](#) box.

Ordering the auto selected profiles:

1. Highlight a profile in the [Auto Selected Profiles](#) box.
2. Click [Move Up](#) or [Move Down](#) as appropriate.

The first profile in the Auto Selected Profiles box has highest priority, and the last profile has lowest priority.

3. Click [OK](#).
4. Check the [Auto Select Profiles](#) box.
5. Save the modified configuration file.

When auto profile selection is enabled by checking [Auto Select Profiles](#) on the Profile Management tab, the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID, and so on.

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

Switching to a different configuration profile

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

The Profile List provides icons that specify the operational state for that profile. The list also provides icons that specify the [signal strength](#) for that profile.

See also [Scan Available Networks](#).

Import and Export Profiles

Importing a Profile

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

Exporting a Profile

1. From the [Profile Management](#) tab, highlight the profile to export.
2. Click the [Export](#) button. The Export Profile window appears.
3. Browse to the directory to export the profile to.
4. Click [Save](#). The profile is exported to the specified location.

TCP/IP Configuration

Configuring the TCP/IP Address for the network device:

1. After configuring the wireless network adapter properties, open the Control Panel and open [Network and Dial-up Connections](#).
2. Find the Local Area Connection associated with the wireless network adapter. Right-click that connection, and click [Properties](#).
3. Select [Internet Protocol \(TCP/IP\)](#) and click [Properties](#).
4. Click the radio button [Use the following IP address](#), then enter an IP address and Subnet mask. Assigning an IP address and Subnet mask allows stations to operate in [access point mode](#) (infrastructure mode) or in [ad hoc mode](#) and to have Internet access. Default gateway and DNS server information is also required.

IP configuration information (DHCP to assign the IP address, gateway and DNS server IP addresses) is usually obtained from the corporate IT staff.

5. Click [OK](#) to finish.

General Tab

In the Atheros Client Utility, access the General tab by clicking [New](#) or [Modify](#) on the Profile Management tab.

Edit the fields in the General tab to configure the configuration profile. Make sure to also edit the [Security](#) and [Advanced](#) tabs.

Profile Name	Identifies the configuration profile. This name must be unique. Profile names are not case sensitive.
Client Name	Identifies the client machine.
Network Names (SSIDs)	The IEEE 802.11 wireless network name. This field has a maximum limit of 32 characters. Configure up to three SSIDs (SSID1, SSID2, and SSID3).

See also:

- [Configure a Profile for Ad Hoc Mode](#)
- [Configure a Profile for Access Point \(Infrastructure\) Mode](#)

Advanced Tab

In the Atheros Client Utility, access the Advanced tab by clicking [New](#) or [Modify](#) on the Profile Management tab, then clicking the Advanced tab in Profile Management. Edit the Advanced tab of Profile Management to configure the profile. Also edit the [General](#) and [Security](#) tabs.

Transmit Power Level	Selects the transmit power level for 80211b/g or 802.11a in mW. Actual transmit power may be limited by regulatory domain or hardware limitations.
Power Save Mode	Specify: <ul style="list-style-type: none"> • Maximum mode causes the access point to buffer incoming messages for the wireless adapter. The adapter up periodically polls the access point to see if any messages are waiting. • Normal uses maximum when retrieving a large number of packets, then switches back to power save mode after retrieving the packets. • Off turns power saving off, thus powering up the wireless adapter continuously for a short message response time.
Network Type	Specifies the network as either infrastructure (access point mode) or ad hoc .
802.11b Preamble	Specifies the preamble setting in 802.11b. The default setting is Short & Long (AP mode), which allows both short and long headers in the 802.11b frames. The adapter can only use short radio headers if the access point supports and uses them. Set to Long Only to override allowing short frames.
Wireless Mode	Specifies 5GHz 54 Mbps, 2.4 GHz 54 Mbps, 2.4 GHz 11 Mbps, or Super A/G operation in an access point network. The wireless adapter must match the wireless mode of the access point it associates to.
Wireless Mode when Starting an Ad Hoc Network	Specifies 5GHz 54 Mbps, 5GHz 108 Mbps, or 2.4 GHz 54/11 Mbps to start an ad hoc network if no matching network name is found after scanning all available modes. This mode also allows selection of the channel the wireless adapter uses. The channels available depend on the regulatory domain. If the adapter finds no other ad hoc adapters, this selection specifies the which channel with the adapter starts the ad hoc network with. The wireless adapter must match the wireless mode and channel of the clients it associates to.
802.11a Authentication Mode	Select the mode the wireless adapter uses to authenticate to an AP: <ul style="list-style-type: none"> • Auto causes the adapter to attempt authentication using shared, but switches it to open authentication if shared fails. • Open enables an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match. • Shared only allows the adapter to associate with access points that have the same WEP key.

For infrastructure (access point) networks, click the [Preferred APs](#) button to specify up to four access points to which the client adapter should attempt to associate.

Security Tab

In the Atheros Client Utility, access the Security tab by clicking [New](#) or [Modify](#) on the Profile Management tab. Click the Security tab in the Profile Management window.

Edit the fields in the Security tab of Profile Management to configure the profile. To define the security mode, select the radio button of the desired security mode. Make sure to also edit the [General](#) and [Advanced](#) tabs.

<p>WPA</p>	<p>Enables the use of Wi-Fi Protected Access (WPA). Choosing WPA opens the WPA EAP drop-down menu. The options include:</p> <ul style="list-style-type: none"> • EAP-TLS • EAP-TTLS • PEAP (EAP-GTC) • PEAP (EAP-MSCHAP V2) • LEAP
<p>WPA Passphrase</p>	<p>Enables WPA Passphrase security. Click on the Configure button and fill in the WPA Passphrase.</p>
<p>802.1x</p>	<p>Enables 802.1x security. This option requires IT administration.</p> <p>Choosing 802.1x opens the 802.1x EAP type drop-down menu. The options include:</p> <ul style="list-style-type: none"> • EAP-TLS • EAP-TTLS • PEAP (EAP-GTC) • PEAP (EAP-MSCHAP V2) • LEAP <p>If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.</p>
<p>Pre-Shared Key (Static WEP)</p>	<p>Enables the use of pre-shared keys that are defined on both the access point and the station.</p> <p>To define pre-shared encryption keys, choose the Pre-Shared Key radio button and click the Configure button to fill in the Define Pre-Shared Keys window.</p> <p>If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.</p>
<p>None</p>	<p>No security (not recommended).</p>

Using EAP-TLS Security

To use EAP-TLS security In the Atheros Client Utility, access the [Security tab](#) in the Profile Management window.

1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose EAP-TLS from the drop-down menu.

Enabling EAP-TLS security:

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

1. If EAP-TLS is supported, choose EAP-TLS from the drop-down menu on the right, then click the [Configure](#) button.
2. Select the appropriate certificate authority from the list. The server/domain name and the login name are filled in automatically from the certificate information. Click [OK](#).
3. Click [OK](#).
4. Activate the profile.

Using EAP-TTLS Security

To use EAP security In the Atheros Client Utility, access the [Security tab](#) in the Profile Management window.

1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose EAP-TTLS from the drop-down menu.

Enabling EAP-TTLS security:

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

1. If EAP-TTLS is supported, choose EAP-TTLS from the drop-down menu on the right, then click the [Configure](#) button.
2. Select the appropriate certificate from the drop-down list and click [OK](#).
3. Specify a user name for EAP authentication:
 - Check [Use Windows User Name](#) to use the Windows user name as the EAP user name.
 - OR: Enter a EAP user name in the User Name field to use a separate user name and password and start the EAP authentication process.

PRELIMINARY

4. Click [Advanced](#) and:
 - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
 - Enter the domain name of the server from which the client will accept a certificate.
 - Change the login name if needed.
5. Click [OK](#).
6. Enable the profile.

Using PEAP-GTC Security

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

1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-GTC) from the drop-down menu.

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

1. Click the [Configure](#) button.
2. Select the appropriate network certificate authority from the drop-down list.
3. Specify a user name for inner PEAP tunnel authentication:
 - Check [Use Windows User Name](#) to use the Windows user name as the PEAP user name.
 - OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
4. Choose [Token](#) or [Static Password](#), depending on the user database.

Note that Token uses a hardware token device or the Secure Computing SoftToken program (version 1.3 or later) to obtain and enter a one-time password during authentication.

5. Click [Advanced](#) and:
 - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
 - Enter the domain name of the server from which the client will accept a certificate.

The login name used for PEAP tunnel authentication, fills in automatically as PEAP-xxxxxxxxxxxx, where xxxxxxxxxxxx is the computer's MAC address. Change the login name if needed.

6. Click [OK](#).

7. Enable the profile.

Using PEAP-MSCHAP V2 Security

To use PEAP-MSCHAP V2 security In the Atheros Client Utility, access the [Security tab](#) in the Profile Management window.

1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-MSCHAP V2) from the drop-down menu.

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

1. Click the [Configure](#) button.
2. Select the appropriate certificate from the drop-down list.
3. Specify a user name for inner PEAP tunnel authentication:
 - Check [Use Windows User Name](#) to use the Windows user name as the PEAP user name.
 - OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
4. Click [Advanced](#) and:
 - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
 - Enter the domain name of the server from which the client will accept a certificate.
 - The login name used for PEAP tunnel authentication, fills in automatically as PEAP-xxxxxxxxxxx, where xxxxxxxxxxxx is the computer's MAC address. Change the login name if needed.
5. Click [OK](#).
6. Enable the profile.

Using LEAP Security

To use security in the Atheros Client Utility, access the [Security tab](#) in the Profile Management window.

LEAP security requires that all infrastructure devices (e.g. access points and servers) are configured for LEAP authentication. Check with the IT manager.

- [Configuring LEAP](#)
- [Enabling LEAP](#)

Configuring LEAP:

- On the Security tab, choose the WPA radio button. Choose WPA-LEAP from the drop-down menu.
 - OR: On the Security tab, choose the 802.1x radio button. Choose LEAP from the drop-down menu.
1. Click the [Configure](#) button.
 2. Specify a user name and password:
Select to [Use Temporary User Name and Password](#) by choosing the radio button:
 - Check [Use Windows User Name](#) to use the Windows user name as the LEAP user name.
 - OR: Check [Manually Prompt for LEAP User Name and Password](#) to manually login and start the LEAP authentication process.
Select to [Use Saved User Name and Password](#) by choosing the radio button:
 - Specify the LEAP user name, password, and domain to save and use.
 3. Enter the user name and password.
 4. Confirm the password.
 5. Specify a domain name:
 - Check the [Include Windows Logon Domain with User Name](#) setting to pass the Windows login domain and user name to the RADIUS server. **(default)**
 - OR: Enter a specific domain name.
 6. If desired, check [No Network Connection Unless User Is Logged In](#) to force the wireless adapter to disassociate after logging off.
 7. 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.
 8. Click [OK](#).
 9. Enable the profile.

Pre-Shared Encryption Keys

Defining pre-shared encryption keys:

1. Click the [Define Pre-Shared Keys](#) radio button on the [Security tab](#).
2. Click on [Configure](#).
3. Fill in the fields in the Define Pre-Shared Keys dialog box:

Key Entry	Determines the entry method for an encryption key: hexadecimal (0-9, A-F), or ASCII text (all keyboard characters except spaces).
Encryption Keys	Selects the default encryption keys used. Only allows the selection for a shared First, Second, Third, or Fourth key whose corresponding field has been completed.
WEP Keys (1-4)	Defines a set of shared encryption keys for network configuration security. At least one Shared Key field must be populated to enable security using a shared key. Click on the radio button to set the key as the default encryption key.
WEP Key Size	Defines the size for each encryption key. The options include: <ul style="list-style-type: none"> – 64-bit (enter 10 digits for hexadecimal, 5 ASCII characters) – 128-bit (enter 26 digits for hexadecimal, 13 digits for ASCII) – 152-bit (enter 32 digits hexadecimal, 16 digits for ASCII)

4. Click [OK](#) for the changes to take effect.

Overwriting an Existing Static WEP Key

1. Click the [Define Pre-Shared Keys](#) radio button on the [Security tab](#).
2. Click on [Configure](#).
3. In the window, all existing static WEP keys are displayed as asterisks for security reasons. Click in the field of the existing static WEP key to overwrite.
4. Delete the asterisks in that field.
5. Enter a new key.
6. Make sure to select the [Transmit Key](#) button to the left of this key is selected for the key to transmit packets.
7. Click [OK](#).

Disabling Static WEP

- To disable static WEP for a particular profile, choose [None](#) on the Profile Management tab and click [OK](#).
- OR: Select any other security option on the Profile Management tab to automatically disable static WEP.

Using WPA Passphrase Security

To use WPA Passphrase security In the Atheros Client Utility, access the [Security tab](#) in the Profile Management window.

1. On the Security tab, choose the WPA Passphrase radio button.
2. Click on the [Configure](#) button.
3. Fill in the WPA Passphrase.

Click [OK](#).

Zero Configuration

This section describes the operation of the Atheros Client Utility (ACU) and Windows XP Wireless Configuration Service (WZCS).

Wireless Network Configuration

The Windows WZCS is an NT service that manages the wireless connection in a largely dynamic way. Only minimal connection information must be identified and configured.

To set Zero Configuration on Windows XP, take the following steps:

1. In Windows XP, open the Wireless Network Configuration Properties dialog box.
2. Select the check box "Use Windows to configure my wireless network settings" to set Zero Configuration.

When this check box is selected, Windows XP takes control of these settings for all configuration profiles:

- SSID
- Security keys
- Ad hoc settings

The Zero Configuration settings override all configuration profiles, even when you select other options. However, the ACU does still control the following settings when Zero Configuration is set:

- [Power settings](#)
- Active/Passive scanning (where applicable)
- [Transmit power](#)
- Wireless band
- [Short/Long preamble](#) (802.11b)

When Zero Configuration is in use, a pop-up message is displayed on the ACU when you attempt to create or edit a configuration profile from the Station Configuration tab of the ACU.



To turn Zero Configuration off on Windows XP, take the following steps:

1. In Windows XP, open the Wireless Network Configuration Properties dialog box.
2. Clear the check box “Use Windows to configure my wireless network settings” to set Zero Configuration.

When this check box is cleared, all profile settings are controlled by the configuration profile, which is set up from the Station Configuration tab of the ACU.

Check the Status Information or Diagnostics

The Atheros client utility includes a number of tools to display current diagnostics and status information.

- [Check current status](#)
- [Check driver information](#)
- [Check receive and transmit diagnostics](#)

Current Status

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

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

Profile Name	The name of the current selected configuration profile. Set up the configuration name on the General tab .
Link Status	Shows whether the station is associated to the wireless network.
Wireless Mode	Displays the wireless mode . Configure the wireless mode on the Advanced tab .
IP Address	Displays the computer's IP address.
Network Type	The type of network the station is connected to. The options include: <ul style="list-style-type: none"> • Infrastructure (access point) • Ad Hoc Configure the network type on the Advanced tab .
Current Channel	Shows the currently connected channel.

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

Click the [Advanced](#) button to see the advanced status diagnostics.

Adapter Information Button

The Adapter Information button contains general information about the network interface card (the wireless network adapter) and the network driver interface specification (NDIS) driver. Access the adapter information from the [Diagnostics tab](#).

Card Name	The name of the wireless network adapter.
MAC Address	The MAC address of the wireless network adapter.
Driver	The driver name and path of the wireless network adapter driver.
Driver Version	The version of the wireless network adapter driver.
Driver Date	The creation date of the wireless network adapter driver.
Client Name	The name of the client computer.

Diagnostics Tab

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

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

- Multicast frames transmitted and received
- Broadcast frames transmitted and received
- Unicast frames transmitted and received
- Total bytes transmitted and received

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

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

Transmitted Frames

- Frames transmitted OK
- Frames retried
- Frames dropped
- NoACK frames
- ACK frames
- RTS Frames
- Clear-to-send (CTS) Frames
- No CTS frames
- Retried RTS frames
- Retried data frames

Received Frames

- Frames received OK
- Beacons
- Frames with errors
- CRC errors
- Encryption errors
- Duplicate frames
- AP mismatches
- Data rate mismatches
- Authentication time-out
- Authentication rejects: the number of AP authentication failures received by the wireless network adapter
- Association time-out
- Association rejects: the number of access point authentication rejects received by the wireless network adapter
- Standard MIC OK
- Standard MIC errors
- CKIP MIC OK
- CKIP MIC errors

Scan Available Networks

Click the [Scan](#) button on the [Profile Management tab](#) to scan for available infrastructure and ad hoc networks. On this list, click [Refresh](#) to refresh the list at any time.

Connecting to a different network

- Highlight a network name and click the [Activate](#) button to connect an available network. If no configuration profile exists for that network, the Profile Management window opens to the General tab. Fill in the profile name and click [OK](#) to [create the configuration profile](#) for that network.



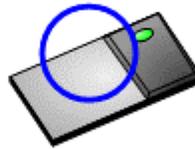
Infrastructure
(AP) Network



Connected
Infrastructure
(AP) Network



Ad Hoc
Network



Connected
Ad Hoc
Network



Encryption
Active

Display Settings

To change the display settings, choose Options > Display Settings from the menu.

The display settings dialog box contains tools to set the:

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.

ACU Tools

Use the Action menu to access the Atheros Client Utility tools:

Enable/Disable Radio	Enable or disable the RF Signal on all Atheros station reference designs.
Enable/Disable Tray Icon	Enable or disable the tray icon .
Troubleshooting	Run the optional Troubleshooting Utility .
Manual LEAP Login	Log in to LEAP manually, if LEAP is set to manually prompt for user name and password on each login.
Reauthenticate	Reauthenticate to a LEAP-configured access point.
Exit	Exit the Atheros Client Utility application.

Tray Icon

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



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

Right-click on the tray icon to:

- Help** Open the online help.
- Open Atheros Client Utility** Launch the Atheros Client Utility (ACU). Use the ACU to [configure the profile](#) or [view status and statistics information](#).
- Troubleshooting** Run the [Troubleshooting Utility](#).
- Preferences** Set the startup options and menu options for the ACU. Check whether the program should start automatically when Windows starts, and check the menu items that should appear on the popup menu.
- Enable/Disable Radio** Enable or disable the RF Signal.
- Manual LEAP Login** [Log in to LEAP](#) manually, if LEAP is set to manually prompt for user name and password on each login.
- Reauthenticate** Reauthenticate to the access point.
- Select Profile** Click a configuration profile name to switch to it. If no configuration profile exists for a connection, [add](#) a profile first.
- Show Connection Status** Display the Connection Status window. This window displays information about the connection:
 - Active Profile** Displays the name of the active [configuration profile](#).
 - Auto Profile Selection** Shows whether [auto profile selection](#) is enabled.
 - Connection Status** Displays whether the adapter is connected to a wireless network.
 - Link Quality** Lists the quality of the link connection.

PRELIMINARY

SSID	Displays the SSID of the associated network.
Access Point Name	Shows the name of the access point the wireless adapter is connected to.
Access Point IP Address	Shows the IP address of the access point the wireless adapter is connected to.
Link Speed	Lists the speed of the link connection.
Client Adapter IP Address	Displays the IP address of the wireless adapter.

Exit Exit the Atheros Client Utility application.

The colors are defined as follows:

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

*Received signal strength indication RSSI. [Displayed](#) in dB or percentage.

Enable or disable the tray icon in the [Action menu](#).

Troubleshooting Utility

The Troubleshooting Utility is an optional utility that identifies and resolves wireless adapter configuration and association problems when the adapter is in access point (infrastructure) mode.

This utility is available only in Mini PCI solutions.

To run the Troubleshooting Utility:

- From the [Diagnostics tab](#), click the [Troubleshooting](#) button to run the Troubleshooting Utility.
- OR: Select Action > Troubleshooting from the action menu.

Click [Run Test](#) to run the troubleshooting utility tests:

- Driver Installation
- Card Insertion
- Card Enable
- Radio
- Association
- Authentication
- Network

The utility posts the test results as:

- Test passed: Successful test completion
- Test failed: The test failed because the wireless adapter is not configured improperly to associate to an access point
- Test bypassed: The test was not required for the active profile

To view a report of the tests, click [View Report](#).

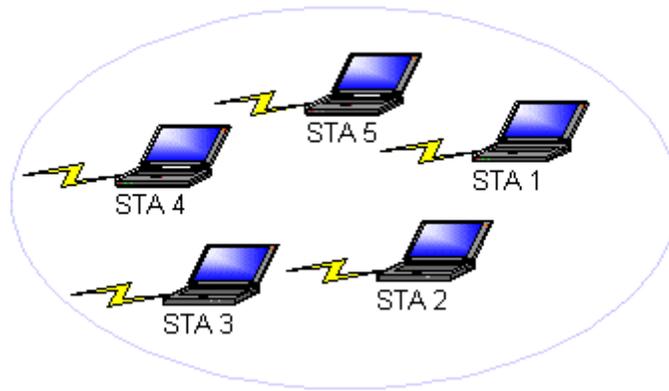
- To save the report, click [Save Report](#) and browse to the directory to save the report to.

Name the file and click [Save](#).

- Click [Start Test](#) to re-run the troubleshooting utility.

Ad Hoc Mode

In ad hoc mode, a wireless network adapter works within an independent basic service set (IBSS), as illustrated here. All stations communicate directly with other stations without using an access point (AP).



To connect to an ad hoc network, [configure the profile for ad hoc mode](#).

Ad Hoc Mode Profile Configuration

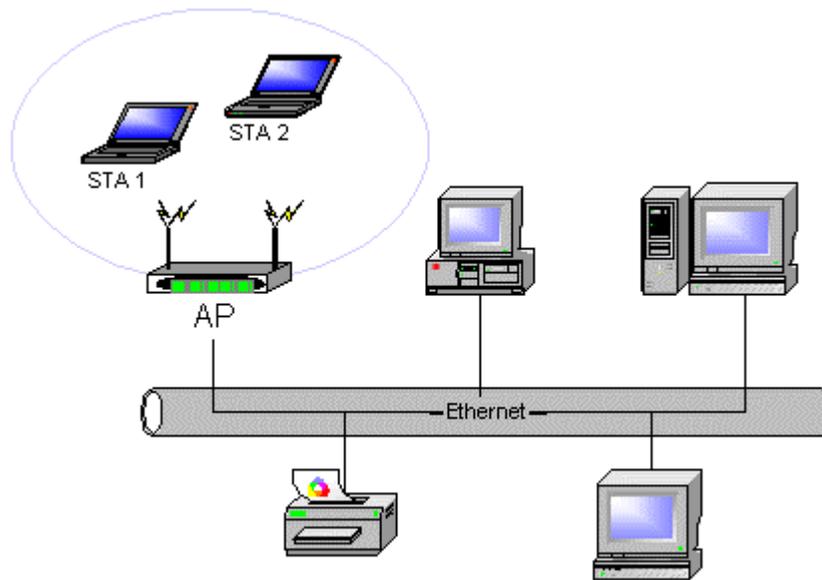
To configure a profile in [ad hoc](#) mode, change the Network Type in the Profile Management's [Advanced tab](#). For [ad hoc](#) mode, modify the settings:

- Network Name (on [General Tab](#))
- [Transmit Power Level](#)
- [802.11b Preamble](#) (if using 802.11b)
- [Wireless Mode When Starting an Ad Hoc Network](#)

Make sure to also edit the [General](#) and [Security](#) tabs.

Infrastructure (Access Point) Mode

In infrastructure (access point (AP)) mode, the wireless network adapter participates in a basic service set (BSS) as a station, and communicates with the other stations through an AP, as illustrated here.



To connect to an access point network, [configure the profile for access point mode](#).

Infrastructure (Access Point) Mode Profile Configuration

To [configure a profile in infrastructure \(access point\) mode](#), change the Network Type in the [Advanced tab](#). For [access point mode](#), modify the settings:

- [Transmit Power Level](#)
- [Power Save Mode](#)
- [802.11b Preamble](#) (if using 802.11b)
- [Wireless Mode](#)
- [802.11a Authentication Mode](#) (if using 802.11a)

Make sure to also edit the [General](#) and [Security](#) tabs.

Uninstall an Old Driver

Uninstall an old driver before upgrading to a new NDIS driver release.

To remove the newly installed driver from the system if the system does not have previously installed versions of the NDIS driver, proceed to [Step 4](#).

1. To remove the NDIS driver from the OS, go to Device Manager, right-click [Atheros Wireless Network Adapter](#), and choose [Uninstall](#).
2. Click [OK](#) to uninstall the device.
3. When the device is uninstalled from Device Manager, search for and delete the driver files that reside in the system.
 - a. Go to the Start menu and choose Search > For Files or Folders.
 - b. Enter **oem*.inf** in the Search for files or folders named: field, and enter **Atheros** in the [Containing text:](#) field.
 - c. Click [Search Now](#).
 - d. A few files matching these criteria are possible, if previous drivers have not been removed properly.
 - e. Choose the files that have been found and delete them from the system.
4. To complete the uninstallation, remove the file **ar5211.sys** from the folder **WINNT\system32\drivers**.

Additional Security Features

These security features prevent attacks on a wireless network's WEP keys. The wireless adapter automatically supports each of these features, but these features must be enabled on the access point.

Message Integrity Check (MIC)

MIC prevents bit-flip attacks on encrypted packets. In a bit-flip attack, someone intercepts an encrypted message retransmits it after some alterations. Thus the receiver accepts the message as legitimate. The MIC adds some bytes to each packet to protect it against tampering.

Temporal Key Integrity Protocol (TKIP)

This feature prevents attacks on WEP in which someone catches encrypted packets and uses their initialization vector (IV) to decipher the WEP key. TKIP removes the predictability to protect both unicast and broadcast WEP keys.

Broadcast Key Rotation

EAP authentication provides dynamic unicast WEP keys for wireless adapters, but uses static broadcast keys. In broadcast WEP key rotation, the access point supplies a dynamic broadcast WEP key and changes it at intervals.

Advanced Status Information

Click the [Advanced](#) button on the [Current Status tab](#) of the Atheros Client Utility to see advanced information about the program and its operations. The Current Status tab does not require any configuration.

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

Network Name (SSID)	Displays the wireless network name. Configure the network name on the General tab .
Server Based Authentication	Shows whether server based authentication is used.
Data Encryption	Displays the encryption type the driver is using. Configure the encryption type on the Security tab .
Authentication Type	Displays the authentication mode . Configure the authentication mode on the General tab .
Message Integrity Check	Shows whether MIC is enabled. MIC prevents bit-flip attacks on encrypted packets.
Associated AP Name	Displays the name of the access point the wireless adapter is associated to.
Associated AP IP Address	Shows the IP address of the access point the wireless adapter is associated to.
Associated AP MAC Address	Displays the MAC address of the access point the wireless adapter is associated to.
Power Save Mode	Shows the power save mode . Power management is disabled in ad hoc mode. Configure the power save mode on the Advanced tab .
Current Power Level	Displays the transmit power level rate in mW. Configure the transmit power level on the Advanced tab .
Available Power Levels	Shows the 802.11a and/or 802.11b/g available power levels.
Current Signal Strength	Shows the current signal strength in dBm.
Current Noise Level	Displays the current noise level in dBm.
Up Time	Shows how long the client adapter has been receiving power (in hours:minutes:seconds). If the adapter runs for more than 24 hours, the display shows in days:hours:minutes:seconds.
802.11b Preamble	Displays the 802.11b preamble format. Configure the preamble format on the Advanced tab .
Current Receive Rate	Shows the current receive rate in Mbps.

PRELIMINARY

Current Transmit Rate	Displays the current transmit rate in Mbps.
Channel	Shows the currently connected channel.
Frequency	Displays frequency the station is using.
Channel Set	Shows the current channel set.

Compliance

FCC Radio-Frequency Exposure Notice:

FCC ID#: PPD-AR5BMB6

This device generates and radiates radio-frequency energy. In order to comply with FCC radio-frequency radiation exposure guidelines for an uncontrolled environment, this equipment has to be installed and operated while maintaining a minimum body to antenna distance of 20cm.

The antenna(s) used for this transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

This product does not contain any user serviceable components. Any unauthorized product changes or modifications will invalidate warranty and all applicable regulatory certifications and approvals. This product must be installed by a professional technician/installer

FCC Part 15 Notice (Applicable to Use Within the USA):

802.11a radio only:

This product is for indoor use only when using channels 36, 40, 44, or 48 (5150–5250 MHz). 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.

WARNING: 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 or more 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 the one which the receiver is connected to.
- Consult the dealer or an experienced radio/TV technician for help.
- The user may find the following booklet prepared by the Federal Communications Commission helpful:
The Interference Handbook
This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-00345-4.

PRELIMINARY

FCC OEM Labeling instructions:

OEM should add following label:

Contains FCC ID: PPD-AR5BMB6

Above should be clearly visible on products where AR5BMB6 modules are installed.

Industry Canada Notice (Applicable to Use Within Canada):

This device complies with Canadian RSS-210.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmitting antenna) that is installed outdoors is subject to licensing. The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's web site www.hc-sc.gc.ca/rpb.

Avis de Conformité à la Réglementation d'Industrie Canada:

Pour empêcher toute interférence aux services faisant l'objet d'une licence, cet appareil doit être utilisé à l'intérieur seulement et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal.

L'installateur du présent matériel radio doit s'assurer que l'antenne est située ou pointée de manière à ce que cette dernière n'émette pas de champs radioélectriques supérieurs aux limites spécifiées par Santé Canada pour le grand public; consulter le Code de sécurité 6, disponible sur le site Web de Santé Canada, à l'adresse suivante: www.hc-sc.gc.ca/rpb.

European Community—CE Notice (802.11a Radio):

Marking by the symbol:

CE Mark with notified body number

CE0336

CE mark with NB# indicates compliance with the essential requirements of Directive 73/23/EC and the essential requirements of articles 3.1(b), 3.2 and 3.3 of Directive 1999/5/EC. Such marking is indicative that this equipment meets or exceeds the following technical standards:

EN 301 893 - Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive.

EN 301 489-17—Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.

EN 60950—Safety of information technology equipment, including electrical business equipment.

Marking by the symbol:

Exclamation Mark !

Indicates that usage restrictions apply.

PRELIMINARY

- This product is for indoor use only when using channels 36, 40, 44, 48, 52, 56, 60, or 64 (5150–5350 MHz).
- Turbo mode is not allowed in EC countries.

European Community—CE Notice (802.11b Radio)

Marking by the symbol:

CE Mark with exclamation mark

indicates compliance with the essential requirements of Directive 73/23/EC and the essential requirements of articles 3.1(b), 3.2 and 3.3 of Directive 1999/5/EC. Such marking is indicative that this equipment meets or exceeds the following technical standards:

- EN 300 328-2—Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques
- EN 301 489-17—Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.
- EN 60950—Safety of information technology equipment, including electrical business equipment.

Marking by the symbol: **Exclamation Mark** indicates that usage restrictions apply.