

USER'S MANUAL



Netw

COMPEX *iWave*Port SERIES

WLP54G 3C WLP54AG 3C WLP54G 3B WLP54G 6C (RoHS-compliant) WLP54AG 6C (RoHS-compliant) WLP54G 6B (RoHS-compliant)

Manual Number: U-0539-V1.6C

© Copyright 2006 Compex Systems Pte Ltd

All Rights Reserved

This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

Trademark Information

Compex[®], ReadyLINK[®] and MicroHub[®] are registered trademarks of Compex, Inc. Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. All other brand and product names are trademarks or registered trademarks of their respective owners.

Notice: Copyrights © 2006 by Compex, Inc. All rights reserved. Reproduction, adaptation, or translation without prior permission of Compex, Inc. is prohibited, except as allowed under the copyright laws.

Manual Revision by Daniel

Manual Number: U-0539-V1.6C Version 1.6, December 2006

Disclaimer

Compex, Inc. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Compex, Inc. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Compex, Inc will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

Your Feedback

We value your feedback. If you find any errors in this user's manual, or if you have suggestions on improving, we would like to hear from you. Please contact us at:

Fax: (65) 62809947 Email: feedback@compex.com.sg

Technical Support Information

The warranty information and registration form are found in the Quick Install Guide.

For technical support, you may contact Compex or its subsidiaries. For your convenience, you may also seek technical assistance from the local distributor, or from the authorized dealer/reseller that you have purchased this product from. For technical support by email, write to support@compex.com.sg.

Refer to the table below for the nearest Technical Support Centers:

	Technical Support Centers
Со	ntact the technical support center that services your location.
	U.S.A., Canada, Latin America and South America
🖂 Write	Compex, Inc.
	840 Columbia Street, Suite B,
	Brea, CA92821, USA
🖀 Call	Tel: +1 (714) 482-0333 (8 a.m5 p.m. Pacific time)
Ewil	Tel: +1 (800) 279-8891 (Ext.122 Technical Support)
🚔 Fax	Fax: +1 (714) 482-0332
Asia	, Australia, New Zealand, Middle East and the rest of the World
🖂 Write	Compex Systems Pte Ltd
	135, Joo Seng Road #08-01, PM Industrial Building
	Singapore 368363
🖀 Call	Tel: (65) 6286-1805 (8 a.m5 p.m. local time)
Ewil	Tel: (65) 6286-2086 (Ext.199 Technical Support)
🚔 Fax	Fax: (65) 6283-8337
Internet	E-mail: support@compex.com.sg
access/	FTPsite: Ftp.compex.com.sg
Website:	http://www.cpx.com or http://www.compex.com.sg

About This Document

The product described in this document, Compex Wireless-G PCI Network Adapter, Compex WLP54 is a licensed product of Compex Systems Pte Ltd. This document contains instructions for installing, configuring and using Compex WLP54. It also gives an overview of the key applications and the networking concepts with respect to the product.

This documentation is for both Network Administrators and the end user who possesses some basic knowledge in the networking structure and protocols.

It makes a few assumptions that the host computer has already been installed with TCP/IP and already up & running and accessing the Internet. Procedures for Windows 2000/XP operating systems are included in this document.

How to Use this Document

This document may become superseded, in which case you may find its latest version at: <u>http://www.compex.com.sg</u>

The document is written in such a way that you as a user will find it convenient to find specific information pertaining to the product. It comprises of chapters that explain in detail the installation and configuration of Compex WLP54.

Drivers & Utilities

This manual is written based on Drivers version 5.0.0.108; Utility version 5.0.0.272

Conventions

In this document, special conventions are used to help and present the information clearly. The Compex Wireless PCI Network Adapter is often referred to as Compex WLP54 in this document. Below is a list of conventions used throughout.



NOTE

This section will consist of important features or instructions



CAUTION

This section concerns risk of injury, system damage or loss of data



WARNING

This section concerns risk of severe injury

References on Menu Command, Push Button, Radio Button, LED and Label appear in **Bold**. For example, "Click on **Ok**."

Copyrights © 2006 Compex Systems Pte Ltd	. i
Trademark Information	. i
Disclaimer	. i
Your Feedback	. i
Technical Support Information	.ii
About This Document	iii
How to Use this Document	iii
Drivers & Utilities	iii
Conventions	iv

1.1 Introduction 8 1.2 Features and Benefits 8 Chapter 2 Basic Setup 9 2.1 Hardware Installation 9 2.2 Driver & Utility Installation 10 Chapter 3 Using the System Tray Utility 15 Chapter 4 Utility Features 22 4.1 Current Status Tab 22 4.2 Profile Management Tab 24 4.3 Diagnostics Tab 25 4.4 Country Code Selector 29 Chapter 5 Utility Configuration 31 5.1 Ad-hoc Mode 32 5.3 Infrastructure Mode 42 5.4 Configuration on Infrastructure Mode 42 5.5 Profile Management 48 5.5.1 Advanced Tab 59 Chapter 6 Types of Authentication and Encryption mode 63 6.1 <	Cha	apter 1	Product Overview	8
Chapter 2 Basic Setup. 9 2.1 Hardware Installation 9 2.2 Driver & Utility Installation 10 Chapter 3 Using the System Tray Utility 15 Chapter 4 Utility Features 22 4.1 Current Status Tab. 22 4.2 Profile Management Tab. 24 4.3 Diagnostics Tab 25 4.4 Country Code Selector 29 Chapter 5 Utility Configuration 31 5.1 Ad-hoc Mode 32 5.3 Infrastructure Mode 41 5.4 Configuration on Infrastructure Mode 42 5.5 Profile Management 48 5.5.1 Advanced Tab 59 Chapter 6 Types of Authentication and Encryption mode 63 6.1 Ad-hoc Network Security 63 6.2 Infrastructure Network Security 63	1.1 1.2	Introdu Feature	ction es and Benefits	8 8
2.1 Hardware Installation 9 2.2 Driver & Utility Installation 10 Chapter 3 Using the System Tray Utility 15 Chapter 4 Utility Features 22 4.1 Current Status Tab. 22 4.2 Profile Management Tab. 24 4.3 Diagnostics Tab 25 4.4 Country Code Selector 29 Chapter 5 Utility Configuration 31 5.1 Ad-hoc Mode 32 5.3 Infrastructure Mode 41 5.4 Configuration on Infrastructure Mode 42 5.5 Profile Management 48 5.5 Profile Management 48 5.5.1 Advanced Tab 59 Chapter 6 Types of Authentication and Encryption mode 63 6.1 Ad-hoc Network Security 63 6.2 Infrastructure Network Security 63	Cha	apter 2	Basic Setup	9
Chapter 3 Using the System Tray Utility 15 Chapter 4 Utility Features 22 4.1 Current Status Tab 22 4.2 Profile Management Tab 24 4.3 Diagnostics Tab 25 4.4 Country Code Selector 29 Chapter 5 Utility Configuration 31 5.1 Ad-hoc Mode 32 5.3 Infrastructure Mode 41 5.4 Configuration on Infrastructure Mode 42 5.5 Profile Management 48 5.5.1 Advanced Tab 59 Chapter 6 Types of Authentication and Encryption mode 63 6.1 Ad-hoc Network Security 63 6.2 Infrastructure Network Security 63	2.1 2.2	Hardwa Driver 8	are Installation Wility Installation	9 10
Chapter 4 Utility Features224.1 Current Status Tab.224.2 Profile Management Tab.244.3 Diagnostics Tab254.4 Country Code Selector29Chapter 5 Utility Configuration315.1 Ad-hoc Mode325.3 Infrastructure Mode325.4 Configuration on Infrastructure Mode415.5 Profile Management485.5.1 Advanced Tab59Chapter 6 Types of Authentication and Encryption mode636.1 Ad-hoc Network Security636.2 Infrastructure Network Security63	Cha	apter 3	Using the System Tray Utility	.15
4.1 Current Status Tab	Cha	apter 4	Utility Features	. 22
Chapter 5 Utility Configuration 31 5.1 Ad-hoc Mode 31 5.2 When to set up Ad-hoc Mode 32 5.3 Infrastructure Mode 41 5.4 Configuration on Infrastructure Mode 42 5.5 Profile Management 48 5.5.1 Advanced Tab 59 Chapter 6 Types of Authentication and Encryption mode 63 6.1 Ad-hoc Network Security 63 6.2 Infrastructure Network Security 63	4.1 4.2 4.3 4.4	Current Profile M Diagno Country	Status Tab Management Tab stics Tab y Code Selector	. 22 24 25 29
5.1 Ad-hoc Mode	Cha	apter 5	Utility Configuration	. 31
Chapter 6 Types of Authentication and Encryption mode	5.1 5.2 5.3 5.4 5.5	Ad-hoc When to Infrastru Configu Profile N 5.5.1	: Mode o set up Ad-hoc Mode ucture Mode uration on Infrastructure Mode Management Advanced Tab	. 31 . 32 . 41 . 42 . 48 . 59
6.1 Ad-hoc Network Security	Cha	apter 6	Types of Authentication and Encryption mode	. 63
	6.1 6.2	Ad-hoc Infrastru	: Network Security ucture Network Security	63 65

 6.2.1 EAP 6.2.2 EAP 6.2.3 PEA 6.2.4 PEA 6.2.5 LEAF 6.2.6 EAP 6.2.7 WPA 	-TLS -TTLS P (EAP-GTC) P (EAP-MSCHAP V2) - FAST	
6.2.8 Pre-	shared Key (Static WEP)	83
Appendix I Ur	plug PCI Adapter from the System	85
Appendix II Ur	ı-install	86
Appendix III	Certificate Application for WPA mode	
AIII-1Installing W AIII-2Installing c AIII-3Applying fo AIII-4Becoming	/indow XP Service Pack Patch File ertificate on your server or Client Certifications a domain member	90 91 92 95
Appendix IV	Wireless Zero Configuration Utility	
AIV-1 Enable AIV-2 Disable	Wireless Zero Configuration Utility Wireless Zero Configuration Utility	98 100
Appendix V	Technical Specifications	

Chapter 1 Product Overview

1.1 Introduction

Thank you for purchasing this Wireless 108Mbps PCI Network Adapter. Data security is facilitated with WPA, IEEE 802.1x Authentication and 64-bit, 128-bit and 152-bit WEP (Wired Equivalent Privacy). They support easy Plug and Play installation and combine simplicity, data privacy, and reliability for your wireless network.

1.2 Features and Benefits

• Interoperability

The PCI adapter is able to inter-operate with other wireless network devices using different standards. In addition, the dynamic rate shifting capability allows automatic selection of optimum connection speed to any wireless LAN devices or access points.

Easy Monitoring

The client manager (Atheros Wireless Utility) comes with a built-in monitoring & diagnostic software that detects wireless sites or access points, providing valuable information like signal strength and channels used. It also allows testing of your wireless card hardware, software driver and firmware integrity through the card diagnostic option for easier troubleshooting of the network adapter.

Profile Management

The client manager allows the user to configure different profiles, allowing the wireless card to operate in different wireless networks by simply changing to the relevant profile.

Networking Modes

The network adapter supports two types of networking modes: infrastructure mode and ad-hoc mode. In infrastructure mode, clients communicate with each other through an access point. Whereas in ad-hoc mode, clients directly communicate with one another without the need for an access point.

Chapter 2 Basic Setup

This chapter outlines the basic requirement for the installation and configuration of the network adapter.

This network adapter is a plug-and-play device. You can plug it into the PCI slot of your PC for auto-detection.

2.1 Hardware Installation

- 1. Turn off your PC and switch off the power from the main power supply.
- 2. Remove the back cover of the PC.
- 3. Then insert the network adapter into your PCI slot as shown below. Ensure that the network adapter is properly seated into the slot.
- 4. Replace the back cover.
- 5. Power on your PC.



2.2 Driver & Utility Installation

- 1. Insert the Product CD into your computer CD-ROM drive.
- 2. Click on **Driver & Utility** section and the system will run the *setup.exe* automatically.
- 3. Next, the Atheros Client Installation Program screen appears. Click on the Next> button to proceed.

Atheros Client Installation	Program	×
	Atheros Client Installation Program	
	This program installs the driver and client utilities for your Atheros Wireless LAN Client Adapter.	
	< Back Next> Cancel	

 When the License Agreement screen appears, you are required to read and accept the agreement to continue. Click on the Next> button to proceed. 5. Select your preferred setup:



Install Client Utilities and Driver (Recommended) option

You are recommended to select this setup type. This option will install both the driver and utility that support your PCI adapter.

Install Driver Only option (For Windows XP user only)

Select this option if you are going to use the Wireless Zero Configuration Utility to configure your PCI adapter. Note that only Windows XP comes with the Wireless Zero Configuration Utility.

Make Driver Installation Diskette(s)

Select this option if you wish to make a duplicate copy of the driver and store to the diskette/s.

6. Click on the **Next>** button and follow the instructions stated on the screen.

For Windows XP users

7. If you are using Windows XP as operating system, the following screen will appear. Read the notice carefully and click on the **Next>** button to proceed.



8. Select your choice of tool to assist you in configuring your USB adapter. Click on the **Next>** button to proceed.

Atheros Client Installation Program	
Choose Configuration Tool	N.
Which tool will you use to configure your client adapter?	
 Atheros Client Utility (ACU) and Supplicant. 	
Third Party Supplicant	
InstallShield	Cancel

Atheros Client Utility (ACU) and Supplicant option

Select this option to install your network adapter. (Recommended)

Third Party Supplicant option

Select this option if you decide to use Wireless Zero Configuration Utility to configure your wireless device. Installing this tool will only allow you to view the status of the connected wireless device/s through the utility; configuration using the utility will not be allowed. If you have selected **Third Party Supplicant** configuration tool, a screen similar to that below will appear, prompting you to enable/disable the system tray icon.

 Click on the checkbox besides Enable Atheros System Tray Utility and click on the Next> button to proceed.

Enable Tray Icon		1
Would you like to enable the Atheros ACL features and is accessible from	s System Tray Utility? This u an icon in the Windows sys	tility provides a tem trav
Enable Atheros System Tray Utilit	2	
	•~	

10. The screen below appears to inform you that the driver will be automatically installed if you have already inserted your client adapter into the PCI slot of your computer.

Atheros	Client Installation Program
<u>^</u>	The installation program installs the driver automatically when the client adapter is inserted. Insert the adapter now if it is not yet inserted, cancel the Found New Hardware Wizard if it appears, and proceed with the installation. Click OK to continue.
	OK

Cancel the **Found New Hardware** Wizard if it appears and click on the **OK** button to begin the installation.

11. If a similar screen similar to the one shown below appears, click on the **Continue Anyway** button to continue the installation.



12. Click on the **OK** button to reboot your system and this will complete the installation.

Atheros	Client Installation Program
!	The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Click OK to reboot the system.

Chapter 3 Using the System Tray Utility

This chapter will elaborate on the Atheros system tray utility found at the right bottom corner of your screen. Right click on the utility icon and the menu will appear.

Cyre Atheros Client Utility Troubleshooting Preferences Disable Radio Manual Login Reauthenticate Select Profile	E.ab	
Open Atheros Client Utility Troubleshooting Preferences Disable Radio Manual Login Reauthenticate Select Profile	EXIC	
Troubleshooting Preferences Disable Radio Manual Login Reauthenticate Select Profile	Open Atheros Client Ut	ility
Preferences Disable Radio Manual Login Reauthenticate Select Profile	Troubleshooting	
Disable Radio Manual Login Reauthenticate Select Profile	Preferences	
Manual Login Reauthenticate Select Profile	Disable Radio	
Reauthenticate Select Profile	Manual Login	
Select Profile	Reauthenticate	
	Select Profile	•
	Show Connection St	latus

The following explains the different options available on the menu:

<u>Help</u>

Open the online help.

Exit

Exit the Atheros Client Utility application. Once you exit, the icon will disappear from the system tray.

Open Atheros Client Utility...

Launch the Client Utility.

Wireless-G Excellent Signal Strength Example



Troubleshooting

This option allows you to identify and resolve the wireless adapter configuration and association problems only when the network adapter is operating in the infrastructure mode.

Atheros Troublesh	ooting Utility	X
Test result / report		
	Run Test Save Report View Report	

Click on **Run Test**. The button display then changes to **Start Test** and at the same time, the test messages are displayed. To stop the incoming test messages, click **Stop Test**.

	<u> </u>		
Test result /	report		
Running	river installation test		
T	est passed		
Running	ard insertion test		
T	est passed		
Running (ard enable test		
T	est passed		
Running F	adio test		
T	est passed		
Running A	ssociation test		
T	est passed		
Running A	uthentication test		
T	est bypassed.		
Running N	etwork test		
T	est passed		

To save the report to your desired directory on disk, click Save Report.

To view the detailed summary of the configuration tests, click View Report.

Preferences

This option allows you to set the startup and menu options for the utility. You can decide whether the program should start automatically when Windows starts, and which menu items should appear on the pop up menu.

Startup Options	
Run the program automatical	ly when Windows starts
Menu Options	
Check the items that you want to items are hidden.)	appear on the popup menu. (Unchecke
lelp	
✓Exit	
Open Atheros Client Utility	
✓ Troubleshooting	
☑Disable Radio	
Manual Login	
Reauthenticate	
Select Profile	
Show Connection Status	
	OK Cancel

Disable/Enable Radio

If you are unable to detect the RF signal, disable and enable the radio again. Once the radio is enabled, the system will prompt you that the RF signals have been successfully enabled.

Atheros Client Utility	
The RF signals for the following network card(s) have been succe Atheros AR5005GS Wireless Network Adapter	ssfully enabled:

Click on the **OK** button to proceed.

Manual LEAP Login

If you select this option, you will have to manually start the LEAP authentication process to login to the network instead of being prompted for your LEAP username and password during your windows logon.



Reauthenticate

Reauthenticate to a LEAP-configured access point each time you login to a LEAP network.



Select Profile

Click on a configuration profile name to switch to a particular wireless network. If no configuration profile exists, you will need to add a profile first.

Connection Status

To view the connection status of your wireless PCI adapter.

Alternatively, you may also double click on the utility icon in the system tray.

Connection Status		\mathbf{X}
Active Profile: Auto Profile Selection: Connection Status: Link Quality:	Default Disabled Associated Excellent	Total 80211 Environment
SSID: Access Point Name: Access Point IP Address: Current Receive Rate: Current Transmit Rate: Client Adapter IP Address:	demo Unavailable Unavailable 6.0 Mbps 54.0 Mbps 192.168.168.100	
		ОК

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	States the quality of the link connection.
SSID	Displays the SSID of the network to which the network adapter is associated.
Access Point Name	Shows the name of the access point the wireless adapter is connected to (if any).
Access Point IP Address	Shows the IP address of the access point the wireless adapter is connected to (if any).
Current Receive Rate	Displays the data rate at which the wireless adapter is currently receiving from the wireless network.
Current Transmit Rate	Displays the data rate at which the wireless adapter is currently transmitting to the wireless network.
Link Speed	States the speed of the link connection.
Client Adapter IP Address	Displays the IP address of the wireless adapter.

Chapter 4 Utility Features

This chapter shows you how to make use of the utility to view the status of your wireless connection, to change your settings and also to monitor your wireless performance via the network statistics.

NOTE	

NOTE It is advisable to activate only one of the utilities: Either the Wireless Zero Configuration Utility OR the Atheros Utility.

4.1 Current Status Tab

Displays the performance of the network adapter in the wireless network.

VVir	eless-G Ci	urrent Stat	us
A Atheros Client Utility - Currer	nt Profile: Workstati	on 2	? 🛛
Action Options Help			
Current Status Profile Management	Diagnostics		
Total 80211 Profile Name:	Workstation 2		Total 80211
ATHEROS Link Status:	Authenticated		ATHEROS
Wireless Mode:	2.4 GHz 54 Mbps	IP Address:	192.168.168.43
Network Type:	Infrastructure	Current Channel:	1
Server Based Authentication:	None	Data Encryption:	AES
Signal Strength:			Excellent
			Advanced

Wireless-AG Current Status

\Lambda Atheros Client Utility - Current	Profile: czech	? ×
Action Options Help		
Current Status Profile Management	Diagnostics	
Total 80211 ATHEROS Link Status:	czech Not Associated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: Scanning
Server Based Authentication:		Data Encryption:
IP Address:	0.0.0.0	
Signal Strength:		No Link
		Advanced

Upon clicking on the **Advanced** button, you will be able to view all information on the respective profile, e.g. the types of encryption and authentication, the signal strength, the MAC address of the connected AP (if you are in Infrastructure mode), etc.

Advanced Status			? 🛛
Network Name (SSID): Server Based Authentication: Data Encryption: Authentication Type: Message Integrity Check:	wireless:AP None AES Open AES	Current Signal Strength: Current Noise Level: Up Time: 802.11b Preamble: Current Receive Rate:	-60 dBm -100 dBm 02:40:14 Short & Long 36.0 Mbps
Associated AP Name: Associated AP IP Address: Associated AP MAC Address;	Unavailable Unavailable 00-80-48-00-34-8D	Current Transmit Rate: Channel:	48.0 Mbps 1
Power Save Mode: Current Power Level:	Normal 50 mW	Frequency: Channel Set:	2.412 GHz United States
Available Power Levels (802.11b/g):	100, 63, 50, 30, 20, 10 mW	C	ок 💦

4.2 Profile Management Tab

Selecting this tab displays the profiles and the details.

You only need to create a profile if you have more than one wireless connection.

rrent Status Profile Managem	nent Diagnostics	
wireless-AP		New
default		Modify
		Remove
		Activate
Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name (SSID):	Any	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	

4.3 Diagnostics Tab

The **Diagnostics** tab lists the following receive and transmit diagnostics for packets received by or transmitted to the network adapter.

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

in Options Help		
rrent Status Profile Mana	gement Diagnostics	
Transmit		
Multicast Packets:	5	Adapter information
Broadcast Packets:	180	Advanced Statistics
Unicast Packets:	267	
Total Bytes:	23167	Troubleshooting
Receive		
Multicast Packets:	0	
Broadcast Packets:	62	
Unicast Packets:	3	
Total Bytes:	6756	

Adapter Information

This button contains general information about the network interface card and the network driver interface specification (NDIS).

Adapter Informa	tion 🛛 🖓 🔀
Card Name:	Atheros AR5005GS Wireless Network Adapter
MAC Address: Driver:	UU-U3-7F-U5-21-44 C:\\w/IND0\w/S\Sustem32\DBIVEBS\ar5211.sus
Driver Version:	4.0.0.167
Driver Date:	10 Feb 2005 23:07:50
Client Name:	WINXP-0R1RRT3PJ
Serial Number:	MB5182L_0324
	ОК

Card Name	The name of the network adapter
MAC Address	The MAC address of the network adapter
Driver	The driver name and path
Driver version	The version of the driver
Driver date	The creation date of the driver
Client Name	The name of the client computer
Serial Number	The serial number of the network adapter

Advanced Statistics

This button shows more detailed statistical information on frames that are either received by or transmitted by the network adapter.

Ivanced Statistics			?
Transmit			
Frames Transmitted OK:	6649	RTS Frames:	0
Frames Retried:	402	CTS Frames:	0
Frames Dropped:	3055	No CTS Frames:	0
No ACK Frames:	47	Retried RTS Frames:	0
ACK Frames:	6649	Retried Data Frames:	402
Receive			
Beacons Received:	588	Authentication Time-Out:	0
Frames Received OK:	20	Authentication Rejects:	0
Frames Received with Errors:	198	Association Time-Out:	0
CRC Errors:	95	Association Rejects:	0
Encryption Errors:	0	Standard MIC OK:	0
Duplicate Frames:	0	Standard MIC Errors:	0
AP Mismatches:	0	CKIP MIC OK:	0
Data Rate Mismatches:	0	CKIP MIC Errors:	0
			OK N



This button allows you to run the diagnostic test, save the test report and view the test results on the wireless adapter configuration and association.

Atheros Troubleshoot	ng Utility				^
Troubleshooter report.	**				
Report date: Wednes	day, July 20, 200	15			
Name: Driver installati	on test				
Description: This test	is to check the ra	adio driver insta	llation.		
The radio's registry ke	ys are OK.				
Nic name	Atheros AR5005	GS Wireless N	etwork Adapter		
Driver name	Atheros AR500	5GS Wireless N	letwork Adapter (Micro	soft's Packet Schedu	
Driver path:	C:\WINDOWS\	System32\DRIN	/ERS\ar5211.sys		
Driver version	4.0.0.167				
Active Profile Name	: Default				
Test Done: The radio	driver has been	installed.			~
<				>	

4.4 Country Code Selector

The Country Code Selector sets the wireless configuration certified for the wireless regulatory domain by country. Different wireless regulatory domains have different certifications and this feature ensures that the wireless operation has valid certification.

	JUICUL			Sphons.
∧ Atheros Cl	ient Utility - Curren	t Profile: Default		? 🛛
Action Options	Help			
Current Status	Profile Management D	iagnostics		
Total 802.11	Profile Name:	Default		Total 80211
ATHEROS	Link Status:	Associated		ATHEROS
	Wireless Mode:	2.4 GHz 54 Mbps	IP Address:	192.168.168.28
	Network Type:	Infrastructure	Current Channel:	10
Serve	er Based Authentication:	None	Data Encryption:	None
	Signal Strength:	******	********	Excellent
				Advanced
r				- J

Select Country Code under Options.

In Atheros Desktop Utility Country Code Selector, select the Country (Example: Czech Republic), and click OK.

Atheros Desktop Utility Country Co	ode Selector
Country:	Czech Republic
	Dominican Republic Ecuador Egypt Estonia
Atheros Desktop Utility Country Co	ode Selector
Country:	Czech Republic



NOTE

Country Code Selector is only available for Driver Version 5.0.0.108 and Utility Version 5.0.0.272 which is also included on the Product CD.

The default Driver and Utility does not feature the **Country Code Selector**.

To check the versions, select Help - About Atheros Client Utility.

\Lambda Atheros Clier	nt Utility – Current Profile: wp18-ip19-bo		<u>?</u> ×
Action Options	Help		
Current Status	Atheros Client Utility Help		
Total 802.11	About Atheros Client Utility		
ATHEROS	Profile Name:		
	Link Status: Not Associated	Network Type:	
	Wireless Mode:	Current Channel:	
Server B	lased Authentication:	Data Encryption:	
	IP Address:		
	Signal Strength:	No Link	
14		Ad <u>v</u> anced	

About page displays Driver Version and Utility Version.

About		×
Δ	Atheros Client Utility	ОК
	Configuration Utility: 5.0.0.272	Help
	Application Interface: 5.0.0.272	
	Authentication Interface: 1.0.634.3	
Authe	entication Protocol Driver: 1 .0.0.45	
	Wireless Device Driver: 5.0.0.108	
	Copyright © 2001-2006 Atheros Communications	s, Inc.

Chapter 5 Utility Configuration

This chapter will elaborate on the Client Manager configuration of the network adapter using some simple examples.

This network adapter can be configured for 2 types of wireless architectures – Ad-hoc and Infrastructure. The different operational modes are shown in the following diagrams to allow you to easily understand how to configure your network adapter.

5.1 Ad-hoc Mode

In an Ad-hoc architecture, the wireless clients communicate directly with one another. No access point exists in such a wireless LAN configuration. Each wireless client can directly transfer data packets with each other.

Usually, the operation would be automatically detected and configured between the peers. However, if you wish to, you can also set a common channel for all Ad-hoc clients to use. This will be illustrated in the following section.



Wireless client

5.2 When to set up Ad-hoc Mode

Ad-hoc mode is also referred to as peer-to-peer mode or as Independent Basic Service Set (IBSS). Ad-hoc mode is useful when wireless devices are within range of each other and can discover and communicate among themselves without an AP. The figure below illustrates a family using Ad-hoc mode to share files and devices directly with one another.



For PC1

1. Set your PC1's IP address to *192.168.168.11*; subnet mask to *255.255.255.0* and activate your Utility.



NOTE

Ad-hoc mode works best when the network uses static IP addressing. The IP addresses of all the computers in the Ad-hoc network must be in the same subnet (e.g. 192.168.168.xxx); and the subnet mask must also be the same.

2. Proceed to the **Profile Management** tab.

Once you have installed the utility, the system will automatically create a default profile.

If you wish to create a new profile, click on **New** button. If not, simply click on **Modify** button to change the default settings.

Atheros Client Utility - Current Profile: Default	?
tion Options Help	
Current Status Profile Management Diagnostics	
Default	New
	Modify
	Remove
	Activate
Details	
Network Type: Infrastructure	Import
Security Mode: None	
Network Name 1 (SSID1): <empty></empty>	Export
Network Name 2 (SSID2): <empty></empty>	Scan
Network Name 3 (SSID3): <empty></empty>	Joean
Auto Select Profiles	Order Profiles
Auto Select Profiles	Order Profiles

3. Enter your own profile name, e.g. *son*. The **Client name** refers to the name that is registered to your PC.

4. Set the SSID to *PCI-CLIENT* and click on the **OK** button to update the changes.

Please ensure that all the clients in your Ad-hoc network use the same SSID, which in our example is set to *PCI-CLIENT*.

ofile Management		
seneral Security Advance	be	
Profile Settings		
Profile Name:	Son	
Client Name:	Tom_Teo	
Network Names		
SSID1:	PCI-CLIENT	
SSID2		
SSID3:		
		OK Cancel

- 5. Next, proceed to **Advanced** tab. Set your **Network Type** to *AdHoc* and **802.11b Preamble** to *Short &Long*.
- 6. You may leave the Transmit Power Level at their default values.
- 7. In the **Wireless Mode** section, check and confirm whether all options are ticked.
- 8. Next, proceed to Wireless Mode when starting Ad-hoc Network section. The channels available depend on the regulatory domain. If no other wireless adapters are found matching the ad hoc mode, this selection specifies the channel with which the adapter starts a new ad hoc network. Please note that the wireless adapter must match the wireless mode and channel of the other wireless clients it associates to.

9. Set the **Channel** to *Auto* to let the network adapter automatically detect the channel to use.

However, if you wish to set a specific channel, you must ensure that all the wireless clients are in the same channel to enable them to communicate with one another.

erietal Security Astronoco			
Transmit Power Level	Power Save Mode:	DII	
802.11b/g: 100 mW	Network Type:	Ad Hoc	~
802.11a: 40 mW	802.11b Preamble:	Short & Long	Long Only
Vireless Mode 2 4 GHz 54 Mbps 2 4 GHz 11 Mbps	Wireless Mode When Starting	g Ad Hoc Network	
Ime ween the strength of the	O 2.4 GHz 54 Mbps	Channet [/	Auto
₩ QoS	O Auto	pen 🔿 S	hared

10. Proceed to the Security tab. Select Pre-Shared Key (Static WEP) option and click on the Configure... button.

ofile Management	2
General Security Advan	red
Set Security Options	
O WPA/WPA2	WPA/WPA2 EAP Type: LEAP
O WPA/WPA2 Pass	chrate .
() 802.1x	802.1×EAP Type: LEAP
O None	Allow Association to Mixed Cells

11. Click on the radio button for **WEP Key Size:** *128*, type in, e.g. *1234567890abcdef1234567890* and click on the **OK** button to update the changes.

Note that the length of the WEP key depends on the type of encryption key that you have selected: For 64- bit WEP: 10 hexadecimal or 5 ASCII Text For 128-bit WEP: 26 hexadecimal or 13 ASCII Text For 152-bit WEP: 13 hexadecimal or 16 ASCII Text

ley Entry	⊙ Hex	adecimal (0-9, A-F)	ASCII Text (all keyboard	characters)
ncryption Keys	5			
	Transmit Keu			WEP Key Size:
WEP Key 1:	•	1234567890ABCDEF1234567	890	64 128 152
WEP Key 2:				000
WEP Key 3:				000
WEP Key 4:				000

You may now go to the **Current Status** tab to check the status of the connection. Notice that if there is no connection established (Refer to Link Status), this indicates that your WLP54 has not yet detected any other wireless client with SSID set to PCI-CLIENT.

A Atheros Client Utility - Currer	nt Profile: Son		? 🛛
Action Options Help			
Current Status Profile Management	Diagnostics		
Profile Name:	Son		Total 80211
Link Status:	Not Associated		ATHEROS
Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	0.0.0.0
Network Type:	Ad Hoc	Current Channel:	Scanning
Server Based Authentication:		Data Encryption:	
Signal Strength:			No Link
			Advanced L
Now, we proceed to configure PC2.

For PC2

- 1. Set your PC's IP address to *192.168.168.12*; subnet mask to *255.255.255.0*.
- 2. Go to the **Profile Management** tab and click on the **Scan** button to look for *PCI-CLIENT* (the SSID that you had previously created in PC1).
- 3. Once detected, highlight this profile and click on the **Activate** button.

Network Name (SSID)	69	S	ignal Strength	Channel	Wireless Mode
1 Any		1l	5 dB	3	2.4 GHz 11 Mbp
👗 Any		11	3 dB	3	2.4 GHz 11 Mbc
1 Any		11	4 dB	3	2.4 GHz 54 Mbc
1 Any	~3	11	4 dB	1	2.4 GHz 54 Mbc
1 Any		11	28 dB	10	2.4 GHz 54 Mbc
local-sales	5	all	28 dB	6	2.4 GHz 54 Mbc
PCI-CLIENT	-	11	41 dB	2	2.4 GHz 54 Mbc
Any	~ 3	all.	32 dB	8	2.4 GHz 54 Mbc
🕻 Weak Signal Test	-	11	2 dB	11	2.4 GHz 54 Mbc
(>

Notice that there is a key beside the Network name (SSID). This shows that you need the encryption key to connect to this network.

Next, you can see that the **SSID** is set to the same SSID as PC1 and that **Client Name** is pre-configured to the name registered to PC2. You need to give a name to your profile, e.g. *Daddy*.

Profile Management		? 🛛
General Security Advance	d	
Profile Settings Profile Name:	Daddy	
Client Name:	Thomas_Teo	
~ Network Names SSID1:	PCI-CLIENT	
		OK Cancel

4. Next, proceed to the **Security** tab and set the same security settings as for PC1.



NOTE

The SSID and encryption key for PC1, PC2 and the notebook must be the same in order to communicate with one another. Also, if you are using a specific channel instead of Auto, PC1, PC2 and notebook must be set with the same channel. Click on the OK button and go to the Current Status tab. Notice that once the connection has been successfully established, the link status will display <associated> and the signal strength will appear as a green bar.

ion Options	нер			
urrent Status	Profile Management	Diagnostics		
Total 802.11	Profile Name:	Daddy		Total 802
THEROS	Link Status:	Associated		ATHERO
	Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	0.0.0.0
	Network Type:	Ad Hoc	Current Channel:	2
Serve	er Based Authentication:	None	Data Encryption:	None
	Signal Strength:			Excellent

If you go to view the current status from PC1, the status for **Profile:** *Son* will be updated as shown below:

A Atheros Client Utility - Curren	t Profile: Son	? 🛛
Action Options Help		
Current Status Profile Management	liagnostics	
Total 80211 Profile Name:	Son	Total 80211
ATHEROS Link Status:	Associated	ATHEROS
Wireless Mode:	2.4 GHz 11 Mbps IP A	Address: 192.168.168.43
Network Type:	Ad Hoc Current C	Channel: 2
Server Based Authentication:	None Data End	cryption: None
Signal Strength:		Good
		Advanced

Alternatively, you may also go to the MS-DOS Prompt window of each PC to ping the other PC.

- 1. From the Start menu, go to Run...
- 2. Type in *cmd* and *c*lick on the **OK** button.

From the MS-DOS Prompt window of PC2, type *ping 192.168.168.11 –t*, to ping PC1.

When this screen appears: Pinging 192.168.168.11: bytes=32 time=2ms TTL=128 Pinging 192.168.168.11: bytes=32 time=2ms TTL=128

This indicates that the connection between PC1 and PC2 has been established successfully! You can now access to one another wirelessly!

For notebook

For setting up another wireless client, e.g. the notebook in the daughter's room, you may refer to the steps mentioned for configuring PC2.

If your other wireless clients are not using this network adapter, you may refer to the manual of these other adapters for details on Ad-hoc configuration.

Note:

All clients need to use the same SSID, channel, security mode and encryption key.

5.3 Infrastructure Mode

In infrastructure architecture, the wireless clients communicate through access points, which are devices that act as base station for all wireless communication. Data packets from the wireless clients are transferred to the access points before being transmitted to other hosts on the network. The number of wireless clients supported depends on the access points.



5.4 Configuration on Infrastructure Mode

In this example, two notebooks and PC2 act as wireless clients to communicate with the wireless AP. Once all configuration has been done, wireless clients with the same SSID as the AP will be able to access wirelessly to PC1 via the wireless AP.



For AP

Ensure that you have enabled the DHCP server in your access point and that your wireless clients are set to receive their IP address dynamically so that the wireless AP can assign an IP address to them. Note the wireless configuration settings of your access point as shown in the figure above.

For PC 2

- 1. Activate your utility.
- 2. Go to the **Profile Management** tab, click on the **Scan** button to look for the wireless AP.

Atheros Client Utility - Curre tion Options Help	nt Profile: default	?
Current Status Profile Management	Diagnostics	
Contraction default		New
		Modify
		Remove
		Activate
Details		
Network Type: Ad	Hoc	Import
Network Name 1 (SSID1): US	ie 3-CLIENT	Export
		Scan
Auto Select Profiles		Order Profiles

 Click on the **Refresh** button if your system is unable to detect your wireless AP. Once found, select the **Network Name (SSID)** used by the AP: *wireless-AP* and click on the **Activate** button to add it to your profile list.

Network Name (SSID)	¢3	Signal Strength	Channel	Wireless Mode
🕻 Weak Signal Test		1] 7 d8	3	2.4 GHz 54 Mbp
Veak Signal Test	=3	1] 4 dB	1	2.4 GHz 54 Mbp
Veak Signal Test		1] 4 dB	3	2.4 GHz 54 Mbp
Veak Signal Test		1]] 1 dB	3	2.4 GHz 54 Mbp
Veak Signal Test		11 32 dB	10	2.4 GHz 54 Mbc
L local-sales	=3	11 51 dB	6	2.4 GHz 54 Mbc
I PMD-28G	-3	1 35 dB	2	2.4 GHz 54 Mbc
wireless-AP	=3	11 30 dB	8	2.4 GHz 54 Mbp
Veak Signal Test	-3	1] 0 dB	11	2.4 GHz 54 Mbr
<				>

Notice that the SSID has already been pre-configured in this profile.

The SSID of both the wireless AP and the wireless client must be the same for them to communicate with one another.

4. Enter the **Profile Name**, e.g. *Workstation 2* for easy identification.

Profile Management		? 🛛
General Security Advance	bed	
Profile Settings Profile Name:	Workstation 2	
Client Name:	shawn	
Network Names		
SSID1:	wireless-AP	
SSID2:		
SSID3:		
		OK Cancel

5. Next, proceed to the **Security** tab. The wireless client must use the same security mode as the AP. In our example, select **WPA Passphrase** and click on the **Configure...** button.

neral Security Advanced			
Set Security Options			
○ WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	×
WPA/WPA2 Passphrase			
O 802.1x	802.1x EAP Type:	LEAP	*
O Pre-Shared Key (Static WEP)			
O None			
Continue N	Allow Association	in Mixed Calls	
conigure		o mixed Cells	

6. Enter the encryption key in the field provided. Please note that this key must be the same as the one that you had configured for your access point.

7. Click on the **OK** button to update the changes.



Proceed to your **Current Status** tab to monitor the connection between the access point and the wireless client (PC2).

A Atheros Cli	ent Utility - Currei	nt Profile: Workstati	on 2	? 🛛
Action Options	Help			
Current Status	Profile Management	Diagnostics		
Total 802.11	Profile Name:	Workstation 2		Total 80211
ATHEROS	Link Status:	Authenticated		ATHEROS
	Wireless Mode:	2.4 GHz 54 Mbps	IP Address:	192.168.168.43
	Network Type:	Infrastructure	Current Channel:	1
Serve	r Based Authentication:	None	Data Encryption:	AES
	Signal Strength:			Excellent
				Advanced N

Alternatively, you can also check the connection from the MS-DOS Prompt. From PC2, simply proceed to the **Start** Menu, **Run**... and type in *cmd*. Click on the **OK** button.

In the MS-DOS Prompt window, type *ping 192.168.168.1 –t*, whereby this IP address belongs to your access point.

```
When the screen appears:
Pinging 192.168.168.1: bytes=32 time=2ms TTL=128
Pinging 192.168.168.1: bytes=32 time=2ms TTL=128
Pinging 192.168.168.1: bytes=32 time=2ms TTL=128
```

This indicates that the connection between the access point and the wireless client has been established successfully!

For the rest of the workstations

Refer to the steps for configuring PC2.

If your other wireless clients are not using this network adapter, you may refer to the manual of these other adapters for details on Infrastructure configuration.

5.5 Profile Management

This option allows you to manage your profile(s), set your security options, and scan for other wireless networks.

n Options Help		
rent Status Profile Mana	agement Diagnostics	
wireless-AP		New
default	default Any	
		Remove
		Activate
Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name (SSID): Any	Export
Network Name 2 (SSI	D2): <empty></empty>	Scan
Network Name 3 (SSI	D3): <empty></empty>	

New...

Click on **New** button to create a new profile. Enter the profile name (a unique name to identify this profile), a client name and the SSID of the wireless network to connect to. Note that the **Client name** refers to the name that is registered to your PC. You can enter up to 3 different SSIDs in order of preference, per profile. We are using *ABC* as the profile name and *APP* as the SSID1.

	Profile Management	? 🛽
For details on how to set the different authentication and encryption types available under the Security Tab, kindly refer to Chapter 7 "Types of Authentication and Encryption mode"	General Security Advanced Profile Name: ABC Client Name: shawn Network Names SSID1: APP SSID2: SSID3:	

Click on the OK button to update the changes.

Notice that ABC has been added to the profile list.

ction Options	Help	ant Fromes why
Current Status	Profile Management	Diagnostics
wireless default Any ABC	AP	
NE		

Modify...

To modify an existing profile, select the profile that you wish to modify and click on this button. We are using profile: *Any* as an example.

ent Status Profile Manager	nent Diagnostics	
wireless-AP		New
default Any		Modify
ABC		Remove
		Activate
Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name (SSID):	Any	Export
Network Name 2 (SSID2)	<empty></empty>	Scan
Network Name 2 (CCID 2)	(emphi)	Jordan.

Remove

To delete an existing profile, select the particular profile that you wish to delete and click on this button. We are using profile: *default* as an example.

Note that the active profile (the profile that you are currently using) cannot be deleted!

	▲ Atheros Client Utility - Current Profile: Any	? 🛛
	Action Options Help	
	Current Status Profile Management Diagnostics	
	wireless-AP	New
	Cerault Se Any	Modify
	ABC	Remove
A ativa profile		Activate
Active profile	Details	
indicated by this	Network Type: Infrastructure Securitu Mode: None	Import
Icon cannot be	Network Name (SSID): adfa	Export
deleted!	Network Name 2 (SSID2): <empty> Network Name 3 (SSID3): <empty></empty></empty>	Scan
	Auto Select Profiles	Order Profiles

Activate

To activate a profile, select the profile and click on this button. We are using profile: *wireless-AP* as an example.

rent Status Profile Mana	gement Diagnostics	
wireless-AP		New
ABC		Modify
		Remove
		Activate
Details		N
Network Type:	Infrastructure	Import
Security Mode:	WPA Passphrase	- Fur est
Network Name (SSID):	wireless-AP	Export
Network Name 2 (SSIE)2): <empty></empty>	Scan
Network Name 3 (SSIE)3): <empty></empty>	

Once a profile is activated, this *icon* will appear next to the profile name: *wireless-AP*.

t heros Client Utility on Options Help rrent Status Profile Mana	- Current Profile: wireless-AP gement Diagnostics	?
		New
Any 45 ABC		Modify
		Remove
		Activate
Details		
Network Type:	Infrastructure	Import
Security Mode: Network Name (SSID)	WPA Passphrase wireless-AP	Export
Network Name 2 (SSI Network Name 3 (SSI	02): <empty> 03): <empty></empty></empty>	Scan
Auto Select Profiles		Order Profiles

-	
Export	

This function allows you to save the settings of your profile onto disk. Select the profile that you wish to save and click on this button. We are using profile: *ESSID* as an example.

Choose the folder to save to, enter the name under which to save the profile and click on the **Save** button.

Export P	rofile	? 🛛
Save in:	🧼 DOCUMENT (D:)	🔽 🥝 🌶 📂 🛄 •
i 1-Manı 4-M-M. b4a550 FMlist Outloo	ual 🚞 quotation- anage 📄 tools be7a7 k Express m Files	
File name:	ESSID	Save
Save as ty	pe: Config files (*.prf)	Cancel

Now, your profile is saved to your selected folder.

Import

This function allows you to retrieve a saved profile from disk. We are using profile: *ESSI*D as an example.

Go to the folder where you have saved your profile, select *ESSID.prf* and click on the **Open** button.

Import Prof	ile			? 🔀
Look in: 🕯	DOCUMENT (D:)	v 0		
1-Manual 4-M-Manai b4a550be FMlist Outlook Ex Program F	c quotation ge tools 7a7 CESSID kpress lies			
File name:	ESSID			Open L
Files of type:	Config files (*.prf)		•	Cancel

Notice that the profile: ESSID has been imported to the list of profiles.

🔨 Atheros Client Utility - C	urrent Profile: wireless-AP	? 🔀
Action Options Help		
Current Status Profile Managem	ent Diagnostics	
🝆 wireless-AP		New
ABC		Modify
ESSID		Remove
		Activate
- Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name (SSID):	ESSID	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	Julia
Auto Select Profiles		Order Profiles

Scan...

This function allows you to scan for wireless networks detected by the adapter.

Network Name (SSID)	1 St	uper XR	Signal Strength	Channel	Wirele +
i test			40 dB	52	5 GH:
i test			11 28 dB	48	5 GH;
VAP1			11 28 dB	48	5 GH2-
VAP2			11 28 dB	48	5 GH:
i test			11 41 dB	44	5 GH:
136-ftp-test	-		11 26 dB	40	5 GH:
i test			11 28 dB	36	5 GH;
i test			11 14 dB	36	5 GHa
i test			11 57 dB	36	5 GH:
i closed			-11 54 dB	13	246

Wireless-G Available Infrastructure and Ad Hoc Networks only displays Channel 1 to 13.

Av	ailable Infrastructure	and Ad I	Hoc Networks		1	2 🗙
						_
	Network Name (SSID)	¢3	Signal Strength	Channel	Wireless Mode	^
	i.		45 dB	10	2.4 GHz 54 Mbp	
	👗 Any	~ 3	18 dB	7	2.4 GHz 54 Mbp	
	💡 Any		1 33 dB	1	2.4 GHz 54 Mbp	
	i Any		11]8d8	10	2.4 GHz 54 Mbp	2
	1 Any		1 29 dB	1	2.4 GHz 54 Mbp	
	1 Any		11 36 dB	3	2.4 GHz 11 Mbp	
	🛔 Any		11 15 dB	10	2.4 GHz 54 Mbc	-
	1 Any	~ 3	11 33 dB	1	2.4 GHz 54 Mbp	
	local-sales	-3	1 34 dB	6	2.4 GHz 54 Mbr	
	1 DMD 2000	-2	al no an	n	DACIL- FAML-	≚
	`					
			Activate	Refresh	ОК	

The icons shown beside the Network Name (SSID) indicate the type of WLAN detected.



Infrastructure (AP) Network



Connected to Infrastructure (AP) Network



Ad-hoc Network



Connected to Ad-hoc Network



Click on the Refresh button to renew the list of wireless networks detected.

Click on the **OK** button to exit the window.

Order Profiles ...

If you have created several profiles, this function allows you to establish the priority order in which the network adapter should try to connect to a WLAN. If the network adapter is unable to connect to a wireless network through the 1st profile, it will then try to connect using the 2nd profile and so on.



When auto profile selection is enabled, the network adapter scans for available wireless networks and will connect to the highest priority profile that matches the networks detected.

To do so, simply click on the **Add** button from the **Available Profiles** list. Refer to the screen shown below.

Network Type:	Infrastructure
Security Mode:	WPA Passphrase
Network Name 1 (SSID1):	wireless-AP
Network Name 2 (SSID2):	<empty></empty>
Network Name 3 (SSID3):	<empty></empty>

Please note that you need AT LEAST TWO profiles to activate the **Auto Select Profiles** function; and that each of your profile must connect to at least one **Network Name (SSID)**.

Ame	Add
ABC ESSID	48
to Selected Profiles:	
	Move up
	Move down

Notice that when a selected profile has been added, it will be transferred to the **Auto Selected Profiles** list.

Select and click on the Add button to transfer another profile.

Any	Add a
ABC ESSID	- Add A
uto Selected Profiles:	
-	
wireless-AP	Move up
wireless-AP	Move up Move down
wireless-AP	Move up Move down Remove

You need to transfer at least two profiles to the **Auto Selected Profiles** list to activate the **Auto Select Profile** function.

5.5.1 Advanced Tab

This option allows you to configure the more advanced connection settings of your wireless client.

Wireless-G Profile Management Advanced



Transmit Power Level

Specifies the wireless transmit power to be used. Reducing the power level lowers the risk of interference with other nearby wireless devices and conserves battery power but decreases radio range.

Power Save Mode (Only applicable to Infrastructure mode)

This feature reduces power consumption by the PCI adapter. There are 3 options for this mode:

• Off

The power management is disabled and the card consumes full power from the computer.

Normal

The driver turns off the power to the adapter for brief periods over briefly spaced time intervals.

Maximum

The driver turns off power to the adapter for longer periods over more widely spaced time intervals.

The guideline for choosing between the **Normal** and **Maximum** options:

The PCI adapter wakes up more often and responds sooner to network requests in **Normal** mode than in **Maximum** mode; and the **Maximum** mode consumes less power than **Normal** mode.

Network Type

Select either **Infrastructure** if you are connecting to the WLAN using an access point or **Ad-hoc** if you are connecting directly to another computer equipped with a wireless adapter.

802.11b Preamble

The preamble is part of the IEEE 802.11b physical layer specification. It is mandatory for all 802.11b devices to support the long preamble format, but they may optionally support the short preamble. This PCI adapter supports both the short and long preambles.

Short & Long

This option allows communication with other 802.11b devices that support short preamble to boost the throughput.

Long Only

If your device is having trouble to communicate with other 802.11b devices, you may try to select the Long Only option.

Wireless Mode

Specifies 5GHz 54Mbps (Wireless-AG), 2.4 GHz 54 Mbps (Wireless-G), 2.4 GHz 11 Mbps (Wireless-G), Extended Range(XR) or QoS operation, in a wireless network where there is an access point.

The wireless adapter must match the wireless mode of the access point it associates to.

Wireless Mode when starting Ad-hoc Network (Only applicable to Ad-hoc mode)

Specifies the mode: **5GHz 54Mbps** (Wireless-AG), **2.4GHz 54Mbps** (Wireless-G), or **2.4 GHz 11Mbps** (Wireless-G), in which to start an ad hoc network if no network name is found after scanning for all available networks.

This mode also allows selection of the channel used by the wireless adapters in the Ad-hoc network. The channels available depend on the regulatory domain. If no other wireless adapters are found matching the ad hoc mode, this selection specifies the channel with which the adapter starts a new ad hoc network.

The wireless adapter must match the wireless mode and channel of the other wireless clients it associates to.

802.11 Authentication Mode (Only applicable to Infrastructure mode, after you have enabled the encryption mode)

Select which mode the wireless adapter uses to authenticate to an access point:

Auto

Causes the PCI adapter to attempt authentication using shared authentication. It then switches to open authentication if shared authentication fails.

• Open

Enables the PCI adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if its WEP settings match those of the access point.

• Shared

Allows the adapter to authenticate and associate only if it has the same WEP settings as the access point.

Note:

The network adapter authentication mode settings must match those of the AP it is trying to connect to for successful communication.

Chapter 6 Types of Authentication and Encryption mode

This chapter illustrates the different types of authentication and encryption that can be used in the wireless LAN.

6.1 Ad-hoc Network Security

In a Ad-hoc network, only Pre-shared key (Static WEP) can be configured.

rofile M	lanagem	ent				?
General	Security	Advanced				
Set 9	Security Op	otions				
	WPANYP	A2	WPA/WPA2 EAP Type	LEAP	~	
	WPA/WP	A2 Passphrase				
	802.1x		802.1x EAP Type	LEAP	~	
۲	Pre-Share	d Key (Static W	EP)			
0	None					
L C	Config		Allow Association	to Mixed Cells		
-	cong					
						ancer

Click on the **Configure**.. button and the following screen will appear:

 Hexadecimal (0-9, 4 	\-F)	ASCII Text (all keyb	oard character	s)	
incryption Keys			WE	P Keu S	lize:
Transmit I	Key		64	128	152
WEP Key 1: 💿	1234567890		•	0	0
WEP Key 2: 🔘			•	0	0
WEP Key 3: 🔘			•	0	0
WEP Key 4: 🔘			•	0	0

Key Entry Method

There are 2 types of key entries:

- Hexadecimal: Enter only digits 0 ~ 9 and letters a ~ f/A ~ F.
- ASCII Text: Enter any character that can be found on the keyboard.

WEP Key (1 ~ 4)

Defines a set of shared keys for network security. You must enter at least one WEP key to enable security using a shared key.

If the key that you entered is too long, the utility will truncate it to fit.

WEP Key size

Defines the length of each encryption key.

- 64-bit WEP: 10 hexadecimal or 5 ASCII Text
- 128-bit WEP: 26 hexadecimal or 13 ASCII Text
- 152-bit WEP: 32 hexadecimal or 16 ASCII Text

6.2 Infrastructure Network Security

Extensible Authentication Protocol (EAP) is used to authenticate network clients before letting them access the enterprise network. It allows the network administrator to create an arbitrary authentication scheme (such as EAP-TLS, etc) to validate network access.

6.2.1 EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) makes use of client-side and server-side certificates for mutual authentication.

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

Toffle Management General Security Advanced

WPA-WPA2

802.1x
 Pre-Shared Key (Static WEP)
 None

Profile Management

O WPA/WPA2 Pattohrate

Configure

veral Security Advanced

Set Security Options

WPA/WPA2
WPA/WPA2 Passphrase

802.1x
 Pre-Shared Key (Static WEP)
 None
 Configure

WPA/WPA2 EAP Type: EAP-TLS

WPA/WPA2 EAP Type EAP TLS

802.1x EAP Type: EAP-TLS

Allow Association to Mixed Cells

802.1x EAP Type: LEAP

1. You can select

WPA/WPA2 radio button (WPA stands for Wi-Fi Protected Access)

Or

802.1x radio button (802.1x enables 802.1x security.

If the access point that the wireless adapter is associating to has WEP set to **Optional** while the wireless adapter has WEP enabled, ensure that **Allow Association to Mixed Cells** is checked to allow association.

Note that this option is available only in 802.1x and Pre-Shared Key (Static WEP).

2. Choose EAP-TLS from the drop-down menu and click on the Configure... button.



NOTE

To enable this security, you must ensure that your PC has already downloaded its EAP-TLS certificates. Check with your system administrator for details.

3. If your system does not support EAP-TLS, the following message will pop up:

Profile Management (Security)	X
No user certificates were found on your computer. Machine certificates will be use Information For Domain Logon" checkbox is checked.	d for Domain Logon if the "Use Machine
ок	

If EAP-TLS is supported, select the appropriate certificate authority from the list. The server/domain name and the login name are filled in automatically from the certificate information.

4. Click on the **OK** button twice to activate the profile.

6.2.2 EAP-TTLS

EAP-TILS (Tunnel Transport Layer Security) authentication is an extension to EAP-TLS. It uses certificates and EAP-TLS to authenticate the server only and establish an encrypted tunnel. Then within that tunnel, the client authenticates to the server using either a username and password or a token card.

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

- 1. You can select file Management General Security Advanced WPA/WPA2 radio button Set Security Dotions WPA/WPA2 EAP Type: EAPTTLS WPAMPA2 WPA/WPA2 Parentyane 0 802 1+ 802.1x EAP Type: EAP-TLS O Pre-Shared Key (Static WEP) () None Configure Allow Association to Mared Cells Or Profile Management General Security Advanced Set Security Options 802.1x radio button O WPA/WPA2 WPA/WPA2 EAP Type: EAP-TTLS O WPA/WPA2 Passphrase 802.1x EAP Type: EAP-TTLS @ 802.1x O Pre-Shared Key (Static WEP) O None Allow Association to Mixed Cells Configure
- 2. Choose **EAP-TTLS** from the drop-down menu and click on the **Configure...** button.
- 3. Select the appropriate certification authority (CA) from which the server certificate will be downloaded from the **Trusted Root Certification Authorities** drop-down list.

- 4. The EAP username is pre-defined in the **User Name** field. IF not, specify your username (which is registered with the server) for EAP authentication. Enter your password in both the **Password** and **Confirm Password** fields.
- 5. Click on the **Settings...** button.

efine EAP-TTLS Configur	ation ?
Use Machine Information For Trusted Root Certification Auth	or Domain Logon writies
Microsoft Root Certificate Aut	hority
User Information for EAP-TTI User Name:	LS Authentication thomas_teo
Password:	•••••
Confirm Password:	•••••
s	ettings Cancel

- 6. Leave the **Specific Server or Domain** field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the CA listed previously. The login name is pre-defined in the **Login name** field.
- 7. Click the **OK** button.

Configuration Settings	? 🛛
Specific Server or Domain:	
Login Name:	thomas_teo
	OK Cancel

6.2.3 PEAP (EAP-GTC)

Similar to EAP-TTLS, PEAP (Protected EAP) also uses certificates to authenticate the server before creating an encrypted TLS tunnel through which the client can authenticate itself to the server using a challenge response authentication method such as EAP-GTC or EAP-MSCHAPv2.

To use PEAP-GTC security, access the **Security** tab in the **Profile Management** window.

1. You can select ofile Management General Security Advanced Set Security Options WPA/WPA2 radio button ● WPA/WPA2 WPA/WPA2 EAP Type: PEAP (EAP-GTC) O WPA/WPA2 Passphrase 802.1x EAP Type: EAP-TTLS O 802 1x O Pre-Shared Key (Static WEP) O None CAllow Association to Mared Cells Or Profile Management General Security Advanced 802.1x radio button Set Security Options ⊙ WPA/WPA2 WPA/WPA2 EAP Type: PEAP (EAP.GTC) WPA/WPA2 Passphrase O 802.1x 802.1x EAP Type: EAPITTLS O Pre-Shared Key (Static WEP) None

Configure_

Adow Association to Mixed Cells

- 2. Choose **PEAP-GTC** from the drop-down menu and click on the **Configure...** button.
- 3. Select the appropriate certificate authority (CA) from which the server certificate is downloaded from the **Trusted Root Certification Authority** drop-down list.

- 4. Enter your PEAP username (which is registered with the server) in the **User Name** field.
- 5. Specify whether you are using a **Token** or a **Static Password**. Click on the **Settings...** button.

Note that the Token can take the form of hardware token device or the Secure Computing SofToken Program (version 1.3 or later) to obtain and enter a one-time password for authentication.

147 A. M. J.	
Microsoft Hoot Certificate Au	thority 💽
Set Password	
O Token	
Static Password	
Use Windows User Name	and Password
User Information for PEAP (GTC) Authentication
User Information for PEAP (User Name:	GTC) Authentication thomas_teo
User Information for PEAP (User Name: Password:	GTC) Authentication thomas_teo

6. Leave the **Specific Server or Domain** field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the CA listed previously.

7. The login name will be pre-defined in the field provided. This login name is used for PEAP tunnel authentication. It will be filled in automatically as PEAP-*xxxxxxxxxx*, where xxxxxxxxxxx is the computer's MAC address. You may change the login name if needed. Click on the **OK** button to save your settings.

Configuration Settings	? 🛛
Specific Server or Domain:	[]
Login Name:	PEAP-00-80-48-10-00-9F
	OK Cancel

6.2.4 PEAP (EAP-MSCHAP V2)

MS-CHAPv2 uses a one-way cryptographic hash on the password and stores the hash value on the server. An authorized client knows the hash method used and reproduces it, sending the hashed password to the server during the challenge/response authentication. MSCHAPv2 is natively supported in Windows 2000 SP4 and Windows XP.

To use PEAP-MSCHAP V2 security, access the **Security** tab in the **Profile Management** window.

1. You can select

WPA/WPA2 radio button

802.1x radio button

Set Security Options			
· WPA/WPA2	WPA/WPA2 EAP Type:	FEAP (EAP MSCHAP V2)	•
WPA/WPA2 Passphrase			
O 802.1x	802.1x EAP Type:	PEAP (EAP-GTC)	
O Pre-Shared Key (Static WEP)			
O None			
Configure N	TAR A A A A A A A A A A A A A A A A A A	to Manel Calls	

Or

General Security Advanced	
Set Security Options	
O WPA/WPA2	WPA/WPA2 EAP Type: FEAP EAP-MSCHAP V2
WPA/WPA2 Passphrase	
@ 802.1x	802 1x EAP Type: PEAP (EAB MSCHAP V2)
O Pie-Shared Key (Static W	EPJ
O None	
Configure	Allow Association to Mixed Cells

- 2. Choose **PEAP (MS-CHAPV2)** from the drop-down menu and click on the **Configure...** button.
- 3. Enter your PEAP username and password (which are registered with the server) in the User Name and Password field respectively. Re-type the password in the Confirm Password field.
4. Click on the **Settings....** button.

<any></any>	
Use Windows User Name a	and Password
User Information for PEAP (E	AP-MSCHAP V2) Authentication
User Name:	thomas_teo
Password:	•••••

- 5. Leave the **Specific Server or Domain** field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the CA listed previously.
- 6. Click the **OK** button.

Configuration Settings	?×
Specific Server or Domain:	
Login Name:	thomas_ted
	OK Cancel

6.2.5 LEAP

Lightweight Extensible Authentication Protocol (LEAP) security requires all infrastructure devices (e.g. access points and servers) to be configured for LEAP authentication.

To use LEAP security, access the **Security** tab in the **Profile Management** window.

- 1. You can select rofile Management General Security Advanced WPA/WPA2 radio button Set Security Options WPA/WPA2 EAP Type: LEAP WPA/WPA2 O WPA/WPA2 Passphrase 802 1x EAP Type: PEAP (EAP MISCHAP V2) O 802.1x O Pre-Shared Key (Static WEP) O None Configure. Allow Association to Mixed Cells Or file Management 802.1x radio button neral Security Advanced Set Security Options WPA/WPA2 EAP Type O WPA/WPA2 WPA/WPA2 Passolyace @ 802.1x 802.1x EAP Type: LEAP v O Pre-Shared Key (Static WEP) None Configure Allow Association to Mixed Cells
- 2. Choose LEAP from the drop-down menu and click on the **Configure...** button.
- 3. You may set your username and password to:
 - Use Temporary User Name and Password

Each time your PC reboots, you will be required to enter your LEAP username and password in order to be authenticated and obtain access to the network.

- Use Saved User Name and Password.

Authentication is obtained using a saved username and password (registered with the server) so you will not be required to enter your LEAP username and password, each time your PC reboots.

Temporary User Name and Password

1. The login page will pop up as shown below. Fill up the respective fields and click on the **OK** button twice.

ter Wireless	Network Password	?
	Please enter your LEAP username and password to log on to the wireless network	OK Cancel
User Name :	sampleUserName	
Password :		
Log on to :	sampleDomain	
Card Name :	Atheros USB 2.0 Wireless Network Adapter	
Profile Name :	Default	

Next, the system will start the LEAP authentication.

LEAP Authentication Status	? _ X
Card Name: Atheros Wireless Network Adapter Profile Name: default	CISCO [®] Compatible
Steps Status	
-> 1. Starting LEAP Authentication Proces	ising
2. Checking Link Status	
3. Renewing IP address	
 Detecting IPX Frame Type 	
5. Finding Domain Controller	
☐ Show minimized r	est time Cancel

Saved User Name and Password

- Enter the username, password and re-enter password in Confirm Password field. (Optional) You may enter a specific domain name, which will be passed to the server.
- 2. Enter the LEAP Authentication Timeout Value (between 30 and 500 seconds) to specify how long LEAP should wait before considering an authentication as failed, and sending an error message. The default is 90 seconds.
- 3. Click on the **OK** button.

Check the Include Windows Logon Domain with User Name option to automatically send your Windows login domain together with your user name to the RADIUS server. (Default)

Check the No Network Connection unless User is logged in option to force the wireless adapter to disassociate after you log off.

Always Resume the Secu	ire Session
User Name and Password S	Settings
C Use Temporary Use	r Name and Password
C Automatically F	Prompt for User Name and Password
C Manually Prom	pt for User Name and Password
 Use Saved User Nar 	me and Password
User Name:	sampleUserName
Password	•••••
Confirm Password:	
Domain:	sampleDomain
Include Windows L	ogon Domain with User Name
🖉 🔽 No Network Conne	ction Linless Liser is Logged in
	(uthentication Timonut) (alua (in accords)
+	Authentication Fillebox Value (in seconds)
	OK C

6.2.6 EAP-FAST

Extensible Authentication Protocol-Fast Authentication via Secure Tunneling performs the similar authentication methods as EAP-TLS and PEAP. Comparing EAP-TLS and PEAP, EAP-FAST offers a more efficient and better support for security provisioning, and minimizes the number of mechanisms required for asymmetric cryptography and certificate validation. It also provides highlevel protection from network attacks such as man-in-the-middle, authentication forging, weak IV attack (AirSnort), packet forgery (replay attack), and dictionary attacks.

EAP-FAST gives support to users who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types and supports password expiration and change.

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

1. You can select WPA/WPA2 radio button
Or
Potile Management
Image Southy Options
I

802.1x radio button

eneral Security Advanced		
Set Security Options		
O WPA/WPA2	WPA/WPA2 EAP Type: EAPFAST	1.0
O WPA/WPA2 Passphras		
@ 802.1x	802.1x EAP Type: EAP FAST	~
O Pre-Shared Key (Static V	VEP)	
O None		
Configure	Allow Association to Mixed Cells	

2. Choose **EAP-FAST** from the drop-down menu and click on the **Configure...** button.

- 3. You may set your username and password to:
 - Use Temporary User Name and Password

Each time your PC reboots, you will be require to enter your EAP-FAST username and password in order to be authenticated and obtain access to the network.

- Use Saved User Name and Password.

Authentication is obtained using a saved username and password (registered with the server) so you will not be require to enter your EAP-FAST username and password each time your PC reboots.

Temporary User Name and Password

4. The login page will pop up as shown below. Fill up the respective fields and click on the **OK** button twice.

ter Wireless	Network Password	?
	Please enter your EAP-FAST username and password to log	ОК
	on to the wireless network.	Cancel
User Name :	sampleUserName	1
Password :		
Log on to :	sampleDomain	
Card Name :	Atheros USB 2.0 Wireless Network Adapter	
Profile Name :	Default	

Next, the system will start the EAP-FAST authentication.

EAP-FAST Authentication Status		? _ 🗆 🗙
Card Name: Atheros Wireless Networ Profile Name: default	ik Adapter	
Steps	Status	
-> Starting EAP-FAST Authentication	Processing	
2. Checking Link Status		
3. Renewing IP address		
4. Detecting IPX Frame Type		
5. Finding Domain Controller		
☐ Show n	ninimized next time	Cancel

Saved User Name and Password

5. Enter the username, password and re-enter password in **Confirm Password** field.

(Optional) You may enter a specific domain name, which will be passed to the server.

 Enter the EAP-FAST Authentication Timeout Value (between 30 and 500 seconds) to specify how long EAP-FAST should wait before considering an authentication as failed, and sending an error message. The default is 90 seconds.

7. Click on the **OK** button.

Check the Include Windows Logon Domain with User Name option to automatically send your Windows login domain together with your user name to the RADIUS server. (Default)

Check the **No Network Connection unless User is logged in** option to force the wireless adapter to disassociate after you log off.

EAP-FAST Settings	? 🔀
Username and Password Settings Use Temporary User Name and Password Use Windows User Name and Password Automatically Prompt for User Name and Password Manually Prompt for User Name and Password	
Use Saved User Name and Password	
User Name:	
Password:	
Confirm Password:	
Domain:	
 ✓ Include Windows Logon Domain with User Name ✓ No Network Connection Unless User Is Logged In Authentication Timeout Value (in seconds) 	
Protected Access Credentials (PAC)	
Allow Automatic PAC Provisioning for this Profile Select a PAC Authority to use with this profile	
Select Mor	e
OK Car	ncel

Protected Access Credentials (PAC)

The PAC is a unique shared credential used to mutually authenticate client and server. It is associated with a specific client username and a server authority ID.

EAP-FAST provides two ways to supply a client with a new PAC:

Automatic PAC provisioning

A new PAC will be sent to the client over a secured network connection.

• Manual PAC provisioning This requires the PAC file to be manually installed onto the client.

- Tick the Allow Automatic PAC Provisioning for this Profile checkbox if you want to allow automatic PAC provisioning for the profile you are using. Otherwise user access will be denied and PAC provisioning must be performed manually.
- To select a PAC Authority for the profile you are using, click Select More. Then you will be asked to decide whether to use a Public or Private PAC Authority.

Protected Access Credentials (PAC)		
Select a PAC Authority to use with this profile		Select More
	ОК	Cancel

10. Next, click **Import** to get the PAC from your own directory to add in the list under the **Select the PAC** section. Click **OK**.

Select EAP-FAST	PAC	? 🛽
Select the PAC St	ие	
O Public	O Private	
Select the PAC		Import
		Delete
		ОК
		Cancel



NOTE

After the PAC has been successfully provisioned, EAP-FAST authentication is restarted to gain network access. Therefore, after a successful PAC provisioning, an EAP failure will occur to terminate the previous EAP-FAST session and establish an authenticated wireless connection using a new PAC.

6.2.7 WPA/WPA2 Passphrase

WPA/WPA2 Passphrase is also known as WPA-PSK (Pre-shared Key). It provides strong encryption protection for home/SOHO users who do not use an enterprise authentication server.

1. Click on the **WPA/WPA2 Passphrase** radio button and click on the **Configure...** button.

orne m	anagem	ent			الگا
Seneral	Security	Advanced			
Set 5	Security Op	tions			
0	WPA/WP	A2	WPA/WPA2 EAP Type:	LEAP	~
۲	WPA/WP	A2 Passphrase			
0	902.1x		802.1x EAP Type:	EAP-FAST	~
0	Pre-Share	d Key (Static WEP)	1		
0	None				
-	0.1		The Average		
	Configu	te G	Allow Atsociation	to Maled Cela	
					OK Cancel

2. Enter the password and click on the **OK** button.

Define WPA/WPA2 Pre-Shared Key	? 🛛
Enter a WPA/WPA2 passphrase (8 to 63 ASCII or 64 hexa	cimal characters)
1234567890	
	OK Cancel

Note:

The WPA/WPA2 Passphrase must match that used by the AP/other wireless clients in the network.

6.2.8 Pre-shared Key (Static WEP)

Wired Equivalent Privacy is a security protocol that allows the wireless client adapter to communicate ONLY with access points or other wireless clients that have the same WEP key.

WEP Key is categorized into two types: Hexadecimal and ASCII. Hexadecimal values consist a to f and numbers 0 to 9 whereas ASCII values consist of alphanumeric characters a to z; 0 to 9.

To define pre-shared encryption keys,

1. Choose the **Pre-shared Key (Static WEP)** radio button and click the **Configure...** button to fill in the encryption key.

eneral	Security	Advanced			
Set S	Security Op	otions			
0	WPA/WP	A2	WPA/WPA2 EAP Type:	LEAP	~
0	WPA/WP	A2 Passphrase			
0	802.1x		802.1x EAP Type:	EAP-FAST	×.
۲	Pre-Share	d Key (Static WE	(P)		
0	None				
	0.6	121		- March Calls	
	Configu	ne 10	Allow Association	to Mixed Cells	
			7		
_					
				(OK Car

If the access point that the wireless adapter is associating to has WEP set to **Optional** while the wireless adapter has WEP enabled, ensure that **Allow Association to Mixed Cells** is checked to allow association.

Note that this option is available only in 802.1x and Pre-Shared Key (Static WEP).

2. Enter your WEP key and click on the **OK** button.

efine Pre-Sha	ired Key	/5			?
Key Entry	⊙ He	kadecimal (0-9, A-F)	O ASCII Text (all keyboard characte	ers)
Encryption Key	s Tranomit) (/E)	P Kou Sizo:
	Key			64	128 152
WEP Key 1	۲	1234567890		•	00
WEP Key 2				۲	00
WEP Key 3				•	00
WEP Key 4					00
				ОК	Cancel

WEP Key size

- 64-bit WEP: 10 hexadecimal or 5 ASCII Text
- 128-bit WEP: 26 hexadecimal or 13 ASCII Text
- 152-bit WEP: 32 hexadecimal or 16 ASCII Text

Appendix I Unplug PCI Adapter from the System

To safely remove your PCI adapter from your system,

1. Go to the **Start** menu to select **Shutdown**.



- 2. Power off your PC and switch off the power from the main power supply.
- 3. Remove the back cover of the PC.
- 4. Next, carefully unplug the PCI adapter from the PCI slot of your PC.
- 5. Replace the back cover and turn on your PC.

Appendix II Un-install

Please note that in case there is a software upgrade for the network adapter, you will need to un-install the current software version before installing the new software.

When you un-install the software, any existing profiles will be removed. If you want to re-use your profiles, please refer to **Section 5.2 Profile Management Tab** for further details on how to export a profile to disk. You are advised to close all programs and to leave the network adapter in the PCI slot of your PC before un-installing current software.

- 1. From your **Start** menu, go to **Settings, Control Panel** and then click on the **Add or Remove Programs** icon.
- 2. Highlight the Atheros Client Installation Program and click on the Change/Remove button.



 Wait until you see the Atheros Client Installation Program screen. Select Uninstall the previous installation. Then click on the Next> button to proceed.

			a new
The installation program has detected that do?	a previous installatio	n exists. What do	you want to
 Update the previous installation 			
O Uninstall the previous installation			

4. The prompt screen appears to notify you that the uninstall option requires the system to be rebooted at the end of the uninstall process. Click on the **Yes** button to proceed.

Questio	a de la companya de l	×
?	The option you have selected requires the system to be rebooted at the end of the operation. Do you want continue?	to
	Yes No	

5. Your system will prompt you to confirm whether you want to remove the application completely. Click **OK** to proceed.



6. You will be asked to decide whether to remove the device driver or not. Click on the **Yes** button to accept.



7. The uninstall process will then begin. Soon the prompt screen will appear informing you that the uninstall process is successful, and that your system needs to be rebooted.

Atheros	: Client Installation Program 🛛 🛛 🕅
	The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Click OK to reboot the system.

8. Click **OK** to reboot the system.

Appendix III Certificate Application for WPA mode

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancement that strongly increases the level of data protection (encryption) and access control (authentication) in your wireless network. The technical components of WPA include Temporal Key Integrity Protocol (TKIP) for dynamic key exchange, and 802.1x for authentication.

WPA requires a RADIUS Server to complete the authentication among wireless stations and Access Points. Typically, this mode is used in an enterprise environment. WPA-PSK does not require a RADIUS Server and is very convenient for home/SOHO users. In this chapter, we will explain how to apply for a certificate in order to access to a wireless network using WPA mode.

NO	TE
_	

NOTE

For Windows XP users with Service Pack 1 (SP1), you need to upgrade to SP2, available from the Microsoft website or to install the two patch files provided in the Product CD.

Overall procedures to apply certificate for WPA mode

- Install Windows XP Service Pack 2 or patch files for Service Pack 1.
- Apply certification via Internet Browser
- Become domain member

AIII-1 Installing Window XP Service Pack Patch File

(For Windows XP users)

To check whether you have already installed Windows XP SP2, go to **My Computer**, right click and select **Properties**.





If you are using the Windows XP SP1 and do not intend to upgrade to SP2, you will need to install the two patch files provided in the Product CD.

After ensuring that you have installed Windows XP SP1, insert the Product CD into your CD-ROM drive. Go to Windows Explorer and click on your CD-ROM drive icon. From your software folder, select the **WPA_Patch** folder and install both files: *WindowsXP- Q815485_WXP_SP2_x86_ENU.exe* followed by *WindowsXP-KB826942-x86-ENU.exe*.



AllI-2 Installing certificate on your server

If you are using Microsoft Certificates services,

1. Click on the **Install this certificate** link in the window to start the installation.

Microsoft Certificate Services - Microsoft Internet Explorer	
Elle Edit View Favorites Iools Help	27
😋 Back 🔹 💿 🗧 📓 🏠 🔎 Search 🤺 Favorites 🜒 Media 🤣 🔗 - 🌺 🚍	
Address 🙆 http://192.168.88.26/certsrv/certfnsh.asp	🔽 🛃 Go 🛛 Links 🎽
<i>Microsoft</i> Certificate Services test Certificate Issued	Home
The certificate you requested was issued to you.	

2. Click on the **Yes** button on the pop up window to continue with the installation.

Potentia	al Scripting Violation
1	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
_	<u>Yes</u> <u>N</u> o

3. To add the certificate to the Root Store, click on the Yes button.

Root Ce	rtificate Store 🛛 🔀
1	Do you want to ADD the following certificate to the Root Store? Subject : test, aaa, workgroup, aa, aa, CN, asdf@test.com Issuer : Self Issued Time Validity : Thursday, April 15, 2004 through Saturday, April 15, 2006 Serial Number : 25089187 7818439B 4038DA5B A924B4AA Thumbprint (sha1) : D5709557 B078B014 E40F2568 34966067 593BE0F8 Thumbprint (md5) : AF45D0FF DC4D7953 EE31B864 6C529AB6 <u>Yes</u>

4. The following window will appear showing that the certificate has been successfully installed into your PC.



AllI-3 Applying for Client Certifications

If you have installed Microsoft SP2 or Microsoft XP SP1 with the 2 patch files provided on the Product CD, you are now ready to apply for a certificate for your wireless client.

At this stage, ensure that your wireless client has connectivity to the CA server. You should disable your key encryption.

- 1. Open your Internet browser; enter e.g. *http://192.168.88.26/certsrv* where 192.168.88.26 is the server's IP address.
- Next, you need to connect to your server in order to get a certification. Enter your username and password that are provided by your system administrator.

Connect to 192	2.168.88.26 🛛 😨 🔀
R	GR .
Connecting to 19	2.168.88.26
User name:	🖸 user1 💌 🔐
Password:	••••
	Remember my password
-	OK Cancel

 Once you get connected to your server, the following screen shot will appear. Select the Request a certificate radio button and click on the Next> button. Follow the instructions shown on the screen.



The screen below will appear to indicate that a certificate has been successfully issued to your PC.

Microsoft Certificate Services - Microsoft Internet Explorer	
Elle Edit View Favorites Jools Help	A *
🔇 Book • 🔘 - 🖹 🖻 🐔 🔎 Search 👷 Favorites 🕐 Media 🥝 🔗 🔩 🚍	
Address 🗃 http://192.168.08.26/certsrv/certrmpn.asp	🕶 🛃 Go Unis **
Microsoft Certificate Services teat	Heme
Certificate Installed	
Your new certificate has been successfully installed.	

 To confirm whether you have received your certificate, go to your web browser and select Internet Options... from your Tools pull down menu.



5. Go to the **Content** tab and click on the **Certificates...** button. Notice that your username is in the listing. This shows that the certificate has been issued to you.

Issued To Issued By Expirato Friendly Name User1 test 5/18/2005 <none> mport Export Eemove Advance wthforke intended approass</none>	rsonal Other Pe	sople I	ntermediate Certifica	tion Authorities	Trusted	Root Certification
Inseed for Logination. The by head of Logination. The by head of Logination of Loginat	Icourd To	er researce	Terrind Ru	Evoirat	- Er	ondki Nomo
ngort Export Eemove Advanc	Eluser1		test	5/18/20	05 </td <td>one></td>	one>

All-4 Becoming a domain member

Next, you need to join the correct network domain so that you can communicate with the access point connected to your server.

- From the My Computer icon on your desktop, right click and go to Properties.
- 2. Go to the **Computer Name** tab and select **Change...** button as shown in the screen on the right.



3. From the **Member of** section, select the **Domain**: radio button and enter the name of your domain. In this example, we are using *test* as the domain name.

Computer Na You can chang computer. Char	me Change e the name a ges may affe	es Ind the mer Ind access I	nbership of o network	this resources.
Computer name	E.			
test1				
Full computer n test1. Member of Omain:	ame:			More
test				
O <u>W</u> orkgro	ар: ROUP			
				Cancel

- 4. Next, you need to enter your username and password again for verification. Please note that your system administrator provides this information.
- 5. Click on the **OK** button to proceed.

Computer Nan	ne Changes	? 🛛
80 .		
Enter the name	and password of an accoun in	t with permission
to join the domai	«њ	
User name:	🖸 user1	*

6. When done, a message will appear as shown below. You may need to restart your computer for the changes to take effect.

Comput	er Name Changes	X
į)	Welcome to the test d	omain.
	ОК	

Appendix IV Wireless Zero Configuration Utility

If your computer is running under the Windows XP operating system, you can opt to configure the **Wireless Network Connection** from your Windows XP operating system, instead of the Atheros Utility. You need to exit from the Atheros Utility before accessing to Windows XP's Wireless Zero Configuration Utility.

AIV-1Enable Wireless Zero Configuration Utility

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

 From the system tray, right click on the Wireless Network icon and select View Available Wireless Networks option.



2. Click on the **Change advanced settings** option on the left-hand column.



3. Select the check box Use Windows to configure my wireless network settings to activate Wireless Zero Configuration Utility.

eneral Wireless Networks	Advanced
Use Windows to configure	my wireless network settings
Available <u>n</u> etworks:	
To connect to, disconnect fr about wireless networks in ra	om, or find out more information ange, click the button below.
	View Wireless Networks
1	1 Parentering
	Move up Move down
Add	Move <u>up</u> Move <u>down</u>

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

- SSID
- Security Keys
- Ad-hoc settings

When the Wireless Zero Configuration Utility is in use, a pop-up message is displayed on the Utility when you attempt to create or edit a configuration profile from the **Profile Management** tab of the Atheros utility.

Atheros Client Utility		
This Device is controlled by the Windows XP Security and other settings from this profile	Automatic Wireless Network Configuration. It ma	y override Network Name,



CAUTION

If you activate BOTH (not recommended) the Wireless Zero Configuration Utility and the Atheros Utility simultaneously, the Profile setting configured by the Atheros Utility will be overridden by those of the Wireless Zero Configuration Utility.

AIV-2Disable Wireless Zero Configuration Utility

To turn Wireless Zero Configuration Utility off on Windows XP,

- 1. Open the Wireless Zero Configuration Properties dialog box.
- 2. Clear the check box Use Windows to configure my wireless network settings.
- 3. When this check box is cleared, all profile settings will be controlled by the utility.

Appendix V Technical Specifications

Network Protocol,	Standards and Electrical Emissions
Industry Standards (WLP54G)	IEEE 802.11gIEEE 802.11b
Industry Standards (WLP54AG)	 IEEE 802.11g IEEE 802.11b IEEE 802.11a
	Performance
Frequency Band (WLP54G) IEEE 802.11g: IEEE 802.11b:	2.312 ~ 2.484GHz 2.312 ~ 2.472GHz
Frequency Band (WLP54AG) IEEE 802.11g: IEEE 802.11b: IEEE 802.11a:	2.312 ~ 2.484GHz 2.312 ~ 2.472GHz 5 ~ 5.850GHz
Modulation	 Binary Phase Shift Keying (BPSK) Quadrature Phase Shift Keying (QPSK) Complementary Code Keying (CCK) 16 QAM 64 QAM DBPSK DQPSK
Antenna Type	External 2dBi antenna and an SMA-type connector
Network Interface	PCI 2.3 compatible

Operating Channel (WLP54G)	 802.11g 11 Channels (US & Canada) 13 Channels (Europe, Asia) 14 Channels (Japan)
Operating Channel (WLP54AG)	 802.11g 11 Channels (US & Canada) 13 Channels (Europe, Asia) 14 Channels (Japan)
	 802.11a 13 Channels (US & Canada) 19 Channels (Europe, Asia) 10 Channels (Japan)
Drivers/Operating system Supported	Windows XP/2000
Wireless Transmission Power (WLP54G 3CA1100, 3CA1300, 3CA1100S, 3CA1300S, 3BA1100, 3BA1300)	
IEEE 802.11b: IEEE 802.11g:	20 dBm typical 19 dBm typical
Wireless Transmission Power (WLP54G 3CA1100P23, 3CA1300P23)	
IEEE 802.11b: IEEE 802.11g:	23 dBm typical 19 dBm typical
Wireless Transmission Power (WLP54AG 3CA1100, 3CA1300, 3CA1100S, 3CA1300S)	
IEEE 802.11b: IEEE 802.11g: IEEE 802.11a:	20 dBm typical 19 dBm typical 17 dBm typical

Receive Sensitivity	Up to –90dBm
Wireless Security	 64-bit/128-bit/152-bit WEP IEEE 802.1x support – EAP-TLS, EAP-TTLS, PEAP-GTC, PEAP-MSCHAPv2, LEAP, EAP-FAST WPA/WPA2, WPA-PSK
Wireless Operating Range (WLP54G 3CA1100, 3CA1300, 3CA1100P23, 3CA1300P23, 3BA1100, 3BA1300)	
IEEE 802.11g: IEEE 802.11b:	80m (54Mbps outdoor), 20m(54Mbps indoor) 300m (11Mbps outdoor), 100m (11Mbps indoor)
Wireless Operating Range (WLP54AG 3CA1100, 3CA1300)	
IEEE 802.11g: IEEE 802.11b:	80m (54Mbps outdoor), 20m(54Mbps indoor) 300m (11Mbps outdoor), 100m (11Mbps indoor)
IEEE 802.11a:	85m (54Mbps outdoor), 20m(54Mbps indoor)
Wireless Operating Range (WLP54G 3CA1100S, 3CA1300S)	
, IEEE 802.11g:	80m (108Mbps outdoor), 20m(108Mbps indoor)
IEEE 802.11b:	300m (11Mbps outdoor), 100m (11Mbps indoor)
Wireless Operating Range (WLP54AG 3CA1100S, 3CA1300S)	
IEEE 802.11g:	80m (108Mbps outdoor), 20m(108Mbps indoor)
IEEE 802.11b:	300m (11Mbps outdoor), 100m (11Mbps indoor)
IEEE 802.11a:	85m (54Mbps outdoor), 20m(54Mbps indoor)

Physical and Environment		
Environmental Requirements		
Operating temperature:	0°C to 50°C	
Storage temperature:	-20°C to 70°C	
Operating humidity:	10% to 70% RH	
Non-operating humidity:	5% to 90% RH	
Power Consumption	3.3V DC, 500mA	
	350mA Tx	
	250mA Rx	
Physical Dimension	120mm x 64.5 mm x 1.6 mm (LxWxD)	
-		