PHILIPS

User’s Manual

802.11 Combo MiniPCI WLAN Card,
PH11107-X

Version1.0
29 July 2002

Notice

Philips Electronics North America [Corporation] shall not be liable for technical or editorial errors or omissions contained herein. The information in this guide is subject to change without notice ©2002 Philips.

Except for use in connection with the accompanying Philips product, no part of this guide may be photocopied or reproduced in any form without prior written consent from Philips. Philips and the Philips logo are trademarks of Philips Electronics North America.

Microsoft, Windows®, Windows® NT, and other names of Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. All other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

TABLE OF CONTENTS

1 ABBREVIATIONS

API	Application Programming Interface
MAC	Media Access Control
SE	Second Edition
UI	User Interface
WEP	Wired Equivalent Privacy

2 INTRODUCTION

The Philips Wireless Local Area Network (WLAN) Interface enables high-speed access without wires to network assets. The interface uses the IEEE 802.11a protocol to enable communications between the host computer and other computers, using the 5GHz ISM Radio Band (**U-NII Band)**for the communications medium. The host computer uses Philips Wireless LAN for communications in the same way that it would use an Ethernet Network Interface Card.

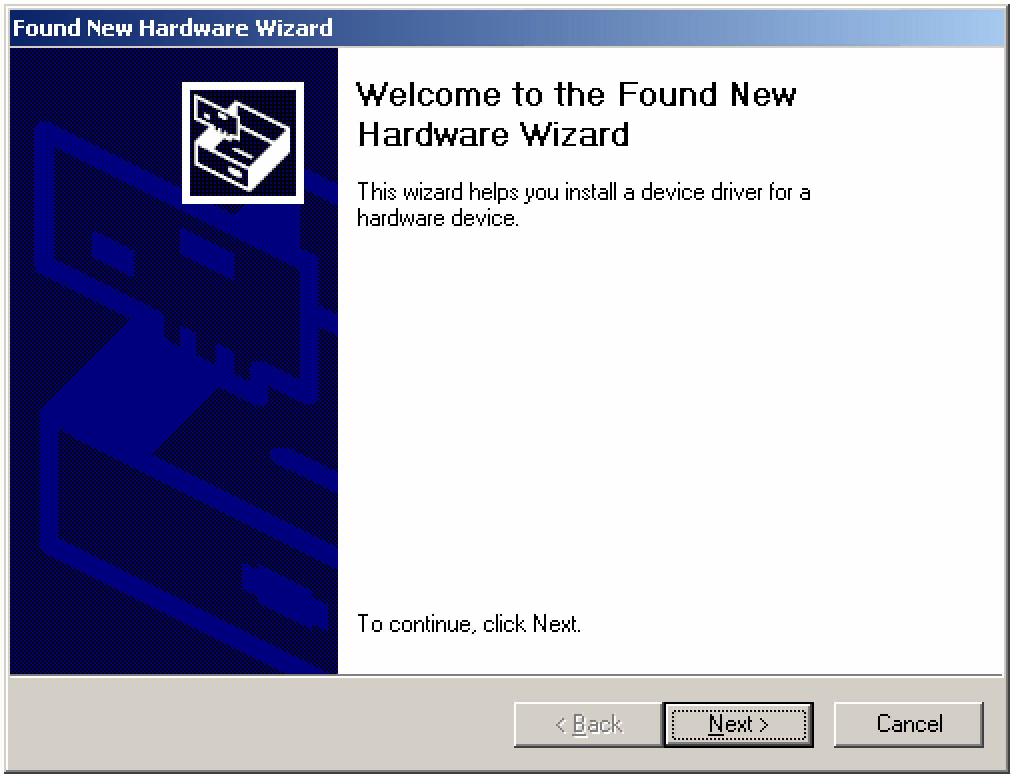
The Philips 802.11a/b MiniPCI Card WLAN is a Windows application that allows the user of a computer equipped with a Philips WLAN Interface to configure and display the current configuration and status.

Driver installation works with Windows® 98 SE, Windows® Me, Windows® 2000, Windows® NT 4.0, and Windows® XP operating systems.

3 DRIVER INSTALLATION

Install Philips miniPCI 802.11a/b card. Laptop is turn off during installation. Once the card is installed, turn on the laptop.

1. Wait for the following dialog box to display, and click Next to continue.



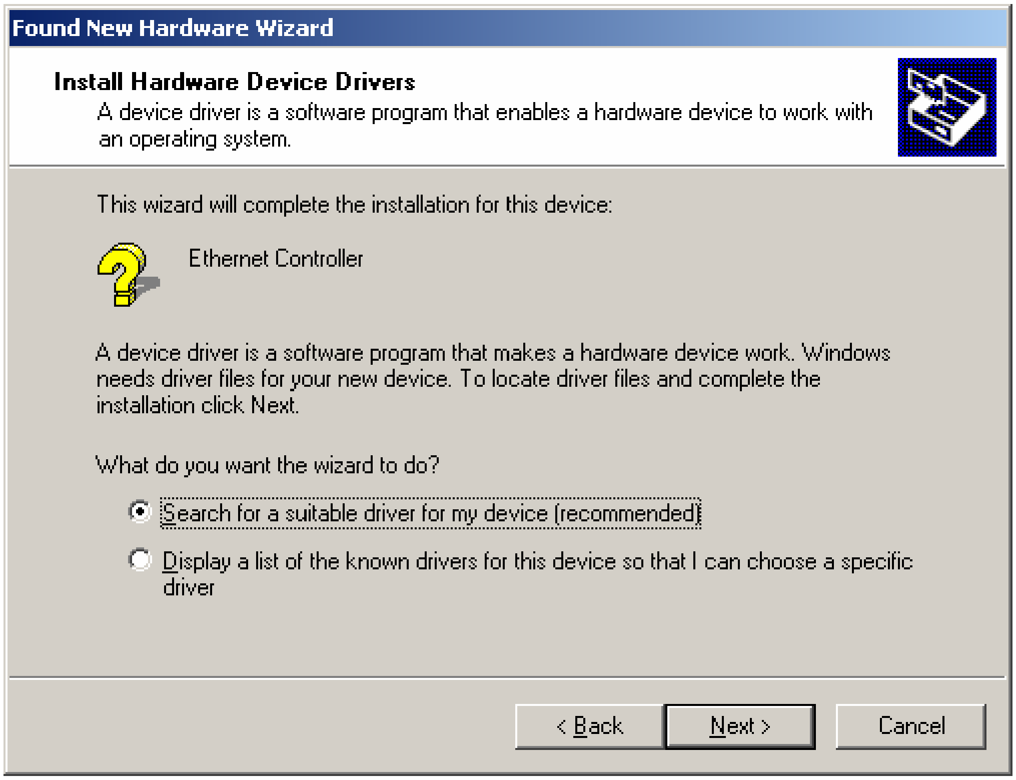
Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install a device driver for a hardware device.

To continue, click Next.

2. Choose “Search for a suitable driver for my device (recommended),” and click Next.



Install Hardware Device Drivers

A device driver is a software program that enables a hardware device to work with an operating system.

This wizard will complete the installation for this device:

Ethernet Controller

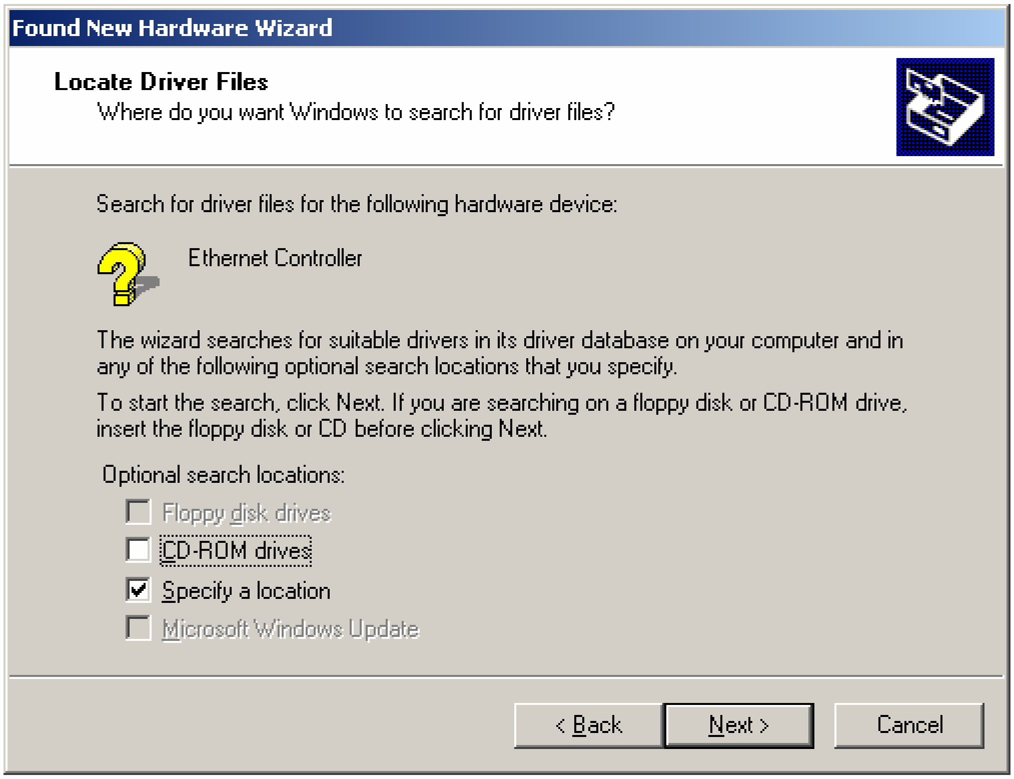
A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.

What do you want the wizard to do?

● Search for a suitable driver for my device (recommended)

○ Display a list of the known drivers for this device so that I can choose a specific driver

3. Insert the CD in your CD-ROM drive. Choose “Specify a location” under “ Optional search locations,” and click Next to continue.



Found New Hardware Wizard

Locate Driver Files

Where do you want Windows to search for driver files?

Search for driver files for the following hardware device:

Ethernet Controller

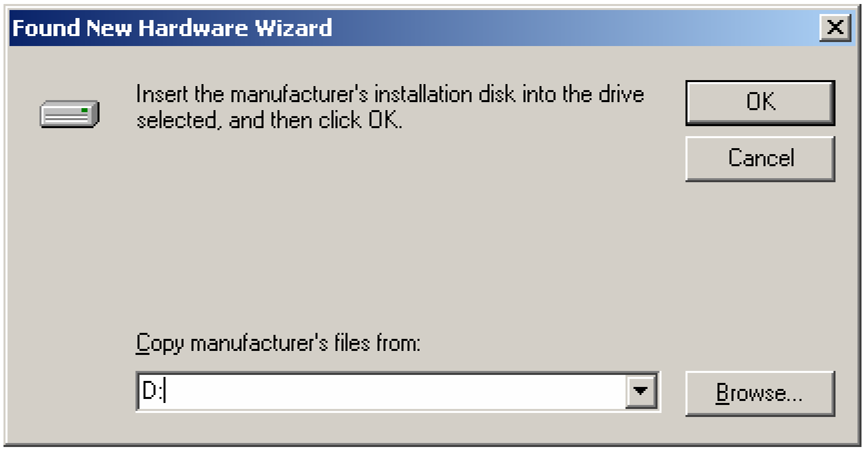
The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.

To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.

Optional search locations:

☐ Floppy disk drives
☐ CD-ROM drives
☑ Specify a location
☐ Microsoft Windows Update

4. Browse to the location where the NDIS driver is located (assuming D is the CD-ROM drive), the default folder is D: .Click OK to continue.



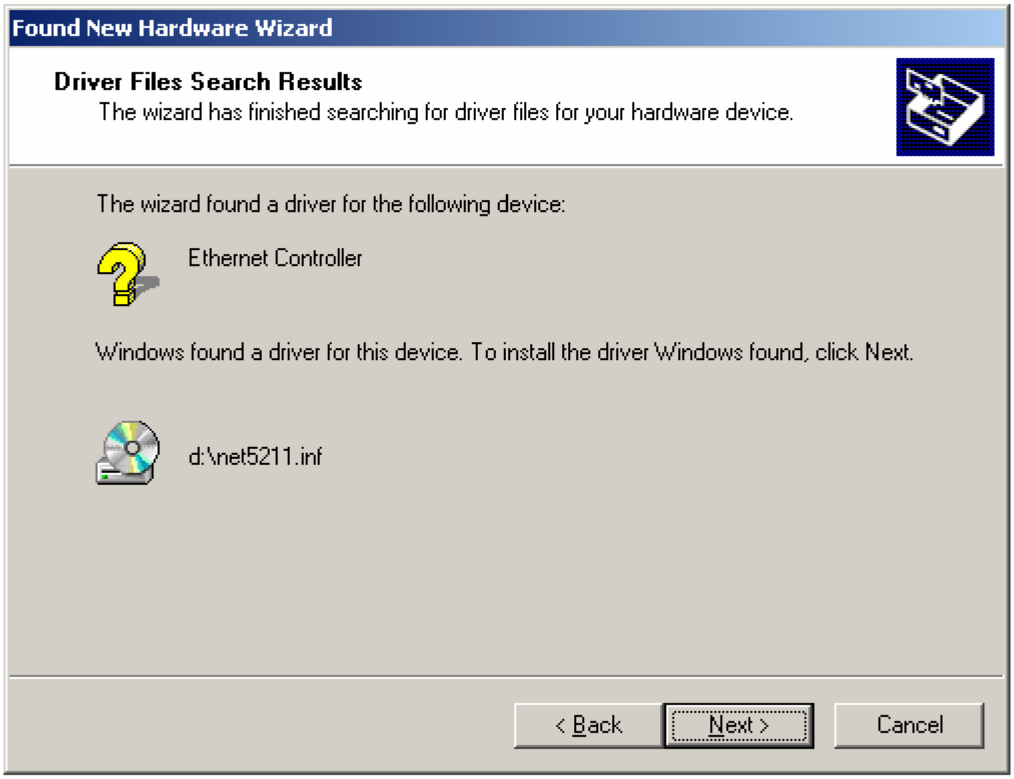
Found New Hardware Wizard

Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from:

D:

5. When you find the driver installation file (net5211.inf), click Next to continue.



Found New Hardware Wizard

Driver Files Search Results

The wizard has finished searching for driver files for your hardware device.

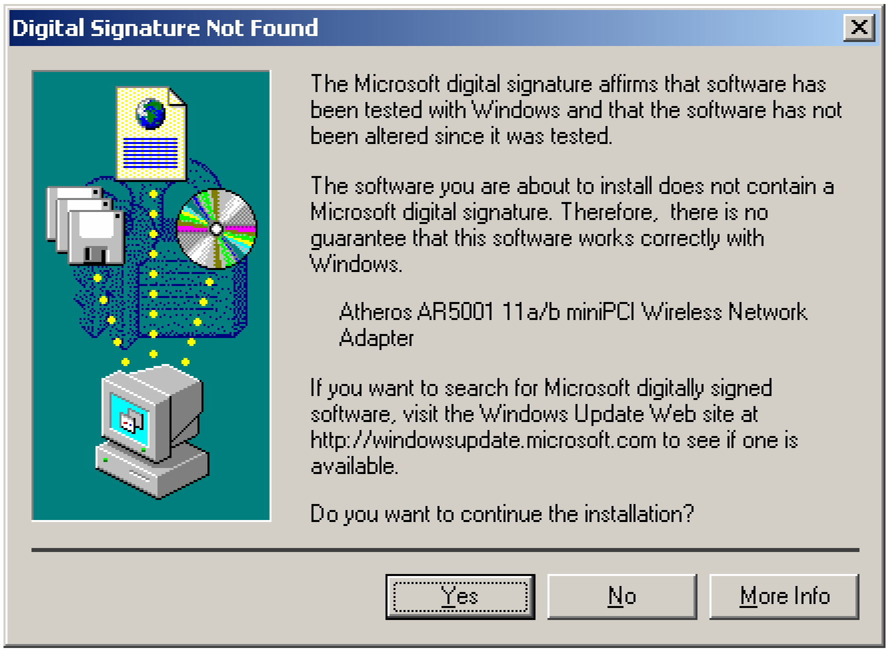
The wizard found a driver for the following device:

Ethernet Controller

Windows found a driver for this device. To install the driver Windows found, click Next.

d:\net5211.inf

6. The evaluation driver currently does not have a digital signature from Microsoft. There, Windows shows a warning message. Click Yes to proceed with the driver installation.



The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

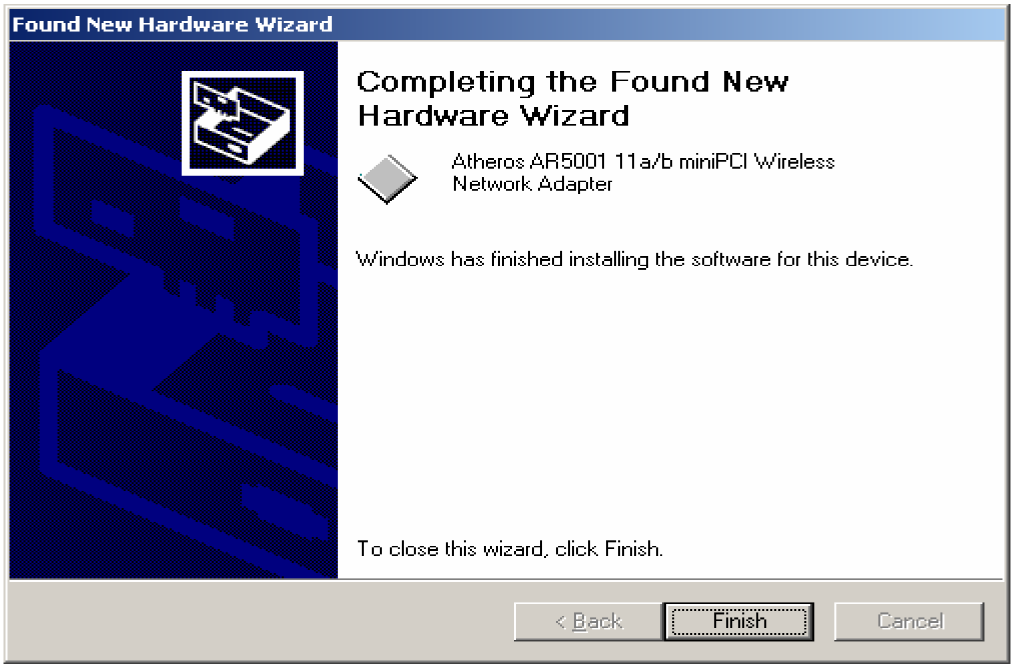
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

Atheros AR5001 11a/b miniPCI Wireless Network Adapter

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

7. Click Finish to complete the driver installation. See Section 3.0 for the device configuration.



Completing the Found New Hardware Wizard

Atheros AR5001 11a/b miniPCI Wireless Network Adapter

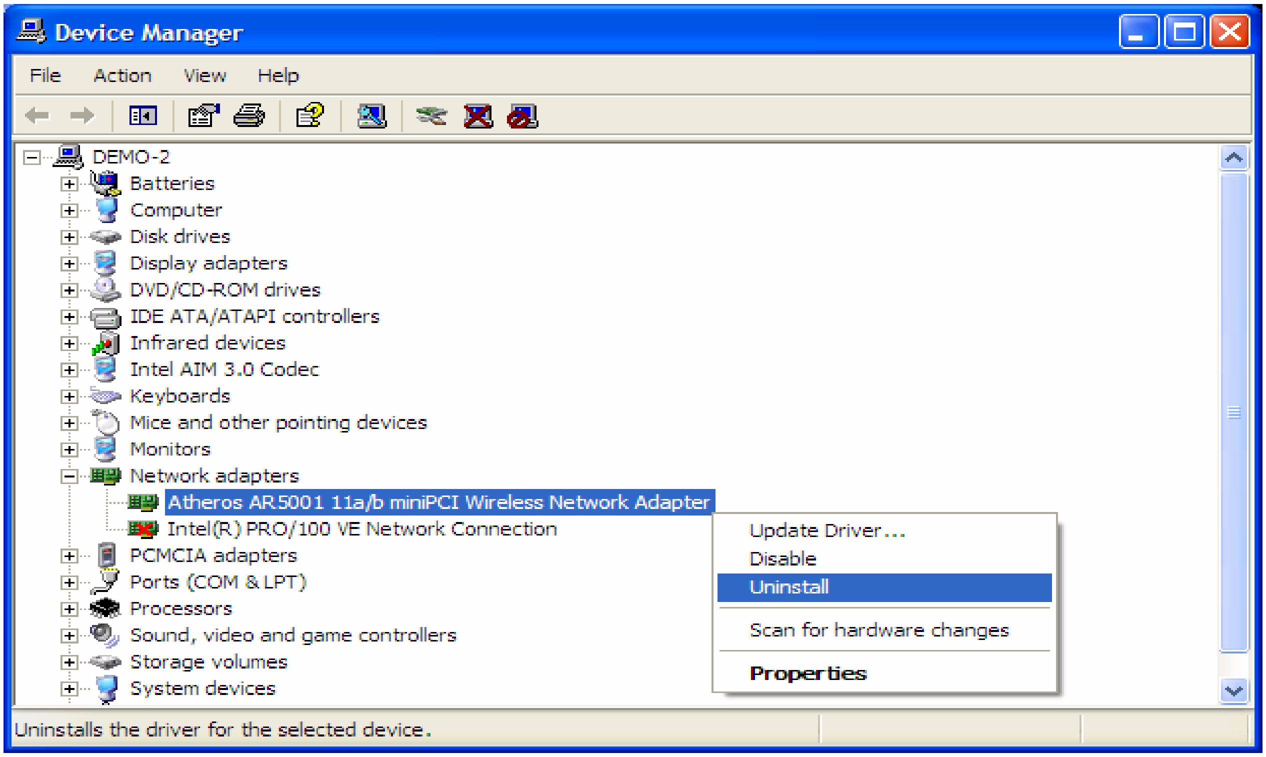
Windows has finished installing the software for this device.

To close this wizard, click Finish.

4 Driver Un-Installation

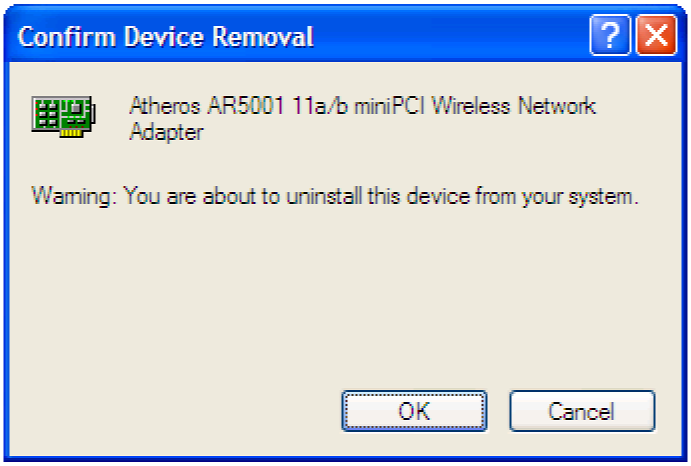
This section provides information about uninstallation procedures required for upgrading the NDIS driver from previous Atheros software releases.

1. To remove the NDIS driver from the OS, go to Device Manager, right- click “Atheros AR5001 11a/b miniPCI Wireless Network Adapter,” and choose Uninstall.



Uninstalls the driver for the selected device.

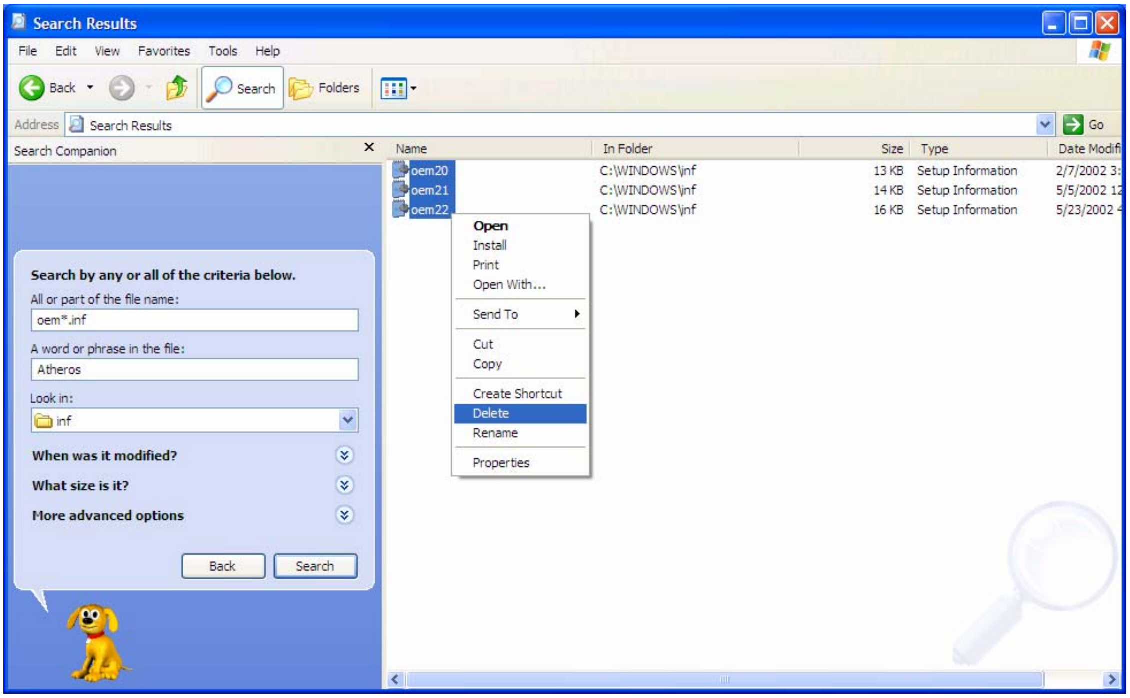
2. Click OK to uninstall the device.



Atheros AR5001 11a/b miniPCI Wireless Network Adapter

Warning: You are about to uninstall this device from your system.

3. When the device is uninstalled from Device Manager, search for and delete the driver files that reside in the system. To do so, go to the **Start** menu and choose **Search For Files or Folders**, enter “**oem*.inf**” in the “Search for files or folders named:” field, and enter “**Atheros**” in the “Containing text:” field. Click Search Now. A few files matching these criteria are possible, if previous drivers have not been removed properly. Choose the files that have been found and delete them from the system



Search by any or all of the criteria below.

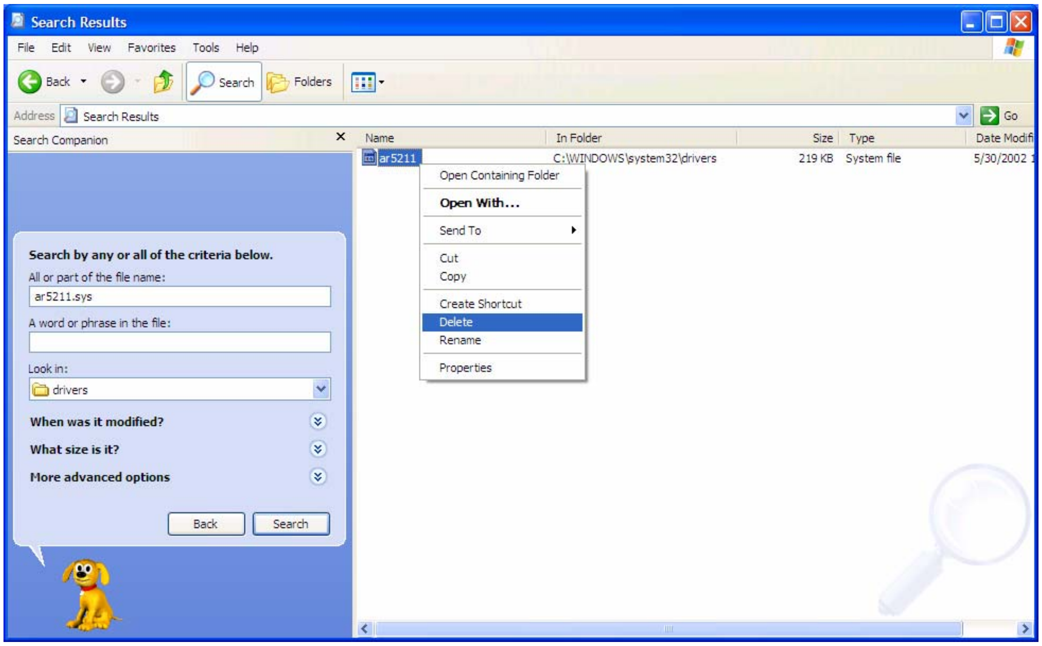
All or part of the file name: oem*.inf

A word or phrase in the file: Atheros

Look in: inf

Name	In Folder	Size	Type	Date Modifi
oem20	C:\WINDOWS\inf	13 KB	Setup Information	2/7/2002 3:
oem21	C:\WINDOWS\inf	14 KB	Setup Information	5/5/2002 12
oem22	C:\WINDOWS\inf	16 KB	Setup Information	5/23/2002 4

4. To complete the uninstallation, “ar5211.sys” should also be removed from the “\WINNT\system32\drivers” folder.



Search by any or all of the criteria below.

All or part of the file name: ar5211.sys

A word or phrase in the file:

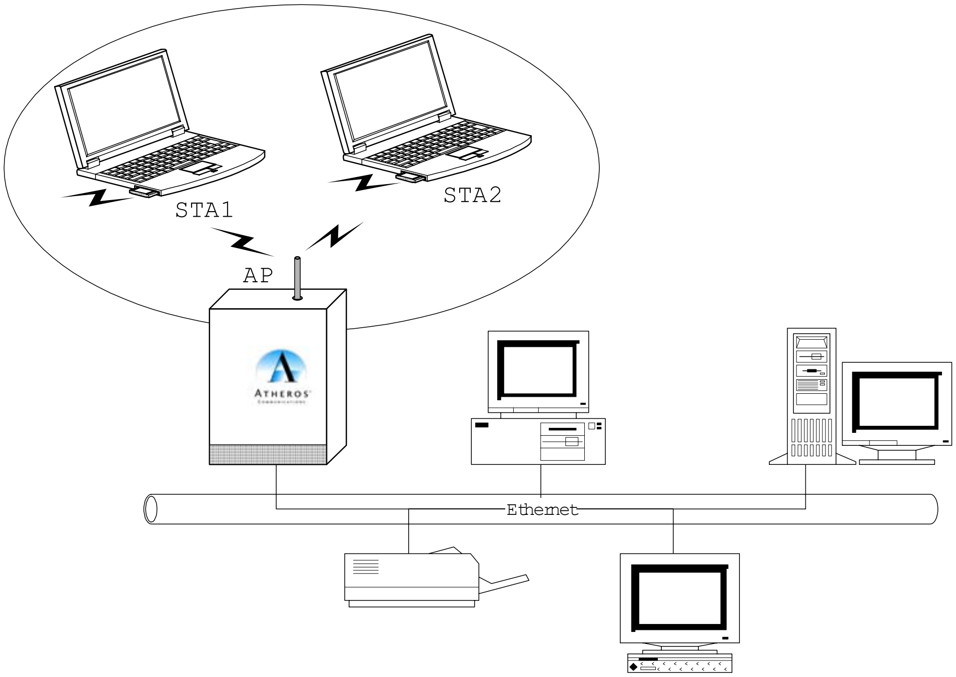
Look in: drivers

Name	In Folder	Size	Type	Date Modifi
ar5211	C:\WINDOWS\system32\drivers	219 KB	System file	5/30/2002 1

5 Device Configuration

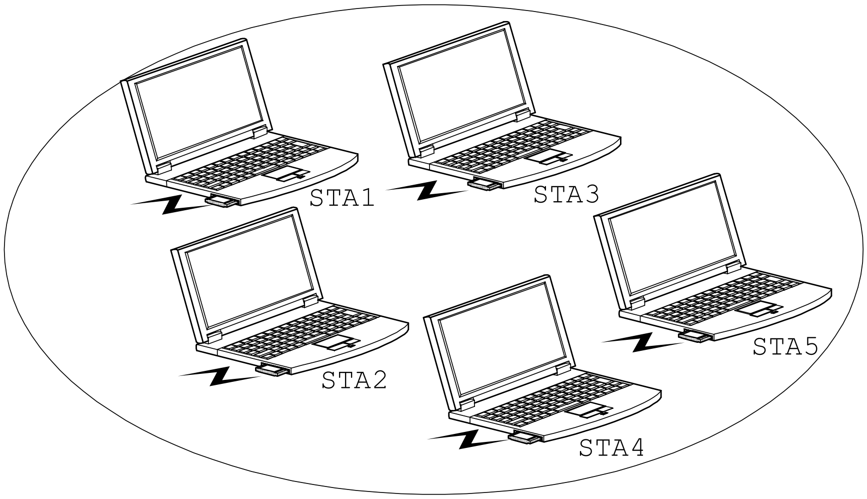
Configuration of the Philips miniPCI Wireless Network Adapter can be done through the Network Control Panel (NCP) in adapter properties. You can set the Wireless Network Adapter to work in one of two modes, either infrastructure mode (which leverages an AP) or ad hoc mode (which consists of a group of stations participating in the WLAN).

In infrastructure 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 below.



Infrastructure Mode

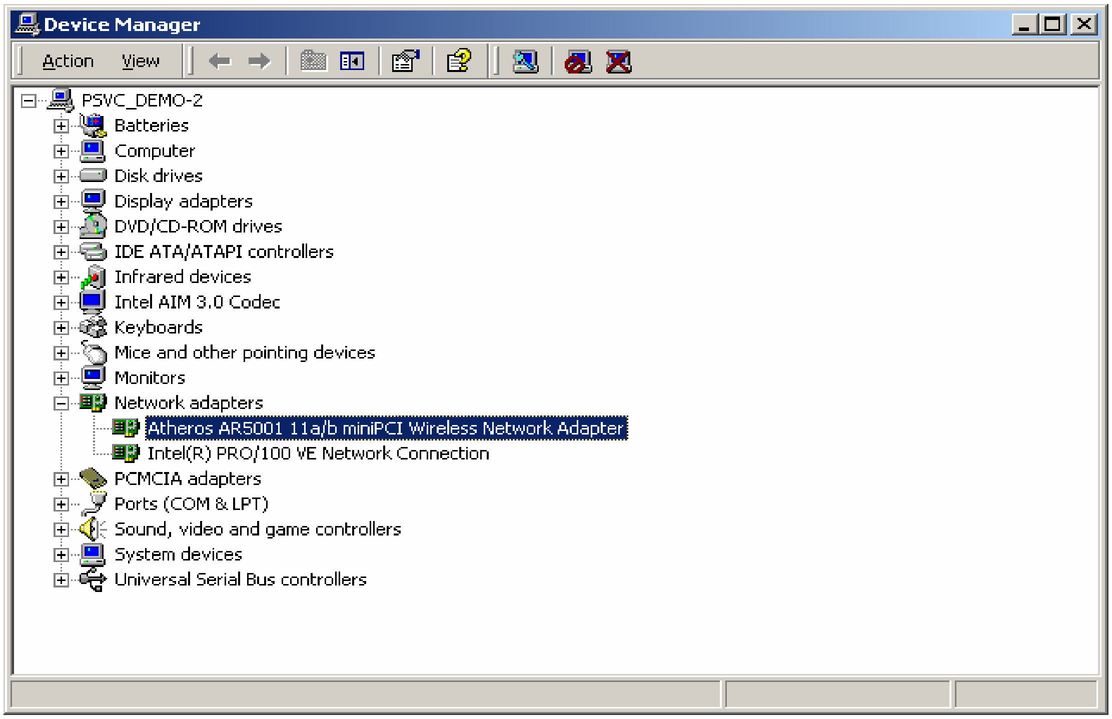
In ad hoc mode, a Wireless Network Adapter works within an independent basic service set (IBSS), as illustrated in below. All stations communicate directly with other stations without an AP.



Ad Hoc Mode

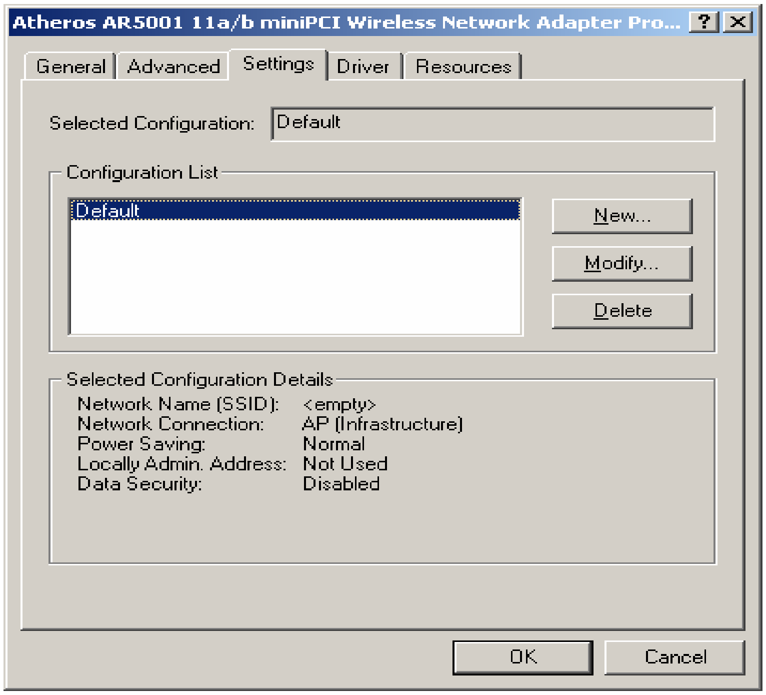
To configure the Philips miniPCI Wireless Network Adapter:

1. In the Device Manager, right-click "Atheros AR5001 11a/b miniPCI Wireless Network Adapter," and click Properties to access the properties of the adapter.



PSVC_DEMO-2
- Batteries
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- IDE ATA/ATAPI controllers
- Infrared devices
- Intel AIM 3.0 Codec
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
  - Atheros AR5001 11a/b miniPCI Wireless Network Adapter
  - Intel(R) PRO/100 VE Network Connection
- PCMCIA adapters
- Ports (COM & LPT)
- Sound, video and game controllers
- System devices
- Universal Serial Bus controllers

2. Configuration additions, modifications, and deletions are made under the "Settings" tab of the "Atheros AR5001 Wireless Network Adapter" properties.



Selected Configuration: Default

Default

Selected Configuration Details

```
Network Name (SSID):      <empty>
Network Connection:       AP (Infrastructure)
Power Saving:             Normal
Locally Admin. Address:   Not Used
Data Security:            Disabled
```

3. Select one of the configurations under the configuration list, and click Modify to show the "Network Configuration Settings" screen. This property sheet has three pages: General, Security and Advanced. The General page has the following fields:

Configuration Name: This field identifies the configuration. This name must be unique. Configuration names are case insensitive.

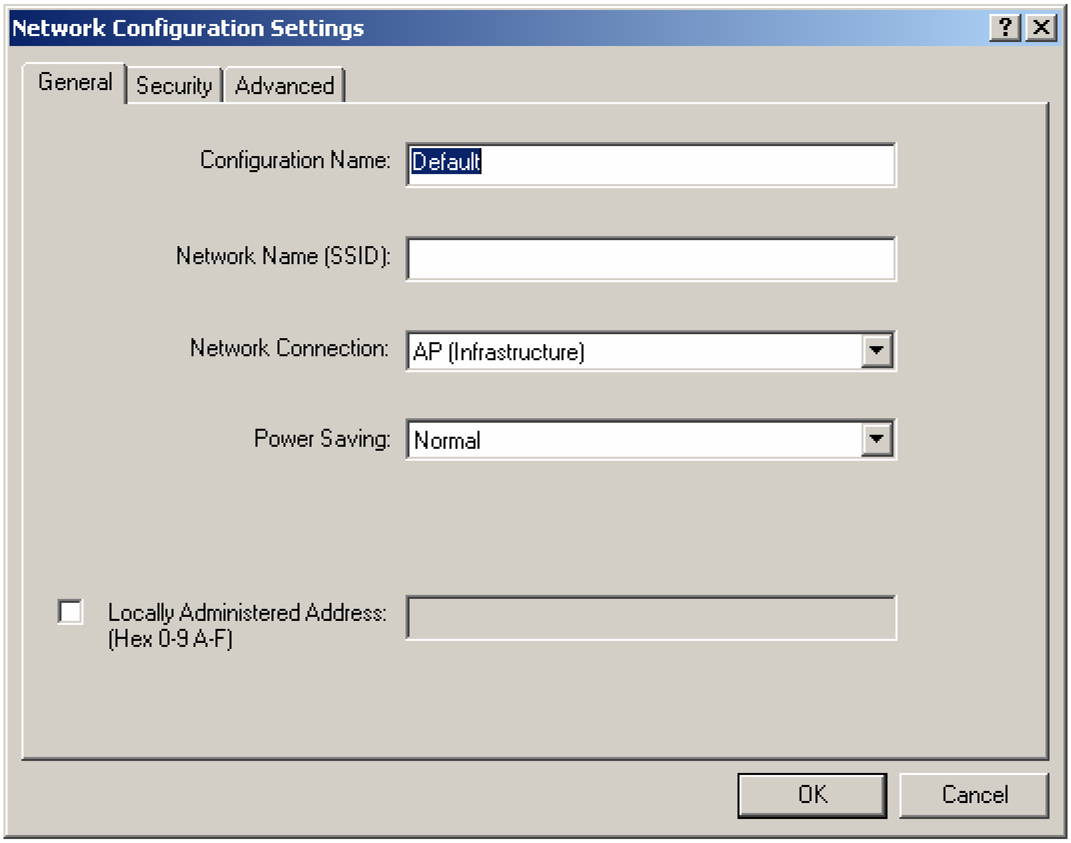
Network Name (SSID): This is the name of the IEEE 802.11a wireless network, for example, "Atheros 802.11a Wireless Network." This field has a maximum limit of 32 characters.

Network Connection: This field defines whether the STA is configured for an ad hoc or infrastructure network.

Power Saving: This field allows the configuration of power management options. The options are Off, Normal, and Maximum. Power management is disabled when ad hoc mode is selected in the Network Connection field. When the Power Saving setting is Off, the adapter receives full power from the PC. When the Power Saving setting is Normal, the driver turns off power to the adapter for brief periods over briefly spaced time intervals. When the Power Saving setting is Maximum, the driver turns off power to the adapter for longer periods over more widely spaced time intervals.

Turbo Mode: This field enables or disables Atheros turbo mode.

Locally Administered Address: This field defines the locally administered MAC address (LAA). To enter a value in the address field, the check box needs to be selected. Typically, an LAA is not required, because the driver automatically loads a unique, globally administered address from the EEPROM.



Configuration Name: Default

Network Name (SSID):

Network Connection: AP (Infrastructure)

Power Saving: Normal

☐ Locally Administered Address:
(Hex 0-9 A-F)

4. The next tab on this property sheet allows for the selection of security features. The fields on this page are as follows:

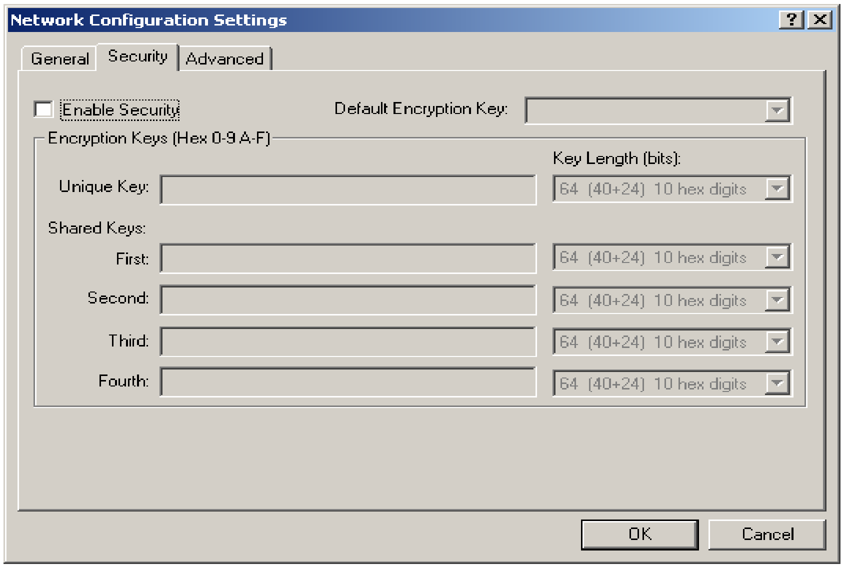
Enable Security: This field completely enables or disables the IEEE 802.11 wired equivalent privacy (WEP) security feature.

Default Encryption Key: This field defines the type of encryption key to use (either Unique Key or Shared Keys). This field allows you to select only a key (Unique, First, Second, Third, or Fourth) whose corresponding field has been completed.

Unique Key: This field defines the unique encryption key for security for the current network configuration. In ad hoc mode, this encryption key type is not used. To enable security using a Unique Key, this field must be populated.

Shared Keys: These fields define a set of shared encryption keys. To enable security using Shared Keys, at least one Shared Key field must be populated.

Key Length: This field defines the length for each encryption key. As the Key Length is changed, the number of available characters in the field is changed automatically. If after a key is entered the length is adjusted to a smaller number, the key is automatically truncated to fit. If the length is increased again, the field is not automatically updated to its previous value.



☐ Enable Security

Default Encryption Key:

Encryption Keys (Hex 0-9 A-F)

Key Length (bits):

Unique Key: 64 (40+24) 10 hex digits

Shared Keys:

First: 64 (40+24) 10 hex digits

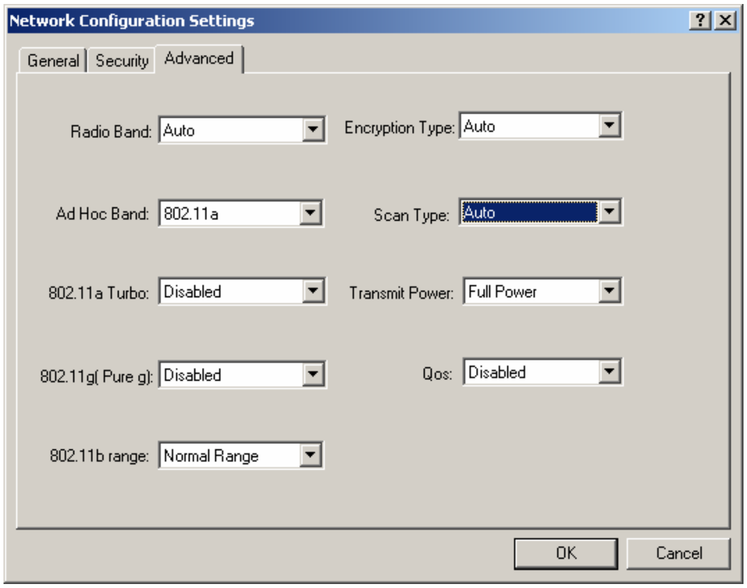
Second: 64 (40+24) 10 hex digits

Third: 64 (40+24) 10 hex digits

Fourth: 64 (40+24) 10 hex digits

All encryption key fields are displayed only when initially entered. On subsequent entry into the security property page, the fields are masked. The keys must be entered as hexadecimal digits.

5. The next tab on this property sheet allows for the selection of advanced features.



Radio Band: Auto

Encryption Type: Auto

Ad Hoc Band: 802.11a

Scan Type: Auto

802.11a Turbo: Disabled

Transmit Power: Full Power

802.11g(Pure g): Disabled

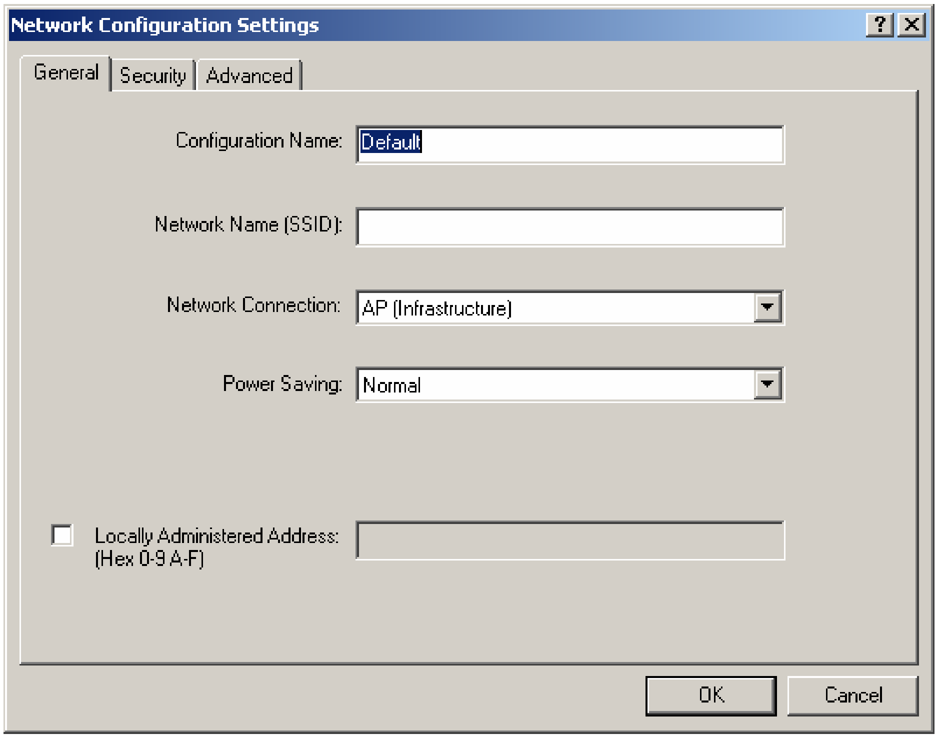
Qos: Disabled

802.11b range: Normal Range

5.1 Infrastructure Mode

To configure an Philips miniPCI Wireless Network Adapter in infrastructure mode:

1. Ensure that the “Locally Administered Address” checkbox is unchecked.



Configuration Name: Default

Network Name (SSID):

Network Connection: AP (Infrastructure)

Power Saving: Normal

□ Locally Administered Address:
(Hex 0-9 A-F)

2. Choose the following settings:

Configuration Name: This field identifies the configuration. This name must be unique. Configuration names are case insensitive.

Network Name (SSID): This is the name of the IEEE 802.11a wireless network, for example, “Atheros 802.11a Wireless Network.” This field has a maximum limit of 32 characters. If this field is left blank, the STA connects to the AP with the best signal strength.

Network Connection: AP (infrastructure).

Power Saving: This field allows the configuration of power management options. The options are Off, Normal, and Maximum.

Turbo Mode: This field enables or disables Atheros turbo mode.

Locally Administered Address: This field defines the locally administered MAC address (LAA). To enter a value in the address field, the check box needs to be selected.

Usually infrastructure mode is used in an enterprise environment where APs are installed and maintained by corporate IT staff. Much of the data in the enterprise network is confidential. It is important to configure security to make sure only stations with appropriate keys can receive sensitive data. The Philips miniPCI Wireless Network Adapter and NDIS driver support key lengths of 40 bits, 104 bits, and 128 bits. Typically, the appropriate encryption and decryption keys are supplied by the corporate IT staffs.

5.3 Ad Hoc Mode

An ad hoc network usually is a short-lived network with a small number of stations. The network is usually created for a special purpose such as exchanging data between friends, or between customer and client. Because the duration of the ad hoc network tends to be limited, Power Saving and Security features are not typically a requirement. For ad hoc network activity, the Power Saving and Security features can be disabled. Currently, shared key security is supported in ad hoc mode. Future Atheros software implementations will provide unique key support.

In ad hoc mode, a station scans the air for an existing BSS. If no BSS is found, the station establishes a BSS for other stations to join. When other stations scan the air and find an established BSS in place, they join that BSS to form an ad hoc network. If a specific set of stations requires ad hoc network connectivity, it is recommended to have one station establish a BSS first before configuring the remaining stations. This prevents the scenario of several stations trying to form a BSS at the same time, which can result in multiple singular BSSs being established, rather than a single BSS with multiple stations.

Configuration Name: This field identifies the configuration. This name must be unique. Configuration names are case insensitive.

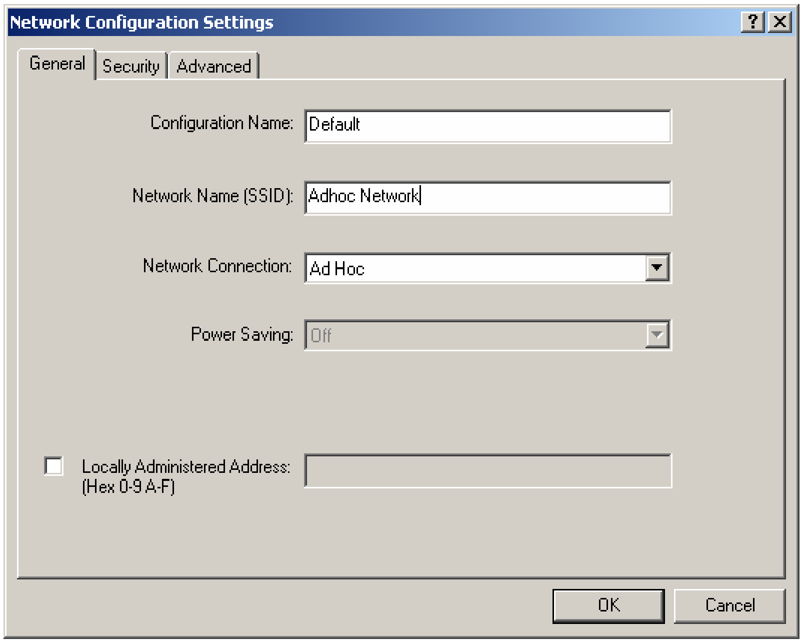
Network Name (SSID): A Network Name is mandatory for ad hoc mode. The SSID for all stations in a single ad hoc network must be the same.

Network Connection: Ad Hoc.

Power Saving: Power saving mode is not currently supported in an ad hoc network.

Turbo Mode: All stations participating in the ad hoc network must have the same rate setting.

Locally Administered Address: This field defines the locally administered MAC address (LAA). To enter a value in the address field, the check box needs to be selected.



Configuration Name: Default

Network Name (SSID): Adhoc Network

Network Connection: Ad Hoc

Power Saving: Off

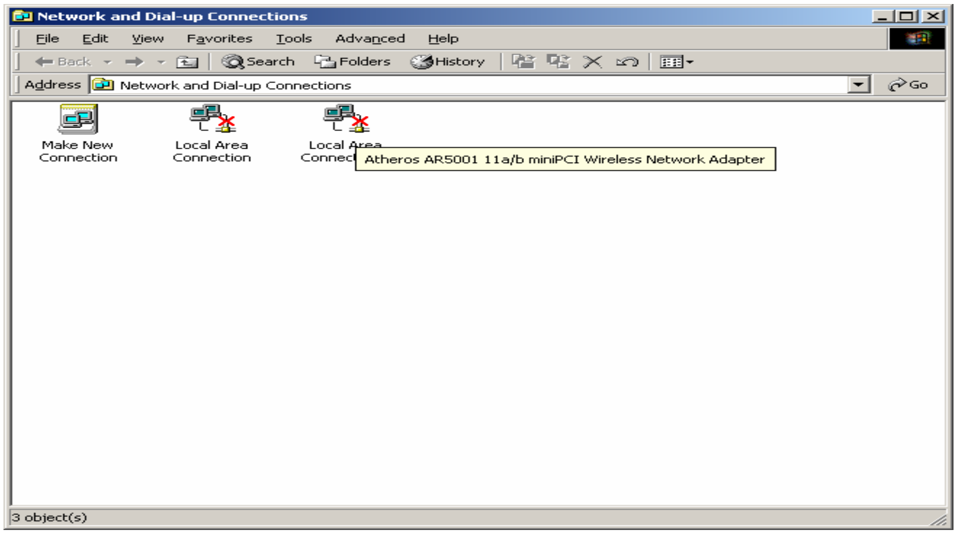
☐ Locally Administered Address: (Hex 0-9 A-F)

5.3 TCP/IP Setup

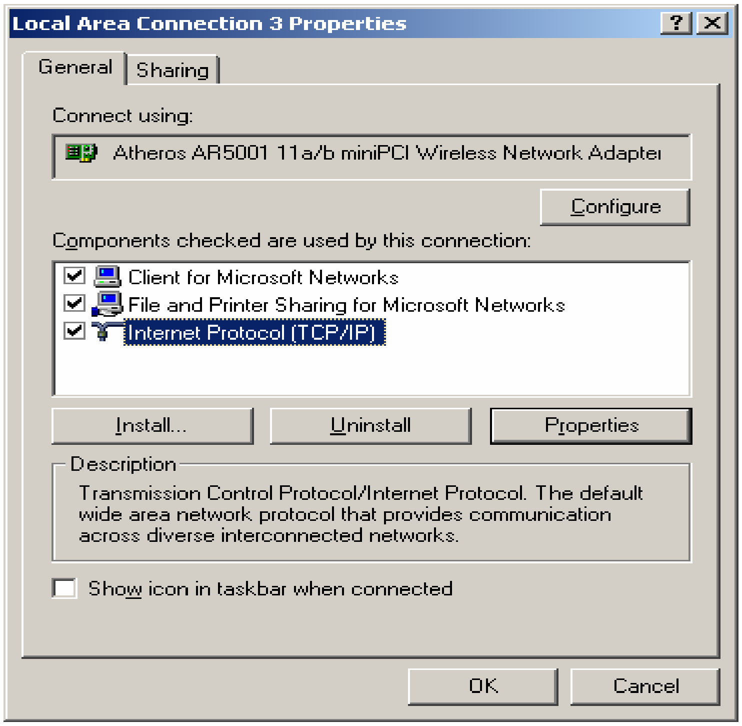
After configuring the Philips miniPCI Wireless Network Adapter through the Network Control Panel, the TCP/IP address for the network device must be configured.

3. Open the “Control Panel” and click “Network and Dial-up Connections.”

4. Find the “Local Area Connection” that is associated with the Atheros AR5001 11a/b miniPCI Wireless Network Adapter. Right-click that connection, and click Properties.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection
Local Area Connect
Atheros AR5001 11a/b miniPCI Wireless Network Adapter
3 object(s)

5. Select “Internet Protocol (TCP/IP)” and click Properties.



Local Area Connection 3 Properties

General | Sharing

Connect using:

Atheros AR5001 11a/b miniPCI Wireless Network Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

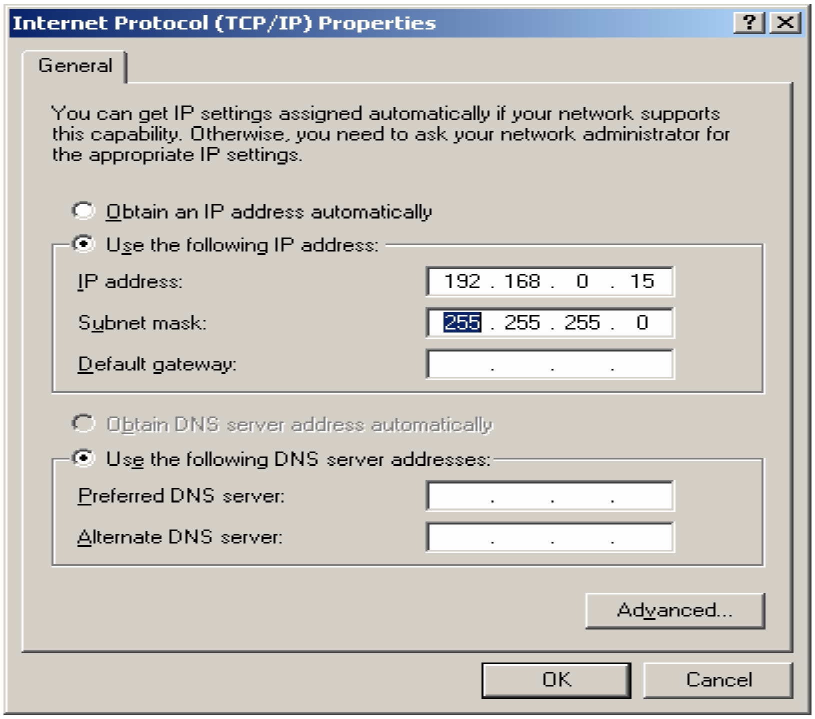
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

6. Click “Use the following IP address” and input an IP address and Subnet mask. Assigning an IP address and Subnet mask allows stations to operate in infrastructure mode and to have Internet access. “Default gateway” and “DNS server” information is also required. IP configuration information (DHCP or assigned IP address, Gateway and DNS server IP addresses) is usually obtained from the corporate IT staff.

7. After obtaining IP configuration information from the appropriate IT staff, click OK in both “Internet Protocol (TCP/IP) Properties” and “Local Area Connection Properties” to complete the IP configuration.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 15

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

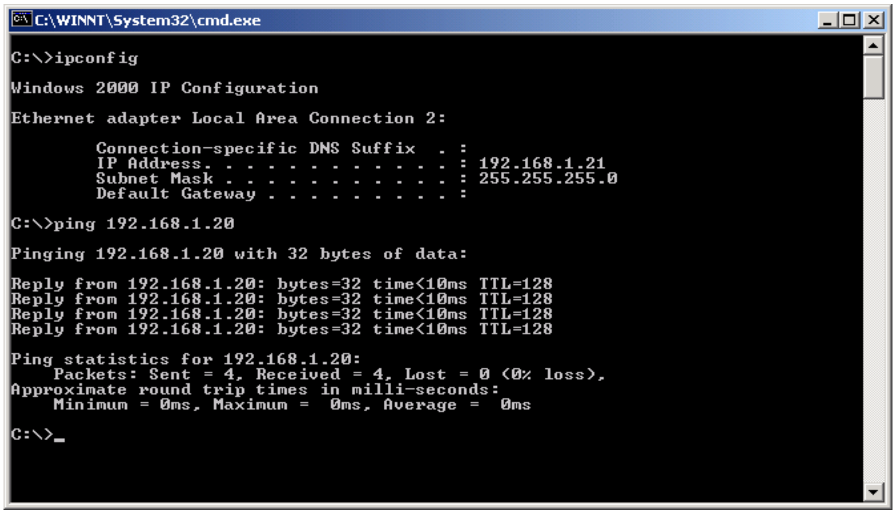
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

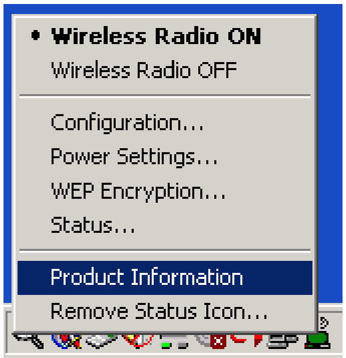
8. Choose Start > Programs > Accessories > Command Prompt to open the DOS command prompt window. Type “ipconfig” at the C:\> prompt to determine if the TCP/IP configuration has taken effect. To test IP connectivity in ad hoc or infrastructure mode, use the “ping <ipaddress>” command. When a TCP/IP connection is established, the LinkMon utility can be used to monitor the Philips miniPCI Wireless Network Adapter operating status.



```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.21
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time<10ms TTL=128
Reply from 192.168.1.20: bytes=32 time<10ms TTL=128
Reply from 192.168.1.20: bytes=32 time<10ms TTL=128
Reply from 192.168.1.20: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

6 System Tray Application

6.1.1 Screen Layout



6.1.1.1.1 Figure 1: System Tray Icon and Menu

The system tray application provides status information to users via an icon displayed in the Windows system tray.

The system tray app provides visual indication of the radio state and signal strength. It indicates if the signal strength is weak (< 20%), fair (< 40%) or strong (> 40%) by displaying a different icon for each state. Also, the system tray app displays a distinct icon to indicate that the radio is currently turned off.

The system tray icon has an associated context menu, which allows users to turn the radio on and off, and to launch directly into various screens in our Control Panel application. The menu items are described below:

6.5 System Tray Menu Items

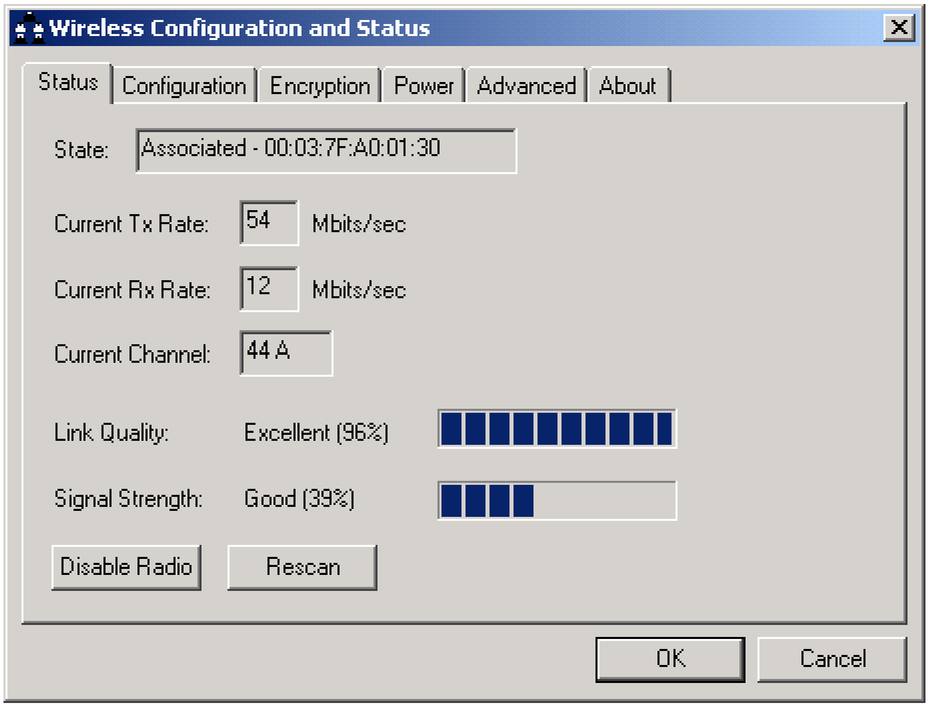
- *Wireless Radio On:* Turns the radio on. If the radio is already on, an adjacent dot indicator is displayed.
- *Wireless Radio Off* Turns the radio off. If the radio is already off, an adjacent dot indicator is displayed
- *Configuration*: Launches our Control Panel Application with the “Configuration” screen displayed.
- *WEP Encryption* : Launches our Control Panel Application with the “Encryption” screen displayed.
- *Status*: Launches our Control Panel Application with the “Status” screen displayed.

- *Product Information*: Launches our Control Panel Application to the “About” screen, displaying copyright and version information for our product.

- *Remove Status Icon*: Removes our icon from the Windows system tray, and also closes our system tray application. To restart our system tray app, the user must double-click a program icon in our program folder (or in the File Manager).

6.6 Status Screen

6.1.2 Screen Layout



State: Associated - 00:03:7F:A0:01:30

Current Tx Rate: 54 Mbits/sec

Current Rx Rate: 12 Mbits/sec

Current Channel: 44 A

Link Quality: Excellent (96%)

Signal Strength: Good (39%)

Figure 2 (Status Screen)

The Status Screen is the first tab in our Control Panel application. It displays status information about the 802.11a/b card, including the connection state, the associated server MAC address (if any), transmit and receive rates, link quality and signal strength. The information is automatically updated on a regular basis. The user can also turn the radio on or off from this screen.

6.5 Controls on the Status Screen

Field	Description
State	Displays link status, along with associated MAC address (if any).
Current Tx Rate	Displays the current transmit rate, depending on link quality and configuration parameters
Current Rx Rate	Displays the current receive rate
Current Channel	Displays the current channel on which the radio is operating
Link Quality	Displays the current perceived link quality
Signal Strength	Displays the signal strength based on specific radio parameters
Disable Radio	Allows users to turn the radio on or off. The button is labeled “Disable Radio” or “Enable Radio”, depending on the current radio state.
Rescan	The Rescan button allows the user to update the screen contents immediately. NOTE: Is this the true intent of the Rescan button? If so, do we really need this, given our automatic refresh rate?

6.1.3 Interaction of Status Screen Controls

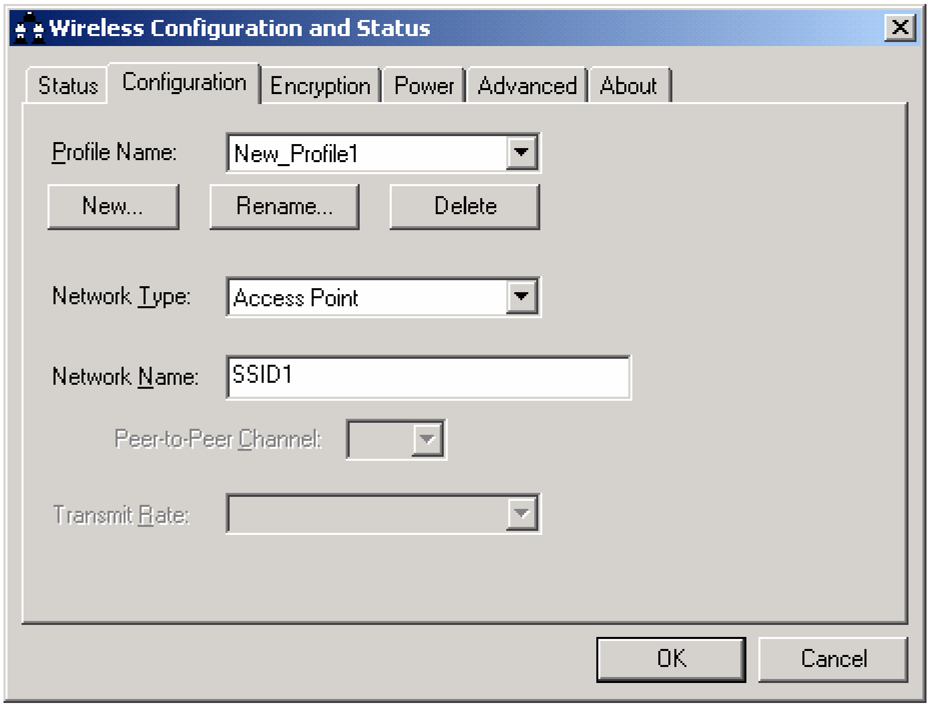
1) Other than the two push buttons, all controls on this screen are display-only. Display-only values are updated at regular intervals (currently every 3 seconds).

2) By pressing the Rescan button, the user can force a refresh of the display-only information.

3) The “Disable/Enable Radio” button will turn the radio on or off, depending upon its current state. (NOTE: The functionality is provided by our system tray application.)

6.6 Configuration Screen

6.1.4 Screen Layout



Wireless Configuration and Status

Profile Name: New_Profile1

Network Type: Access Point

Network Name: SSID1

Peer-to-Peer Channel:

Transmit Rate:

Figure 3 (Configuration Screen)

The Configuration screen is the second tab in our Control Panel application. It displays a list of existing configuration profiles, which can be modified, renamed or deleted by the user. The user can also create new profiles on this screen. Initially, there is only one profile shipped with the product, with a name of “Default”.

Configuration settings for the selected profile are displayed (and modifiable) on the Configuration, Encryption, Power and Advanced screens. Therefore, selecting a profile from the “Profile Name” list will determine the contents of the Configuration screen as well as those other three screens.

When the user presses the “OK” button (from any screen in the control panel application), all changes the user has made are saved. If changes were made to the active profile (or if a different profile was selected as the active profile), the driver is unloaded and reloaded. Upon driver reload, the settings of the selected profile will be in effect.

6.5 Controls on the Configuration Screen

Field	Description
Profile Name	List of available profiles. User may select from list to activate or modify a profile.
New/Rename/Delete Buttons	For creating, renaming and deleting profiles from the list above.
Network Type	Allows selection of either “Ad-hoc” or “Access Point (Infrastructure)”.
Network Name	Lets the user specify an SSID for the selected profile.
Peer-to-Peer Channel	The configurable peer-to-peer channel for the selected profile.
Transmit Rate	Configurable transmit rate. Chosen automatically by the 802.11a/b combo adapter or set by the user to a fixed rate.
OK Button	From any screen in control panel app, submits changes made during session.
Cancel Button	From any screen in control panel app, cancels all changes made during session.

6.1.5 Interaction of Configuration Screen Controls

(1) Selecting a different profile in the “Profile Name” list causes different settings values to be displayed in the controls on the Configuration screen, as well as the Encryption, Power and Advanced screens.

(2) When the control panel application is launched, the active profile (whose settings are currently in use by the device driver) will be shown as the selected profile in the “Profile Name” list.

(3) Clicking the “Rename” or “Delete” button while the selected profile is “Default” will result in an error message indicating that the default profile can not be renamed or deleted.

(4) Clicking the “Rename” or “New” button will display a dialog (titled “New Profile” or “Rename Profile”, respectively) that prompts the user to enter a profile name.

(5) Setting the “Network Type” to be “Access Point” will disable the “Adhoc Net Start” field on the Advanced screen.

(6) Currently “Peer-to-Peer Channel” is not implemented (always disabled).

(7) Currently “Transmit Rate” setting is not implemented (always disabled).

(8) The OK button causes all changes (on all the tabs) to be saved. Configuration changes for all profiles (not just the selected one) will be saved. If any changes have been made to the active profile, or if a new active profile is selected, then

the 802.11a/b driver will be unloaded and reloaded. Upon reload, the new settings will take effect. This button is active from any screen in the control panel application.

(9) The Cancel button will back out any and all changes made during this invocation of the control panel application. This includes any change made to any profile on any screen. This button is active from any screen in the control panel application.

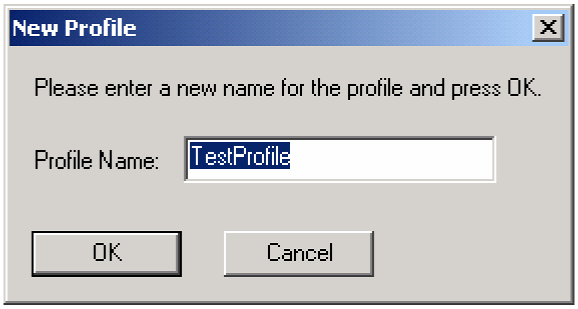
6.5 Configuration Screen Input Validation

An error message is displayed, and the user is prevented from leaving the Configuration screen (except via Cancel button) under the following conditions:

(1) The Network Type is “Adhoc” and the Network Name field is blank.

6.6 New Profile and Rename Profile Dialogs

6.1.6 Screen Layout



New Profile

Please enter a new name for the profile and press OK.

Profile Name: TestProfile

6.1.6.1.1.1.1 Figure 4: New Profile Dialog

The New Profile and Rename Profile dialogs are actually the same dialog. Only the title text and the instructional text differ depending upon whether the user is creating a new profile or renaming an existing one.

This dialog is displayed in response to the "New" button and the "Rename" button on the Configuration screen.

6.1.7 Controls on the New/Rename Profile Dialogs

Field	Description
Profile Name	Edit field used to specify the new name for the profile.
OK button	Submits the profile name for validation and, if valid, completes the new/modify profile operation.
Cancel button	Cancels the "New" or "Rename" operation.

6.1.8 New/Rename Profile Input Validation

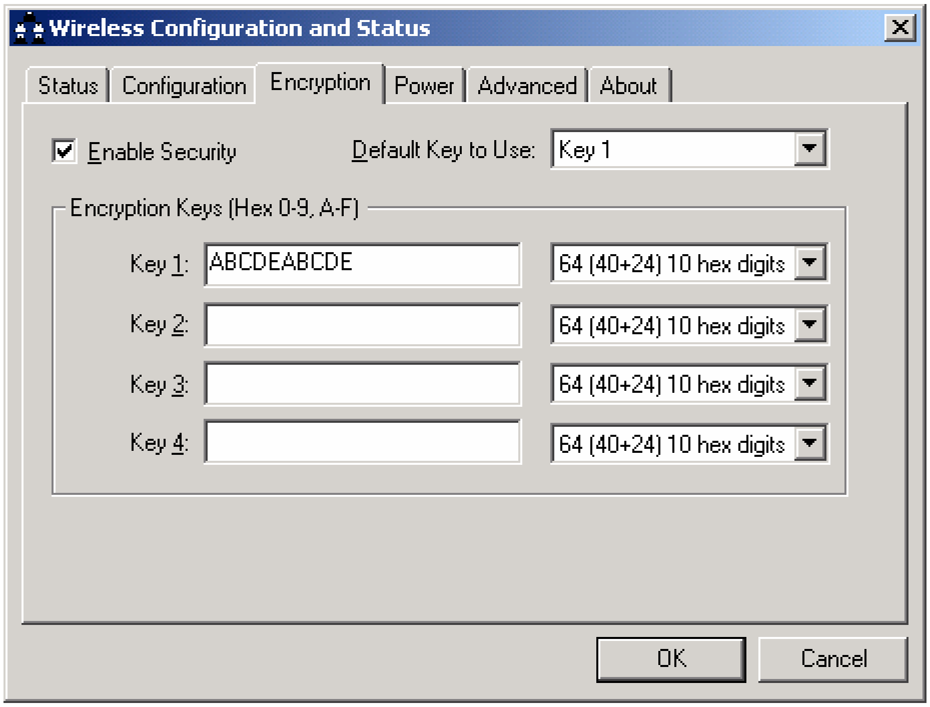
An error message is displayed, and the user is prevented from leaving the New/Rename Profile dialog (except via Cancel button) under the following conditions:

(1) A profile already exists with the name specified.

(2) No profile name is specified

6.2 Encryption Screen

6.2.1 Screen Layout



☑ Enable Security

Default Key to Use: Key 1

Encryption Keys (Hex 0-9, A-F)

Key 1:	ABCDEABCDE	64 (40+24) 10 hex digits
Key 2:		64 (40+24) 10 hex digits
Key 3:		64 (40+24) 10 hex digits
Key 4:		64 (40+24) 10 hex digits

Figure 5 (Encryption Screen)

The Encryption screen is the third tab in our Control Panel application. It allows the user to view and modify security settings for the selected profile. Up to four encryption keys may be specified.

6.2.2 Controls on the Encryption Screen

Field	Description
Enable Security checkbox	Allows user to enable or disable security (encryption) for the selected profile.
Default Key to Use	Used to identify which encryption key (Key1-Key4) is to be used by default.
Key 1-4 edit controls	Used to enter up to four encryption keys for the selected profile. Keys must contain only hex digits. Each key's length is specified in the drop-list to its right.
Key 1-4 length drop-lists	Used to select the length of the corresponding key field. There are three choices: 10, 26, or 32 hex digits.

6.2.3 Interaction of Encryption Screen Controls

(1) Un-checking the “Enable Security” checkbox causes encryption to be disabled, and causes all other screen controls (default key, keys and lengths) to become disabled.

(2) Upon initial display of the Encryption screen, previously entered key values will not be displayed. Each hex digit in these keys will be displayed as an asterisk (*) character.

(3) Any modification to a key that is displayed as asterisk characters will cause the key value to be erased. The new key must be entered in its entirety.

(4) Keys are restricted to contain only hex digits (0-9,A-F). The edit control for each key will ignore entry of any non-hex digits. Digits may be upper or lower case.

(5) Each key value is restricted to the length specified by the list control to its right.

(6) If a key has been entered (or partially entered), and the user changes its length selection, the key will be truncated if necessary. For example, if the user has entered 18 hex digits for Key 1, and then the user selects “10 Hex Digits” in its corresponding length drop-list, then the last 8 digits of the key will be erased.

(7) If the user changes the key length selection for a key that is displayed as asterisks, then the key value will be cleared, as described in (3) above.

6.2.4 Encryption Screen Input Validation

An error message is displayed, and the user is prevented from leaving the Encryption screen (except via Cancel button), under the following conditions:

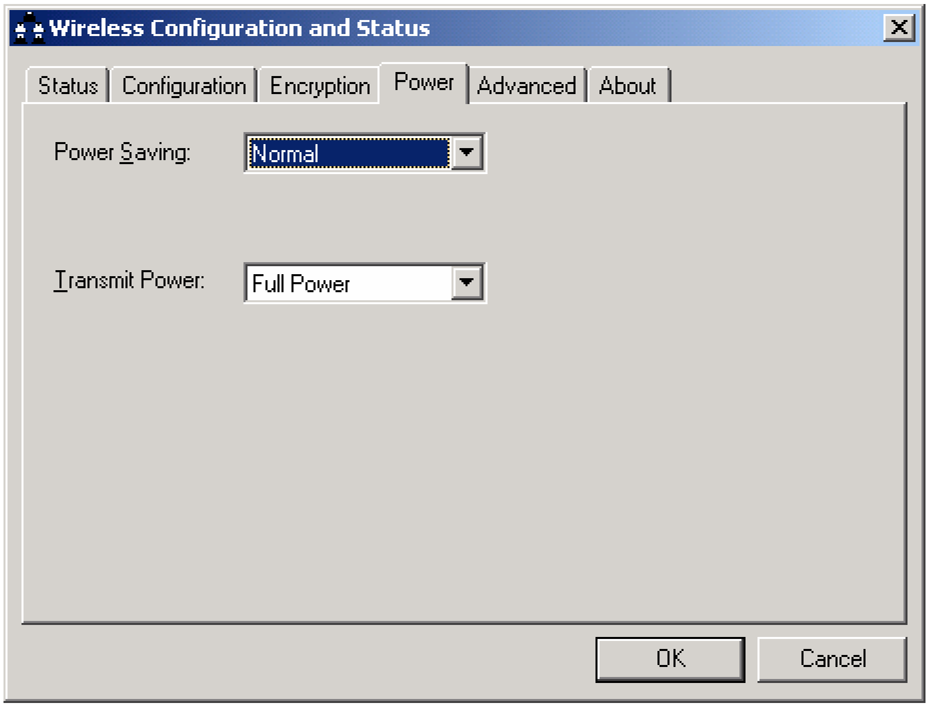
(1) Security is enabled, and no encryption key has been specified.

(2) The “Default Key to Use” selection is a key that has not been entered.

(3) The length of one of the non-blank encryption keys does not match the corresponding key length specified.

6.3 Power Screen

6.3.1 Screen Layout



Power Saving: Normal

Transmit Power: Full Power

Figure 6 (Power Screen)

The Power screen is the fourth tab in our Control Panel application. It allows the user to view and modify power settings for the selected profile. Currently the only available settings are the Power Saving mode and Transmit Power level.

6.3.2 Controls on the Power Screen

Field	Description
Power Saving	Used to specify the Power Saving Mode for the selected profile. Offers three choices: Off, Normal, or Maximum.
Transmit Power	Used to specify the Transmit Power level for the selected profile. Offers five choices: Full Power, 50% Power, 25% Power, 12% Power and Lowest Power.

6.3.3 Interaction of Power Screen Controls

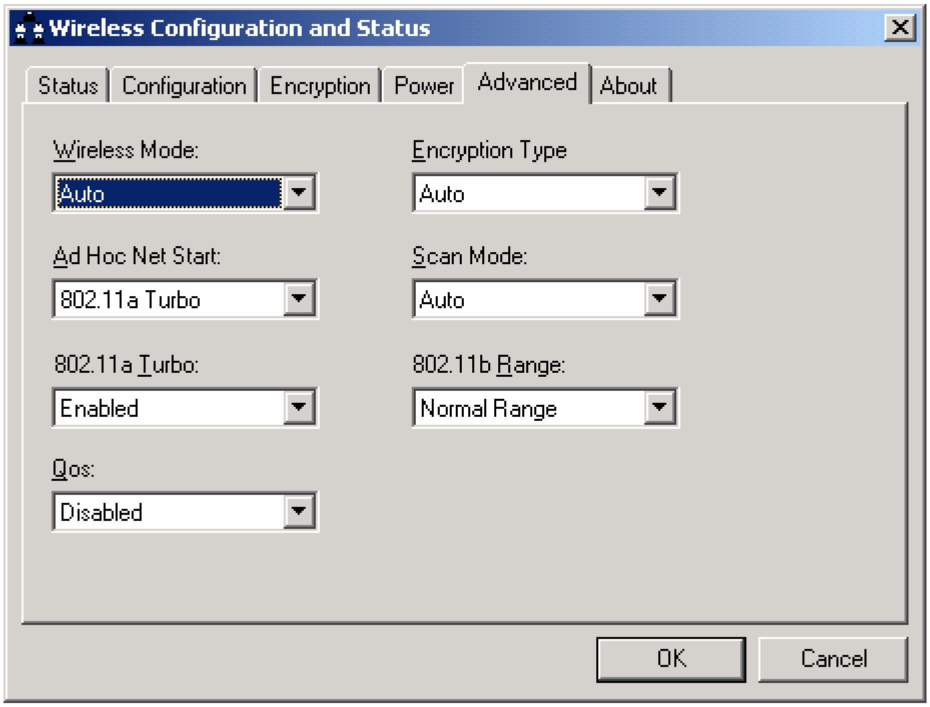
Currently, there is no special interaction between controls on the Power screen.

6.3.4 Encryption Screen Input Validation

Currently there is no input validation for the Power screen.

6.4 Advanced Screen

6.4.1 Screen Layout



Wireless Mode: Auto

Encryption Type: Auto

Ad Hoc Net Start: 802.11a Turbo

Scan Mode: Auto

802.11a Turbo: Enabled

802.11b Range: Normal Range

Qos: Disabled

Figure 7 (Advanced Screen)

The Advanced screen contains some miscellaneous settings for the selected profile. Users can view and modify configuration parameters that might be considered too complicated or obscure for a typical user.

6.4.2 Controls on the Advanced Screen

Field	Description
Wireless Mode	Allows user to specify whether the radio should operate in 802.11a mode, 802.11b mode, or "Auto" mode to have the a/b card automatically choose the mode.
Adhoc Net Start	Allows user to specify the mode to use when starting up in Adhoc mode. Choices are: 802.11a, 802.11b, or 802.11a Turbo.
802.11a Turbo	Choices are: Enabled or Disabled
Qos	Choices are: Enabled or Disabled.
Encryption Type	Allows user to select what type of encryption will be used. Choices are: WEP, AES or Auto
Scan Mode	Allows user to select what mode will be used by the card for scanning. Choices are: Active Scan, Passive Scan or Auto
802.11b Range	Allows user to choose the range of the radio in 802.11b mode. Choices are: Extended Range, or Normal Range.

6.4.3 Interaction of Advanced Screen Controls

1) The "Adhoc Net Start" control is disabled on the Advanced screen if the selected profile has Network Type set to "Access Point" (on the Configuration screen).

2) The "Wireless Mode" value drives the state of several other fields on the Advanced screen. In particular:

   a) When "Wireless Mode" is set to 802.11b, the Adhoc Net Start control will be disabled, and its value will be set to "802.11b".

   b) When "Wireless Mode" is set to 802.11b, the "802.11a Turbo" control is disabled, and its value is set to "Disabled".

   c) When "Wireless Mode" is set to 802.11a, the Adhoc Net Start control will be disabled, and its value will be set to "802.11a".

   d) When "Wireless Mode" is set to 802.11a, the "802.11b Range" control is disabled, and its value is set to "Disabled".

   e) Setting Wireless Mode to "Auto" will re-enable all of the controls disabled above.

3) When "Adhoc Mode" is set to 802.11a Turbo, then the "802.11a Turbo" control is disabled, and its value is set to "Enabled".

4) Changing "Adhoc Mode" from "802.11a Turbo" to any other value will re-enable the 802.11a Turbo combobox control.

6.4.4 Advanced Screen Input Validation

An error message is displayed, and the user is prevented from leaving the Advanced screen (except via Cancel button), under the following conditions:

1) “Adhoc Net Start” is set to 802.11a Turbo, and the 802.11a Turbo combobox has a value of “Disabled”.

7 GLOSSARY

2.4 GHz ISM Radio Band

The Industrial, Scientific and Medical (ISM) radio bands were originally reserved internationally for non-communications uses of RF electromagnetic fields for industrial, scientific and medical purposes. In recent years they have also been used for license-free error-tolerant communications applications such as wireless LANs and Bluetooth

Access Point

The major network interconnection point that serve to tie all the wireless network access cards with the wired local area network or other access point in the infrastructure network

Channel

One of multiple transmission paths within a single link between network points.

IEEE

Institute of Electrical and Electronics Engineers

MAC Address

The MAC (Media Access Control) address is the computer's unique hardware number that identifies it on the IP network.

Passphrase

A passphrase is a string of characters longer than the usual password (which is typically from four to 16 characters long) that is used in creating a digital_signature (an encoded signature that proves to someone that it was really you who sent a message) or in an encryption or a decryption of a message.

PCI card/Slot

A card/slot that complies with the spec of PCI (Peripheral Component Interconnect) which is an interconnection system between a microprocessor and attached devices in which expansion slots are spaced closely for high speed operation.

Peer-to-Peer

A communications model in which each party has the same capabilities and either party can initiate a communication session. Peer-to-peer is one of the 802.11b operating modes, often called 'AdHoc' mode. It is ad-hoc because it has no central base station; an ad-hoc network will exist so long as any members of that network remain on the air. In AdHoc mode, the system must be configured as a specific IP address, and all IP addresses of each station must be in the same network domain. This means all connected computers should have the same net-id and subnet-id .

RSSI

Received Signal Strength Indication.

Glossary
continued

SSID

"Service Set Identifier", which is used to identify the particular wireless LAN to be accessed.

System tray icon

The system tray (or "systray") is a section of the taskbars in the Microsoft Windows desktop user interface that is used to display the clock and the icons of certain programs so that a user is continually reminded that they are there and can easily click one of them.

Throughput

The amount of data moved successfully from one place to another in a given time period.

Tx (transmit) Rate

The amount of data per second transferred from source to destination.

U-NII Band:

FCC established Unlicensed National Information Infrastructure (U-NII) band in 1997 to provide cost-effective wireless networking for businesses, schools and hospitals. U-NII is a 300 MHz band in the 5 GHz range (5.15 GHz - 5.35 GHz and 5.725 GHz - 5.825 GHz). U-NII band is license-free, but all equipment that operates in U-NII band is subjected to FCC regulations.

WEP security

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

WLAN

A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection.

8 Regulatory Information

- To identify this product refer to the part or model number on the product label

8.1 Federal Communications Commission (FCC)

FCC Modular Labeling Requirements:

The modular transmitter must be labeled with its own FCC ID PUBWCM1008, and, if the FCC ID is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following: “Contains Transmitter Module FCC ID: PUBWCM1008” or “Contains FCC ID: PUBWCM1008.”

FCC Notice:

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.

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 that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for
help.

FCC RF Exposure Warning:

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from the from the person and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC RF interference requirements:

This device is restricted to indoor use due to its operations in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoor for the frequency range 5.15-5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite Systems.

Modifications:

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Philips Components may void the user's authority to operate the equipment.

8.2 Industry Canada (IC):

"Operation is subject to the following two conditions: (1) this device may not cause interference,
and (2) this device must accept any interference, including interference that may cause undesired operation of the device."

"To prevent radio interference to the licensed service, this device must be operated indoors only and should be kept away from windows to provide maximum shielding.

8.3 European Community Notice:

Marking by the symbol CE 0984 (!) indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN 301 893
EN 301 489-17
EN 60950
ETS 300 328-2

5GHZz operation of this device is not allowed in the following European Community countries: Germany, Greece and Spain. The radio spectrum authorities in these countries do not currently allow operation of this radio device in the 5GHz bands.

Operation of this device in the U.K. currently requires the end user or installer to contact the U.K. Radiocommunications Agency (phone: 0207 211 0181) to request a **Temporary Use License for 5GHz operation**. The Temporary Use License requirement will be removed once pending U.K. license exemption legislation is finalized.

This device is restricted **to indoor use** when operated in the European Community using channels in the 5150-5350 MHz band to reduce the potential for harmful interference to other users of the band.

- **European Community Declaration of Conformity:**

English	Hereby, *Philips Components*, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	*Valmistaja Philips Components* vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart *Philips Components* dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
	Bij deze verklaart *Philips Components* dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente *Philips Components* déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
	Par la présente, *Philips Components* déclare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
Swedish	Härmed intygar *Philips Components* att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede *Philips Components* erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
German	Hiermit erklärt *Philips Components*, dass sich *dieser/diese/dieses* Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)

	Hiermit erklärt *Philips Components* die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* *Philips Components* *ΔΗΛΩΝΕΙ ΟΤΙ* Radio LAN device *ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*
Italian	Con la presente *Philips Components* dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente *Philips Components* declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Portuguese	*Philips Components* declara que este Radio LAN device está conforme com os requisi essenciais e outras disposições da Directiva 1999/5/CE.