

Part No. 216669-A
September 2004

4655 Great America Parkway
Santa Clara, CA 95054

Installing and Using the Nortel Networks Wireless LAN Mobile Adapter 2202 Release 3.0.0.0

Copyright © 2004 Nortel Networks

All rights reserved. September 2004.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks and the Nortel Networks logos are trademarks of Nortel Networks.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated, Windows 2000 and Windows XP are trademarks of Microsoft Corp, and Pentium is a trademark of Intel.

Nortel Networks and the Nortel Networks logo are trademarks of Nortel Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Asterisks denote trademarks.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Compliances

Federal Communication Commission Interference Statement

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 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 Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment, and the antenna of this device must be integral.

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.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Nortel declared that WLAN-Mobile Adapter 2202 is limited in CH1~11 by specified firmware controlled in USA from 2400~2483.5MHz.

Nortel declared that WLAN-Mobile Adapter 2202 has been disabled for operation in the USA in the 5.470~5.725 MHz UNII band by specified firmware control.

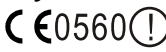
This equipment has been SAR-evaluated for use in laptops (notebooks) with side slot configuration.

Exposure to Radio Frequency Radiation

The radiated output power of the Nortel Networks Wireless LAN Mobile Adapter 2202 radio is far below the FCC radio frequency exposure limits. Nevertheless, the wireless radio shall be used in such a manner that the potential for human contact during normal operation is minimized.

The Nortel Networks Wireless LAN Mobile Adapter 2202 radio operates within guidelines found in radio frequency safety standards and recommendations, which reflect the consensus of the scientific community. Nortel Networks therefore believes the internal wireless radio is safe for use by consumers. The level of energy emitted is far less than the electromagnetic energy emitted by wireless devices such as mobile phones. However, the use of wireless radios may be restricted in some situations or environments, such as aboard airplanes. If you are unsure of restrictions, you are encouraged to ask for authorization before turning on the wireless radio.

European Community Notice

Marking by the symbol  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

This device should not be operated in 802.11a mode in the following European Community countries: Greece. The radio spectrum authorities in these countries do not currently allow operation of this radio device in the 5GHz bands.

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.

To remain in conformance with European National spectrum usage laws, the following channel limitations apply per the table below. **The user should use the utility provided with the product software to check the current channel of operation.** If operation is occurring outside of the allowable frequencies as listed in the table, the user should cease operating the product and consult with the local technical support staff responsible for the wireless network.

This device is restricted from operating in **ad-hoc mode using channels in the 5GHz bands in the European Community.** Ad-hoc mode is direct communication between two client devices without an Access Point.

Allowable Frequencies of Operation	Countries
5150-5250 MHz (Channels 36, 40, 44, 48)	Austria, Germany, Liechtenstein

5150-5350 MHz (Channels 36, 40, 44, 48, 52, 56, 60, 64)	Belgium, France, Ireland, U.K., Switzerland
5150-5350 & 5470-5725 MHz (Channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140)	Denmark, Finland, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden

European Community Declaration of Conformity:

English	Hereby, Nortel Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	<i>Valmistaja</i> Nortel Networks 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 Nortel Networks 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 Nortel Networks dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/CE.
French	Par la présente Nortel Networks 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, Nortel Networks 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 Nortel Networks 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 Nortel Networks erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
German	Hiermit erklärt Nortel Networks, dass sich <i>dieser/diese/dieses</i> Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW i) Hiermit erklärt Nortel Networks die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	ÏÀ ÔÇÍ ÐÁÑÏÓÓÁ Nortel Networks ÆÇËÛÏÁË ÎÔÉ Radio LAN device ÓÏÏÏÑÏÛÏÁÔÁÉ ÐÑÏÓ ÔÉÓ ÏÔÓËÛÁÁÉÓ ÁÐÁÉÔÇÓÁÉÓ ÊÁÉ ÔÉÓ ËÏËÐÁÓ Ó×ÁÔÉÊÁÓ ÆÉÁÔÁÏÁÉÓ ÔÇÓ ÏÏÇÁÉÁÓ 1999/5/ÏË
Italian	Con la presente Nortel Networks 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 Nortel Networks 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	Nortel Networks declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

Canada IC Statement

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 is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

To prevent radio interference to the licensed service (i.e. co-channel Mobile Satellite systems) this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Because high power radars are allocated as primary users (meaning they have priority) in 5250-5350 MHz, these radars could cause interference and/or damage to license exempt LAN devices.

Contents

Preface	13
Text conventions	13
Hard-copy technical manuals	14
How to get help	14
Chapter 1	
Overview	17
Nortel Networks WLAN - Mobile Adapter 2202 configuration modes	17
Infrastructure (access point) mode	17
Ad hoc mode	18
Added support for Advanced Encryption Standard (AES)	19
Product package checklist	19
System requirements	20
Mobile Adapter 2202 LEDs	21
Chapter 2	
Quick start software installation	23
Chapter 3	
Driver and utility software installation and uninstallation	25
Installing the driver and utility software	25
Additional installation information	30
Uninstalling the Mobile Adapter 2202	30
Chapter 4	
Configuring basic network settings	35
Creating a new network profile	35
Connecting to a network	40
Managing Auto Profile Selection	42
Configuring advanced settings for Windows XP	45
Chapter 5	
Configuring network security	47
Overview	47
Authentication sequence	48
EAP security	49
Enabling EAP-TLS security	49
Enabling EAP-TTLS security	50

8 Contents

PEAP security	53
Enabling PEAP (EAP-GTC) security	54
Enabling PEAP (EAP-MSCHAP V2) security	55
WPA Passphrase (WPA-PSK) security	57
Pre-Shared Key (Static WEP) security	59
Chapter 6	
Upgrading the driver and utility software	63
Upgrading the driver and utility software	63
Appendix A	
Troubleshooting guidelines	69
Verifying driver operation	69
For Windows 2000	69
For Windows XP	69
Troubleshooting tips	70
Appendix B	
Specifications	71
Frequency band	71
Modulation technique	71
Host interface	72
Operating channels supported	72
Operating voltage	72
Power consumption	72
Current consumption	73
Output power	73
Operating systems supported	73
Dimensions	74
Security	74
Operation mode	74
Transfer data rate	74
Operating temperature	74
Storage temperature	74
Humidity	75
Compliance standards	75
Media access protocol	75
Mechanical specification	76

Figures

Figure 1	Infrastructure mode	18
Figure 2	Ad hoc mode	19
Figure 3	Starting the InstallShield Wizard message	26
Figure 4	Mobile Adapter 2202 Installation Program window	26
Figure 5	Choose Destination Location window	27
Figure 6	Insert the Mobile Adapter 2202 card dialog box	27
Figure 7	Inserting an adapter card	28
Figure 8	Installation Program Setup Status window	28
Figure 9	Digital Signature Not Found dialog box	29
Figure 10	Reboot prompt	29
Figure 11	WLAN Mobile Adapter Utility Icon in system tray	29
Figure 12	Uninstall the Mobile Adapter 2202 option	30
Figure 13	Previous Installation Detected window	31
Figure 14	Selected option requires a reboot dialog box	31
Figure 15	Confirm Uninstall dialog box	31
Figure 16	Remove the device driver dialog box	32
Figure 17	Setup Status window	32
Figure 18	Reboot prompt	33
Figure 19	Mobile Adapter 2202 Utility — Profile Management tab	35
Figure 20	Profile Management window — General tab	36
Figure 21	Profile Management — Security tab	37
Figure 22	Profile Management — Advanced tab	38
Figure 23	Mobile Adapter 2202 Utility — Profile Management tab	39
Figure 24	Launching the Mobile Adapter 2202 Utility	40
Figure 25	Mobile Adapter Utility window	40
Figure 26	Mobile Adapter 2202 Client Manager - Site Survey tab	41
Figure 27	Association icon for an access point connected to a wireless infrastructure network	41
Figure 28	Association icon for an ad hoc wireless network	41

10 Figures

Figure 29	Profile Management window — General tab	42
Figure 30	Profile Management tab — ordering profiles	43
Figure 31	Auto Profile Selection Management window	44
Figure 32	CardBus context menu	45
Figure 33	Wireless networks tab	46
Figure 34	EAP-TLS Security Option	50
Figure 35	EAP-TTLS Security Option	51
Figure 36	Define EAP-TTLS Configuration window	52
Figure 37	PEAP (EAP-GTC) Security Option	54
Figure 38	Define PEAP (EAP-GTC) Configuration window	55
Figure 39	PEAP (EAP-MSCHAP V2) Security Option	56
Figure 40	Define PEAP (EAP-MSCHAP V2) Configuration window	56
Figure 41	Security tab — WPA Passphrase option	58
Figure 42	Define WPA Pre-Shared Key window	58
Figure 43	Security tab — Pre-Shared Key option	60
Figure 44	Define Pre-Shared Key window	60
Figure 45	Starting the InstallShield Wizard message	64
Figure 46	Preparing Setup window	64
Figure 47	Previous Installation Detected window	65
Figure 48	Option requires system reboot dialog box	65
Figure 49	Stopping the Configuration Service message	65
Figure 50	Setup Status window	66
Figure 51	Digital Signature Not Found dialog box	67
Figure 52	Reboot prompt	67

Tables

Table 1	Mobile Adapter 2202 LEDs	21
Table 2	Profile Management Settings — General tab	36
Table 3	Profile Management — Advanced tab	38
Table 4	Troubleshooting tips	70

12 Tables

Preface

This guide contains detailed instructions for installing and configuring the Nortel Networks WLAN - Mobile Adapter 2202 (Mobile Adapter 2202).

Chapter 1 provides product overview information and information about what you need to do before you begin the installation process. Chapters 2 through 4 provide installation and configuration information and procedures. Chapter 5 provides instructions for upgrading the Nortel Networks WLAN - Mobile Adapter 2202 driver and utility software. Appendix A provides trouble-shooting tips, and Appendix B contains a list of product specifications.

To ensure successful installation and configuration, complete the installation and configuration procedures in the order in which they are presented in this installing and using guide. Do *not* skip around within the procedures or between chapters.

Text conventions

This guide uses the following text conventions:

angle bracket (>)	Indicates a series of selections to be made from a group of linked menus. Example: Select Start > Control Panel > System.
bold text	Indicates command names and button names, and data or text that you need to enter. Example: Click on OK . Then, click on Finish . Example: Enter alphanet .

14 Preface

<i>italic text</i>	Indicates new terms, book titles, and file names. It is also used for emphasis. Example: Use the <i>setup.exe</i> file to launch the InstallShield Wizard. Example: Do <i>not</i> skip around within the procedures or between chapters.
plain Courier text	Indicates command syntax and system output, for example, prompts and system messages. Example: Set Trap Monitor Filters

Hard-copy technical manuals

You can print selected technical manuals and release notes free of charge, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to <http://www.nortelnetworks.com/help/contact/erc/index.html>.

16 Preface

Chapter 1 Overview

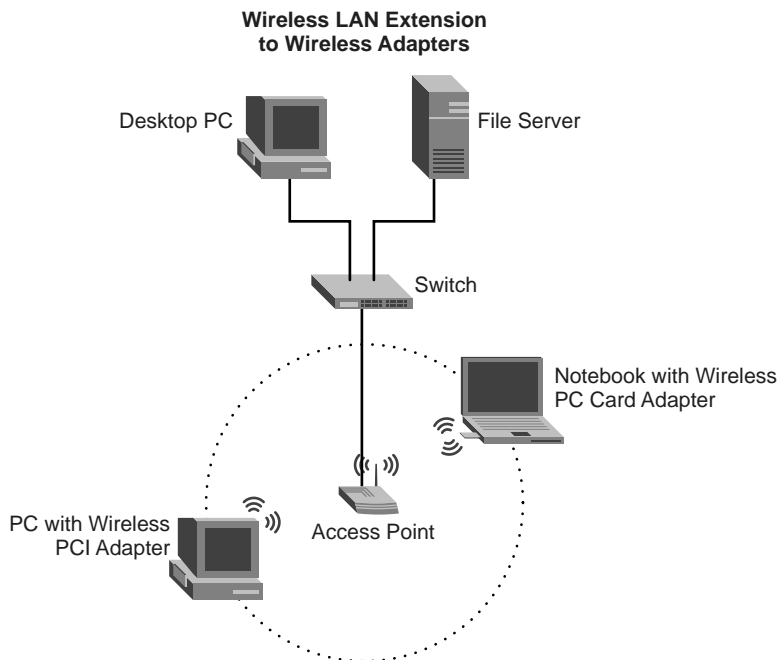
Nortel Networks WLAN - Mobile Adapter 2202 configuration modes

You can configure the Nortel Networks WLAN - Mobile Adapter 2202 to work in either *infrastructure* mode or *ad hoc* mode. For information on specifying the configuration mode, see [“Connecting to a network” on page 40](#).

Infrastructure (access point) mode

In infrastructure mode, devices communicate with each other through an access point (AP). In this mode, wireless devices can communicate with each other as well as with work stations, file servers, and other components on a wired network ([Figure 1](#)). When one AP is connected to a wired network and a set of wireless stations, it is referred to as a BSS (Basic Service Set).

In infrastructure mode, the wireless network adapter utilizes a BSS as a station and communicates with other wireless stations and with the components in the wired network through the access point.

Figure 1 Infrastructure mode

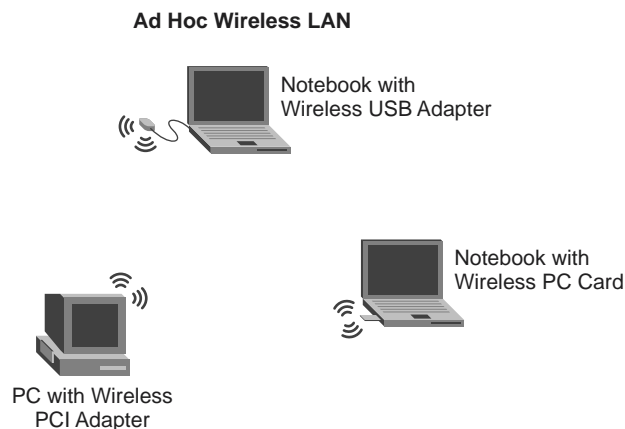
11194FA

Ad hoc mode

In ad hoc mode (Figure 2), wireless network adapters work within an independent basis service set (IBSS) and all stations communicate directly with each other without using an access point (AP). Ad-hoc mode is also called *peer-to-peer mode*.

An ad hoc wireless LAN consists of a group of computers, each of which is equipped with a wireless adapter card, that is connected by radio signals as an independent wireless LAN.

In most cases, computers in an ad hoc wireless LAN automatically detect the channel being used for the ad hoc network. When using ad hoc mode with the 2.4 GHz frequency range, you either can let the computer auto-detect the channel or manually set the channel. When manually setting the channel, all computers in the wireless LAN must be configured to the same radio channel.

Figure 2 Ad hoc mode

Added support for Advanced Encryption Standard (AES)

The Nortel Networks WLAN - Mobile Adapter 2202 Utility enables you to create and edit configuration profiles and to display various diagnostics information pertaining to the Nortel Networks WLAN - Mobile Adapter 2202.

The Nortel Networks WLAN - Mobile Adapter 2202 introduces support for Advanced Encryption Standard (AES) and associated infrastructure from 802.11i. From the information element (IE) in the access point (AP) broadcast beacon, the Mobile Adapter 2202 automatically detects which encryption mode (WPA-AES or WPA-TKIP) is being used by the AP. The Mobile Adapter 2202 also supports roaming from one AP that is using WPA_TKIP to another AP that is using WPA-AES, and vice versa.

Product package checklist

Before you begin the installation, make sure your Nortel Networks WLAN - Mobile Adapter 2202 package is complete. The Mobile Adapter 2202 package includes the following items:

20 Chapter 1 Overview

- 1 Nortel Networks WLAN - Mobile Adapter 2202 adapter card
- 1 installation software CD
- 1 documentation CD



Note: Nortel Networks WLAN - Mobile Adapter 2202 release 3.0.0.0 includes version 3.0.0.0 of the Mobile Adapter 2202 driver and version 3.0.0.0 of the Mobile Adapter 2202 utility.



Note: Nortel Networks WLAN - Mobile Adapter 2202 release 3.0.0.0 is only available via download from the Nortel Networks support site (www.nortelnetworks.com/support). For installation instructions, see “Installing the driver and utility software” on page 25.

System requirements

Before you install the Mobile Adapter 2202 in your laptop or Desktop PC, verify that it has the following features:

- A 32-bit CardBus slot
- 32 MB memory or greater
- 300 MHz processor or higher
- Microsoft Windows 2000 or Windows XP operating system (with latest software patches and updates)

Mobile Adapter 2202 LEDs

There are two LEDs on the Mobile Adapter 2202, labeled LINK and ACT (activity), which indicate the operating status of the unit. You can check the network connectivity status by looking at the LEDs.

Table 1 Mobile Adapter 2202 LEDs

Network Connectivity Status	LINK LED State	ACT LED State
The Mobile Adapter 2202 radio is enabled and the mobile adapter is scanning for APs.	Blinking (200ms on/off)	Off
The Mobile Adapter 2202 is connected to an AP, but there is no Tx or Rx data activity (not including management frames).	On (continuously on)	Off
The Mobile Adapter 2202 is connected to an AP and there is Tx or Rx data activity. (The LEDs will not blink for management frames.)	On (continuously on)	Blinking
The Mobile Adapter 2202 is not connected to an AP. (Between scans, the mobile adapter is "disabled" for 1-2 minutes.)	Off	Off
The Mobile Adapter 2202 radio is disabled.	Off	Off

Chapter 2

Quick start software installation

This chapter is a quick reference for users who are familiar with the process of installing the Nortel Networks WLAN - Mobile Adapter 2202 driver and utility software and are installing the Mobile Adapter 2202 software for the first time on their PC or laptop. If you need more detailed instructions, see “[To install the Mobile Adapter 2202 driver and utility software:](#)” on page 23. If you are installing a new version of the driver and utility software, see “[Upgrading the driver and utility software](#)” on page 63.



Note: If you are installing the driver and utility software from an installation CD, insert the CD in the CD-ROM drive, open the folder that contains the *setup.exe* file, and begin with step 3.

To install the Mobile Adapter 2202 driver and utility software:

- 1 Download the zip file containing the most recent Mobile Adapter 2202 installation files from the Nortel Networks support Web site (www.nortelnetworks.com/support).

To locate the zip file from the support Web site for downloading:

- a Select **Wireless LAN** from Product Families.
 - b Select **WLAN - Mobile Adapter 2202** as the product.
 - c Select **Software** as the content and click on **Go**.
 - d Click on the most recent version of the software and download it to your PC or laptop.
- 2 Expand the zip file and locate the *setup.exe* file.
 - 3 Double-click on **setup.exe** to start the InstallShield Wizard.
 - 4 Click on **Next**. The Choose Destination Location window opens.

24 Chapter 2 Quick start software installation

- 5 Click on **Next**. (Or, alternatively, use the Browse button to select a different destination folder and then click on **Next**.) A message prompting you to insert the Nortel Networks WLAN - Mobile Adapter 2202 card appears.
- 6 Insert the Nortel Networks WLAN - Mobile Adapter 2202 card into the CardBus slot and click on **OK**. The Setup Status window opens.



Note: If the Found New Hardware Wizard appears, click on **Cancel** to continue with the installation.

As the installation progresses, the Setup Status progress bar lets you monitor the installation process.

- 7 If the Digital Signature Not Found dialog box or the Windows XP compatibility testing dialog box appears during driver installation, click on **Yes** (Windows 2000) or on **Continue Anyway** (Windows XP) to continue the installation. Otherwise, go directly to step 8.
- 8 When the installation completes the **Click OK to reboot the system** message appears. Click on **OK** to reboot the system and complete the installation.

Chapter 3

Driver and utility software installation and uninstallation



Warning:

To protect your computer's configuration, you *must* follow the installation instructions for the specific Windows installation you are running.

Installing the driver and utility software

Perform the following procedure to install the Nortel Networks WLAN - Mobile Adapter 2202 driver and utility software from the software installation CD.



Note: You can insert the adapter card now. Inserting the adapter card will display the Found New Hardware Wizard. If this occurs, click on **Cancel** and continue with the installation.

To install the Mobile Adapter 2202 from the installation CD:

- 1 Insert the software installation CD in the CD_ROM drive.
- 2 Open the software folder to display the *setup.exe* file.
- 3 Double-click on **setup.exe** to start the InstallShield Wizard, begin the installation setup process, and launch the Nortel Networks WLAN - Mobile Adapter 2202 Installation Program (Figure 4).

Figure 3 Starting the InstallShield Wizard message

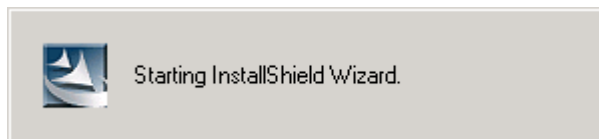
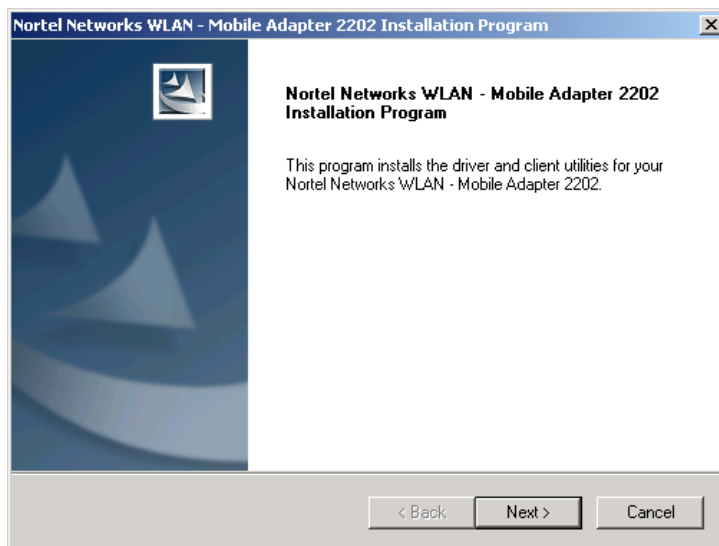
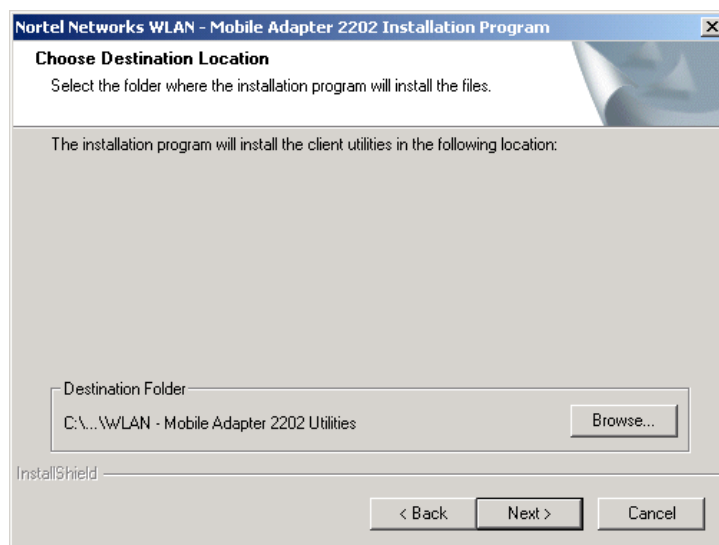


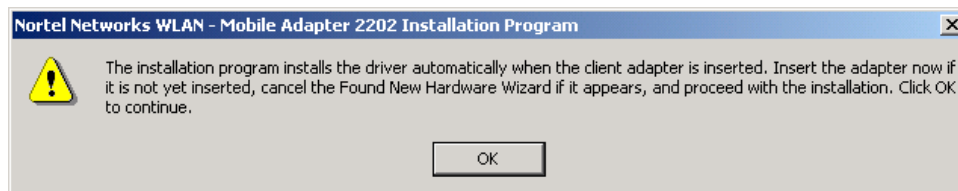
Figure 4 Mobile Adapter 2202 Installation Program window



- 4 Click on **Next**. The Choose Destination Location window opens ([Figure 5](#)).

Figure 5 Choose Destination Location window

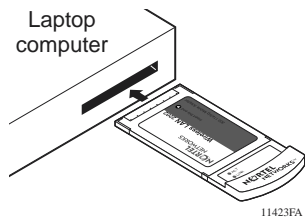
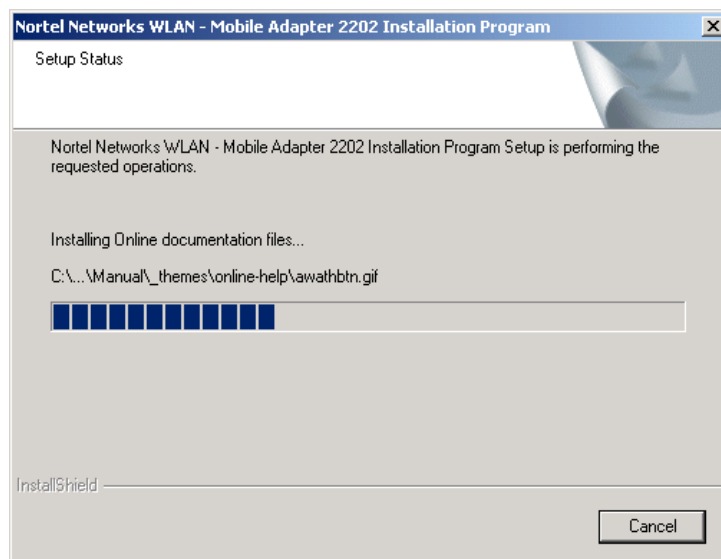
- 5 Click on **Next**. (Or, alternatively, use the Browse button to select a different destination folder and then click on **Next**.) The message dialog box shown in [Figure 6](#) appears.

Figure 6 Insert the Mobile Adapter 2202 card dialog box

- 6 If not already inserted, insert the Nortel Networks WLAN - Mobile Adapter 2202 card ([Figure 7](#)) into the CardBus slot and click on **OK**. The Setup Status window opens ([Figure 8](#)).

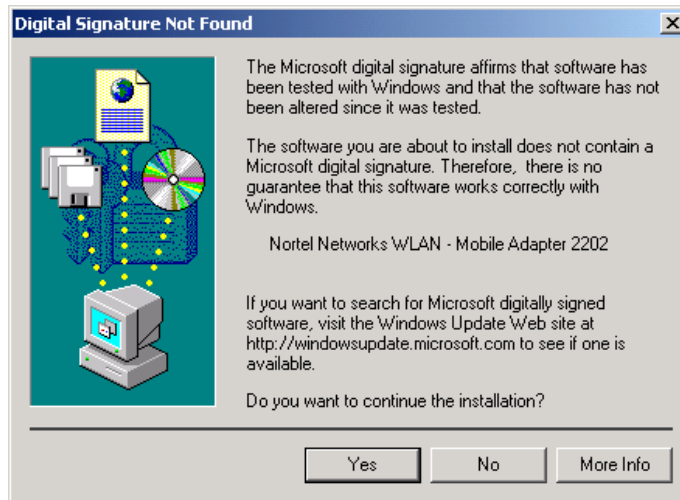


Note: If the Found New Hardware Wizard appears, click on **Cancel** to continue with the installation.

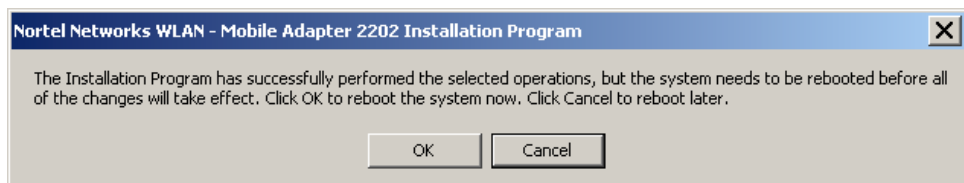
Figure 7 Inserting an adapter card**Figure 8** Installation Program Setup Status window

As the installation progresses, the Setup Status progress bar lets you monitor the installation.

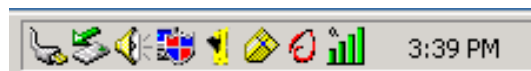
- 7 If the Digital Signature Not Found dialog box (Figure 9) or the Windows XP compatibility testing dialog box appears during driver installation, click on **Yes** (Windows 2000) or on **Continue Anyway** (Windows XP) to continue the installation. Otherwise, go directly to step 8.

Figure 9 Digital Signature Not Found dialog box

- 8 When the installation completes, the utility prompts you to reboot (Figure 10). Click on **OK** or **Cancel** as desired.

Figure 10 Reboot prompt

When the system completes rebooting, the Mobile Adapter 2202 Utility icon appears in the system tray (Figure 11). The Mobile Adapter 2202 Utility icon is the icon to the left of the system time in Figure 11.

Figure 11 WLAN Mobile Adapter Utility Icon in system tray

Periodically, you should check the Nortel Networks support Web site for upgraded versions of the Mobile Adapter 2202 software. If you find a newer version of the 2202 driver and utility software, use the procedure in “[Upgrading the driver and utility software](#)” on page 63 to install it.

Additional installation information

During the software installation procedure, select the **Install the software automatically** option if a window with this option appears. Then, click on **Next** to continue with the installation.



Note: Refer to [“Configuring advanced settings for Windows XP”](#) on [page 45](#) for information on disabling the Windows XP Zero Configuration tool.

Uninstalling the Mobile Adapter 2202

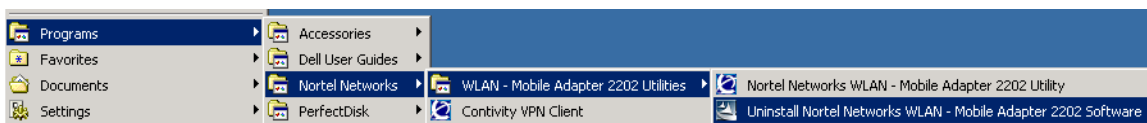


Note: Before uninstalling the Mobile Adapter 2202, close all running programs and make sure that the Mobile Adapter 2202 is inserted in the CardBus slot.

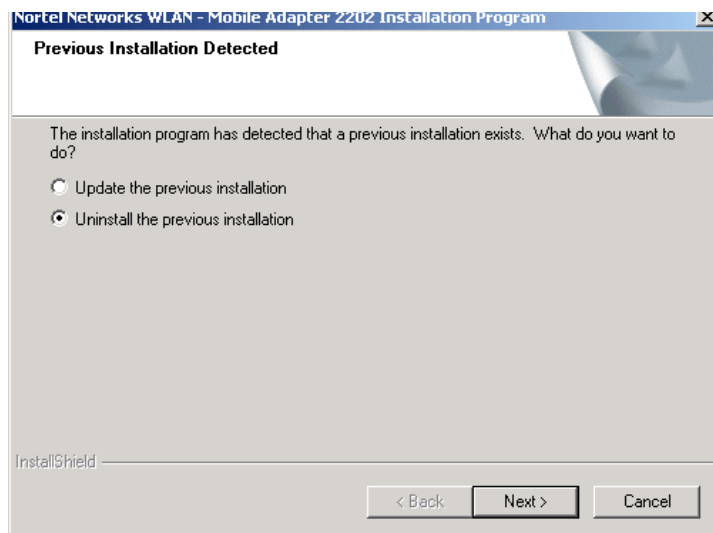
To uninstall the Nortel Networks WLAN - Mobile Adapter 2202:

- 1 Select Start > Programs > Nortel Networks > WLAN - Mobile Adapter 2202 Utilities > Uninstall Nortel Networks WLAN - Mobile Adapter 2202 Software ([Figure 12](#)).

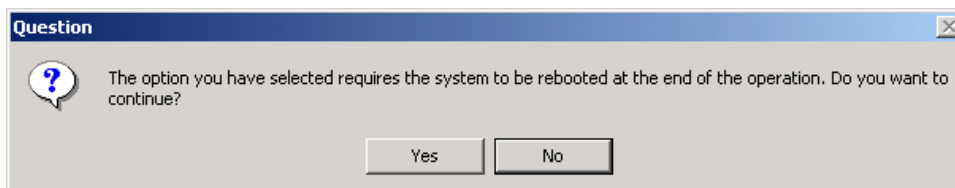
Figure 12 Uninstall the Mobile Adapter 2202 option



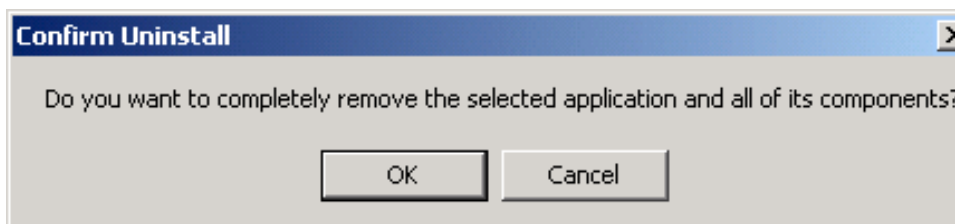
- 2 The Previous Installation Detected window opens ([Figure 13](#)).

Figure 13 Previous Installation Detected window

- 3 Select the **Uninstall the previous installation** radio button and click on **Next**. The **...option you have selected requires the system to be rebooted...** dialog box appears (Figure 14).

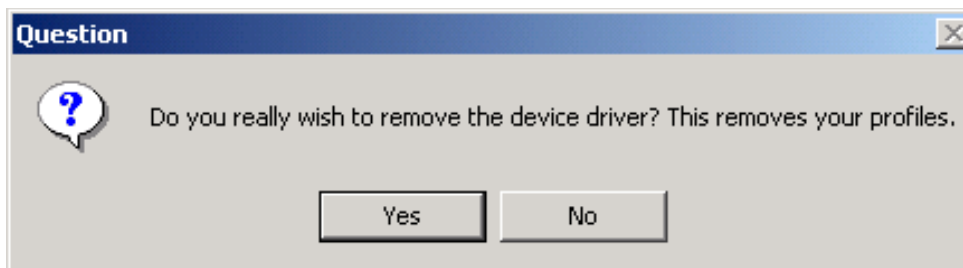
Figure 14 Selected option requires a reboot dialog box

- 4 Click on **Yes**. The Confirm Uninstall dialog box opens (Figure 15).

Figure 15 Confirm Uninstall dialog box

32 Chapter 3 Driver and utility software installation and uninstallation

- 5 Click on **OK**. The **Stopping the Configuration Service. This may take up to thirty seconds...** message appears followed by the **Do you really wish to remove the device driver? This removes your profiles.** dialog box (Figure 16).

Figure 16 Remove the device driver dialog box

- 6 Click on **Yes** unless you plan to reinstall the Mobile Adapter 2202 software or install a newer version of the Mobile Adapter 2202 software in the near future. If you intend to reinstall the Mobile Adapter 2202 software or install a newer version of it in the near future, click on **No** to save your profiles.

The progress bar in the Setup Status window shows the progress of the uninstallation operation (Figure 17). When the uninstallation operation completes, the utility prompts you to reboot (Figure 18).

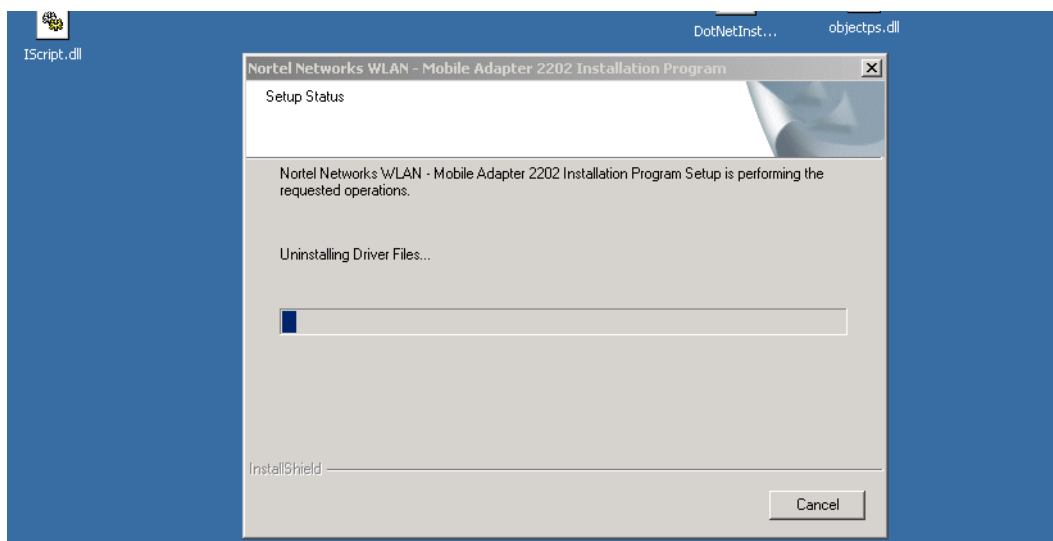
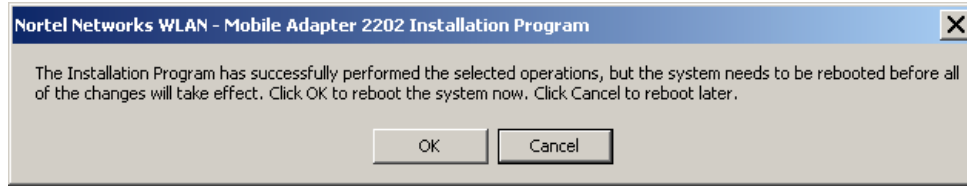
Figure 17 Setup Status window

Figure 18 Reboot prompt

- 7 Click on **OK** to reboot the system now and complete the remaining uninstallation system tasks. Or, click on **Cancel** and reboot later.

34 Chapter 3 Driver and utility software installation and uninstallation

Chapter 4

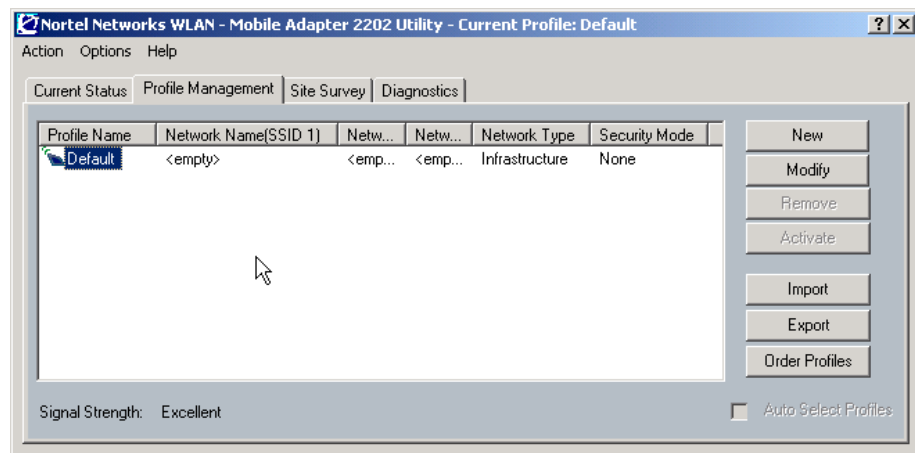
Configuring basic network settings

This chapter provides instructions for using the Mobile Adapter 2202 Utility to configure basic network settings. After you complete these tasks, see “[Chapter 5 Configuring network security](#)” for information on configuring network security.

Creating a new network profile

- 1 To create a new Network Configuration profile, click on the **Profile Management** tab on the Nortel Networks WLAN - Mobile Adapter 2202 Utility window ([Figure 19](#)).

Figure 19 Mobile Adapter 2202 Utility — Profile Management tab



- 2 Click on **New**. The Profile Management window opens ([Figure 20](#)).

Figure 20 Profile Management window — General tab

- 3 Enter a Profile Name and the correct SSIDs for the network that you are going to join. (The Client Name is supplied by the utility.) [Table 2](#) describes the items on the Profile Management Settings - General tab.

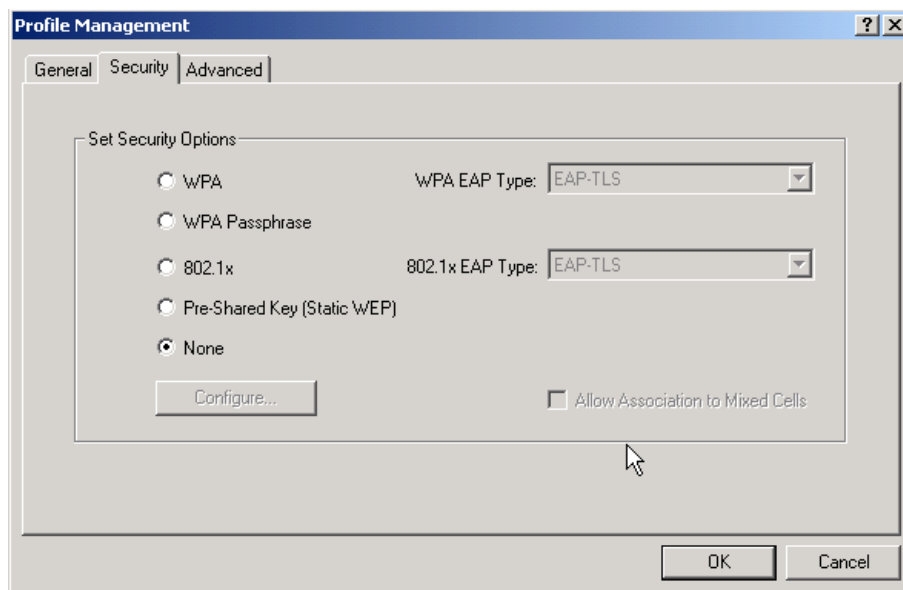
Table 2 Profile Management Settings — General tab

Item	Description
Profile Name	This name identifies the configuration. This name must be unique.
Client Name	The client name is the name of the computer in which the Mobile Adapter 2202 card is installed.
SSID (1-3)	The name of the wireless network. This name cannot be longer than 32 characters. If the field is set to be "ANY" or is left blank, your computer will connect to an AP with the best signal strength.

- 4 Click on the Security tab ([Figure 21](#)) to display the Set Security Options. By default, the security option for the network profile is set to None. To complete the basic configuration procedure, leave the security option set to None for now.

It is recommended that you use one of the security options provided. For information on configuring each of these security options, see “[Chapter 5 Configuring network security](#)” on page 47 after you complete this basic profile configuration procedure.

Figure 21 Profile Management — Security tab



The default profile is configured to use none of the security options. You should configure a security option after you complete the basic profile management configuration.

- 5 Click on the **Advanced** tab to set advanced settings ([Figure 22](#)). [Table 3](#) lists the items on the Profile Management- Advanced tab.

Figure 22 Profile Management — Advanced tab

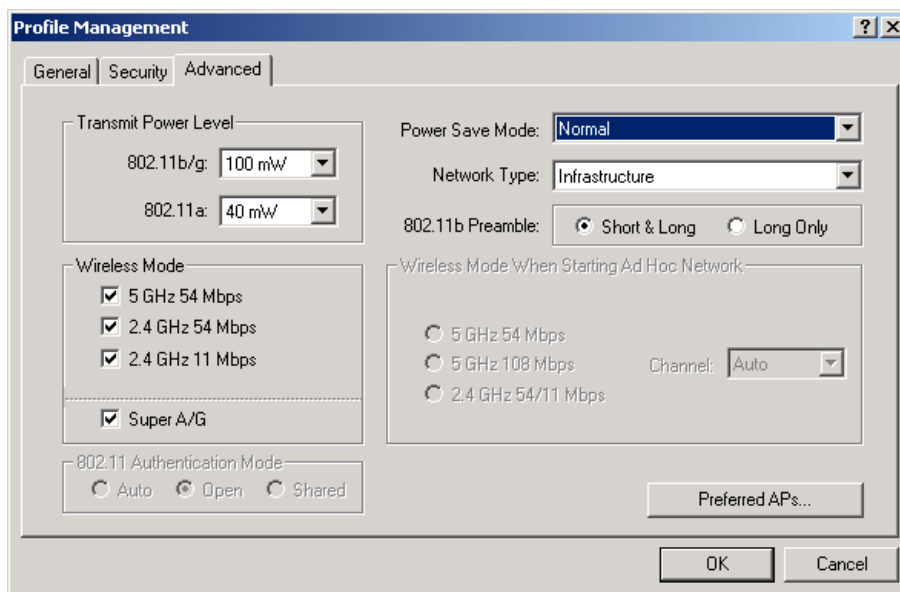


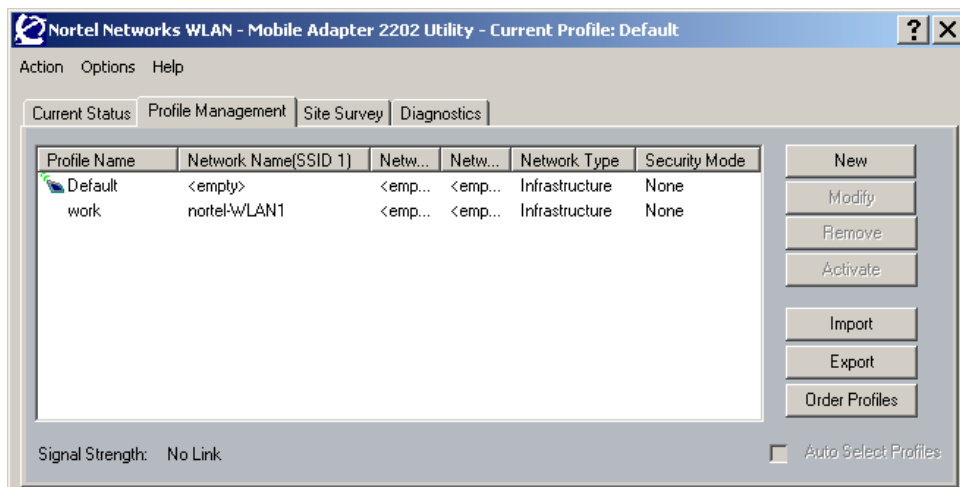
Table 3 Profile Management — Advanced tab

Item	Description
Power Save Mode	The three power management options are “Off,” “Normal” and “Maximum.” In Ad Hoc mode, the Power Save function cannot be enabled.
Network Type	This field specifies the mode of the network. The two options are “Access Point” and “Ad Hoc.”
802.11b Preamble	The two options are “Short & Long” and “Long Only.”
Transmit Power Level	The options are 100, 63, 50, 30, 20, and 10 milliwatts (mW) for 802.11 b/g and 40, 25, 20, 13, and 10 mW for 802.11a.
Wireless Mode	The three options are “5 GHz 54 Mbps,” “2.4 GHz 54 Mbps” and “2.4 GHz 11 Mbps.”
Super A/G	When Super A/G is selected, turbo mode is enabled.

Table 3 Profile Management — Advanced tab (continued)

Item	Description
Wireless Mode When Starting Ad Hoc Network	The options are 5 GHz 54 Mbps, 5 GHz 108 Mbps, and 2.4 GHz 54/11 Mbps. When using 2.4 GHz, additional options for channel are “Auto” or channels 1-11. These options are enabled only if “Ad Hoc” is selected as the Network Type.
802.11 Authentication Mode	<p>The three options are:</p> <ul style="list-style-type: none"> • “Auto”—causes the adapter to attempt authentication using “Shared”, but switches it to “Open” authentication if shared authentication fails. • “Open”—enables an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match. • “Shared”—only allows the adapter to associate with access points that have the same WEP key. <p>Nortel Networks recommends the “Open” setting for enhanced security.</p>

- 6 Once you have entered all the Advanced tab settings, click on **OK**. The newly created profile will be displayed in the Profile Management tab (Figure 23).

Figure 23 Mobile Adapter 2202 Utility — Profile Management tab

Connecting to a network

- 1 Select Start > Programs > Nortel Networks > WLAN - Mobile Adapter 2202 Utilities > Nortel Networks WLAN - Mobile Adapter 2202 Utility (Figure 24) and the Mobile Adapter 2202 Utility window “opens (Figure 25).

Figure 24 Launching the Mobile Adapter 2202 Utility

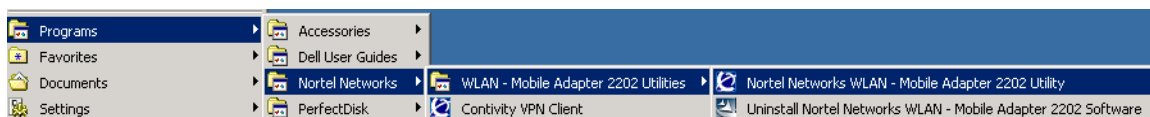
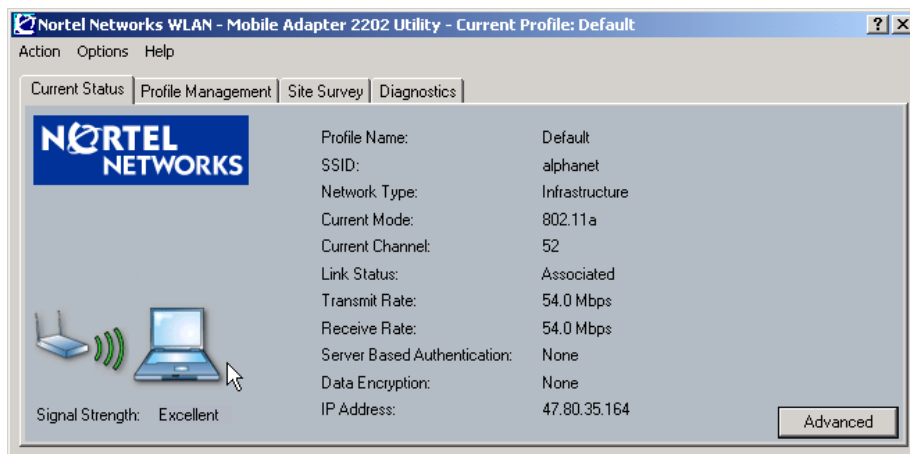
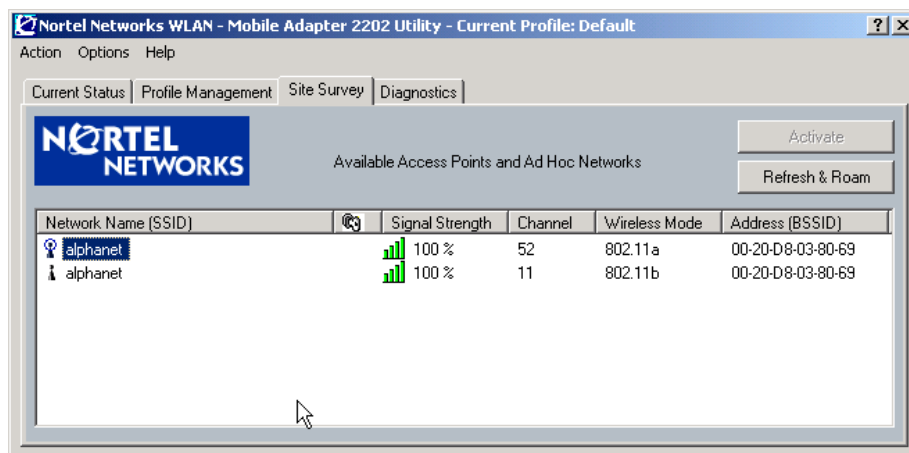


Figure 25 Mobile Adapter Utility window



- 2 Click on the **Site Survey** tab to bring up a list of the available access points and ad hoc networks (Figure 26).

Figure 26 Mobile Adapter 2202 Client Manager - Site Survey tab

Note: An access point shown with no SSID value is configured as a closed system. If the Mobile Adapter 2202 is configured with the matching SSID of an access point configured for a closed system, the site survey will display the SSID of that access point. The Mobile Adapter 2202 will associate to an access point configured for a closed system only when the SSID of the access point matches the SSID of the Mobile Adapter 2202's active profile.

A circle on the icon next to the Network Name (SSID) indicates that the Mobile Adapter 2202 is associated with that access point or ad hoc network (Figure 27 and Figure 28.) See “Nortel Networks WLAN - Mobile Adapter 2202 configuration modes” on page 17 for more information about ad hoc mode and infrastructure mode.

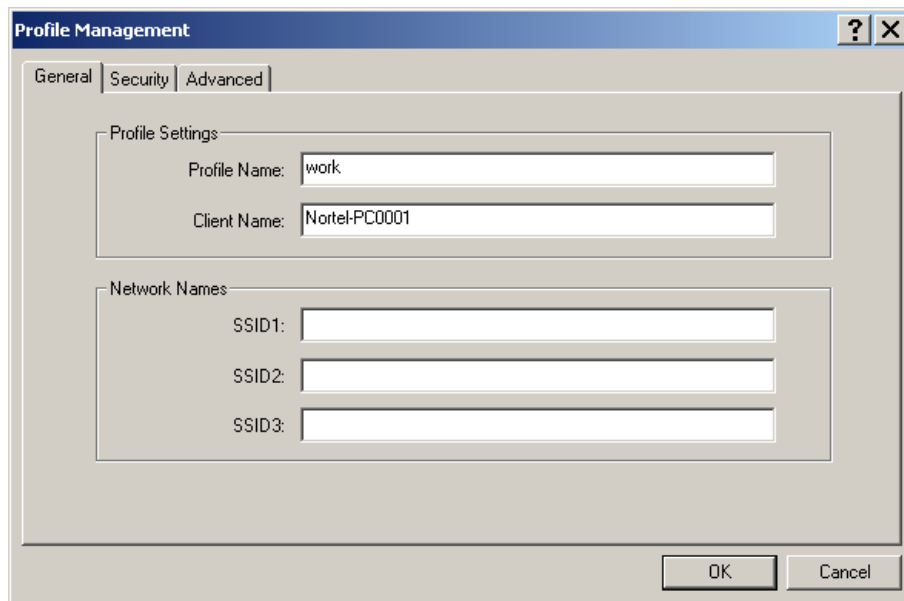
Figure 27 Association icon for an access point connected to a wireless infrastructure network**Figure 28** Association icon for an ad hoc wireless network

42 Chapter 4 Configuring basic network settings

- 3 To connect to a different access point, select the Network Name (SSID) for that access point and click on **Activate**.

If you do not already have a configuration profile created for this association, you will be prompted to create one. The Profile Management window will open (Figure 29).

Figure 29 Profile Management window — General tab



The screenshot shows a window titled "Profile Management" with a blue title bar containing a help icon and a close icon. Below the title bar are three tabs: "General", "Security", and "Advanced". The "General" tab is selected. The main area of the window is divided into two sections. The first section, "Profile Settings", contains two text input fields: "Profile Name" with the text "work" and "Client Name" with the text "Nortel-PC0001". The second section, "Network Names", contains three empty text input fields labeled "SSID1:", "SSID2:", and "SSID3:". At the bottom right of the window are two buttons: "OK" and "Cancel".

To create a new configuration profile, go to [“Creating a new network profile” on page 35](#), and begin with step 3.

Managing Auto Profile Selection

For infrastructure mode profiles, the Mobile Adapter 2202 utility provides the Auto Profile Selection Management feature, which lets you specify the profiles the utility uses to locate an access point to associate with and lets you specify the order of the profiles it uses to scan for an access point. Once you have set up this feature, you no longer have to manually activate a different profile when you change locations; the auto profile feature does the work for you.

This feature is useful when you need to connect to the network from different locations and you have created a profile with different settings for each location.

This feature applies only to profiles that have infrastructure specified as the network type, and to profiles that specify only one SSID. In addition, if more than one profile uses the same SSID, only one of those profiles can be added to the Auto Selected Profiles list.



Note: The “Default” profile cannot be added to the Auto Selected Profiles list.

To add, remove, and order profiles for auto selection:

- 1 Click on the **Order Profiles** button on the Program Management tab (Figure 30) to display the Auto Profile Selection Management window (Figure 31). All the profiles that you created are displayed in the Available Profiles area.

Figure 30 Profile Management tab — ordering profiles

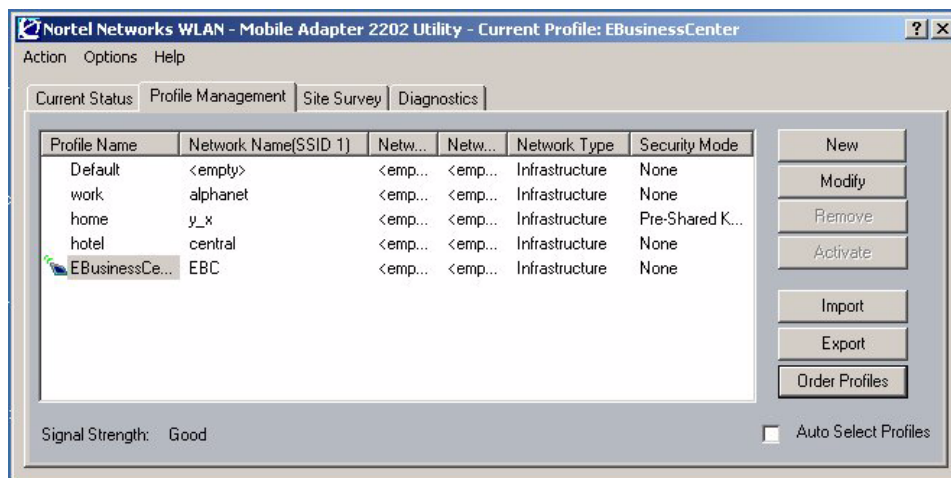
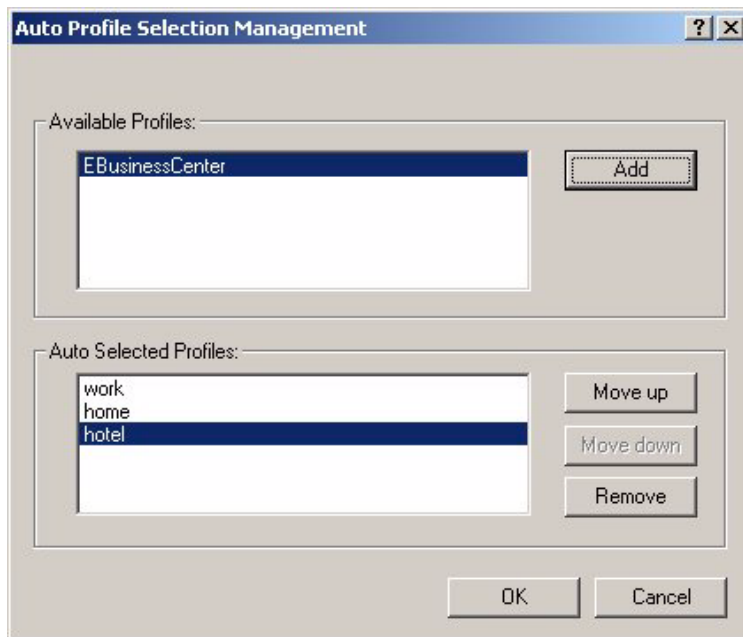


Figure 31 Auto Profile Selection Management window

- 2 To add a profile to the list used for auto selection, highlight the profile name and click on the **Add** button. Repeat this step for each profile you want to add to the Auto Selected Profiles list.
- 3 To remove a profile from the Auto Selected Profiles list and return it to the Available Profiles section, highlight the profile name and click on the **Remove** button.
- 4 To change the order of the profiles in the list, highlight a profile name and use the **Move up** or **Move down** buttons as appropriate until the profiles appear in the order in which you want the utility to scan for an access point to associate with. The utility will use the profiles in order, from the top of the list to the bottom of the list.
- 5 Click on **OK** to save the list and return to the Profile Management tab.
- 6 Select the **Auto Select Profiles** check box to activate the Auto Profile Selection feature.

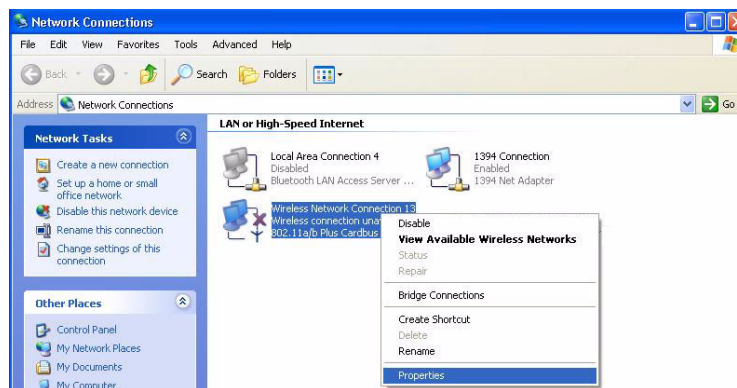
Configuring advanced settings for Windows XP

If you are using Windows XP, it is recommended that you use the Mobile Adapter 2202 Utility rather than the Windows XP Zero Configuration tool.

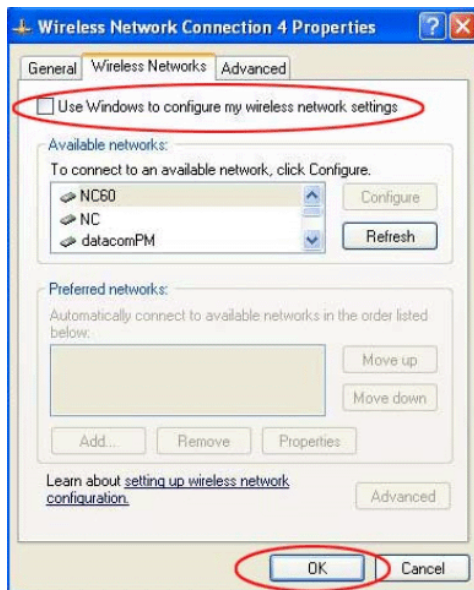
Before using the Mobile Adapter 2202 Utility, please perform the following steps to disable the Windows XP Zero Configuration tool:

- 1 Go to the Control Panel and double-click on **Network Connections**.
- 2 Right-click on **Wireless Network Connection...** and select **Properties** (Figure 32) to display the Properties dialog box.

Figure 32 CardBus context menu



- 3 Select the **Wireless Networks** tab on the Properties dialog box (Figure 33).

Figure 33 Wireless networks tab

- 4 On the Wireless Networks tab, uncheck the **Use Windows to configure my wireless network settings** check box. Then, click on **OK**.

Chapter 5

Configuring network security

Overview

This chapter explains how to use the Nortel Networks WLAN - Mobile Adapter 2202 Utility to configure network security. While using the Mobile Adapter 2202, encrypting data can protect it as it is transmitted through the wireless network.

The Nortel Networks WLAN - Mobile Adapter 2202 Utility lets you use one of the following connection profile options:

- WPA security

This option enables the use of Wi-Fi Protected Access (WPA). This option requires network administration support. This option includes the EAP (with dynamic WEP keys) security protocols: EAP and PEAP.

WPA is a standards-based, interoperable security enhancement that provides data protection and access control for wireless LAN systems. It is derived from and is forward compatible with the IEEE 802.11i standard. WPA leverages Temporal Key Integrity Protocol (TKIP) and Michael message integrity check (MIC) for data protection, and 802.1X for authenticated key management.

WPA supports two mutually exclusive key management types: WPA and WPA passphrase (also known as WPA-Pre Shared Key (PSK)). Using WPA, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). The server generates the PMK dynamically and passes it to the access point.

- WPA-PSK security

This option enables WPA passphrase security (also known as WPA-Pre Shared Key (PSK)).

- 802.1x security

This option enables 802.1x security. This option requires network administration support. This option includes the EAP (with dynamic WEP keys) security protocols: EAP and PEAP.

802.1x is the standard for wireless LAN security defined by IEEE as 802.1x for 802.11, or simply 802.1x.

An access point that supports 802.1x and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network.

- Pre-Shared Key security (static WEP)

This option enables the use of up to four pre-shared (static wired equivalent privacy (WEP)) keys that are defined on both the access point and the station. These keys are stored in an encrypted format in the registry of the Windows device. When the driver loads and reads the client adapter's registry parameters, it also finds the static WEP keys, decrypts them, and stores them in volatile memory on the adapter.

If a device receives a packet that is not encrypted with the matching key, the device drops the packet and never delivers it to the intended receiver.

- No security

Link encryption/decryption is disabled; no keys are installed.

Authentication sequence

Enabling EAP on the access point (AP) and configuring the client adapter for EAP-TLS, EAP-TTLS, PEAP (EAP_GTC), or PEAP (EAP-MSCHAP V2) authentication to the network occurs in the following sequence:

- 1 The client associates to an AP and begins authentication.
- 2 Communicating through the AP, the client and the RADIUS server complete authentication with the password (PEAP) or certificate (EAP-TLS/EAP-TTLS). The password is never transmitted during the process.

- 3 After successful authentication, the client and RADIUS server derive a dynamic WEP key that is unique to the client.
- 4 The RADIUS server transmits the key to the AP using a secure channel on the wired LAN.
- 5 For the length of the session, the AP and the client use this key to encrypt or decrypt all unicast and broadcast packets.

EAP security

To use EAP security, access the Security tab in the Profile Management window of the Mobile Adapter 2202 Utility and perform the following steps:

- 1 In the Profile Management window, click on **New** or **Modify** to edit the security settings.
- 2 Select a profile to edit, or enter a name for the new profile in the Profile Management window, and enter the SSID of the AP to which the station connects.
- 3 On the Security tab, select the **WPA** radio button or the **802.1x** radio button depending on what type of EAP security you want to configure.
- 4 Select **EAP-TLS** or **EAP-TTLS** from either the WPA EAP Type or 802.1x EAP Type drop-down menu as appropriate, depending on what you selected in step 3.
- 5 Do one of the following:
 - To enable EAP-TLS security, go to [“Enabling EAP-TLS security.”](#)
 - To enable EAP-TTLS security, go to [“Enabling EAP-TTLS security.”](#)

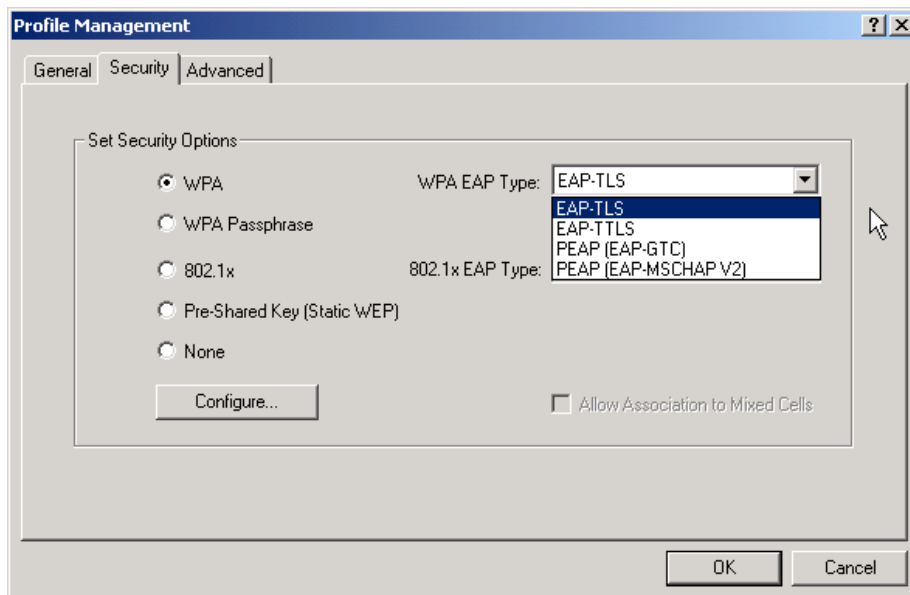
Enabling EAP-TLS security

To use EAP-TLS security, the machine first must have the EAP-TLS certificates downloaded on to it. See your network administrator.

To enable EAP-TLS security:

50 Chapter 5 Configuring network security

- 1 Once the EAP-TLS certificates are downloaded to the adapter card, select **EAP-TLS** from the WPA EAP Type or 802.1x EAP Type drop-down menu (Figure 34).

Figure 34 EAP-TLS Security Option

- 2 Select the appropriate certificate authority from the list. The server/domain name and the login name are filled in automatically from the certificate information. Click on **OK**.
- 3 Click on **OK** to save the security settings for the profile and return to the Profile Management window.
- 4 To enable the profile, highlight the profile and click on the **Activate** button.

Enabling EAP-TTLS security

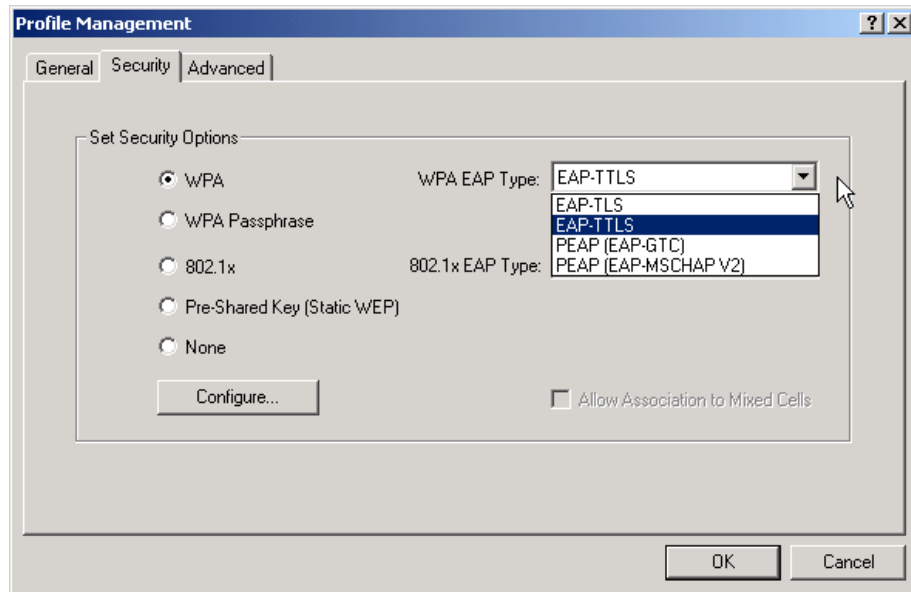
To use EAP-TTLS security, the machine first must have the EAP-TTLS certificates downloaded on to it. See your network administrator.

EAP security uses a dynamic session-based WEP key from the client adapter and the RADIUS server for encryption, and a client certificate for authentication.

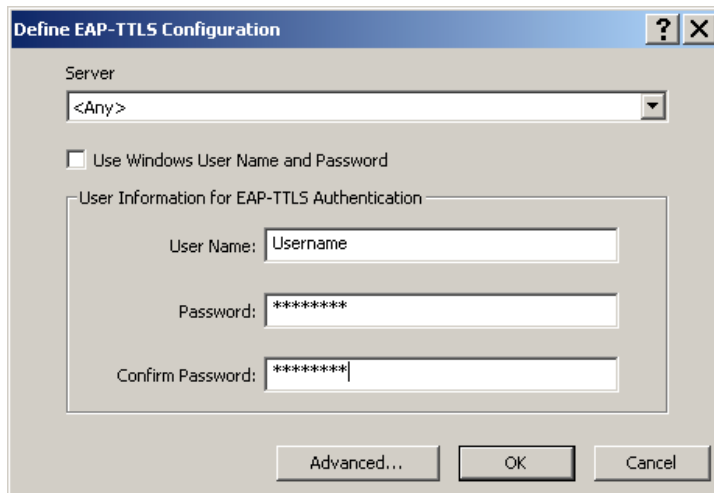
To enable EAP-TTLS security:

- 1 Once the EAP-TTLS certificates are downloaded to the adapter card, select **EAP-TTLS** from the WPA EAP Type or 802.1x EAP Type drop-down list (Figure 35).

Figure 35 EAP-TTLS Security Option



- 2 Click on the **Configure** button. The Define EAP-TTLS Configuration window appears (Figure 36).

Figure 36 Define EAP-TTLS Configuration window

- 3 Select the appropriate certificate from the drop-down list and click on **OK**.
- 4 Specify a user name for EAP authentication:

Select **Use Windows User Name** to use the Windows user name as the EAP user name. Otherwise, enter an EAP user name in the User Name field to use a different user name and password and start the EAP authentication process.
- 5 Click on the **Advanced** button and do one or more of the following:
 - Leave the Server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (recommended method)
 - Enter the domain name of the server from which the client will accept a certificate.
 - Change the login name if needed.
- 6 Click on **OK** to save the security settings for the profile and return to the Profile Management window.
- 7 To enable the profile, highlight the profile and click on the **Activate** button.

PEAP security

Two types of PEAP security are provided as follows:

- PEAP (EAP-GTC) authentication is designed to support one-time password (OTP), the Windows NT or Windows 2000 domain, and L DAP users databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP (EAP-GTC) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

Networks that use an OTP user database require entering a hardware or software token password to start the PEAP (EAP-GTC) authentication process and to gain access to the network. Networks that use a Windows NT or Windows 2000 domain user database or an L DAP user database (such as NDS) require entering a username, password, and domain name in order to start the PEAP (EAP-GTC) authentication process.

- The PEAP (EAP-MSCHAP V2) authentication type is based on EAP-TLS authentication, but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data.

To use PEAP security, access the Security tab in the Profile Management window of the Mobile Adapter 2202 Utility and perform the following steps:

- 1 In the Profile Management window, click on **New** or **Modify** to edit the security settings.
- 2 Select a profile to edit, or enter a name for the new profile in the Profile Management window, and enter the SSID of the AP to which the station connects.
- 3 On the Security tab, select the **WPA** radio button or the **802.1x** radio button depending on what type of EAP security you want to configure.
- 4 Select **PEAP (EAP-GTC)** or **PEAP (EAP-MSCHAP V2)** from either the WPA EAP Type or 802.1x EAP Type drop-down menu as appropriate, depending on what you selected in step 3.
- 5 Do one of the following:

- To enable EAP-TLS security, go to “[Enabling PEAP \(EAP-GTC\) security.](#)”
- To enable EAP-TTLS security, go to “[Enabling PEAP \(EAP-MSCHAP V2\) security.](#)”

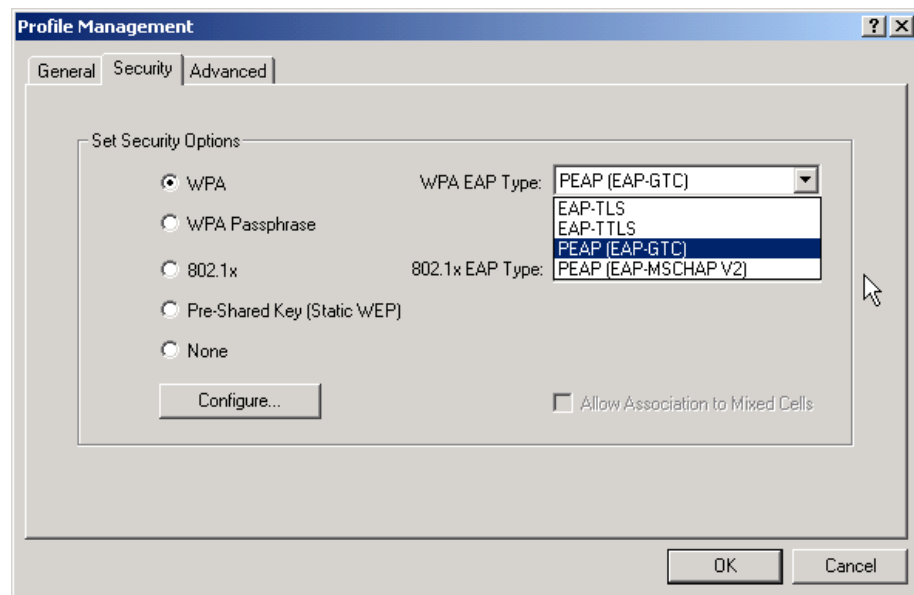
Enabling PEAP (EAP-GTC) security

To use PEAP (EAP-GTC) security, the server first must have PEAP certificates and the server properties must be set already. See your network administrator.

To enable PEAP (EAP-GTC) security:

- 1 Once the PEAP certificates are on the server and the server properties are set, select **PEAP (EAP-GTC)** from the WPA EAP Type or 802.1x EAP Type drop-down menu ([Figure 37](#)).

Figure 37 PEAP (EAP-GTC) Security Option



- 2 Click on the **Configure** button. The Define PEAP (EAP-GTC) Configuration window appears ([Figure 38](#)).

Figure 38 Define PEAP (EAP-GTC) Configuration window

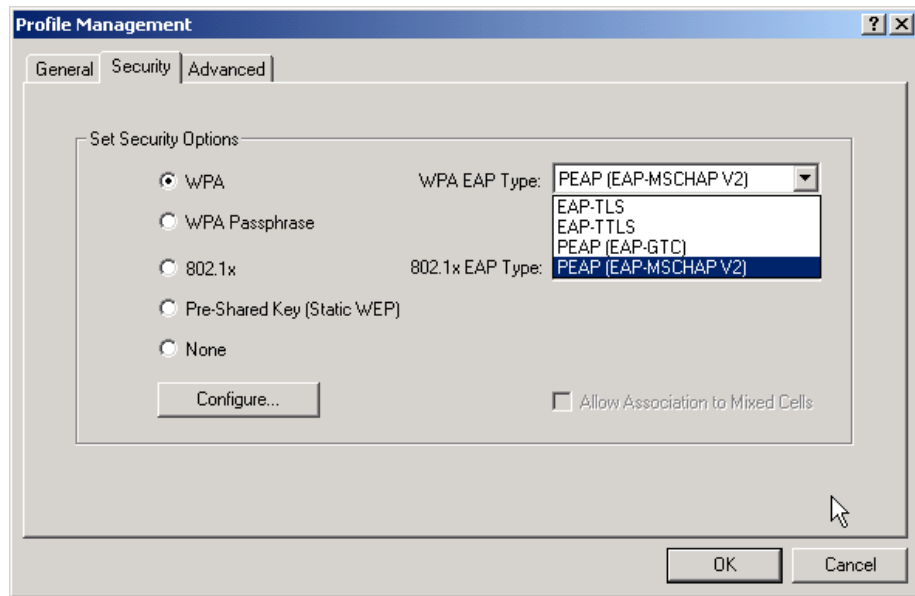
- 3 Enter the server login user name and password and click on the **Advanced** button.
- 4 Enter the domain name and the login name for the network and click on **OK**.
- 5 Click on **OK** to save the security settings for the profile and return to the Profile Management window.
- 6 To enable the profile, highlight the profile and click on the **Activate** button.

Enabling PEAP (EAP-MSCHAP V2) security

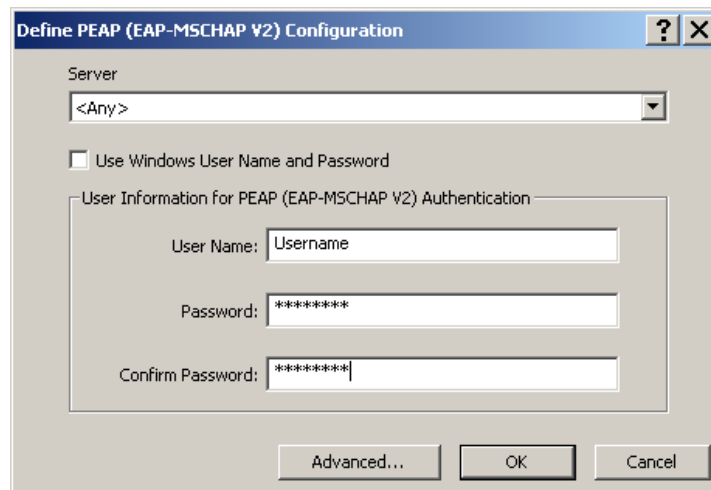
To use PEAP (EAP -MSCHAP V2) security, the server first must have PEAP certificates and the server properties must be set already. See your network administrator.

To enable PEAP (EAP -MSCHAP V2) security:

- 1 Once the PEAP certificates are on the server and the server properties are set, select **PEAP (EAP -MSCHAP V2)** from the WPA EAP Type or 802.1x EAP Type drop-down menu (Figure 39).

Figure 39 PEAP (EAP-MSCHAP V2) Security Option

- 2 Click on the **Configure** button. The Define PEAP (EAP-MSCHAP V2) Configuration window appears (Figure 40).

Figure 40 Define PEAP (EAP-MSCHAP V2) Configuration window

- 3 Select the appropriate certificate from the drop-down menu.

- 4 Specify a user name for inner PEAP tunnel authentication:

Select **Use Windows User Name** to use the Windows user name as the EAP user name. Otherwise, enter an EAP user name in the User Name field to use a different user name and password and start the EAP authentication process.

- 5 Click on the **Advanced** button and:

- Leave the Server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (recommended method)
- Enter the domain name of the server from which the client will accept a certificate.
- The login name for PEAP tunnel authentication fills in automatically as PEAP-xxxxxxxxxxxx, where xxxxxxxxxxxx is the computer's MAC address. Change the login name if needed.

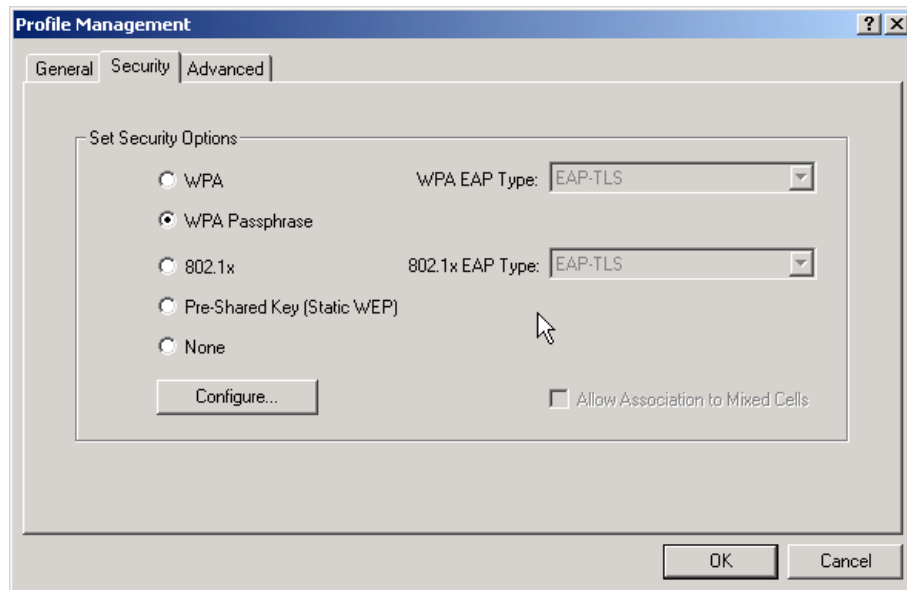
- 6 Click on **OK** to save the security settings for the profile and return to the Profile Management window.

- 7 To enable the profile, highlight the profile and click on the **Activate** button.

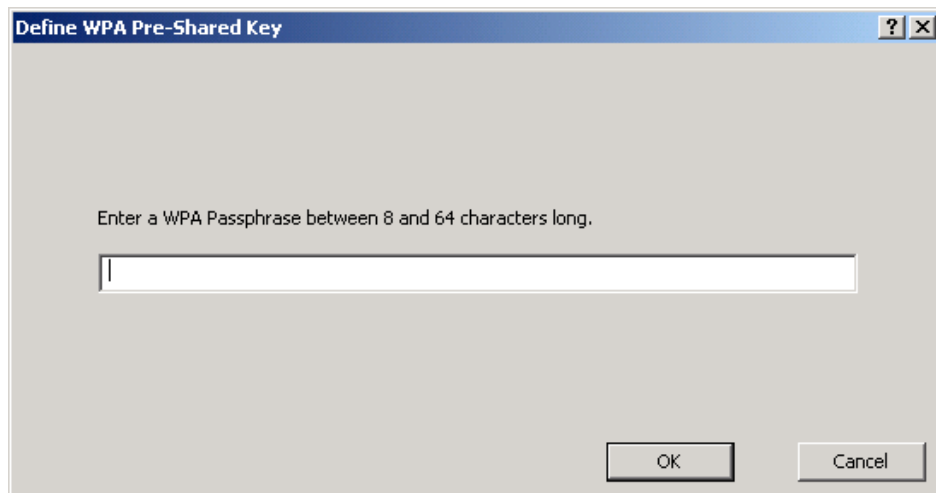
WPA Passphrase (WPA-PSK) security

To use WPA passphrase security, access the Security tab in the Profile Management window of the Mobile Adapter 2202 Utility and perform the following steps:

- 1 On the Profile Management window, click on **New** or **Modify** to edit the security settings.
- 2 Select a profile to edit, or enter a name for the new profile in the Profile Management window, and enter the SSID of the AP to which the station connects.
- 3 On the Security tab, select the **WPA Passphrase** radio button (Figure 41).

Figure 41 Security tab — WPA Passphrase option

- 4 Click on **Configure** to display the Define WPA Pre-Shared Key window (Figure 42).

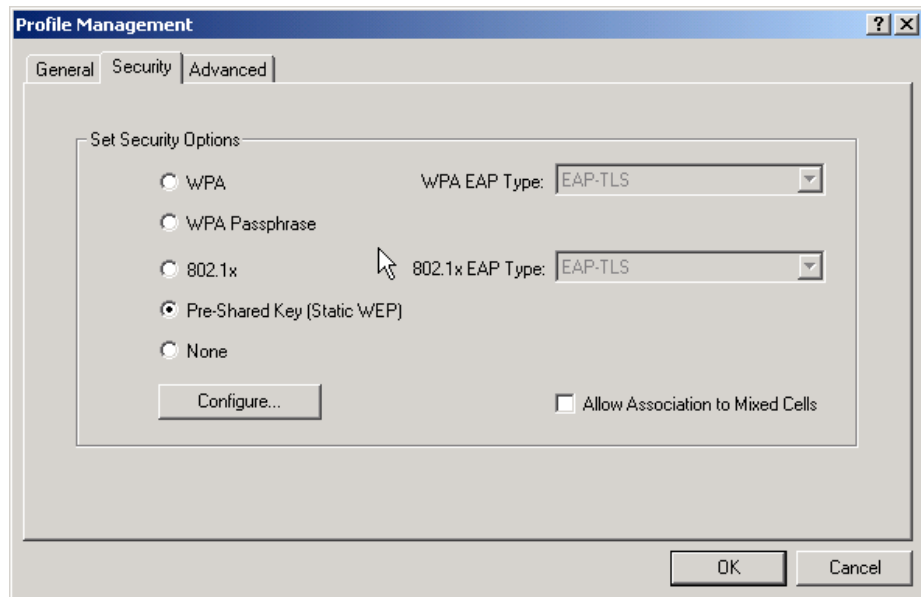
Figure 42 Define WPA Pre-Shared Key window

- 5 Enter the WPA passphrase and click on **OK**. (For ASCII text, enter 8-63 characters. For hexadecimal, enter 64 hexadecimal digits.)
- 6 Click on **OK** to save the security settings for the profile and return to the Profile Management window.
- 7 To enable the profile, highlight the profile and click on the **Activate** button.

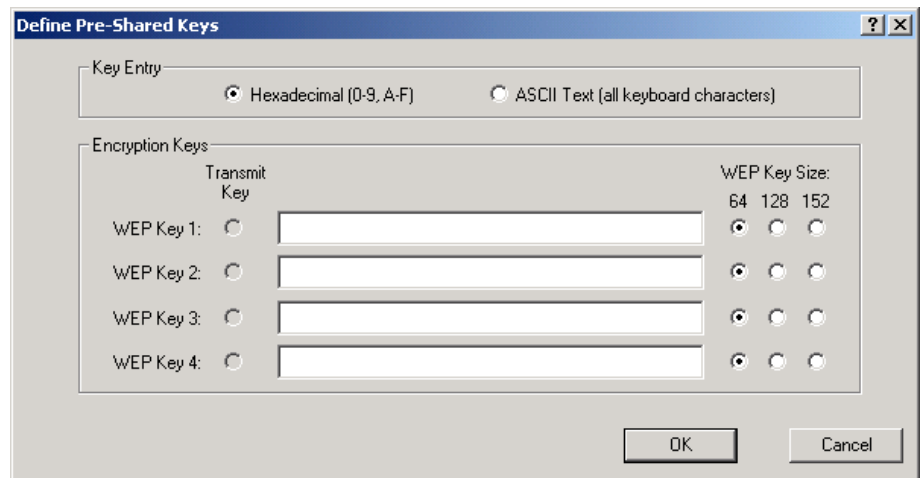
Pre-Shared Key (Static WEP) security

To use Pre-Shared Key (Static WEP) security, access the Security tab in the Profile Management window of the Mobile Adapter 2202 Utility and perform the following steps:

- 1 In the Profile Management window, click on **New** or **Modify** to edit the security settings.
- 2 Select a profile to edit, or enter a name for the new profile in the Profile Management window, and enter the SSID of the AP to which the station connects.
- 3 On the Security tab, select the **Pre-Shared Key (Static WEP)** radio button ([Figure 43](#)).

Figure 43 Security tab — Pre-Shared Key option

- 4 Click on **Configure** to display the Define Pre-Shared Key window (Figure 44).

Figure 44 Define Pre-Shared Key window

- 5 Define the pre-shared keys and select one of the four WEP keys to be used as the default key for transmitting packets. (Typically, WEP Key 1 is used as the default.)
- 6 Click on **OK**.
- 7 If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that **Allow Association to Mixed Cells** is selected on the Security tab to allow association.
- 8 Click on **OK** to save the security settings for the profile and return to the Profile Management window.
- 9 To enable the profile, highlight the profile and click on the **Activate** button.

Chapter 6

Upgrading the driver and utility software

Periodically, you should check the Nortel Networks support Web site for upgraded versions of the Mobile Adapter 2202 software. If you find a newer version of the 2202 driver and utility software, use the procedure in this chapter to install it.



Note: If you currently have the Nortel Networks WLAN - Mobile Adapter 2201 driver and utility software installed, you *must* uninstall it before installing the Mobile Adapter 2202 driver and utility software.

If you are installing a newer version of the Mobile Adapter 2202 driver and utility software, you do not need to uninstall the current version before performing the upgrade.

Upgrading the driver and utility software

Complete the following steps to install a newer version of the Nortel Networks WLAN - Mobile Adapter 2202 driver and utility software:



Note: It is recommended that you have the Mobile Adapter 2202 card inserted into your PC or laptop before beginning the upgrade procedure.

- 1 Download the zip file containing the most recent Mobile Adapter 2202 installation files from the Nortel Networks support Web site (www.nortelnetworks.com/support).

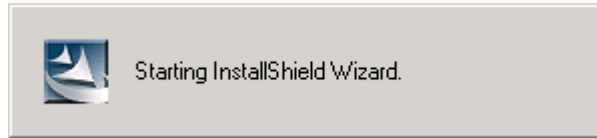
To locate the zip file from the support Web site for downloading:

- a Select **Wireless LAN** from Product Families.
- b Select **WLAN - Mobile Adapter 2202** as the product.

64 Chapter 6 Upgrading the driver and utility software

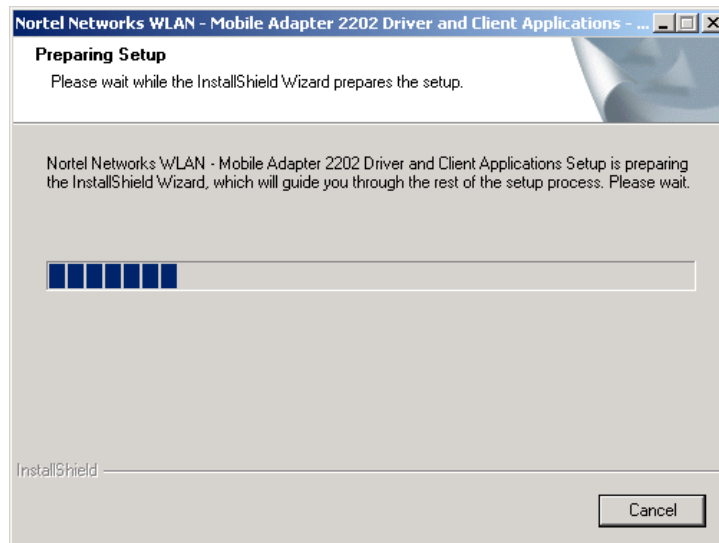
- c** Select **Software** as the content and click on **Go**.
 - d** Click on the most recent version of the software and download it to your PC or laptop.
- 2** Expand the zip file and double-click on **setup.exe** to start the InstallShield Wizard (Figure 45).

Figure 45 Starting the InstallShield Wizard message

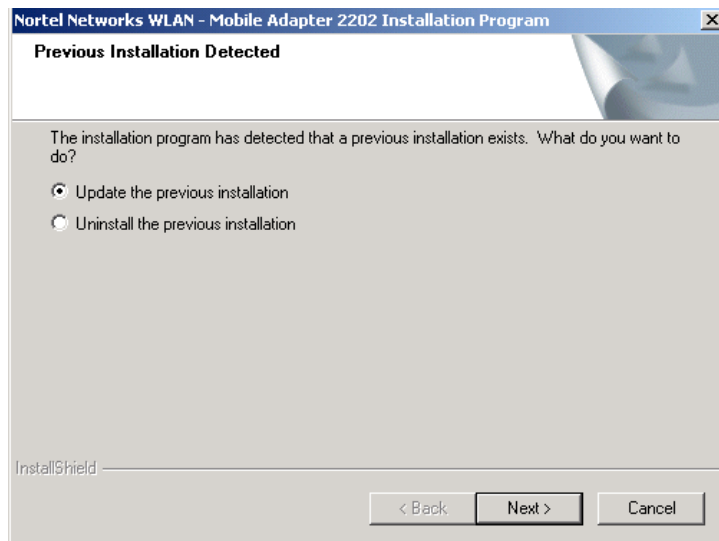


In a few seconds, the Preparing Setup window opens (Figure 46).

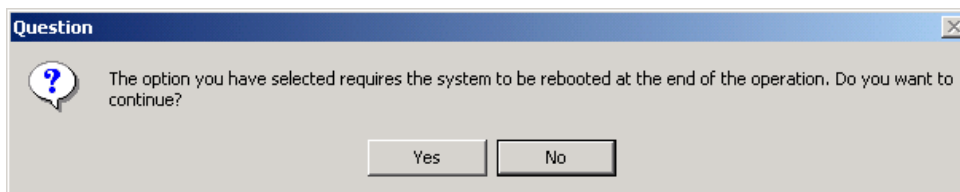
Figure 46 Preparing Setup window



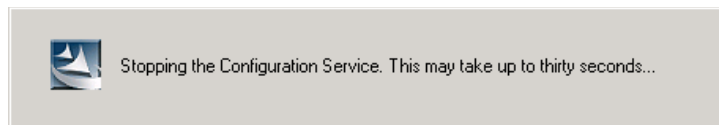
Then, the Previous Installation Detected window opens (Figure 47).

Figure 47 Previous Installation Detected window

- 3 Select **Update the previous installation** if it is not already selected and click on **Next**. The message dialog box shown in [Figure 48](#) appears.

Figure 48 Option requires system reboot dialog box

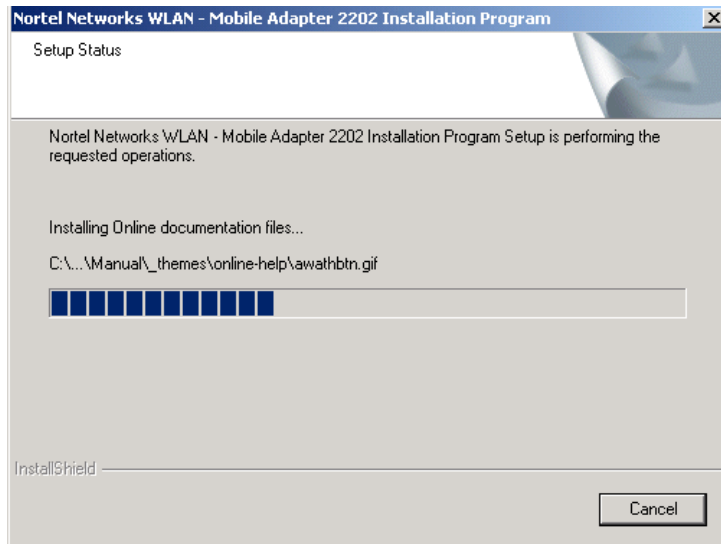
- 4 Click on **Yes**. The **Stopping the Configuration Service** message appears ([Figure 49](#)).

Figure 49 Stopping the Configuration Service message

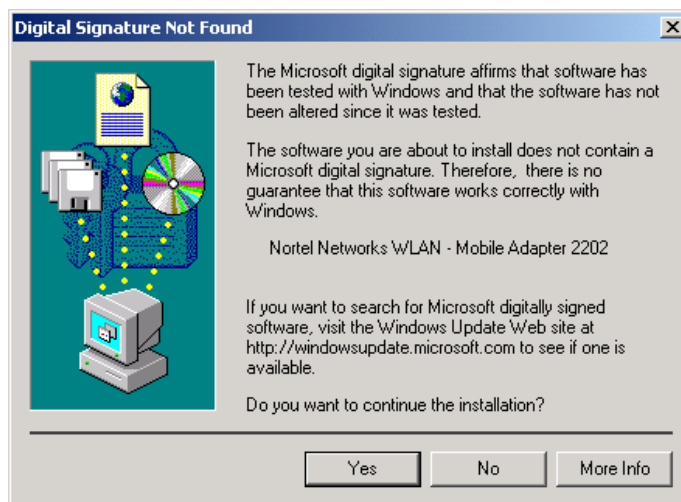
After the configuration service stops, the message disappears and the Setup Status window is visible again ([Figure 50](#)).

Figure 50 Setup Status window

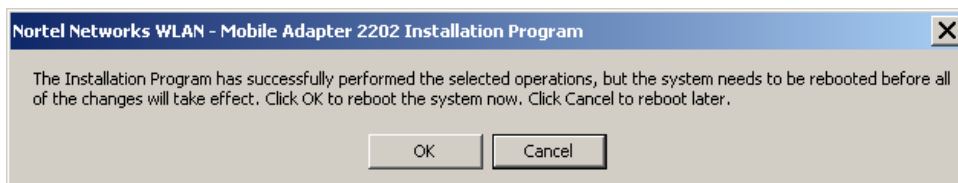
status window



- 5 If the Digital Signature Not Found dialog box (Figure 51) or the Windows XP compatibility testing dialog box appears during driver installation, click on **Yes** (Windows 2000) or on **Continue Anyway** (Windows XP) to continue the installation.

Figure 51 Digital Signature Not Found dialog box

When the installation completes, the utility prompts you to reboot ([Figure 52](#)).

Figure 52 Reboot prompt

6 Click on **OK**. The system reboots and the upgrade installation is complete.

Appendix A

Troubleshooting guidelines

Verifying driver operation

For Windows 2000

- 1 Right-click on the **My Computer** icon on the desktop and select **Properties**.
- 2 Select the **Hardware** tab and click on **Device Manager**. Open **Network adapters**. You should see your Mobile Adapter 2202 in the list. Right-click on this **Mobile Adapter 2202** and choose **Properties**.
- 3 From the “Device status”, you should see the line “This device is working properly.” If, instead, you see error messages displayed, please remove this Mobile Adapter 2202 (right-click on this Mobile Adapter 2202 from the “Network adapters” list and choose “Uninstall”).
- 4 Once you uninstall this Mobile Adapter 2202, restart your PC and repeat the installation process.

For Windows XP

- 1 Click Start > Control Panel > System.
- 2 Select the **Hardware** tab and click on **Device Manager**. Open **Network adapters**. You should see your Mobile Adapter 2202 in the list. Right-click on this adapter and choose **Properties**.
- 3 From the “Device status”, you should see the line “This device is working properly.” If, instead, you see error messages displayed, please remove this Mobile Adapter 2202 (right-click on this Mobile Adapter 2202 from the “Network adapters” list and choose “Uninstall”).
- 4 Once you uninstall this Mobile Adapter 2202, restart your PC and repeat the installation process.

Troubleshooting tips

Review the following troubleshooting tips before contacting Technical Support.

Table 4 Troubleshooting tips

Problems	Possible Solutions
My computer cannot find the Adapter	<ul style="list-style-type: none">• Make sure the Adapter has no physical damage.• Make sure the Adapter is properly inserted in the CardBus slot.• Try the Adapter in other CardBus slots.• Try another Adapter in that particular CardBus slot.• Check whether there are conflicts caused by other network cards in the computer. Remove all other cards then try this Adapter separately.
I cannot access any network resources from the computer.	<ul style="list-style-type: none">• Make sure the correct software is installed.• Uninstall and reinstall the driver/utility (see Chapter 2 for the procedures).• Make sure all network devices are receiving power and working well.• Check whether the SSID is set properly.• Check with the network administrator to see whether the Access Point is configured properly to accept your signal.• If you have trouble accessing the Internet, make sure to check with the network administrator for further instructions.

Appendix B

Specifications

This appendix provides technical specifications for the Nortel Network Wireless LAN Mobile Adapter 2202.

Frequency band

802.11a Radio: 5 GHz

4.90 - 5.00GHz for Japan

5.15 - 5.25GHz (lower band) for US/Canada, Japan

5.25 - 5.35GHz for US/Canada

5.4 - 5.725GHz for Europe

5.725 - 5.850GHz for US/Canada

802.11g Radio: 2.4 GHz

802.11b Radio: 2.4 GHz

USA - FCC 2412-2462MHz (Ch1-Ch11)

Canada - IC 2412-2462MHz (Ch1-Ch11)

Europe - ETSI 2412-2472MHz (Ch1-Ch13)

Japan - STD-T66/STD-33 2412-2484MHz (Ch1-Ch14)

Frequency selection will vary according to current local regulations.

Modulation technique

Direct Sequence Spread Spectrum (DSSS) (with CCK, BPSK, QPSK modulation) and Orthogonal Frequency Division Multiplexing (OFDM) for 2.4 GHz

Orthogonal Frequency Division Multiplexing (OFDM) subcarrier (with BPSK, QPSK, 16-QAM, 64-QAM modulation) for 5 GHz

Host interface

CardBus interface and form factor

Operating channels supported

2.4 GHz (802.11b)	US/Canada: 11 (1 - 11 with 3 non-overlapping channels) Major European countries: 13 (1 - 13 with 3 non-overlapping) Japan: 13 (1 - 13)
5 GHz (802.11a)	US/Canada: 12 non-overlapping channels 5.15 - 5.35 GHz, 5.725 - 5.825 GHz Major European countries: 19 non-overlapping channel 5.15 - 5.35 GHz, 5.47 - 5.725 GHz Japan: 4 non-overlapping channels 5.15 - 5.25 GHz
802.11g	US/Canada: 11 channels in base mode ETSI, Japan: 13 channels

Channel selection will vary according to current local regulations.

Operating voltage

DC operating voltage: 3.3V nominal, 3.0 V minimum, 3.6 V maximum

The power supplied to the WLAN-Mobile Adapter 2202 shall not exceed 15W under normal or fault operation.

Power consumption

Transmission mode	1155 mW (estimated)
Receive mode	1221 mW (estimated)
Standby mode	297 mW (estimated)
Power saving mode	39.6 mW (estimated)

Current consumption

11a: TX: 690mA Max; RX: 360mA Max; Power Saving: 20mA

11g: TX: 550mA Max; RX: 370mA Max; Power Saving: 20mA

11b: TX: 510mA Max; RX: 320mA Max; Power Saving: 20mA

Output power

Worldwide 2.4 GHz: 18 dBm (~65 mW) peak power

US 5 GHz

a. 5.150 - 5.250: peak power to 50mW (17dBm) per FCC 15.407 specification (UNII band operation)

b. 5.250 - 5.350: peak power to 250mW (24 dBm) per FCC 15.407 specification (UNII band operation)

c. 5.470 - 5.725: not allowed

d. 5.725 - 5.850: peak power to 1W (30 dBm) per FCC 15.247 specification (ISM band operation)

Europe 5 GHz

a. 5.150 - 5.250 and 5.250-5.350: European regulations limit power; this limitation varies by current local regulations

b. 5.470 - 5.725: European regulations limit power; this limitation varies by current local regulations

Japan 5 GHz

a. 5.150 - 5.250: Output power varies according to current local regulations

b. 5.250 - 5.350: not allowed

c. 5.470 - 5.725: not allowed

d. 5.725 - 5.825: not allowed

Maximum power setting will vary according to current local regulations.

Operating systems supported

Windows 2000 and Windows XP

Dimensions

118mm (L) x 54mm (W) x 9.4mm (H)

Security

Hardware 64-bit and 128-bit WEP, TKIP, AES-CCM

152-bit WEP Encryption

802.1x Authentication

WPA

Operation mode

Infrastructure & Ad Hoc mode

Transfer data rate

2.4 GHz 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1

5 GHz 54, 48, 36, 24, 18, 12, 9, 6 Mbps, auto-fallback

108, 96, 72, 48, 36, 24, 18, 12 Mbps by using turbo mode

Operating temperature

0 - 55°C ambient

Storage temperature

-20 - 75 °C ambient

Humidity

5-90% noncondensing

Compliance standards

Safety:

UL 60950

CAN/CSA-22.2 No. 60950

IEC 60950/EN60950, CB certificate and report with all national deviations

Radio Approvals:

FCC Part 15.247 (2.4 GHz)

FCC15.407 (5GHz Band I & Band II), FCC15.247 (5GHz Band III)

RSS-139-1, RSS-210 (Canada)

EN 300.329 (Europe, 2.4 GHz)

EN 301.893 (Europe, 5 GHz)

EMI and Susceptibility (Class B):

FCC Part 15.107 and 15.109

ICES-003 (Canada)

EN 301.489-1 and -17 (Europe)

Other:

IEEE 802.11a and 802.11b

FCC Bulletin OET-65C (Human exposure to RF Fields)

RSS-102 (Canada)

Media access protocol

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with positive ACK architecture

Mechanical specification

CardBus Type II