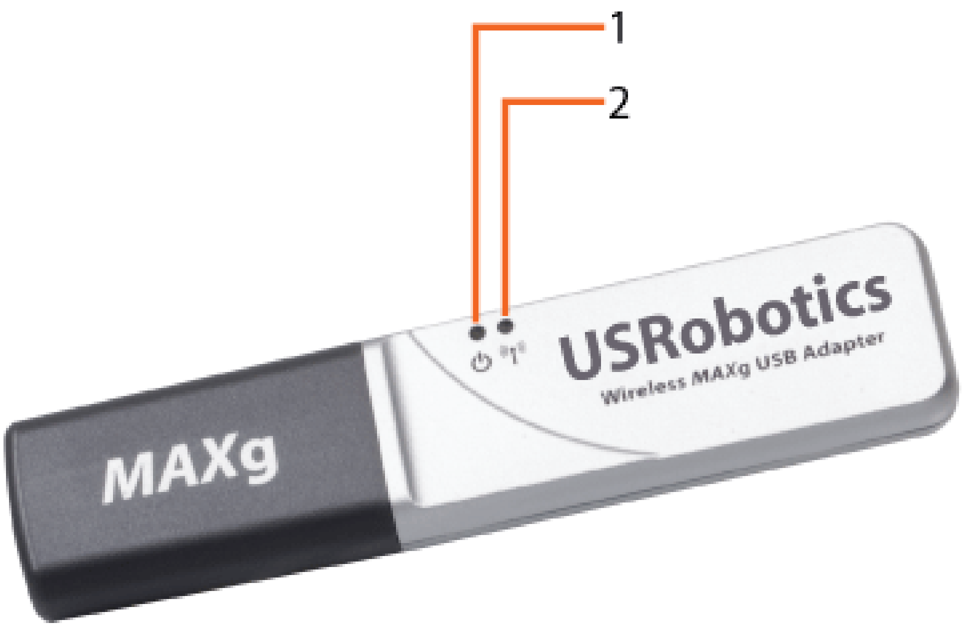
USRobotics Wireless MAXg USB Adapter: User Guide

Introduction

The Wireless *MAX*g USB Adapter is the solution to your home and small business wireless connectivity needs. *MAX*g technology provides the maximum 802.11g range in the industry, delivering optimal wireless connections to your PCs, laptops, and other wireless devices. *MAX*g also provides the maximum speed – up to 125 Mbps – delivering large files like MP3s, digital photos, and digital video through your network fast and efficiently. And with *MAX*g, your network will be protected with a maximum security suite of capabilities, including Wi-Fi Protected Access (WPA), WPA2/802.11i (Windows 2000 and XP only), MAC address filtering, and more.

And to assure a simple, straight-forward installation, USRobotics developed the installation wizard that walks you through the installation of any *MAX*g PC Cards, PCI Adapters, USB Adapters, or Routers in a seamless fashion. In addition, the wizard provides easy-to-understand guidance to set up security for your wireless network. Sharing Internet access securely, wirelessly or wired, has never been easier.

Physical Features



	Symbol	LED Name	State	Condition
1	⏻	Power	Off	No wireless connection: • Wireless driver is not installed • Radio is disabled
			On	Receiving power
2	📡	Wireless	Off	Not sending or receiving data
			On	Sending and receiving data

What You Need to Begin

- PC with an available USB port
- PC with Windows Vista™, Windows® XP, Windows® 2000, Windows® Me, or Windows® 98SE
- A functioning Ethernet-based cable or DSL modem or other WAN connection for Internet access
- A browser that supports HTML 4.01 specification with Javascript enabled

R46.1717.00
rev 0 06/07

USRobotics Wireless MAXg USB Adapter: User Guide

Product Specifications

- Complies with IEEE 802.11g 54 Mbps wireless radio standard
- 100mW power output
- Supports Windows Vista™, Windows® XP, Windows® 2000, Windows® Me, and Windows® 98SE

Security Features

- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access) (Windows 2000 and XP only)
- 802.1x (RADIUS) authentication
- CCX 1.0
- 64/128-bit WEP (Wired Equivalent Privacy) data encryption
- Ability to disable wireless radio

Acknowledgements

This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

USRobotics® *Wireless MAXg USB Adapter: User Guide*

U.S. Robotics Corporation Two (2) Year Limited Warranty

1.0 GENERAL TERMS:

1.1 This Limited Warranty is extended only to the original end-user purchaser (CUSTOMER) and is not transferable.

1.2 No agent, reseller, or business partner of U.S. Robotics Corporation (U.S. ROBOTICS) is authorised to modify the terms of this Limited Warranty on behalf of U.S. ROBOTICS.

1.3 This Limited Warranty expressly excludes any product that has not been purchased as new from U.S. ROBOTICS or its authorised reseller.

1.4 This Limited Warranty is only applicable in the country or territory where the product is intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

1.5 U.S. ROBOTICS warrants to the CUSTOMER that this product will be free from defects in workmanship and materials, under normal use and service, for TWO (2) YEARS from the date of purchase from U.S. ROBOTICS or its authorised reseller.

1.6 U.S. ROBOTICS sole obligation under this warranty shall be, at U.S. ROBOTICS sole discretion, to repair the defective product or part with new or reconditioned parts; or to exchange the defective product or part with a new or reconditioned product or part that is the same or similar; or if neither of the two foregoing options is reasonably available, U.S. ROBOTICS may, at its sole discretion, provide a refund to the CUSTOMER not to exceed the latest published U.S. ROBOTICS recommended retail purchase price of the product, less any applicable service fees. All products or parts that are exchanged for replacement will become the property of U.S. ROBOTICS.

1.7 U.S. ROBOTICS warrants any replacement product or part for NINETY (90) DAYS from the date the product or part is shipped to Customer.

1.8 U.S. ROBOTICS makes no warranty or representation that this product will meet CUSTOMER requirements or work in combination with any hardware or software products provided by third parties.

1.9 U.S. ROBOTICS makes no warranty or representation that the operation of the software products provided with this product will be uninterrupted or error free, or that all defects in software products will be corrected.

1.10 U.S. ROBOTICS shall not be responsible for any software or other CUSTOMER data or information contained in or stored on this product.

2.0 CUSTOMER OBLIGATIONS:

2.1 CUSTOMER assumes full responsibility that this product meets CUSTOMER specifications and requirements.

2.2 CUSTOMER is specifically advised to make a backup copy of all software provided with this product.

2.3 CUSTOMER assumes full responsibility to properly install and configure this product and to ensure proper installation, configuration, operation and compatibility with the operating environment in which this product is to function.

2.4 CUSTOMER must furnish U.S. ROBOTICS a dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) for any warranty claims to be authorised.

3.0 OBTAINING WARRANTY SERVICE:

3.1 CUSTOMER must contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre within the applicable warranty period to obtain warranty service authorisation.

3.2 Customer must provide Product Model Number, Product Serial Number and dated

Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) to obtain warranty service authorisation.

3.3 For information on how to contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre, please see the U.S ROBOTICS corporate Web site at: www.usr.com

3.4 CUSTOMER should have the following information / items readily available when contacting U.S. ROBOTICS Technical Support:

- Product Model Number
- Product Serial Number
- Dated Proof of Purchase
- CUSTOMER contact name & telephone number
- CUSTOMER Computer Operating System version
- U.S. ROBOTICS Installation CD-ROM
- U.S. ROBOTICS Installation Guide

4.0 WARRANTY REPLACEMENT:

4.1 In the event U.S. ROBOTICS Technical Support or its authorised U.S. ROBOTICS Service Centre determines the product or part has a malfunction or failure attributable directly to faulty workmanship and/or materials; and the product is within the TWO (2) YEAR warranty term; and the CUSTOMER will include a copy of the dated Proof of Purchase (original purchase receipt from U.S. ROBOTICS or its authorised reseller) with the product or part with the returned product or part, then U.S. ROBOTICS will issue CUSTOMER a Return Material Authorisation (RMA) and instructions for the return of the product to the authorised U.S. ROBOTICS Drop Zone.

4.2 Any product or part returned to U.S. ROBOTICS without an RMA issued by U.S. ROBOTICS or its authorised U.S. ROBOTICS Service Centre will be returned.

4.3 CUSTOMER agrees to pay shipping charges to return the product or part to the authorised U.S. ROBOTICS Return Centre; to insure the product or assume the risk of loss or damage which may occur in transit; and to use a shipping container equivalent to the original packaging.

4.4 Responsibility for loss or damage does not transfer to U.S. ROBOTICS until the returned product or part is received as an authorised return at an authorised U.S. ROBOTICS Return Centre.

4.5 Authorised CUSTOMER returns will be unpacked, visually inspected, and matched to the Product Model Number and Product Serial Number for which the RMA was authorised. The enclosed Proof of Purchase will be inspected for date of purchase and place of purchase. U.S. ROBOTICS may deny warranty service if visual inspection of the returned product or part does not match the CUSTOMER supplied information for which the RMA was issued.

4.6 Once a CUSTOMER return has been unpacked, visually inspected, and tested U.S. ROBOTICS will, at its sole discretion, repair or replace, using new or reconditioned product or parts, to whatever extent it deems necessary to restore the product or part to operating condition.

4.7 U.S. ROBOTICS will make reasonable effort to ship repaired or replaced product or part to CUSTOMER, at U.S. ROBOTICS expense, not later than TWENTY ONE (21) DAYS after U.S. ROBOTICS receives the authorised CUSTOMER return at an authorised U.S. ROBOTICS Return Centre.

4.8 U.S. ROBOTICS shall not be liable for any damages caused by delay in delivering or furnishing repaired or replaced product or part.

5.0 LIMITATIONS:

5.1 THIRD-PARTY SOFTWARE: This U.S. ROBOTICS product may include or be bundled with third-party software, the use of which is governed by separate end-user license agreements provided by third-party software vendors. This U.S. ROBOTICS Limited Warranty does not apply to such third-party software. For the applicable warranty refer to the end-user license agreement governing the use of such software.

5.2 DAMAGE DUE TO MISUSE, NEGLECT, NON-COMPLIANCE, IMPROPER INSTALLATION, AND/OR ENVIRONMENTAL FACTORS: To the extent permitted by applicable law, this U.S. ROBOTICS Limited Warranty does not apply to normal wear and tear; damage or loss of data due to interoperability with current and/or future versions of operating system or other current and/or future software and hardware; alterations (by persons other than U. S. ROBOTICS or authorised U.S. ROBOTICS Service Centres); damage caused by operator error or non-compliance with instructions as set out in the user documentation or other accompanying documentation; damage caused by acts of nature such as lightning, storms, floods, fires, and earthquakes, etc. Products evidencing the product serial number has been tampered with or removed; misuse, neglect, and improper handling; damage caused by undue physical, temperature, or electrical stress; counterfeit products; damage or loss of data caused by a computer virus, worm, Trojan horse, or memory content corruption; failures of the product which result from accident, abuse, misuse (including but not limited to improper installation, connection to incorrect voltages, and power points); failures caused by products not supplied by U.S. ROBOTICS; damage cause by moisture, corrosive environments, high voltage surges, shipping, abnormal working conditions; or the use of the product outside the borders of the country or territory intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

5.3 TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. U.S. ROBOTICS NEITHER ASSUMES NOR AUTHORISES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, WARRANTY, OR USE OF ITS PRODUCTS.

5.4 LIMITATION OF LIABILITY. TO THE FULL EXTENT ALLOWED BY LAW, U.S. ROBOTICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF U.S. ROBOTICS OR ITS AUTHORISED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT U.S. ROBOTICS OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

6.0 DISCLAIMER:

Some countries, states, territories or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to CUSTOMER. When the implied warranties are not allowed by law to be excluded in their entirety, they will be limited to the TWO (2) YEAR duration of this written warranty. This warranty gives CUSTOMER specific legal rights, which may vary depending on local law.

7.0 GOVERNING LAW:

This Limited Warranty shall be governed by the laws of the State of Illinois, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL, 60173
U.S.A

USRobotics *Wireless MAXg USB Adapter: User Guide*

Regulatory Information

Declaration of Conformity

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL 60173
U.S.A.

declares that this product conforms to the FCC's specifications:

Part 15, Class B

This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following conditions:
1) this device may not cause harmful electromagnetic interference, and
2) this device must accept any interference received including interference that may cause undesired operations.

This equipment complies with FCC Part 15 for Home and Office use.

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

Detachable Antenna Information

FCC Part 15, Subpart C, Section 15.203 Antenna requirement

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment is in direct contact with the body of the user under normal operating conditions. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio and Television Interference:

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. If this equipment is not installed and used in accordance with the manufacturer’s instructions, it 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 to 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.

USR declares that 5425 is limited to CH1 through 11, 2412 to 2462 MHz, in the USA by specific firmware, which is controlled by the manufacturer and cannot be changed by the user.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. End users must follow the specific operating instructions for satisfying RF exposure compliance.

Specific Absorption Rate (SAR) compliance has been established in typical laptop (notebook) computer(s) with a Card Bus slot. This product may be used in a typical laptop (notebook) computer with a Card Bus slot. Other application, such as use with a handheld PC or similar device, has not been verified and may not comply with related RF exposure rules. Such use is prohibited.

UL Listing/CUL Listing:

This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for the uses described in the User Guide. Use this product only with UL Listed Information Technology Equipment (ITE).

For Canadian Users

Industry Canada (IC)

This equipment complies with RSS-210 of the Industry Canada rules.

Operation is subject to the following two conditions:

1. This device may not cause interference.

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 reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropic Radiated Power (EIRP) is not more than that required for successful communication.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment is in direct contact with the body of the user under normal operating conditions. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Compliance

CE0560(!)

Declaration of Conformity

We, U.S. Robotics Corporation of 935 National Parkway, Schaumburg, Illinois, 60173-5157,USA, declare under our sole responsibility that the U.S. Robotics 5425 Wireless *MAX*g USB Adapter to which this declaration relates is in conformity with the following standards and/or other normative documents:

EN300 328
EN301 489-1
EN301 489-17
EN60950-1
EN50392

We, U.S. Robotics Corporation, hereby declare the above named products are in compliance and conformity with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The conformity assessment procedure referred to in Article 10 and detailed in Annex IV of Directive 1999/5/EC has been followed.

This equipment is in compliance with the European recommendation 1999/519/ECC, governing the exposure to the electromagnetic radiation.

This product can be used in the following countries:\

- **European Union countries:** Germany, Austria, Belgium, Netherlands, Luxembourg, Italy, France, UK, Ireland, Spain, Portugal, Sweden, Denmark, Finland, Czech Republic, Poland, Hungary, and Greece
- **Non-European Union countries:** Switzerland, Norway, and Turkey

An electronic copy of the original CE Declaration of Conformity is available at the U.S. Robotics website: www.usr.com.

Regarding IEEE 802.11b/g frequencies, we currently have the following information about restrictions in the European Union (EU) countries:

- Italy

  Please be aware that use of the wireless device is subject to the following Italian regulation:

  1. D.Lgs 1.8.2003, number 259, articles 104 (activities where General Authorization is required) and 105 (free use), for private use;
  2. D.M 28.5.03 and later modifications, for the supplying to public RadioLAN access for networks and telecommunication services

- France

  In France metropolitan, outdoor power is limited to 10mW (EIRP) within 2454MHz – 2483, 5MHz frequency band

  In Guyana and Reunion Islands, outdoor use is forbidden within 2400MHz – 2420MHz frequency band

Regulatory Channel Frequency

Channel	**Frequency (MHz)**	**FCC**	**Canada**	**ETSI**
1	2412	**X**	**X**	**X**
2	2417	**X**	**X**	**X**
3	2422	**X**	**X**	**X**
4	2427	**X**	**X**	**X**
5	2432	**X**	**X**	**X**
6	2437	**X**	**X**	**X**
7	2442	**X**	**X**	**X**
8	2447	**X**	**X**	**X**
9	2452	**X**	**X**	**X**
10	2457	**X**	**X**	**X**
11	2462	**X**	**X**	**X**
12	2467			**X**
13	2472			**X**

Operating Channels:	• IEEE 802.11g compliant • 11 channels (US, Canada) • 13 channels (ETSI)

EU Health Protection

This device complies with the European requirements governing exposure to electromagnetic radiation. These wireless devices are transmitters/receivers and have been designed and manufactured to comply with the exposure limits recommended by the Council of the European Union and the International Commission on Non-Ionizing Radiation Protection (ICNIRP, 1999) for the entire population. The exposure standard for portable equipment uses the "Specific Absorption Rate" as unit of measure. The maximum SAR value of the 5425 Wireless *MAX*g USB Adapter measured in the conformity test is [INSERT SAR VALUE HERE].

Wireless MAXg USB Adapter: User Guide

Copyright Information

U.S. Robotics Corporation
935 National Parkway
Schaumburg, Illinois
60173-5157
USA

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as a translation, transformation, or adaptation) without written permission from U.S. Robotics Corporation. U.S. Robotics Corporation reserves the right to revise this documentation and to make changes in the products and/ or content of this document from time to time without obligation to provide notification of such revision or change. U.S. Robotics Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or ! LICENSE.TXT. If you are unable to locate a copy, please contact U.S. Robotics and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101 (a) and as such is provided with only such rights as are provided in U.S. Robotics standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987) whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

USRobotics ***Wireless MAXg USB Adapter: User Guide***

Installation

Depending on your network configuration and what products you purchased, choose one of the following sets of installation instructions:

Click here if you are installing **BOTH** a **Wireless *MAX*g Router** and **Wireless *MAX*g USB Adapter**.

Click here if you are installing **ONLY** a **Wireless *MAX*g USB Adapter**.

USRobotics *Wireless MAXg USB Adapter: User Guide*

Installation

Windows Me and 98SE Users: During the Installation procedure, you may be prompted for your Windows Operating system CD-ROM. Make sure you have it available in case you need it.

Notice:
If you are installing both a Wireless *MAX*g Router and the Wireless *MAX*g USB Adapter, do not use the instructions on this page. Instead, go to Installing BOTH a Wireless *MAX*g Router and Wireless *MAX*g USB Adapter.

Install the Wireless *MAX*g USB Adapter

1. Insert the Installation CD-ROM for the USB adapter into the CD-ROM drive of the computer on which you are installing the USB adapter. The Installation CD Graphical User Interface (GUI) will appear on your screen. If prompted, select your preferred language.

   If the CD doesn't start automatically, start it manually as follows:

   A. **Windows Vista:** Click Windows **Start > Computer**.

      Windows XP: Click Windows **Start > My Computer**.

      Windows 2000, Me and 98SE: On the desktop, double-click **My Computer**.

B. Double-click the CD drive.

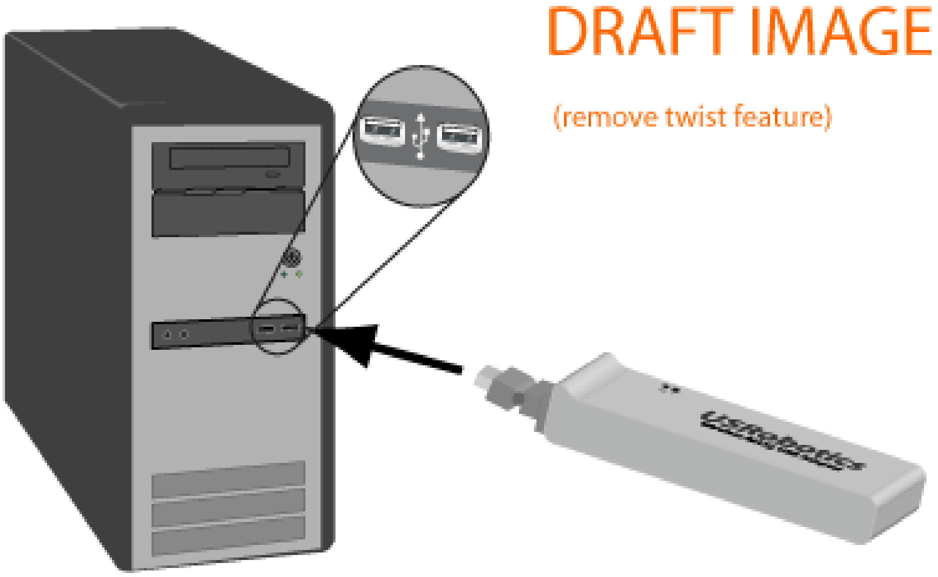
2. If prompted by Windows Security, click **Run autorun.exe**. If prompted by User Access Control, click **Continue**.

3. Click **Install** and follow the on-screen instructions.

4. If a window appears warning that the software has not passed Windows testing, continue with the installation. USRobotics has thoroughly tested the operation of the software with Windows Vista, XP, 2000 and Me to ensure its safe operation.

   Windows Vista: Click **Install driver software anyway**.
   Windows XP: Click **Continue Anyway**.
   Windows 2000: Click **Yes**.

5. When you are prompted, insert the USB adapter.



6. Windows XP only:

   A. If the Found New Hardware Wizard asks to connect to the Windows update Web site to search for software, select **No, not this time** and click **Next**.

   B. With **Install the software automatically** selected, click **Next**.

7. If a window appears warning that the software has not passed Windows testing, continue with the installation. USRobotics has thoroughly tested the operation of the software with Windows to ensure its safe operation.

   Windows Vista: Click **Install driver software anyway**.
   Windows XP only: **Click Continue Anyway**.
   Windows 2000 only: Click **Yes**.

8. Windows XP only: Click **Finish**.

9. When prompted, click **Restart** to restart your computer.

10. Select the option that matches your wireless network and follow the on-screen instructions.

Congratulations!

You have finished installing your product! The Wireless *MAX*g USB Adapter should be connected to the wireless network that you selected.

If you experience any problems connecting to a wireless network, refer to the Troubleshooting section in this guide for more information.

Register your product

Register your product online at http://www.usr.com/productreg

USRobotics *Wireless MAXg USB Adapter: User Guide*

Installing BOTH a Wireless *MAX*g Router and Wireless *MAX*g USB Adapter

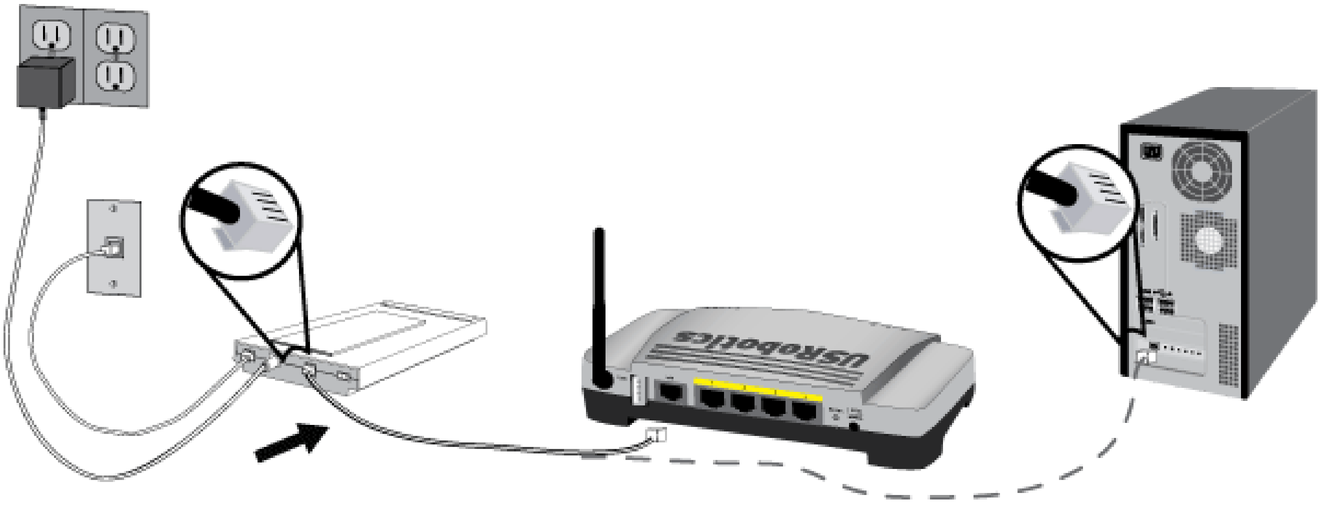
During the Installation procedure, you may be prompted for your Windows Operating system CD-ROM. Make sure you have it available in case you need it.

Step One: Connect Your Router

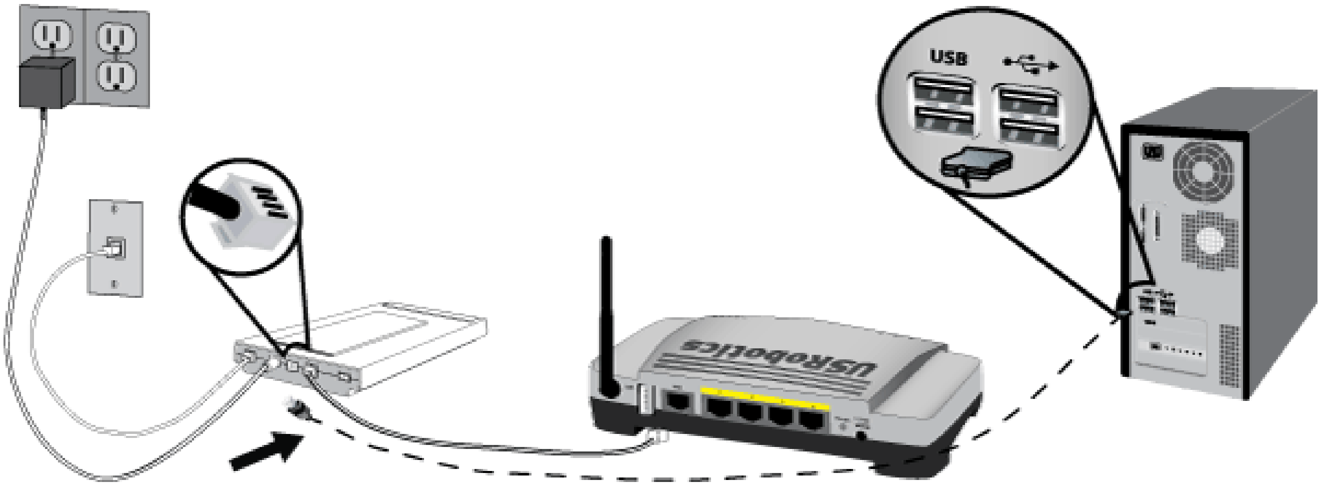
A. Connect your DSL or Cable modem to the router:

1. Power off your computer and your modem.
2. Connect the provided antennas to the back of the router.
3. Do one of the following:

   If your modem connects to your computer with an Ethernet cable: Locate the Ethernet cable that connects your DSL or cable modem to your computer's Ethernet adapter, and disconnect it from your computer only: do not disconnect the cable from your DSL or cable modem.

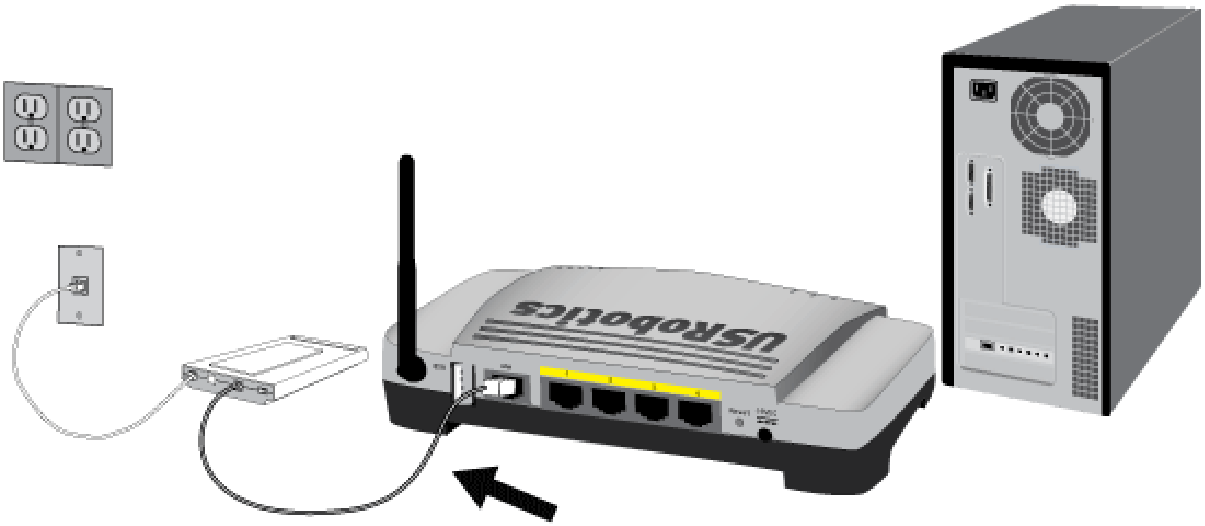


   If your modem connects to your computer with a USB cable: Disconnect the USB cable from both the modem and your computer. You will need another Ethernet cable in addition to the one provided with the router. Connect one end of the Ethernet cable to the Ethernet port on the back of your DSL or cable modem.



Note: The USB port on the router is for connecting a USB printer only. Do not connect your modem to the USB port on the router. For instructions on connecting a printer to the USB print server on your router, see the *Wireless MAXg Router User Guide*.

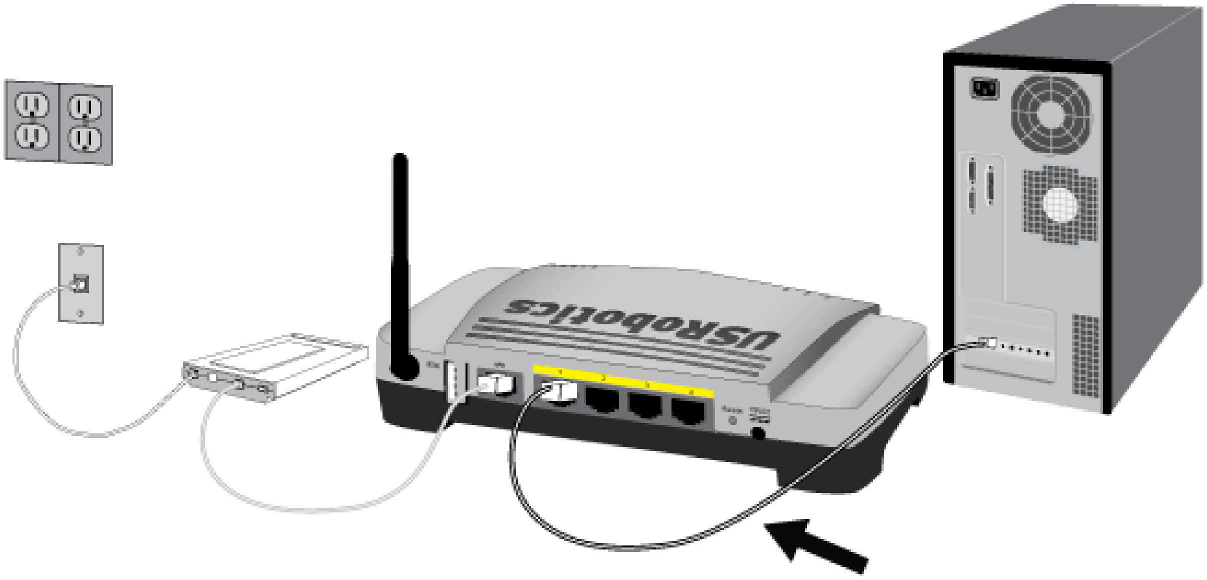
4. Connect the free end of the Ethernet cable to the **WAN** port on the rear of the router.



B. Connect the router to your computer:

1. Connect one end of the supplied Ethernet cable to your computer’s Ethernet adapter.

2. Connect the other end to one of the router’s **LAN** ports.

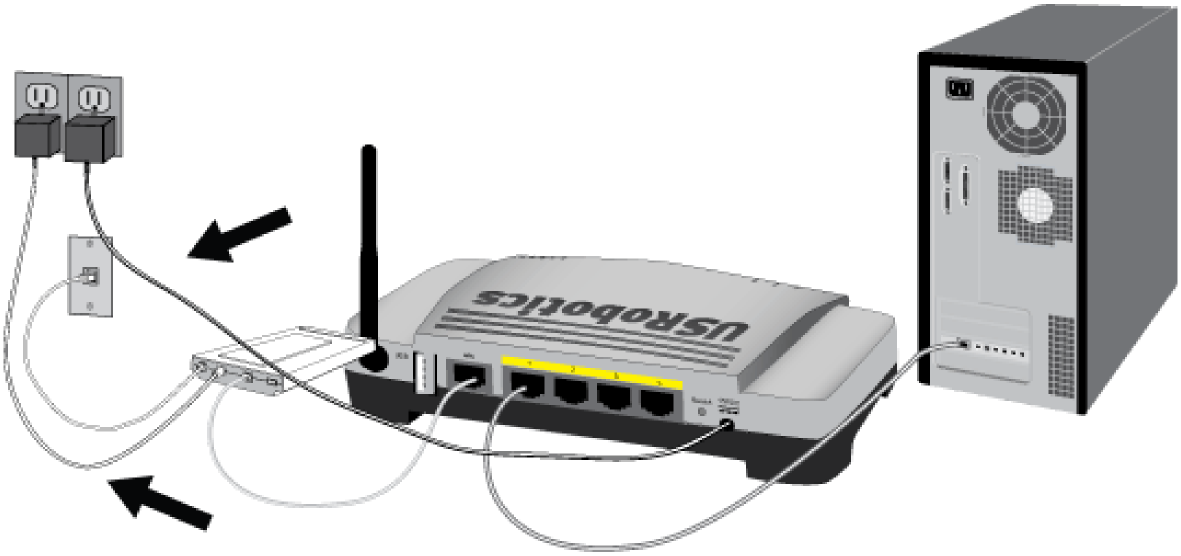


C. Power up the network:

1. Turn on your modem. Wait until the LEDs stabilize before powering up your router.

2. Connect the supplied power cord to the **9VDC** port on the router.

> **Note**: **UK Users**: With the power adapter unplugged, connect the appropriate power plug for your country on to the power adapter. Apply enough pressure to cause a click and firmly seat the plug.



3. Plug the power adapter into a standard power outlet.

> **Note**: **5461**: This product is intended to be supplied by a Listed Direct Plug-in Power Unit marked Class 2 and rated 5VDC, 1500 mA.

Note: **5465**: This product is intended to be supplied by a Listed Direct Plug-in Power Unit marked Class 2 and rated 9VDC, 1200 mA.

4. Turn on your computer.

Step Two: Install the Wireless *MAX*g USB Adapter and drivers

A. Insert the Installation CD-ROM for the USB adapter into the CD-ROM drive of the computer on which you are installing adapter. The Installation CD Graphical User Interface (GUI) will appear on your screen. If prompted, select your preferred language.

If the CD doesn't start automatically, start it manually as follows:

1. **Windows Vista:** Click Windows **Start > Computer**.

   Windows XP: Click Windows **Start > My Computer**.

   Windows 2000, Me and 98SE: On the desktop, double-click **My Computer**.

2. Double-click the CD drive.

B. If prompted by Windows Security, click **Run autorun.exe**. If prompted by User Access Control, click **Continue**.

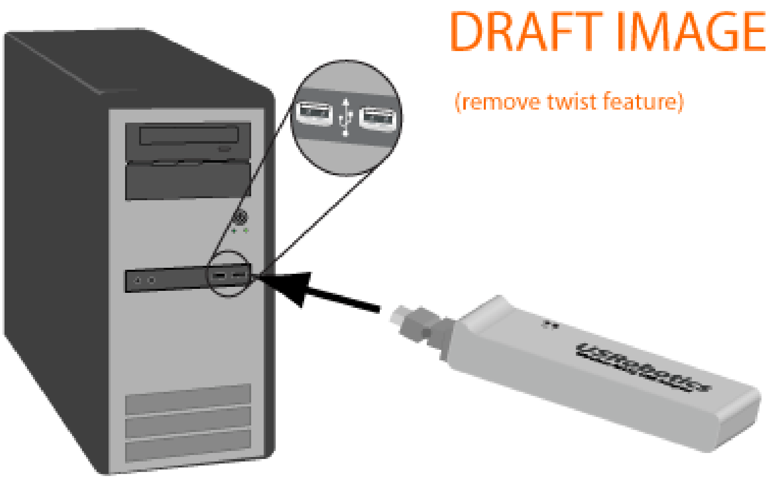
C. Click **Install** and follow the on-screen instructions.

D. If a window appears warning that the software has not passed Windows testing, continue with the installation. USRobotics has thoroughly tested the operation of the software with Windows Vista, XP, 2000 and Me to ensure its safe operation.

Windows Vista: Click **Install this driver software anyway**.
Windows XP: Click **Continue Anyway**.
Windows 2000: Click **Yes**.

E. **Note:** You will need to install this Installation CD-ROM on each computer on which you plan to install a Wireless *MAX*g USB Adapter.

F. When prompted, locate an available USB port and fully insert the Wireless *MAX*g USB Adapter.


DRAFT IMAGE

(remove twist feature)

G. Windows Vista only:

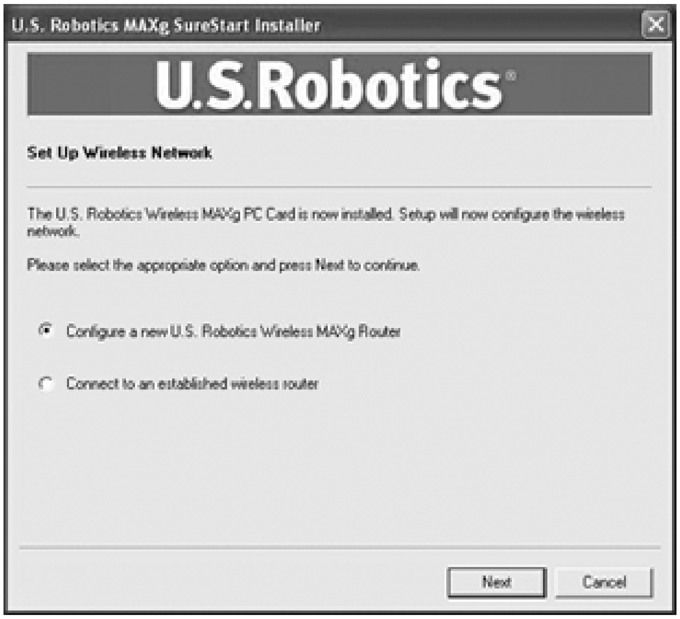
   A. Click **Locate and install driver software (recommended)** in the Found New Hardware window.

   B. If prompted, click **Continue.**

H. When prompted, click **Restart** to restart your computer.

Step Three: Set up a Wireless Network

A. When you are prompted, select **Configure a new U.S. Robotics Wireless *MAX*g Router** and click **Next**. You will need to wait while the USB adapter communicates with the router.


U.S. Robotics MAXg SureStart Installer

U.S.Robotics®

Set Up Wireless Network

The U.S. Robotics Wireless MAXg PC Card is now installed. Setup will now configure the wireless network.

Please select the appropriate option and press Next to continue.

● Configure a new U.S. Robotics Wireless MAXg Router

○ Connect to an established wireless router

B. If prompted, select your Internet Connection type and click **Next**. Depending on the type of Internet Connection that you choose, you may need to enter some additional information.

C. Enter a **Network name** and a **Pass phrase** (also known as network key) for your wireless encryption and click **Next**. You will need to wait while the router and the USB adapter are configured.

> **Note:** USRobotics recommends that you enable WPA so that your wireless network is secure. Make sure you assign the same secret WPA key to all your wireless devices to ensure network connectivity.

D. When prompted, enter a **User name** and **Password** for the router login and then click **Next**. Wait while the configuration continues.

E. You will then see a screen that shows you the settings for your Wireless *MAX*g Router. These settings will be saved to a text file on your computer desktop and you have the option to print them out if your computer is connected to a printer. When you are finished looking at this information, click **Finish**. Your Wireless *MAX*g Router USB adapter should all be configured and ready for use.

Congratulations!

You have finished installing your product! The Wireless *MAX*g USB Adapter should be connected to the wireless network that you set up.

If you experience any problems connecting to a wireless network, refer to the Troubleshooting section in this guide for more information.

Register your product

Register your product online at http://www.usr.com/productreg

Connect to a Wireless Network After Installation

Wi-Fi Protected Setup™ Network

Windows Vista and Windows XP computers can use Wi-Fi Protected Setup™ to connect to a WPS-enabled router or access point. Some USRobotics routers and access points support Wi-Fi Protected Setup™ (WPS). See your wireless router or access point's documentation to determine if it can connect clients using WPS.

Using the WPS Push Button

1. Be ready to start WPS on your router or access point.

   For WPS-enabled USRobotics routers or access points, log in to the configuration pages for the router or access point and click **Add wireless device** on the **Status** page.

2. Click Windows **Start** > (**All**) **Programs** > **USRobotics Wi-Fi Protected Setup Wizard**.

3. Select **Add device with WPS push button** and click **Next**.

4. Start WPS on the router or access point and follow the on-screen instructions in the USRobotics Wi-Fi Protected Setup Wizard.

   To start WPS On WPS-enabled USRobotics routers or access points, click

Find Device on the **Add Wireless Device** page.

The adapter detects the wireless security settings of the router and creates a secure wireless connection to the network.

Using the WPS PIN

1. Be ready to start WPS on your router or access point.

   For WPS-enabled USRobotics routers or access points, log in to the configuration pages for the router or access point and click **Add wireless device** on the **Status** page.

2. Click Windows **Start** > (**All**) **Programs** > **USRobotics Wi-Fi Protected Setup Wizard**.

3. Select **Add device with WPS PIN** and click **Next**.

4. Click **Generate PIN**.

5. Start WPS on the router or access point using the PIN generated in the previous step.

   For WPS-enabled USRobotics routers or access points, enter the **PIN** for the wireless adapter and click **Add device** on the **Add Wireless Device** page.

6. In the USRobotics Wi-Fi Protected Setup Wizard, click **Next** to start WPS on the adapter and follow the on-screen instructions.

   The adapter detects the wireless security settings of the router and creates a secure wireless connection to the network.

Manually Connect

Windows Vista

1. Click Windows **Start > Connect To**.
2. If the wireless network is listed, select the network you want to connect to, and then click **Connect**.

   If the wireless network is not listed, follow the instructions to Manually Create a Network Profile.

Windows XP or 2000

There are two methods you can use to create a wireless connection.

Using the Wireless Networks Wizard

1. Open the USRobotics Wireless Utility and select the **Wireless Networks** tab.
2. Pull down the **Add** menu and select **Use Wizard**. Select a wireless network from the list and click **Next**.
3. If security is enabled for the specified wireless network device, enter the **Network key**, click **Next**, and then **Connect**. If security is not enabled for the specified wireless network device, click **Connect**.
4. You should now be connected to the specified wireless network device.

Using the USRobotics Wireless Utility

1. Open the USRobotics Wireless Utility and select the **Wireless Networks** tab.
2. Pull down the **Add** menu and select **Use Utility**.
3. Click **Select** to display a list of wireless devices.

4. Select a wireless device.

5. If you do not see the correct device, click **Refresh** to update the list. If you still do not see the correct device, click **Cancel** and manually enter the Network Name of the device.

6. Click **Ok**.

7. Enter the appropriate connection and security information for the wireless network device, if applicable, and click **OK**.

8. Click **OK** and the Wireless *MAX*g USB Adapter will attempt a connection to the wireless network. If the card or adapter does not connect to the wireless network, open the Wireless Networks tab in the USRobotics Wireless Utility, select the wireless network, and click **Edit**. Verify that the information for the wireless network device is correct and click **OK**.

Windows Me or 98SE

There are two methods you can use to create a wireless connection.

Using the Quick Connect screen

1. Left-click once on the Utility icon to open the Quick Connect screen.

2. Select a wireless network device in the Available networks screen.

3. If security is enabled for the specified wireless network device, enter the **Network key** and click **Connect**. If security is not enabled for the specified wireless network device, select the checkbox for **Allow me to connect to the selected wireless network, even though it is not secure** and then click **Connect**.

4. You should now be connected to the specified wireless network device. If you experience any problems creating a connection, click **Advanced** to access the USRobotics Wireless Utility.

Using the USRobotics Wireless Utility

1. Either right-click the Utility icon in the system tray and select **Open Utility** or left-click the Utility icon once and then click **Advanced**.

2. In the Wireless Networks screen, browse through the list of available wireless network devices. When you locate the correct device, select it and then click **Configure**. If you do not see the correct device, click **Refresh** to update the list. If the correct device still does not appear, click **Add** under the Preferred networks section and manually enter the appropriate information to create the entry.

3. When the Properties window appears, enter the appropriate connection and security information for the wireless network device, if applicable, and click **OK**.

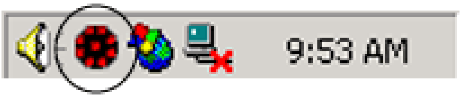
4. On the main screen, click **Apply** and a connection will be established. If a connection is not established, select the device in the Preferred networks list and click **Properties**. Verify the information for the wireless network device is correct, click **OK**, and then click **Apply**.

USRobotics *Wireless MAXg USB Adapter: User Guide*

The USRobotics Wireless Utility

Users of Windows XP, 2000, Me, and 98SE have access to the USRobotics Wireless Utility once the Wireless *MAX*g USB Adapter is installed. With this utility, you can create and edit the settings for wireless connections, view the information regarding your Wireless *MAX*g USB Adapter, and perform diagnostic tests on your device.

You should see a small icon for the USRobotics Wireless Utility in the system tray by your clock on your computer desktop. The USRobotics Wireless Utility icon will be colored to indicate the status of your wireless network: red for disconnected and green for connected with good quality.



Note: Depending on your version of Windows, the USRobotics Wireless Utility may look slightly different.

Opening the USRobotics Wireless Utility

You can open the USRobotics Wireless Utility in two ways:

- Right-click the Utility icon and click **Open Utility**.
- Select **USRobotics Wireless Utility** from the **Start** menu's programs folder or the **Control Panel**.

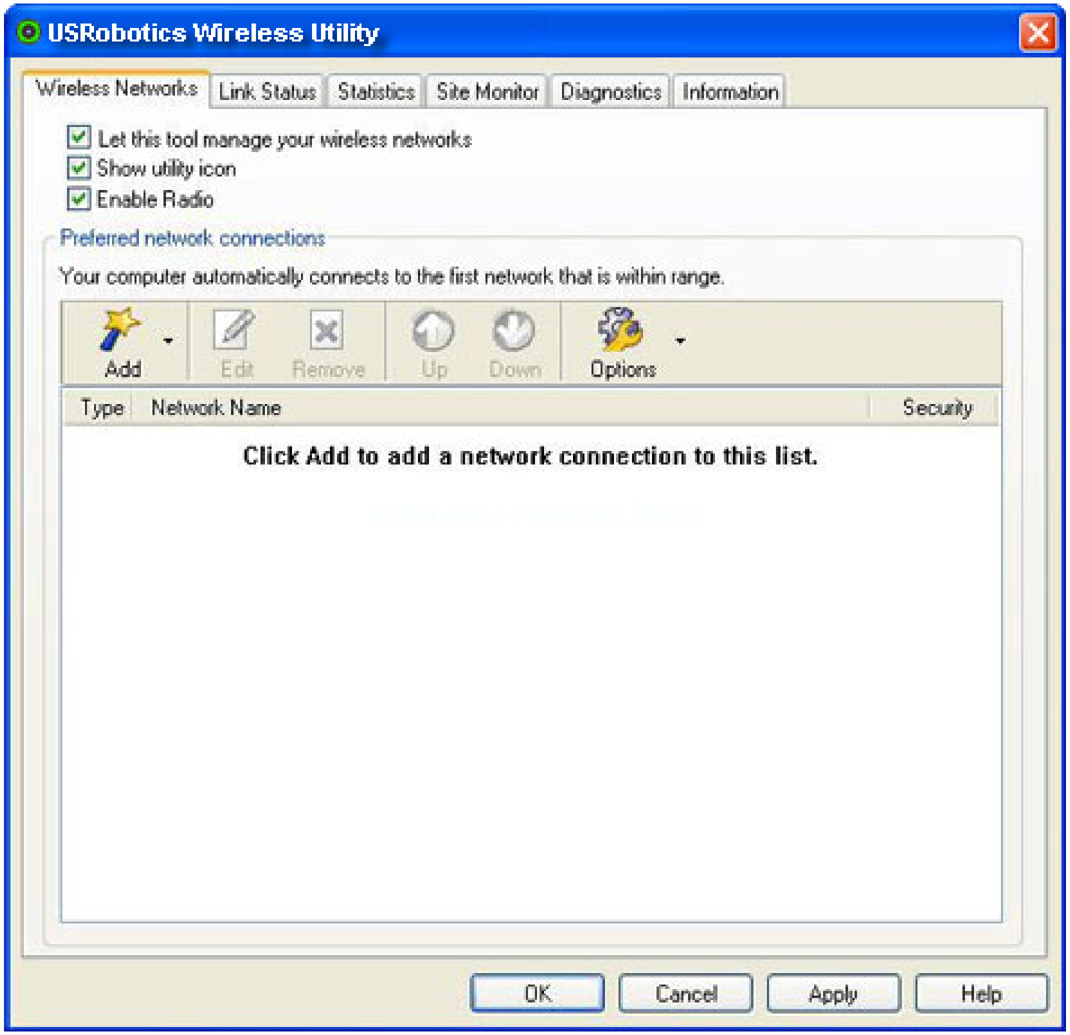
Using the USRobotics Wireless Utility

Each section of the USRobotics Wireless Utility is introduced below. For more detailed information regarding the different areas of the

USRobotics Wireless Utility, click **Help** within the USRobotics Wireless Utility.

In the **Wireless Networks** area, you can locate available wireless network devices and create connections. You can also create new entries for wireless network devices if they do not appear in the list.

Windows XP and 2000:



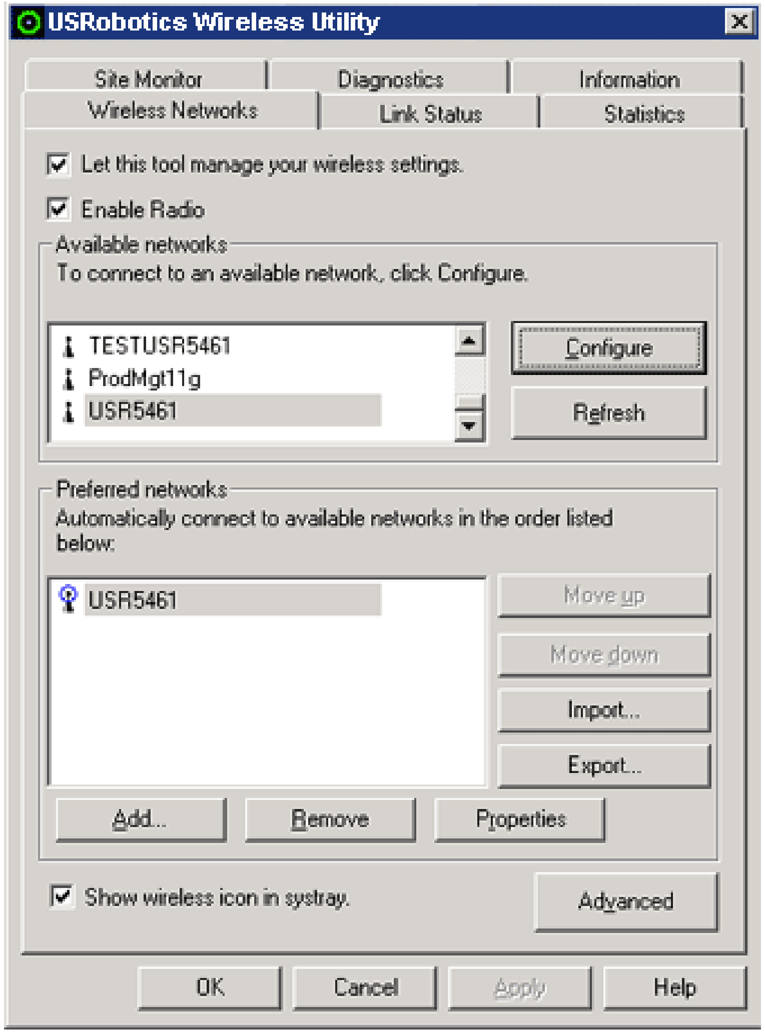
☑ Let this tool manage your wireless networks
☑ Show utility icon
☑ Enable Radio

Preferred network connections

Your computer automatically connects to the first network that is within range.

Click Add to add a network connection to this list.

Windows Me and 98SE:



☑ Let this tool manage your wireless settings.

☑ Enable Radio

Available networks

To connect to an available network, click Configure.

TESTUSR5461
ProdMgt11g
USR5461

Preferred networks

Automatically connect to available networks in the order listed below:

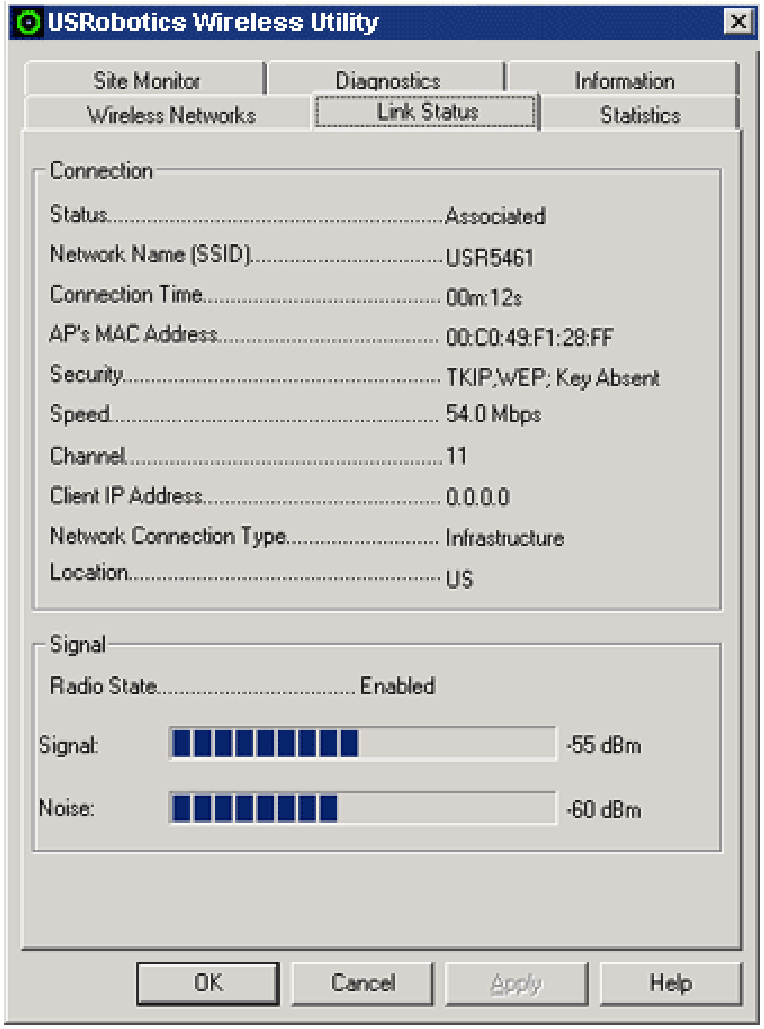
USR5461

☑ Show wireless icon in systray.

In the **Link Status** area, information regarding your current wireless connection is displayed.

Windows XP and 2000:

Windows Me and 98SE:



Connection

Status....................Associated

Network Name (SSID)....................USR5461

Connection Time....................00m:12s

AP's MAC Address....................00:C0:49:F1:28:FF

Security....................TKIP,WEP: Key Absent

Speed....................54.0 Mbps

Channel....................11

Client IP Address....................0.0.0.0

Network Connection Type....................Infrastructure

Location....................US

Signal

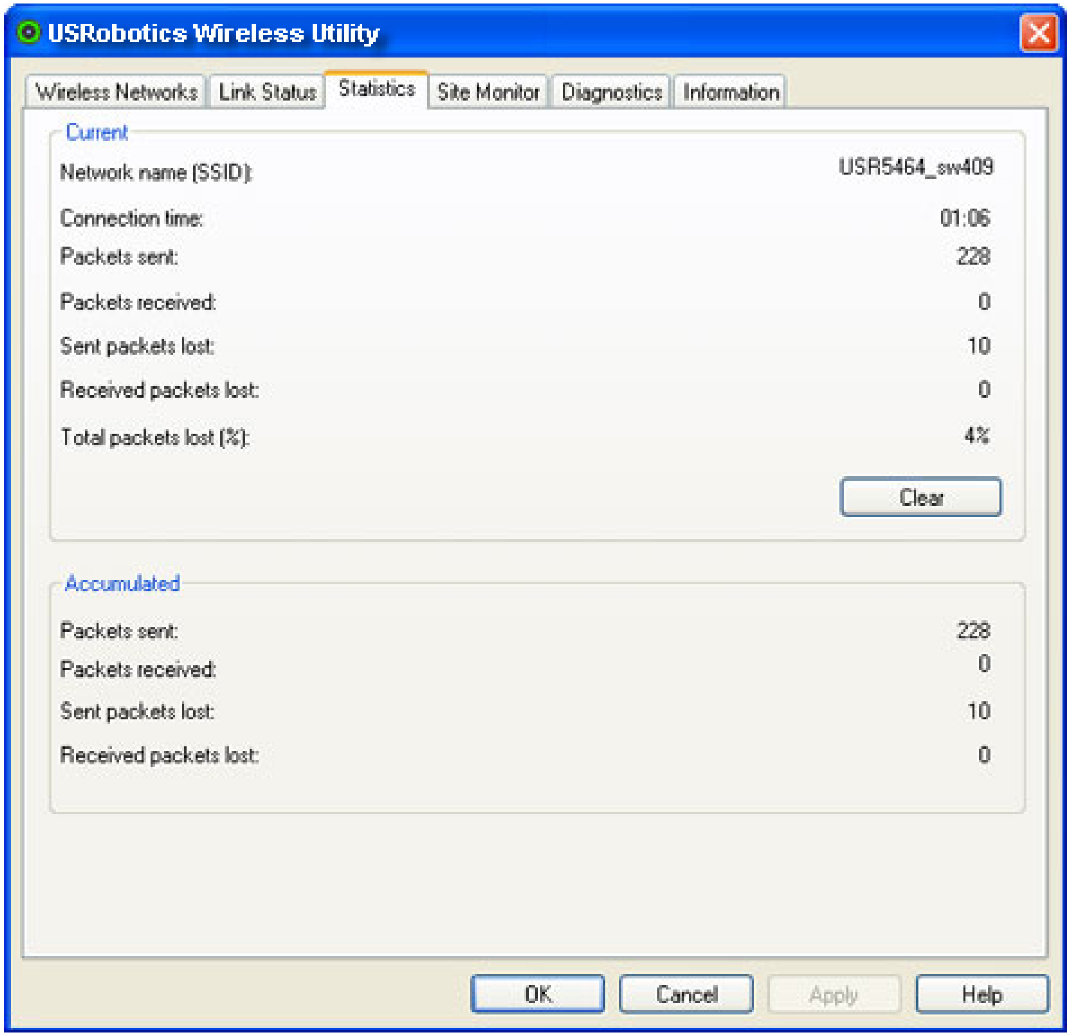
Radio State....................Enabled

Signal: -55 dBm

Noise: -60 dBm

In **Statistics**, you can view the results regarding network traffic over your wireless connection.

Windows XP and 2000:



Current

Network name (SSID): USR5464_sw409

Connection time: 01:06

Packets sent: 228

Packets received: 0

Sent packets lost: 10

Received packets lost: 0

Total packets lost (%): 4%

Accumulated

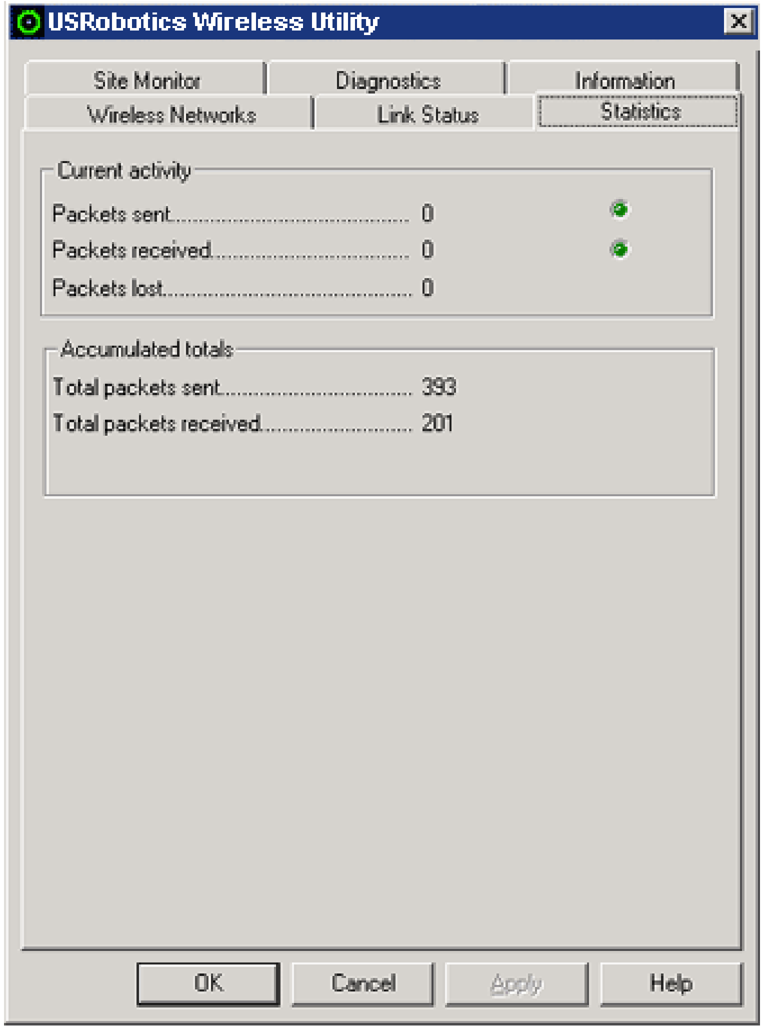
Packets sent: 228

Packets received: 0

Sent packets lost: 10

Received packets lost: 0

Windows Me and 98SE:



Current activity

Packets sent.. 0

Packets received.................................. 0

Packets lost... 0

Accumulated totals

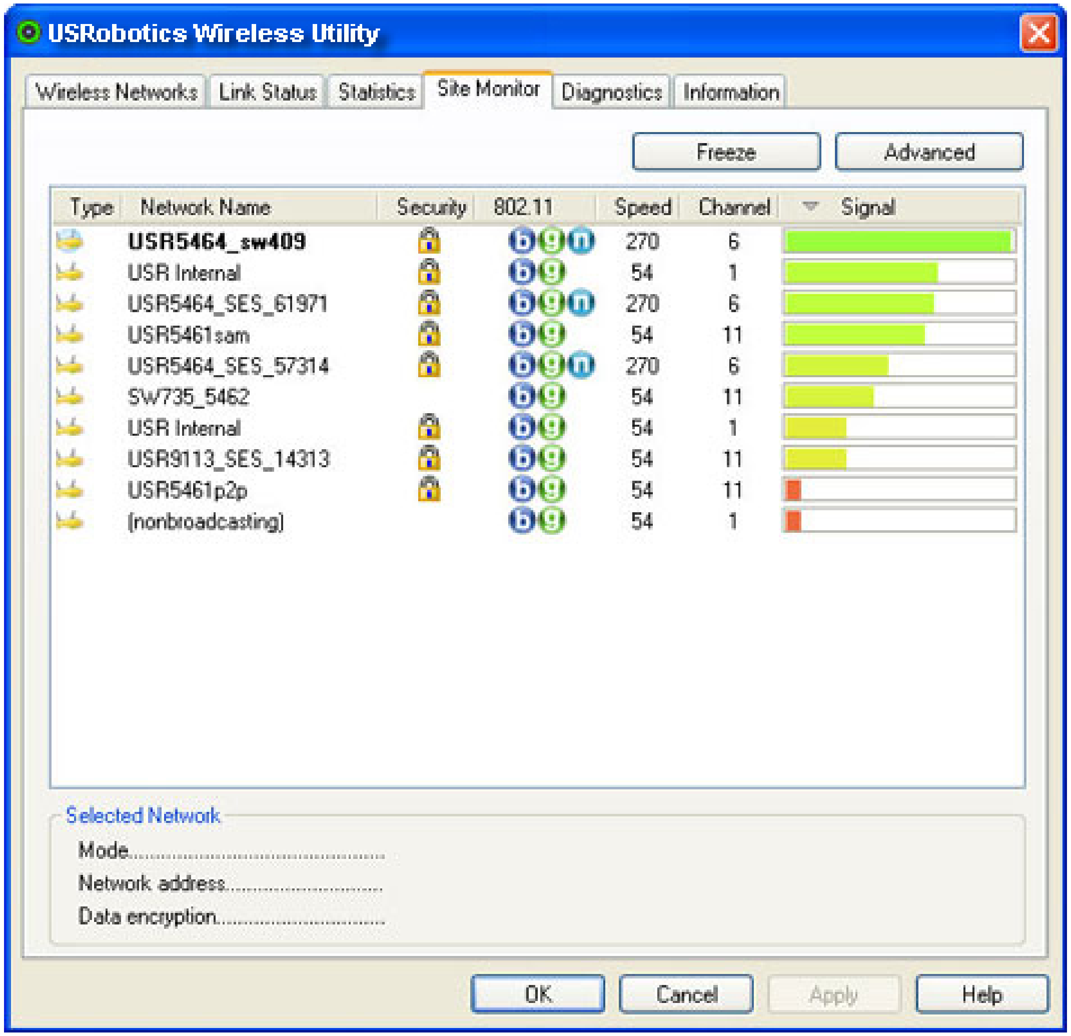
Total packets sent................................. 393

Total packets received.......................... 201

In **Site Monitor**, you can see the wireless network devices that your Wireless Wireless *MAX*g USB Adapter could connect to. If you want to connect to a device that you see in this list, go to the Wireless Networks area.

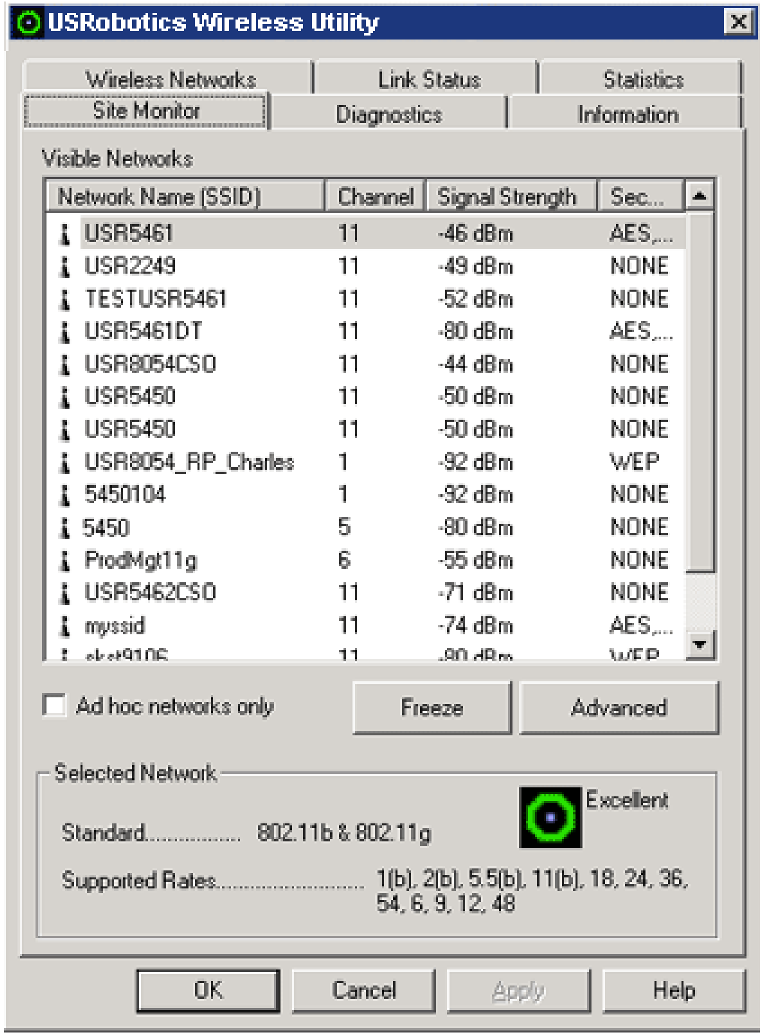
Windows XP and 2000:

Windows Me and 98SE:



Type	Network Name	Security	802.11	Speed	Channel	Signal
	USR5464_sw409	🔒	b g n	270	6	🟩
	USR Internal	🔒	b g	54	1	🟩
	USR5464_SES_61971	🔒	b g n	270	6	🟩
	USR5461sam	🔒	b g	54	11	🟩
	USR5464_SES_57314	🔒	b g n	270	6	🟩
	SW735_5462		b g	54	11	🟩
	USR Internal	🔒	b g	54	1	🟨
	USR9113_SES_14313	🔒	b g	54	11	🟨
	USR5461p2p	🔒	b g	54	11	🟥
	(nonbroadcasting)		b g	54	1	🟥

Selected Network
Mode...
Network address...............................
Data encryption..................................



Visible Networks

Network Name (SSID)	Channel	Signal Strength	Sec...
USR5461	11	-46 dBm	AES,...
USR2249	11	-49 dBm	NONE
TESTUSR5461	11	-52 dBm	NONE
USR5461DT	11	-80 dBm	AES,...
USR8054CSO	11	-44 dBm	NONE
USR5450	11	-50 dBm	NONE
USR5450	11	-50 dBm	NONE
USR8054_RP_Charles	1	-92 dBm	WEP
5450104	1	-92 dBm	NONE
5450	5	-80 dBm	NONE
ProdMgt11g	6	-55 dBm	NONE
USR5462CSO	11	-71 dBm	NONE
myssid	11	-74 dBm	AES,...
skst9106	11	-90 dBm	WEP

☐ Ad hoc networks only

Selected Network

Excellent

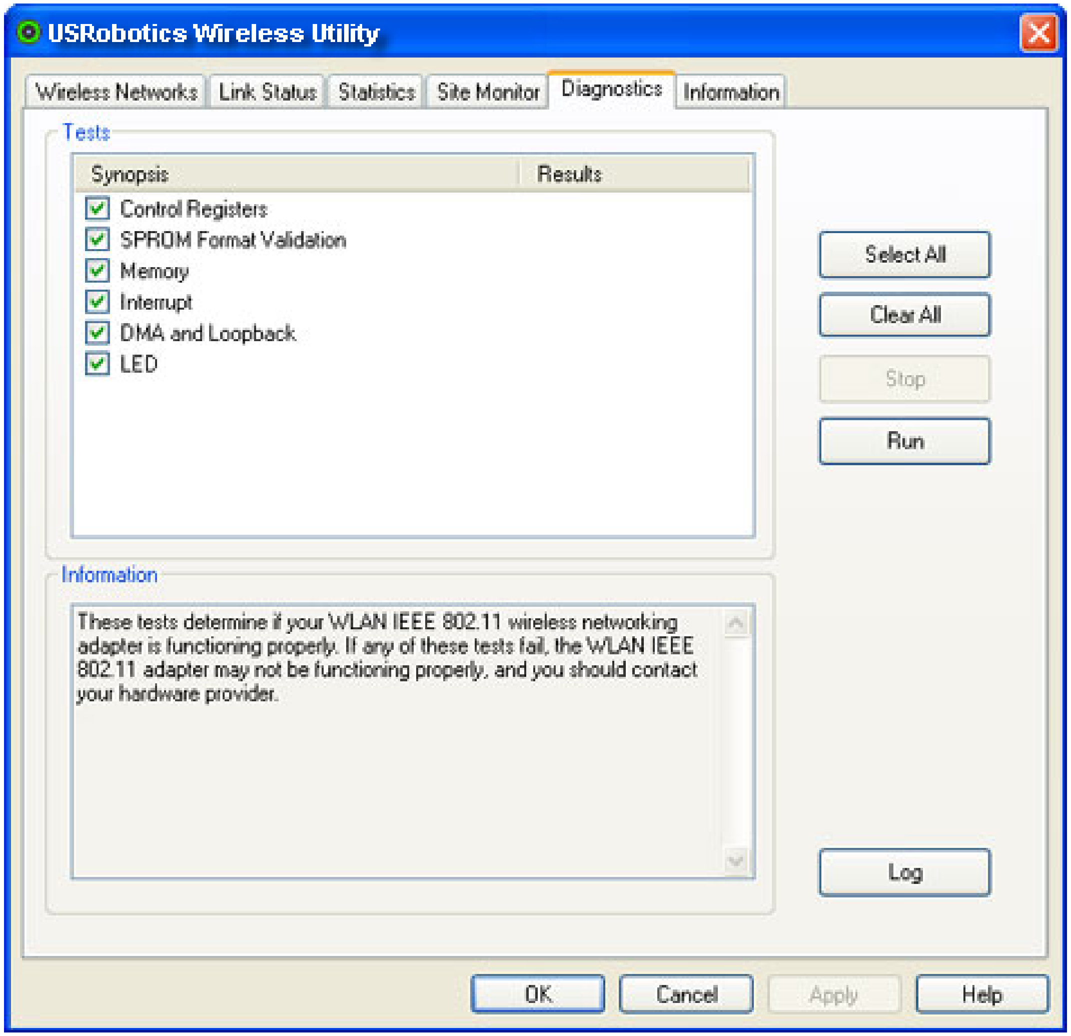
Standard................ 802.11b & 802.11g

Supported Rates......................... 1(b), 2(b), 5.5(b), 11(b), 18, 24, 36, 54, 6, 9, 12, 48

In the **Diagnostics** area, you can run a battery of tests on your Wireless Wireless *MAX*g USB Adapter and on your wireless connection.

Windows XP and 2000:

Windows Me and 98SE:

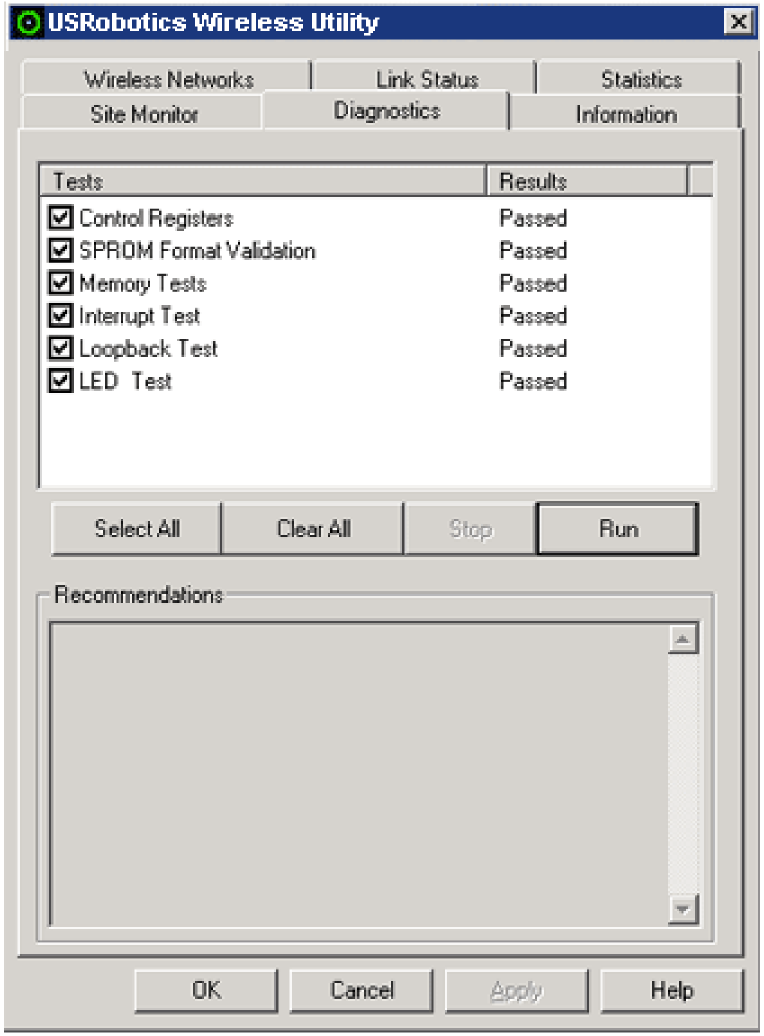


Tests

Synopsis	Results
☑ Control Registers	
☑ SPROM Format Validation	
☑ Memory	
☑ Interrupt	
☑ DMA and Loopback	
☑ LED	

Information

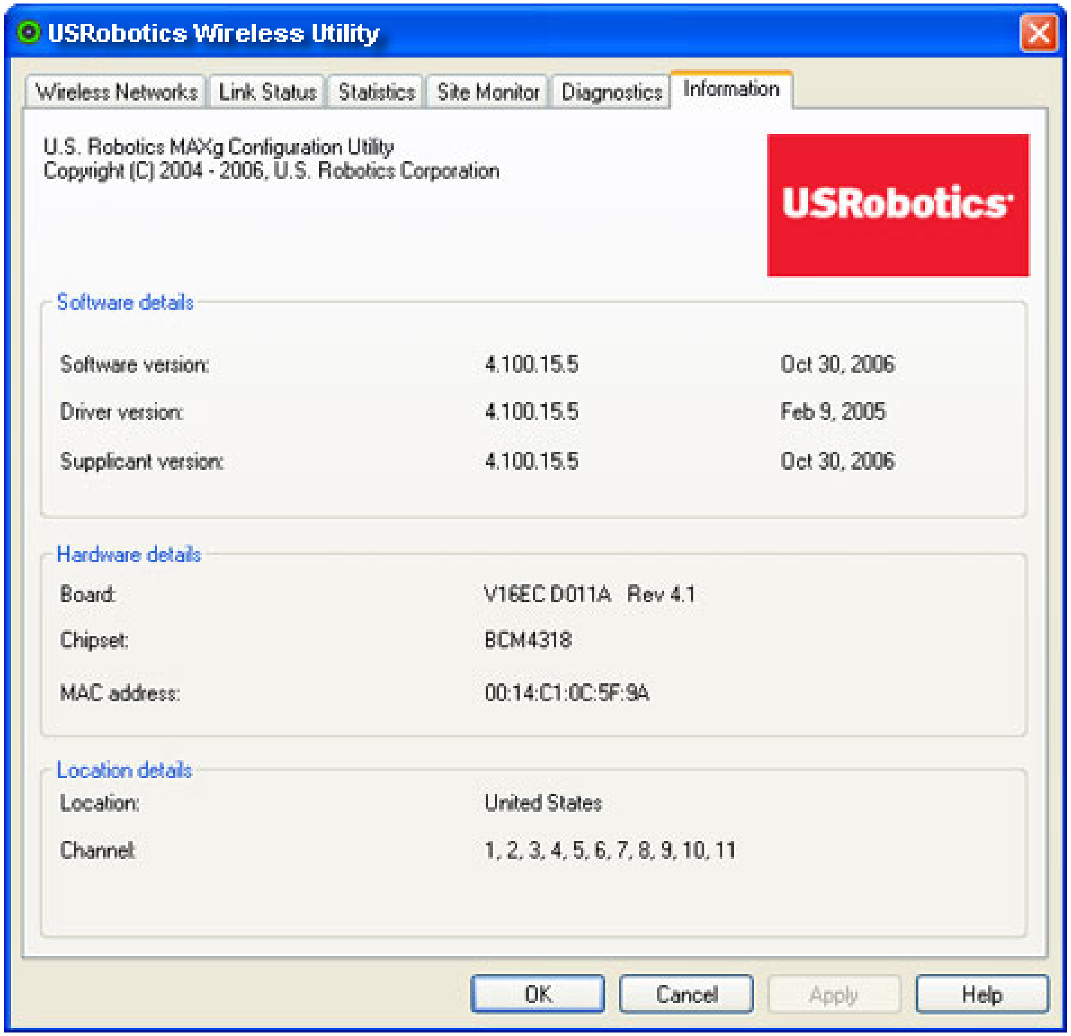
These tests determine if your WLAN IEEE 802.11 wireless networking adapter is functioning properly. If any of these tests fail, the WLAN IEEE 802.11 adapter may not be functioning properly, and you should contact your hardware provider.



Tests	Results
☑ Control Registers	Passed
☑ SPROM Format Validation	Passed
☑ Memory Tests	Passed
☑ Interrupt Test	Passed
☑ Loopback Test	Passed
☑ LED Test	Passed

In the **Information** area, you can view the version information for your Wireless Wireless *MAX*g USB Adapter.

Windows XP and 2000:	**Windows Me and 98SE:**



U.S. Robotics MAXg Configuration Utility
Copyright (C) 2004 - 2006, U.S. Robotics Corporation

Software details

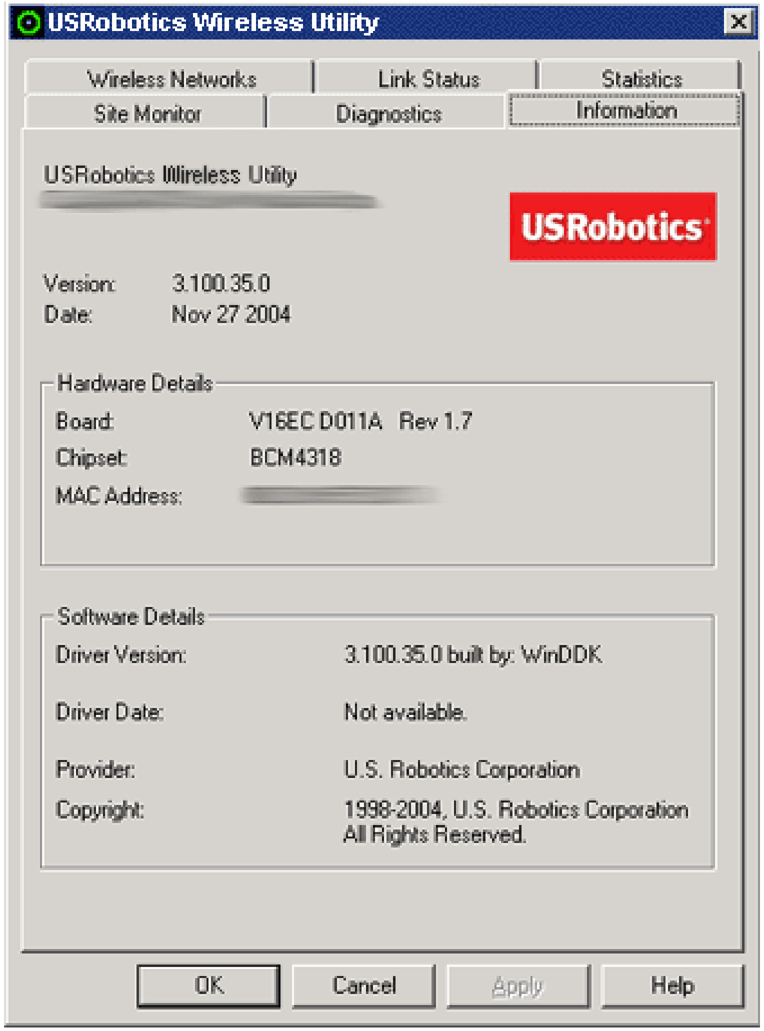
Software version:	4.100.15.5	Oct 30, 2006
Driver version:	4.100.15.5	Feb 9, 2005
Supplicant version:	4.100.15.5	Oct 30, 2006

Hardware details

Board:	V16EC D011A Rev 4.1
Chipset:	BCM4318
MAC address:	00:14:C1:0C:5F:9A

Location details

Location:	United States
Channel:	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11



USRobotics Wireless Utility
[redacted]

Version:	3.100.35.0
Date:	Nov 27 2004

Hardware Details

Board:	V16EC D011A Rev 1.7
Chipset:	BCM4318
MAC Address:	[redacted]

Software Details

Driver Version:	3.100.35.0 built by: WinDDK
Driver Date:	Not available.
Provider:	U.S. Robotics Corporation
Copyright:	1998-2004, U.S. Robotics Corporation All Rights Reserved.

USRobotics **Wireless MAXg USB Adapter: User Guide**

Configuration Using Windows Vista

You can see the networks that are available for you to connect to when you open the wizard. If the network is hidden, you must manually create a network profile, which includes the network name (SSID) and security key (if applicable). Profiles for advanced infrastructure networks also include settings for specific network authentication methods.

After you initially connect to the network, the profile is saved on your computer and is listed at the top of the list in Manage Wireless Networks. Your computer tries to connect to the listed networks in the order that they are listed. You can arrange the profiles in the order you prefer by moving any profile up or down in the list.

Select the configuration task that you want to perform:

- Learn about security protocols
- Connect to a network
- Add a network that is in range of this computer
- Manually create a network profile
- Create an ad hoc network
- Obtain a certificate
- Set advanced properties for the network adapter

Available Network Security Protocols

Several different security protocols are available with your wireless adapter:

- Basic

  - Open
  - Shared
  - WPA-Personal
  - WPA2-Personal
- Advanced
  - 802.1X
  - WPA-Enterprise
  - WPA2-Enterprise

Basic Security

Basic security protocols are described in the following table:

Security type	Description	Encryption type	Authentication method	Encryption method
No authentication (open)	Open security is not really authentication because it only identifies a wireless node using its wireless adapter hardware address.	WEP or none	None	A network key is used for WEP security.
Shared	Shared security verifies that the wireless client joining the wireless network has been configured with a secret key. With an infrastructure network, all of the wireless clients and the	WEP or none	None	A network key is used for

	wireless router/ AP use the same shared key. With an ad hoc network, all of the wireless clients of the ad hoc wireless network use the same shared key.			WEP security.
WPA-Personal WPA2-Personal	For infrastructure environments without the RADIUS infrastructure. WPA-Personal and WPA2-Personal security types support the use of a preshared key and are the next generation of wireless network security for home and small office environments.	TKIP or AES	None	A network key is used.

Advanced Security

802.1X Security with WEP Encryption

IEEE 802.1X-2001 security enforces authentication of a network node before it can begin to exchange data with the network. This mode is for environments with a Remote Access Dial-In User Service (RADIUS) infrastructure. This environment requires heavy technical support to set up and maintain and is intended for use by large corporations.

Authentication methods for 802.1X security are described in the following table.

Authentication method	**Authentication description**
EAP-TTLS/PAP	TTLS EAP authentication with PAP inner authentication. Requires user name and password.
EAP-TTLS/CHAP	TTLS EAP authentication with CHAP inner authentication. Requires user name and password.
EAP-TTLS/MD5	TTLS EAP authentication with MD5 inner authentication. Requires user name and password.
EAP-TTLS/MS-CHAP	TTLS EAP authentication with MS-CHAP inner authentication. Requires user name and password.
EAP-TTLS/MS-CHAPv2	TTLS EAP authentication with MS-CHAP v2 inner authentication. Requires user name and password.
Protected EAP (PEAP)	PEAP EAP authentication with secured password (EAP-MS-CHAP v2) authentication. Requires a user name and password. OR Smart card or other certificate.
Smart card or other certificate	Requires smart card or a client certificate.

WPA-Enterprise or WPA2-Enterprise Security Protocol

With WPA-Enterprise or WPA2-Enterprise security protocols, the network is operating in IEEE 802.1X authentication mode. This mode is for environments with a Remote Access Dial-In User Service (RADIUS) infrastructure. This environment requires heavy technical support to set up and maintain and is intended for use by large corporations.

WPA-Enterprise security protocol uses WPA protocol based on the selected WPA security type, and WPA2-Enterprise security protocol uses WPA2 security based on the selected WPA2 security type. Both WPA-Enterprise security and WPA2-Enterprise security protocols can use either TKIP data encryption or AES data encryption.

Authentication methods for WPA-Enterprise or WPA2-Enterprise security are described in the following table:

Authentication method	Authentication description
EAP-TTLS/PAP	TTLS EAP authentication with PAP inner authentication. Requires user name and password.
EAP-TTLS/CHAP	TTLS EAP authentication with CHAP inner authentication. Requires user name and password.
EAP-TTLS/MD5	TTLS EAP authentication with MD5 inner authentication. Requires user name and password.
EAP-TTLS/MS-CHAP	TTLS EAP authentication with MS-CHAP inner authentication. Requires user name and password.
EAP-TTLS/MS-CHAPv2	TTLS EAP authentication with MS-CHAP v2 inner authentication. Requires user name and password.
Protected EAP (PEAP)	PEAP EAP authentication with secured password (EAP-MS-CHAP v2) authentication. Requires a user name and password. OR Smart card or other certificate.
Smart card or other certificate	Requires smart card or a client certificate.
EAP-TTLS/PAP	TTLS EAP authentication with PAP inner authentication. Requires user name and password.
EAP-TTLS/CHAP	TTLS EAP authentication with CHAP inner authentication. Requires user name and password.
EAP-TTLS/MD5	TTLS EAP authentication with MD5 inner authentication. Requires user name and password.
EAP-TTLS/MS-CHAP	TTLS EAP authentication with MS-CHAP inner authentication. Requires user name and password.
EAP-TTLS/MS-CHAPv2	TTLS EAP authentication with MS-CHAP v2 inner authentication. Requires user name and password.
Protected EAP (PEAP)	PEAP EAP authentication with secured password (EAP-MS-CHAP v2) authentication. Requires a user name and password. OR Smart card or other certificate.
Smart card or other certificate	Requires smart card or a client certificate.

Connect to a Network

1. Click Windows **Start > Connect To**.
2. Select the network you want to connect to, and then click **Connect**.

Add a Network That Is in Range of This Computer

If the network is security-enabled, you must know the security key or passphrase to add a network. Add the network as follows:

1. Click Windows **Start > Control Panel > Network and Internet > Manage Wireless Networks**.
2. Click **Add**, click **Add a network that is in range of this computer**, and then follow the instructions.

Manually Create a Network Profile

1. Click Windows **Start > Control Panel > Network and Internet > Manage Wireless Networks**.
2. Click **Add > Manually create a network profile**.
3. Type the network name in the space provided.
4. Select the appropriate security type for your network in the **Security type** list.
5. Select the appropriate encryption type for your network (if available) in the **Encryption type** list.
6. If your network requires it, type the security key or passphrase in the space provided.
7. Click **Next**.

8. If your network does not require network authentication, click **Connect to**.

   OR

   If your network requires network authentication, click **Change connection settings**.

9. Click the **Security tab**

10. Select the appropriate network authentication method for your network, and then click **Settings**.

For Protected EAP (PEAP) Network Authentication

1. In the **Select Authentication Method** list, select the appropriate authentication method, and then click **Configure**.

2. If you selected **Secured password (EAP-MSCHAP v2)**, select or clear the **Automatically use my Windows logon name and password (and domain if any)** check box, as you prefer.

   OR

   If you selected **Smart Card or other certificate**, configure the properties with the settings you prefer, or accept the default settings.

For Broadcom EAP-TTLS Network Authentication

1. In the **Inner EAP method** list, select the Inner EAP method required by your network.

2. On the **User Name/Password** tab, specify how you want to log on to the network by selecting the appropriate check box. If you selected the Use Windows user name and password check box, type your user name and password in the spaces provided.

3. On the **Client Identity** tab, type your logon or identity in the space provided.

4. If your network does not require server certificates to be validated, ignore the **Server Identity** tab.

   OR

   If your network does require server certificates to be validated, click the **Server Identify** tab, and then select the **Validate server certificate** check box. If the default **Issuer** and **Server name** settings are appropriate for your network, click OK.

   OR

   If the default **Issuer** and **Server** name settings are not appropriate for your network, click **Select**. In the **Show certificate type** list, select the appropriate type of certificate, and then select the specific certificate to use.

For Smart Card or Other Certificate Network Authentication

Configure the properties with the settings you prefer, or accept the default settings.

Create an Ad Hoc Network

You can set up or connect to an ad hoc network that has either of the following security settings:

- WEP
- No authentication (Open)

For more informiton about ad hoc networks, see “IBSS 54g Protection Mode”, “IBSS Mode”, and “IBSS Channel Number”.

To Create an Ad Hoc Network

1. Click Windows **Start > Control Panel > Network and Internet > Manage Wireless Networks**.
2. Click **Add**, and then click **Create an ad hoc network**.
3. Click **Next**.
4. Give your network a name and choose security options.
5. Choose the file and printer sharing option you prefer.
6. Click **Next**.

Obtain a Certificate

The information in this section is intended for network administrators. Certificates can be obtained from a corporate certification authority stored on a Windows 2000 Server/ Windows Server 2003 system or by using the Internet Explorer Certificate Import Wizard.

- Obtain a certificate from Windows 2000 Server/Windows Server 2003
- Obtain a certificate from a file

Obtain a certificate from Windows 2000 Server/Windows Server 2003

1. Open Microsoft Internet Explorer and browse to the **Certificate Authority (CA) HTTP Servic**e.
2. Log on to the **CA Authority** with the user name and password of the user account created on the authentication server. This user name and password are not necessarily the same as your Windows user name and password.
3. On the Welcome page, click **Request a Certificate**.

4. On the **Request a Certificate** page, click **advanced certificate request**.
5. On the **Advanced Certificate Request** page, click **Create and submit a request to this CA**.
6. On the next **Advanced Certificate Request** page under **Certificate Template**, click **User in the list**.
7. Under **Key Options**, verify that the **Mark keys as exportable** check box is selected, and then click **Submit**.
8. On the **Certificate Issued** page, click **Install this certificate**, and then click **Yes** to continue.
9. If your certificate was correctly installed, a message is displayed, indicating that your new certificate has been successfully installed.
10. To verify the installation, on the **Tools** menu in Microsoft Internet Explorer, click **Internet Options**. Click the **Content tab**, and then click **Certificates**. The new certificate is listed on the **Personal tab**.

Obtain a Certificate from a File

1. Right-click the Internet Explorer icon on the desktop, and then click **Properties**.
2. Click the **Content** tab, and then click **Certificates**.
3. Under the list of certificates, click **Import**. This starts the Certification Import Wizard.
4. Click **Next**.
5. Select the file and click the password page.
6. Type the password for the file and ensure that the **Strong private key protection** option is not selected.

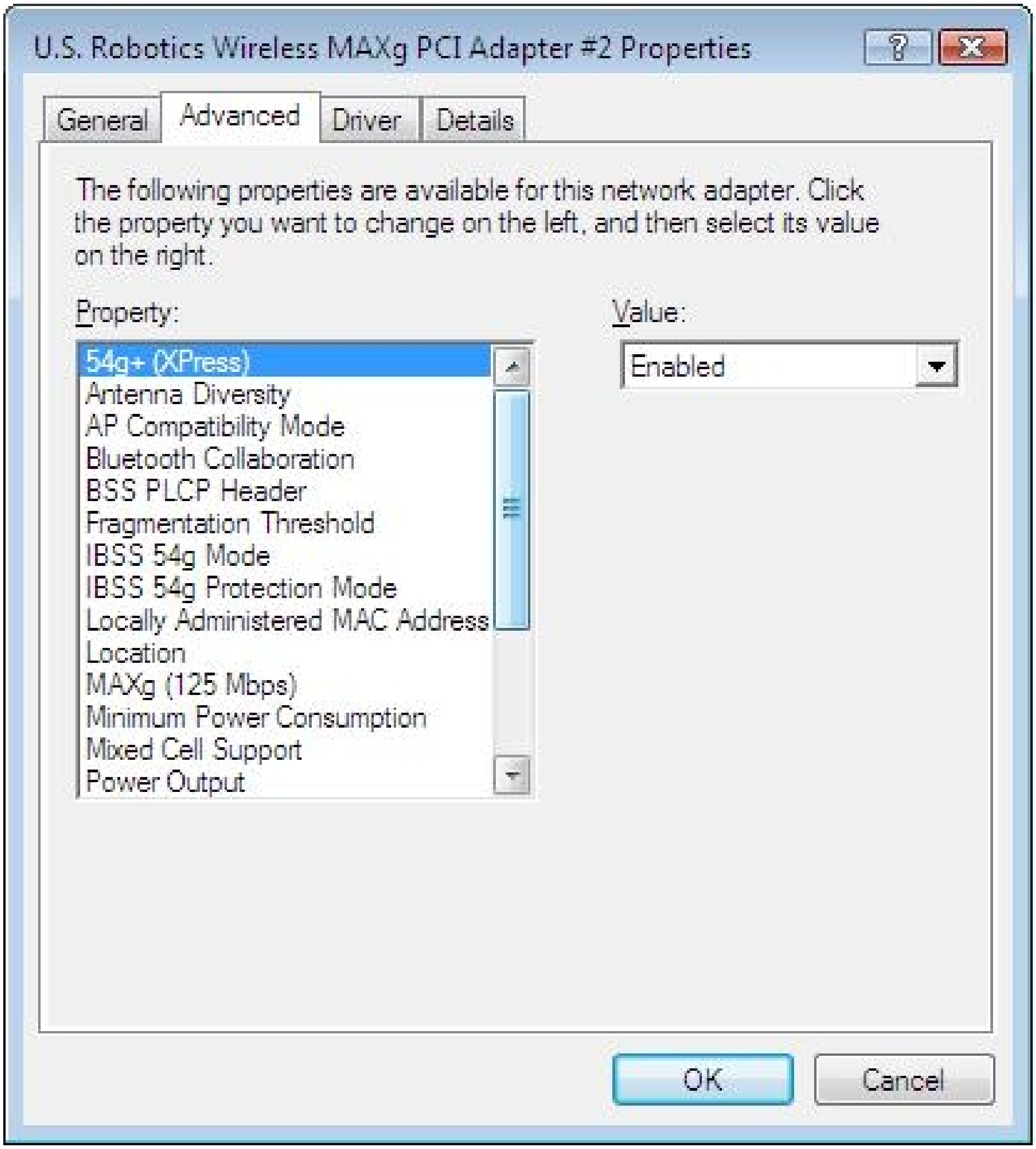
7. On the certification store page, select **Automatically select certificate store, based on the type of certificate.**

8. Complete the certificate import, and then click **Finish**.

Advanced Properties

The Advanced tab from the USRobotics Wireless *MAX*g Network Adapter Properties allows you to view and change the values of the available properties.

To access the Advanced tab, click Windows **Start** > **Control Panel** > **Network and Internet > Network and Sharing Center** > **Manage Wireless Networks** > **Adapter Properties**. In **Wireless Network Connection Properties**, click **Configure**. In the **Network Adapter Properties**, click the **Advanced** tab.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- 54g+ (XPress)
- Antenna Diversity
- AP Compatibility Mode
- Bluetooth Collaboration
- BSS PLCP Header
- Fragmentation Threshold
- IBSS 54g Mode
- IBSS 54g Protection Mode
- Locally Administered MAC Address
- Location
- MAXg (125 Mbps)
- Minimum Power Consumption
- Mixed Cell Support
- Power Output

Value: Enabled

To view the available settings for a given property, click the name of the property in the **Property** list. Then click the down arrow in the **Value** list.

To change a property setting, click an option in the **Value** list or type a new value, as appropriate (selection options are different for different properties).

Note: Some of the properties may not be available on your model of USRobotics Wireless *MAX*g adapter.

54g+ (XPress)

Xpress™ technology is a proprietary frame-bursting technology that improves throughput by repackaging data so that more data can be sent in each frame.

Disabled

Enabled (default)

Antenna Diversity

Antenna Diversity is a function included in most wireless LAN equipment that has two antennas, Main and Aux. When set to Auto, Antenna Diversity monitors the signal from each antenna and automatically switches to the one with the better signal.

Auto (default)

AP Compatibility Mode

Some older APs may have implementations that deviate from IEEE 802.11 standards. Setting this property to Broader Compatibility enables your wireless adapter to better communicate with such APs, but at the expense of some performance loss. The default setting is Higher Performance.

Broader Compatibility

Higher Performance (default)

Bluetooth Collaboration

Bluetooth Collaboration enables general purpose input/output transmit suppression protocol between the IEEE 802.11 media access control (MAC) and an external Bluetooth chip to minimize transmit interference. Bluetooth Collaboration is disabled by default.

Disable (default)

Enable

BSS PLCP Header

The BSS PLCP Header property is used to set the header type used for CCK rates. The type can be Long or Auto (short/long).

Auto (Short/Long) (default)

Long

Fragmentation Threshold

The maximum size in bytes at which packets are fragmented and transmitted a piece at a time instead of all at once. Available values range from 256 to 2346. The default value is 2346.

IBSS 54g Mode

IBSS 54g Mode is used to set the connection type in an ad hoc network. The following options are available:

54g - Auto

54g - Performance

802.11b Only (default)

IBSS 54g Protection Mode

A mechanism of prefixing each OFDM data frame with a request to send/clear to send (RTS/CTS) complimentary code keying (CCK) frame sequence. The duration fields of the RTS and CTS frames should allow the IEEE 802.11b node to correctly set its network allocation vector (NAV) and avoid collisions with the subsequent OFDM frames. As required for Wi-Fi®, protection mechanisms are enabled automatically whenever an IEEE 802.11b STA joins the BSS. If no IEEE 802.11b STA joins, then no protection mechanism is used and full IEEE 802.11g performance is attained.

Auto (default)

Disabled

Locally Administered MAC Address

Locally Administered MAC Address is used to override the MAC address of the Wireless *MAX*g USB Adapter. The Locally Administered MAC Address is a user-defined MAC address that is used in place of the MAC address originally assigned to the network adapter. Every adapter in the network must have its own unique MAC address. This locally administered address consists of a 12-digit hexadecimal number.

Value Assigns a unique node address for the adapter.

Not Present (Default). Uses the factory-assigned node address on the adapter.

The appropriate assigned ranges and exceptions for the locally administered address include the following:

- The range is 00:00:00:00:00:01 to FF:FF:FF:FF:FF:FD.
- Do not use a multicast address (least significant bit of the high byte = 1).
- Do not use all 0s or all F's.

Location

Sets available radio channels based on the location where the adapter was purchased. This value cannot be changed.

Default (default)

MAXg (125 Mbps)

MAXg is a USRobotics proprietary high-performance implementation of a faster throughput added to wireless products that conform to IEEE 802.11g.

Disabled

Enabled (default)

Minimum Power Consumption

When enabled, this property enables the wireless client to either turn off the radio or to not scan when the wireless client network is unassociated or when the computer is in the IDLE state.

Disabled (default)

Enabled

Mixed Cell Support

Mixed Cell Mode is a wireless network environment in which the use of WEP encryption is optional. If "optional encryption" is enabled on the access point, wireless clients that are using WEP encryption send all messages encrypted. At the same time, wireless clients that are not using WEP encryption send all messages unencrypted. Access points, that support mixed cell mode, broadcast that the network is not using encryption, but allow clients to use WEP encryption. When Mixed Cell Support is enabled, the wireless adapter can connect to access points that have “optional encryption” enabled.

Disabled (Default)

Enabled

Power Output

The power output property allows users to reduce the power output of the radio and therefore, the noise level, if excessive noise is a problem.

100% (default)

25%

50%

75%

Priority & VLAN

The Priority & VLAN property controls IEEE 802.1p packet priority and the VLAN identifier (ID). When the property is set to Priority Enabled or Priority & VLAN Enabled, the driver supports “User Priority” values that correspond to the following access classes: background (BG), best-effort (BE), video (VI), and voice (VO). When the property is set to Priority & VLAN Enabled or VLAN Enabled, the driver removes VLAN ID marking in the MAC headers of packets. When the property is set to Priority &VLAN Disabled, the packets in the queue are transmitted on a first-come, first-served basis, regardless of any priority information within the packet.

Priority & VLAN Disabled (default)

Priority & VLAN Enabled

Priority Enabled

VLAN Enabled

Rate

This property allows you to specify the rate (in Mbit/s) at which data is transmitted. The possible values are: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36 48, and 54 . The default is set to Use best Rate. This setting automatically adjusts the transmission rate to the optimal rate based on the capabilities of the other wireless clients and access points.

Note: The default value for this property is set for maximum performance. Therefore, it is not recommended for home users to change the value. Only network administrators or technicians with wireless LAN experience should attempt to make any changes.

Roam Tendency

This property adjusts the roaming thresholds for the Wireless *MAX*g USB Adapter.

Aggressive Roams to wireless networks having a signal strength at least 10 dB greater than the current one.

Conservative Roams to wireless networks having a signal strength at least 30 dB greater than the current one.

Moderate (default) Roams to wireless networks having a signal strength at least 20 dB greater than the current one.

Roaming Decision

This property sets the behaviour of the Wireless *MAX*g USB Adapter when roaming among access points.

Default (default)

Optimize Bandwidth

Optimize Distance

RTS Threshold

RTS Threshold sets the maximum number of frames allowed in a data packet before the Request To Send/Clear To Send Handshake is used. When the RTS Threshold is exceeded, the adapter sends a Request To Send message to the access point prior to sending data. When the access point receives the the Request To Send message, it broadcasts a Clear To Send message. This message tells the requesting adapter to send its message while telling other adapters to refrain from sending data while the requesting adapter sends its message. In environments where there are frequent data collisions between wireless adapters, decreasing the RTS threshold can decrease collisions and improve network performance. However, each RTS/CTS handshake adds communication overhead that can decrease network performance.

The default value is 2347. The range is 0 to 2347.

WMM

Wi-Fi Multimedia (WMM™). The WMM property enables quality of service for audio, video, and voice applications over a wireless network by prioritizing streams of content and optimizing the way the network allocates bandwidth among competing applications.

Auto (default). With WMM set to Auto, when the wireless client connects to the access point, and the access point has Unscheduled Automatic Power Save Delivery (UAPSD) enabled, the wireless client is allowed to enter Power Save mode.

Enabled The wireless client enters Power Save mode for WMM associations independent of whether the access point has UAPSD enabled or disabled.

Disabled The wireless client does not have WMM association.

WZC IBSS Channel Number

The WZC IBSS Channel Number property selects the independent basic service set (IBSS) channel number on which to operate when WZC is managing your wireless networks. The default setting is 11.

USRobotics Wireless MAXg USB Adapter: User Guide

Basic Troubleshooting Procedure

Note: If you are not using a USRobotics Wireless *MAX*g Router, refer to your router manufacturer's documentation for router-specific information.

This procedure addresses a number of symptoms that you might experience with your wireless network:

1. Verify the physical cable connections between your router, your computer, and your modem.

2. Ensure that the power outlets to which the router and modem are connected are a live outlets.

3. Check the LEDs on the router and modem to make sure you are receiving power and that are no errors.

4. For connectivity issues, reboot your DSL or cable modem and wait for the LEDs to stabilize, then reboot your router and wait for the LEDs to stabilize, then reboot your computer.

   Other devices connected to the router may need to re-establish their network connections.

5. Some electronic devices, such as 2.4GHz - 5.8 GHz phones and microwave ovens, may interfere with the wireless signal and affect your wireless range and link quality. Try creating a wireless connection on a different channel.

6. Low link quality or range can be caused by environmental interference, such as lead-based paint and concrete walls. Try to move the antenna of the router or to reposition the wireless clients to improve the link quality. If possible, ensure that there are no obstructions between wireless clients and the router.

If you still have trouble using the router, follow the procedure below that best describes your symptom.

I am no longer able to access the Internet.

My computer does not recognise the Wireless Wireless *MAX*g USB Adapter.

I am unable to communicate with an access point or wireless router.

I accidentally clicked Cancel during the software installation procedure for the Wireless *MAX*g USB Adapter.

The USRobotics installer did not begin when I inserted the Installation CD-ROM.

I inserted the Wireless Wireless *MAX*g USB Adapter before the Installation CD-ROM.

I cannot achieve *MAX*g (125 Mbps) connections to a Wireless *MAX*g Router.

I am unable to create a wireless connection to a wireless router or access point.

The wireless network I want to connect to is not appearing the Available Networks list in the USRobotics Wireless Utility.

The wireless clients seem to be communicating, but they do not appear in the **My Computer** window or in the **My Network Places** window.

My computer does not create a wireless connection to a Wireless *MAX*g Router after I changed the settings.

My Wireless *MAX*g Router is not appearing in the list when I wirelessly scan for it.

I am experiencing poor link quality.

© 2005-2007 U.S. Robotics Corporation

USRobotics **Wireless MAXg USB Adapter: User Guide**

My computer does not recognise the Wireless Wireless *MAX*g USB Adapter.

Possible Solution:

The Wireless *MAX*g USB Adapter may not be fully inserted into the USB port. You can also try installing the USB adapter into a different USB port.

Return to Troubleshooting page

USRobotics **Wireless MAXg USB Adapter: User Guide**

I am no longer able to access the Internet.

1. If you can no longer access the Internet, first see the "Basic Troubleshooting Procedure" section on the main Troubleshooting page.

2. If you are on a computer running Windows, run the **USRobotics Network Test** from the **Troubleshooting** folder on the USRobotics Installation CD-ROM.

   If you run the **USRobotics Network Test**, follow the instructions in the utility, and still cannot connect to the Internet, manually step through the remaining procedures below.

3. When your computer connects to the Internet, a number of devices have to work together, so there are a number of places where the connection from your computer to the Internet might fail. The following procedures cover troubleshooting for each of the connections between your computer and the Internet:

   A. Verify that the wireless adapter can connect to the router. If your adapter cannot communicate with the router, your computer cannot access the Internet.

   B. Verify the router's connection to the Cable or DSL modem. Your router must be communicating with the modem.

   C. Verify the modem's connection to the Internet. Your Internet connection must be up and functioning.

Verify That the Wireless Adapter Can Connect to the Router

1. Access the router's configuration interface. If you can access the router's configuration pages, try again to access the Internet.
   - **If you can connect to the router's configuration pages**: The problem is not in the connection between the wireless adapter and the router. Go to "Verify the Router's Connection to the Cable or DSL Modem".
   - **If you cannot connect to the router's configuration pages**:

     A. Try a wired connection between the computer and your router.

        i. Connect an Ethernet cable between your computer's LAN port and a LAN port on the router. Ensure that the corresponding LAN LED on the router is lit.

        ii. Start a Web browser. Try again to access the Internet.
           - **If you can connect to the router's configuration pages and the internet**: The problem is with your wireless adapter.
           - **If you cannot connect to the router's configuration pages**: Go to step 2 .
           - **If you can connect to the router's configuration pages**: Continue with this procedure.

     B. Go to the status information of the router and verify that the wireless adapter is using the correct Network Name (SSID) and that the wireless security settings match wireless security settings of the router.

     C. Make sure that the router allows wireless connections and is set to broadcast its Network Name.

     D. Determine whether the router has a MAC filter enabled. If the filter is set to allow only specific devices, add the MAC address of the wireless adapter to the router's MAC filtering list.

     E. Disconnect the computer from the router and re-establish your wireless connection to the router.

     F. Try again to access the router's configuration pages.
        - **If you can connect to the router's configuration pages and still cannot access the internet**: Go to "Verify the Router's Connection to the Cable or DSL Modem".
        - **If you cannot connect to the router's configuration pages**:

Continue with this procedure.

2. Release and renew your adapter's network connection.
   - Windows Vista Users
   - Windows XP, 2000 and NT Users
   - Windows Me, 98, and 95 Users

Windows Vista Users

A. Click Windows **Start**.

B. In the **Search** box, type **Command Prompt** and press ENTER.

C. In the resulting list, right-click **Command Prompt** and select **Run as Administrator**.

D. Type **ipconfig /release** and press ENTER.

E. Type **ipconfig /renew** and press ENTER.

Your wireless adapter should acquire an IP address (such as 192.168.2.5) from the router.

F. Type **exit** and press ENTER.

G. Go to step 3.

Windows XP, 2000 and NT Users

A. Click Windows **Start > Run**.

B. In the **Run** dialog box, type **cmd** and click **OK**.

C. Type **ipconfig /release** and press ENTER.

D. Type **ipconfig /renew** and press ENTER.

Your wireless adapter should acquire an IP address (such as 192.168.2.5) from the router.

E. Type **exit** and press ENTER.

F. Go to step 3.

Windows Me, 98, and 95 Users

A. Click Windows **Start > Run**.

B. In the **Run** dialog box, type **command** and click **OK**.

C. Enter **winipcfg** and press ENTER.

D. Press **Release**.

E. Press **Renew**.

Your wireless adapter should acquire an IP address (such as 192.168.2.5) from the router.

F. Close the window.

G. Go to step 3.

3. Try again to access the router's configuration pages. If you can access the router's configuration pages, try again to access the Internet.
   - **If the router's configuration pages appear but you still cannot connect to the Internet** : The problem is most likely with the connection to your cable or DSL modem. Go to "Verify the Router's Connection to the Cable or DSL Modem".
   - **If the router's configuration pages do not appear**:

     A. Reset your router. If your router has a Reset button, follow the instructions of the router manufacturer for using the button to reset the router; otherwise, reboot the router by disconnecting and then reconnecting its power supply.

B. Wait for the LEDs on the router to stabilize.

C. Release and renew your wireless adapter's network connection information again.

4. Try again to access the router's configuration pages. If you can access the router's configuration pages, try again to access the Internet.
   - **If the router's configuration pages appear but you still cannot connect to the Internet**: The problem is most likely with the connection to your cable or DSL modem. Go to "Verify the Router's Connection to the Cable or DSL Modem".
   - **If the router's configuration pages do not appear**: Restore your router to the factory default settings.

> **Note:** When you restore the factory defaults, all your current settings of the router will be lost and you will have to repeat the installation of your router.

5. Try again to access the router's configuration pages.
   - **If you can connect to the router's configuration pages**: Repeat the installation procedure for the router.
   - **If you cannot connect to the router's configuration**: Contact the customer support department of the router's manufacturer.

Verify the Router's Connection to the Cable or DSL Modem

1. Check your cable or DSL modem's power and status LEDs to verify that the modem is powered on and connected to the Internet. Refer to your modem's documentation for information on its LEDs.

2. In the router's configuration pages, find the WAN status information and verify that the router has an IP address (such as 235.42.181.5). This IP address indicates whether the router is communicating with the cable or DSL modem.
   - **If the router has an IP address**: Go to "Verify your modem's connection to the Internet".
   - **If the router does not have an IP address**:

A. Reboot the router.

B. In the router's configuration pages, refresh the WAN status information and verify that the router has an IP address.

C. If there is still no IP address, verify the router's Internet connection information. If you have a DSL modem, you may be required to enter the login information your ISP provided.

> **Note:** If your ISP uses a static WAN protocol, make sure that the WAN IP address of the router is the one that is provided by your ISP or is in the same subnet as the device that is connected to the WAN port of the router.

D. Refresh the Status page and verify that the router has an IP address.

E. If the router cannot obtain a WAN IP address, the problem is most likely with the cable or DSL modem or your ISP. Go to "Verify your modem's connection to the Internet".

Verify the Modem's Connection to the Internet

1. Check the LEDs on your cable or DSL modem to determine if the cable or DSL modem is connected to the Internet. See the documentation for modem for information on the LEDs.

2. Verify that your cable or DSL modem is connected to your wall jack.

3. Restart your cable or DSL modem. See the documentation for your modem for information on how to restart your modem.

4. After the LEDs on the modem have stabilized, reset the router. If your router has a Reset button, follow the instructions of the router manufacturer for using the button to reset the router; otherwise, reboot the router by disconnecting and then reconnecting its power supply.

5. Restart your computer.

6. After the LEDs on the router and DSL or cable modem have stabilized, try to access the Internet again.

   If you still cannot access the Internet: The problem is with the cable or DSL modem or your ISP. Contact your ISP's Customer Support to determine if there is a problem with your modem or Internet connection.

Return to Troubleshooting page

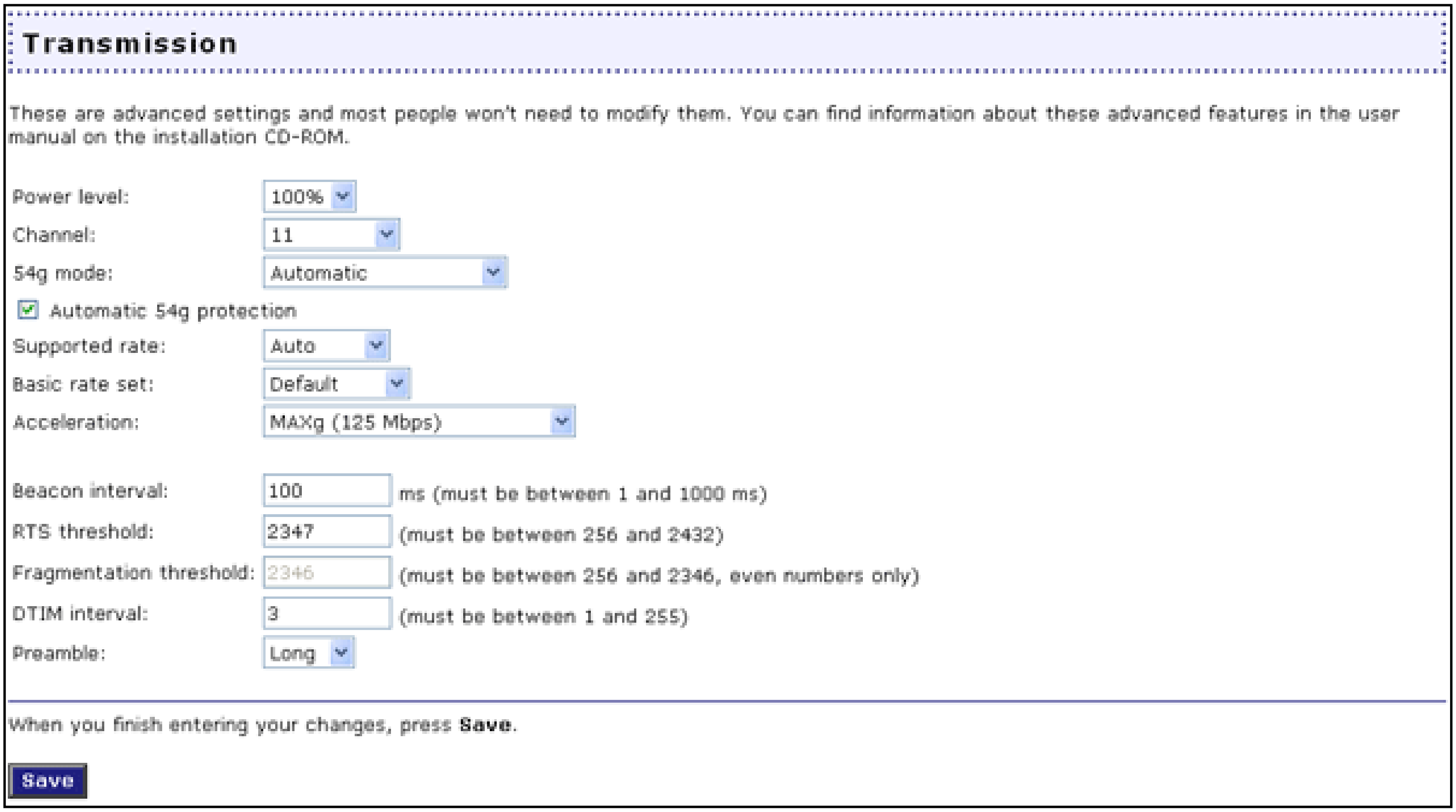
USRobotics *Wireless MAXg USB Adapter:*

User Guide

I cannot achieve *MAX*g (125 Mbps) connections to a Wireless *MAX*g Router.

Possible Solution:

Make sure you have *MAX*g enabled for the **Acceleration** option in the Wireless section of the Wireless *MAX*g Router's Web User Interface. This can be found in the Transmission area in the Wireless section. Launch the Web User Interface, click the **Wireless** tab, and manually set the **Acceleration** to *MAX*g within the Transmission area.



Transmission

These are advanced settings and most people won't need to modify them. You can find information about these advanced features in the user manual on the installation CD-ROM.

Power level: 100%
Channel: 11
54g mode: Automatic
☑ Automatic 54g protection
Supported rate: Auto
Basic rate set: Default
Acceleration: MAXg (125 Mbps)

Beacon interval: 100 ms (must be between 1 and 1000 ms)
RTS threshold: 2347 (must be between 256 and 2432)
Fragmentation threshold: 2346 (must be between 256 and 2346, even numbers only)
DTIM interval: 3 (must be between 1 and 255)
Preamble: Long

When you finish entering your changes, press **Save**.

Possible Solution:

Low link quality or range can be caused by environmental interference, such as lead-based paint and concrete walls. Try to move the antenna of the Wireless *MAX*g Router or to reposition the wireless clients to improve the link quality.

Possible Solution:

Some electronic devices, such as 2.4Ghz phones and microwave ovens, may interfere with the wireless signal and affect your wireless range and link quality. Try creating a wireless connection on a different channel.

Possible Solution:

If there is any wireless client that does not support the *MAX*g feature connected to the Wireless *MAX*g Router, the Wireless *MAX*g Router will switch to normal 54g mode and will not use *MAX*g acceleration.

Return to Troubleshooting page

USRobotics® *Wireless MAXg USB Adapter: User Guide*

I accidentally clicked Cancel during the software installation procedure for the Wireless Wireless *MAX*g USB Adapter.

Possible Solution:

Remove and reinsert the Installation CD-ROM into your CD-ROM drive. Follow the instructions in this guide for installing the software.

Return to Troubleshooting page

The USRobotics Installer did not begin when I inserted the Installation CD-ROM.

Possible Solution:

Some programs may disable the autorun feature of Windows. Close any open applications and reinsert the Installation CD-ROM. If the Installation CD-ROM interface does not run automatically, click Windows **Start** and then click **Run**. In the “Run” dialog box, type **D:\setup.exe**. If your CD-ROM drive uses a different letter, type that letter in place of “D.”

Return to Troubleshooting page

USRobotics® *Wireless MAXg USB Adapter: User Guide*

I inserted the Wireless Wireless *MAX*g USB Adapter before the Installation CD-ROM.

Possible Solution:

If you inserted the Wireless Wireless *MAX*g USB Adapter before the Installation CD-ROM, cancel the installation procedure that is currently running. Insert the Installation CD-ROM, select your language, click **Installation**, and then follow the on-screen instructions.

Return to Troubleshooting page

USRobotics *Wireless MAXg USB Adapter: User Guide*

The wireless clients seem to be communicating, but they do not appear in the My Computer screen or in the My Network Places screen.

Possible Solution:

Verify that File and Printer Sharing is enabled on all the computers on your network.

1. Open **Control Panel**.
   Note for Windows Vista and XP Users: If you are looking at Category View in Windows Vista or XP, click **Switch to Classic View**.

2. In Control Panel, double-click the **Network and Sharing Center** icon, **Network Connections** icon or **Network and Dial-up Connections** icon, depending on your version of Windows.

3. Windows Vista: Click **Manage network connections**. If prompted, click **Continue**.

4. Right-click the network connection for your wireless adapter and then click **Properties**.

5. In the network connection properties screen, verify that the **File and Printer Sharing for Microsoft Networks** check box is selected. If this item is not present, click **Install**. In the Select Network Component Type box, select **Service** and click **Add**. In the Select Network Service box, select **File and Printer Sharing for Microsoft Networks** and click **OK**. Close the network connection properties screen.

6. Close the Network Connections screen.

Return to Troubleshooting page

USRobotics Wireless MAXg USB Adapter: User Guide

I am unable to communicate with an access point or wireless router.

Possible Solution:

Be sure that each Wireless *MAX*g USB Adapter that you want to connect to the wireless network is set to Infrastructure mode within the USRobotics Wireless Utility. If a USB adapter is not set to Infrastructure mode, it will not be able to communicate with an access point or wireless router.

Possible Solution:

Determine the MAC address of the desired wireless router or access point. The MAC address is usually located on a label on the wireless routers and access points. Check the MAC address and verify that you are connecting to the correct wireless router or access point.

Possible Solution:

Ensure that the USRobotics Wireless Utility is installed for your Wireless *MAX*g USB Adapter and that the USRobotics Wireless Utility detects your Wireless Wireless *MAX*g USB Adapter.

Possible Solution:

Ensure that the correct Authentication Mode and encryption key are being used. If you changed the settings in the configuration of your wireless router or access point, you must also change the settings of every Wireless *MAX*g USB Adapter attached to this network. The settings of your Wireless *MAX*g USB Adapter must match the new settings of the wireless router or access point. If you are still experiencing difficulties, reset all of your wireless routers or access points and wireless network adapters to the default settings and try again.

Return to Troubleshooting page

USRobotics **Wireless MAXg USB Adapter: User Guide**

I am unable to create a wireless connection to a wireless router or access point.

Possible Solution:

Ensure that the USRobotics Wireless Utility is installed for your Wireless Wireless *MAX*g USB Adapter and that the USRobotics Wireless Utility detects your Wireless Wireless *MAX*g USB Adapter.

Possible Solution:

Check the USRobotics Wireless Utility icon in the system tray to confirm the connection status. If you are connected to your wireless network device, the icon is green or yellow. If the icon is red, open the USRobotics Wireless Utility, and click the **Wireless Networks** tab. Double-click the network that you are connecting to and follow the prompts.

Possible Solution:

Windows XP and 2000

> Verify that you are using the same SSID, Channel, and Security information as the wireless router or access point. Perform the following steps to verify and, if necessary, update the settings:

1. Right-click the Utility icon in the system tray and select **Open Utility**.

2. On the Wireless Networks tab, pull down the **Add** menu and select **Use Wizard**. Browse through the list of available wireless network devices and locate the correct wireless router or access point. If you do not see the correct device, click **Refresh** to update the list. Double-click the device. If the correct device still does not appear, click **Manually connect to an advanced network** and enter the appropriate information to create the entry. For more information about setting up connection profiles and security features, right click the **USRobotics Wireless Utility icon** and select **Help Files**.

3. When the Properties window appears, verify and, if necessary, update the appropriate connection and security information for the wireless network device. Make sure you do not have the checkbox next to This is a computer-to-computer (ad hoc) network selected. When you are finished, click **OK**.

4. On the main screen, click **Apply** and a connection will be established.

Windows Me and 98SE

Verify that you are using the same SSID, Channel, and Security information as the wireless router or access point. Perform the following steps to verify and, if necessary, update the settings:

1. Either right-click the Utility icon in the system tray and select **Open Utility** or left-click the Utility icon once and then click **Advanced**.

2. In the Wireless Networks screen, browse through the list of available wireless network devices and locate the correct wireless router or access point. If you do not see the correct device, click **Refresh** to update the list. When you locate the correct wireless router or access point, select it and then click **Configure**. If the correct device still does not appear, click **Add** under the Preferred networks section and manually update the appropriate information to create the entry.

3. When the Properties window appears, verify and, if necessary,

update the appropriate connection and security information for the wireless network device. Make sure you do not have the checkbox next to **This is a computer-to-computer (ad hoc) network** selected. When you are finished, click **OK**.

4. On the main screen, click **Apply** and a connection will be established.

Possible Solution:

Change the channel used by the wireless router or access point and check for the network on the **Wireless Networks** tab.

Possible Solution:

Verify that MAC address filtering is not enabled on your wireless router or access point. If MAC address filtering is enabled, the MAC address of the Wireless *MAX*g USB Adapter must be included in the filtering table of the wireless router or access point.

Possible Solution:

Be sure that each Wireless Wireless *MAX*g USB Adapter that you want to connect to the wireless network is set to Infrastructure mode within the USRobotics Wireless Utility. If a Wireless *MAX*g USB Adapter is not set to Infrastructure mode, it will not be able to communicate with an access point or wireless router.

Possible Solution:

Determine the WLAN MAC address of the desired wireless router or access point. The WLAN MAC address is usually located on a label on the wireless routers and access points. Check the WLAN MAC address and verify that you are connecting to the correct wireless router or access point.

Return to Troubleshooting page

My computer does not create a wireless connection to a Wireless *MAX*g Router after I changed the settings.

Possible Solution:

In the USRobotics Wireless Utility for your Wireless Wireless *MAX*g USB Adapter, ensure that you are connecting to the correct Wireless *MAX*g Router by verifying the MAC address, Network name (SSID), and security settings. The MAC address is located on the label on the bottom of the Wireless *MAX*g Router. Ensure that the correct Pass phrase and encryption option are being used. If you changed the settings in the configuration of the Wireless *MAX*g Router, you must also change the settings of every Wireless *MAX*g USB Adapter connecting to this network. The settings of the Wireless *MAX*g USB Adapter must match the new settings of the Wireless *MAX*g Router.

Return to Troubleshooting page

USRobotics Wireless MAXg USB Adapter: User Guide

The wireless network I want to connect to is not appearing in the Available Networks list in the USRobotics Wireless Utility.

Possible Solution:

Verify that your access point or wireless router is functioning correctly.

Possible Solution:

Check the Network name (SSID) of the wireless network and verify that the access point or wireless router is set to broadcast the Network name (SSID).

Possible Solution:

Change the channel on the access point or wireless router to channel 1 and retest. If the problem persists, change the channel on the access point or wireless router to channel 11 and retest. If the problem persists, change the channel on the access point or wireless router to channel 6 and retest.

Return to Troubleshooting page

USRobotics ***Wireless MAXg USB Adapter:***

User Guide

My Wireless *MAX*g Router is not appearing in the list when I wirelessly scan for it.

Possible Solution:

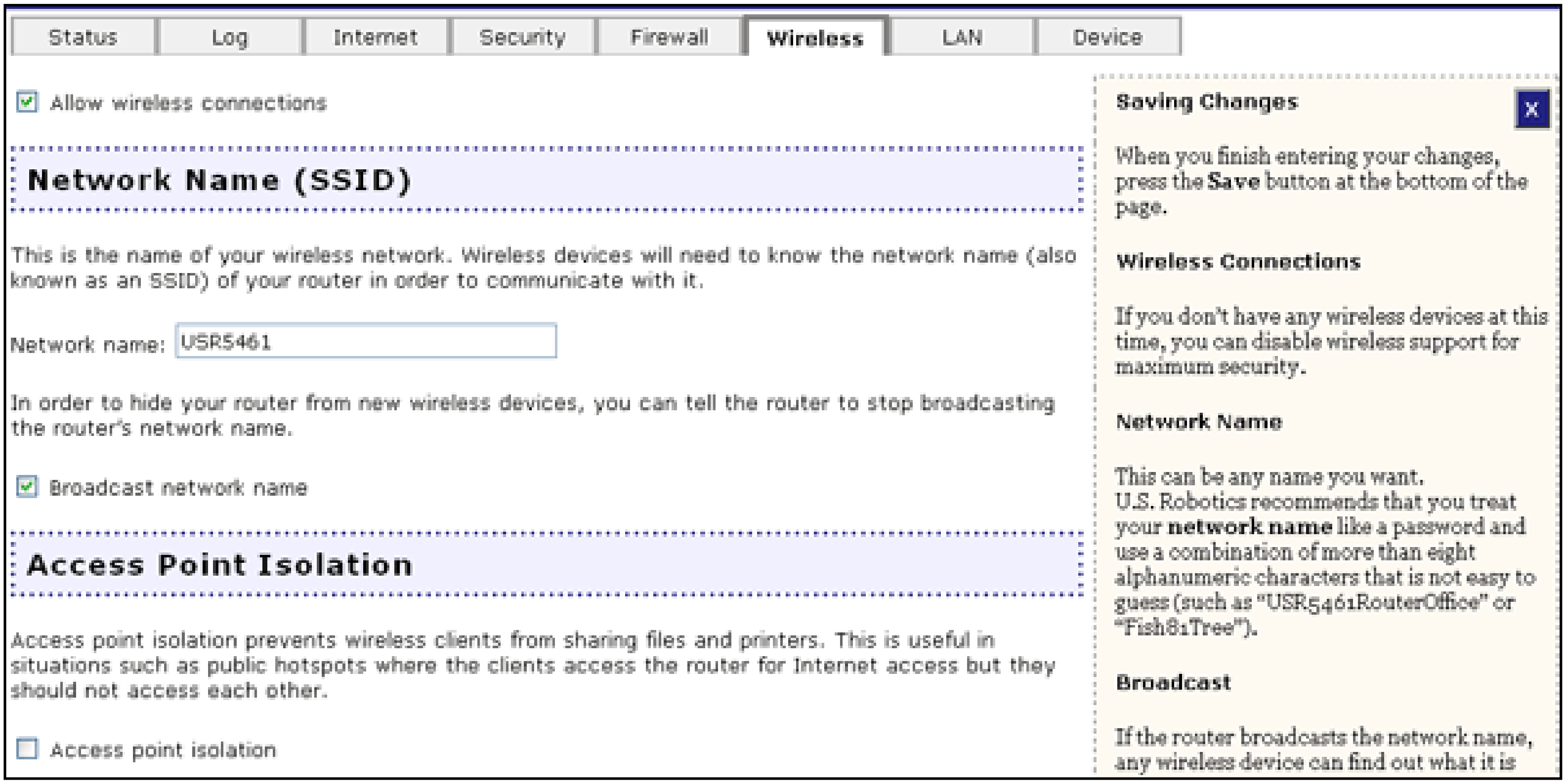
You may be on a computer that is too far away from the Wireless *MAX*g Router. Try moving closer to the Wireless *MAX*g Router and repeating the scan procedure.

Possible Solution:

Verify that you are using the same SSID, Channel, and Security information as set in the Wireless *MAX*g Router.

Possible Solution:

Using a wired connection, launch a Web browser. In the location or address line of your Web browser, type http://192.168.2.1 to log in and access the Web User Interface. Go to the Wireless section and verify **Broadcast network name** is enabled on the Wireless MAXg Router.



☑ Allow wireless connections

Network Name (SSID)

This is the name of your wireless network. Wireless devices will need to know the network name (also known as an SSID) of your router in order to communicate with it.

Network name: USR5461

In order to hide your router from new wireless devices, you can tell the router to stop broadcasting the router's network name.

☑ Broadcast network name

Access Point Isolation

Access point isolation prevents wireless clients from sharing files and printers. This is useful in situations such as public hotspots where the clients access the router for Internet access but they should not access each other.

□ Access point isolation

Saving Changes

When you finish entering your changes, press the **Save** button at the bottom of the page.

Wireless Connections

If you don't have any wireless devices at this time, you can disable wireless support for maximum security.

Network Name

This can be any name you want. U.S. Robotics recommends that you treat your **network name** like a password and use a combination of more than eight alphanumeric characters that is not easy to guess (such as "USR5461RouterOffice" or "Fish81Tree").

Broadcast

If the router broadcasts the network name, any wireless device can find out what it is

Refer to I am no longer able to access the Internet in the Troubleshooting section for more information.

Return to Troubleshooting page

USRobotics® Wireless MAXg USB Adapter: User Guide

I am experiencing poor link quality.

Possible Solution:

Low link quality or range can be caused by environmental interference, such as lead-based paint and concrete walls. Try to move the antenna of the Wireless MAXg Router or to reposition the wireless clients to improve the link quality.

Possible Solution:

Some electronic devices, such as 2.4Ghz phones and microwave ovens, may interfere with the wireless signal and affect your wireless range and link quality. Try creating a wireless connection on a different channel.

Return to Troubleshooting page

USRobotics *Wireless MAXg USB Adapter: User Guide*

Frequently Asked Questions

What is 802.11 wireless networking?

802.11 (sometimes called "Wi-Fi") is a set of protocols that are widely used for small Local Area Networks. Another protocol called Bluetooth allows devices to communicate wirelessly, but it is only useful for very short ranges, and generally not used for home networking. Bluetooth can be useful for networking personal devices in a small area, often called a Personal Area Network (PAN).

802.11 actually encompasses several different protocols. The trailing letters (i.e. the **g** in 802.11g) indicate different speeds and frequency bands used.

What kind of wireless antenna range performance issues might affect my wireless connection?

Radio waves don't really travel the same distance in all directions. Walls, doors, elevator shafts, people, and other obstacles offer varying degrees of attenuation, which cause the Radio Frequency (RF) radiation pattern to be irregular and unpredictable. Attenuation is simply a reduction of signal strength during transmission. Attenuation is registered in decibels (dB), which is ten times the logarithm of the signal power at a particular input divided by the signal power at an output of a specified medium. For example, an office wall (i.e., medium) that changes the propagation of an RF signal from a power level of 200 milliwatts (the input) to 100 milliwatts (the output) represents 3 dB of attenuation. The following provides some examples of the attenuation values of common office construction:

Plasterboard wall: 3dB
Glass wall with metal frame: 6dB
Cinder block wall: 4dB
Office window: 3dB
Metal door: 6dB
Metal door in brick wall: 12.4dB
Other factors that will reduce range and affect coverage area include concrete fiberboard walls, aluminum siding, pipes and electrical wiring, microwave ovens, and cordless phones.

What should I do if I am unable to access my e-mail or the Web page of my ISP?

You should contact your ISP to get the full URL and then perform the following steps:

> **Note:** Linux users can perform steps 3 and 4 after opening a terminal.

1. Connect your broadband modem directly to one of your computers.

2. Open a command prompt as follows:
   - **Windows Vista:**

     A. Click Windows **Start**.

     B. In the **Search** box, type **Command Prompt** and press ENTER.

     C. In the result list, double-click **Command Prompt**.

   - **All other Windows operating systems:**

     A. Click Windows **Start > Run**.

B. In the **Run** dialog box:
Windows XP, 2000, and NT: Type **cmd** and click **OK**.
Windows Me, 98, and 95: Type **command** and click **OK**.

3. All users should then enter the following command: **ping xxx**, where *xxx* is the complete URL for your ISP.
4. After you get the IP address, enter the IP address in the mail server option or in the address line of your Web browser.

Can the wireless router I am wirelessly networked with be used in place of a modem?

No, a broadband modem must still be used to have Internet access over the wireless network.

USRobotics® **Wireless MAXg USB Adapter: User Guide**

Glossary

A B C D E F G H I L M N O P Q R S T U W

A

access point (AP)

A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. An access point has at least one interface that connects it to an existing wired network. See also wireless router/AP

ad hoc network

In ad hoc mode, wireless clients communicate directly with each other without the use of a wireless router/AP. Also known as a peer-to-peer network or a computer-to-computer network.

advanced network

An infrastructure network that uses some form of EAP authentication.

AES

Advanced Encryption Standard A replacement for WEP encryption. AES provides better encryption (is more secure) than WEP.

associated

The state when a wireless client adapter has made a connection with a chosen wireless router/AP.

association

The process by which a wireless client negotiates the use of a logical port with the chosen wireless router/AP.

authenticated provisioning

A provisioning mode supported by EAP-FAST Extensible Authentication Protocol in which provisioning is done inside a server-authenticated (TLS) tunnel.

AID

An authority identity that identifies an EAP-FAST authenticator. The local authenticator sends its AID to an authenticating wireless client, and the client checks its database for a matching AID. If the client does not recognize the AID, it requests a new PAC.

auto-provisioning

A way of managing EAP-FAST Extensible Authentication Protocol networks whereby a Protected Access Credential (PAC) is automatically provided to the wireless client when the user logs on to the network.

authentication

The process whereby preapproved wireless clients may join a collision domain. Authentication occurs before association.

available network

1. A broadcasting network that is within range.
2. Any of the networks listed under **Available networks** on the **Wireless Networks** tab of Windows **Wireless Network Connection Properties**. All broadcasting wireless networks (both infrastructure and ad hoc) that are within receiving range of the wireless client are listed. Any wireless network that you are already connected to is also listed as an available network, even if it is not broadcasting.

B

base station

A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. A base station is usually referred to as an access point (AP). See also access point and wireless router/AP.

basic network

1. An infrastructure network that has any of the following security settings:
   - WPA-PSK authentication
   - WEP (open or shared authentication)
   - None
2. An ad hoc network that has either WEP security settings or no security settings.

BER

bit error rate The ratio of errors to the total number of bits being sent in a data transmission from one location to another.

broadcasting network

A network that is broadcasting its network name.

C

CA

Certification Authority An entity responsible for establishing and vouching for the authenticity of public keys belonging to users (end entities) or other certification authorities. Activities of a certification authority can include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and revoking certificates.

CCK

complimentary code keying The modulation technique for high and medium transmit rates.

CCKM

Cisco Centralized Key Management An authentication method in which an access point is configured to provide Wireless Domain Services (WDS) to take the place of the RADIUS server and to authenticate the client so quickly that there is no perceptible delay in voice or other time-sensitive applications.

CCMP

Counter-Mode/CBC-MAC Protocol An IEEE 802.11i encryption algorithm. In the IEEE 802.11i standard, unlike WPA, key management and message integrity is handled by a single component CCMP built around AES.

Cisco Compatible Extensions

A licensing agreement offered by Cisco Systems to enable interoperability of third-party client adapters and mobile devices with Cisco Aironet wireless local area network (LAN) infrastructure.

Cisco Compatible Extensions v4

Version 4 of Cisco Compatible Extensions.

certificate

A digital document that is commonly used for authentication and secure exchange of information on open networks, such as the Internet, extranets, and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority and can be issued for a user, a computer, or a service. The most widely accepted format for certificates is defined by the ITU-T X.509 version 3 international standard. See also intermediate certificate and root certificate.

certificate store

The storage area on your computer where requested certificates are stored.

The user store is the Personal folder in the certificate store.

The root store is in the Trusted Root Certification Authorities folder in the certificate store.

The machine store is on the authentication server of the certification authority.

CKIP

Cisco Key Integrity Protocol A Cisco proprietary security protocol for encryption in IEEE 802.11 media. CKIP uses key permutation, message integrity check and message sequence number to improve IEEE 802.11 security in infrastructure mode.

CHAP

Challenge Handshake Authentication Protocol An authentication scheme used by Point-to-Point-Protocol servers to validate the identity of the originator of a connection, upon connection or any time later.

CSP

cryptographic service provider A cryptographic service provider contains implementations of cryptographic standards and algorithms. A smart card is an example of a hardware-based CSP.

CSMA/CA

carrier sense multiple access with collision avoidance An IEEE 802.11 protocol that ensures that the number of collisions within a domain are kept to a minimum.

D

dBm

A unit of expression of power level in decibels with reference to a power of 1 milliwatt.

DBPSK

differential binary phase shift keying The modulation technique used for low transmit rate.

DHCP

Dynamic Host Configuration Protocol A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DQPSK

differential quadrature phase shift keying The modulation technique used for standard transmit rate.

DSSS

direct sequence spread spectrum A spreading technique in which various data, voice, and/or video signals are transmitted over a specific set of frequencies in a sequential manner from lowest to highest frequency, or highest to lowest frequency.

E

EAP

Extensible Authentication Protocol EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.

EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling AuthenticationA standards-based extensible framework developed by Cisco Systems that uses symmetric key algorithms to achieve a tunneled authentication process.

EIRP

effective isotropic radiated power Expresses the performance of a transmitting system in a given direction. EIRP is the sum of the power at the antenna input plus antenna gain.

F

file and printer sharing

A capability that allows a number of people to view, modify, and print the same file(s) from different computers.

fragmentation threshold

The threshold at which the USRobotics Wireless *MAX*g adapter breaks the packet into multiple frames. This determines the packet size and affects the throughput of the transmission.

G

GHz

gigahertz A unit of frequency equal to 1 000 000 000 cycles per second.

GINA

Graphical Identification and Authentication A dynamic link library (DLL) file that is part of the Windows operating system. GINA is loaded early in the boot process and handles the user identification and authorization logon process.

GTC

Generic Token Card A type of tunneled authentication protocol used in conjunction with PEAP authentication in which the user types the data displayed by a token card device when logging on to the wireless network.

H

host computer

The computer that is directly connected to the Internet via a modem or network adapter.

I

IEEE

Institute of Electrical and Electronics Engineers, Inc.

IEEE 802.1X-2001

The IEEE standard for Port Based Network Access Control. The IEEE 802.1X standard enforces authentication of a network node before it can begin to exchange data with the network.

IEEE 802.11a

The 54 Mbit/s, 5 GHz standard (1999)

IEEE 802.11b

The 11 Mbit/s, 2.4 GHz standard.

IEEE 802.11d

International (country-to-country) roaming extensions.

IEEE 802.11e

IEEE 802.11e (as of July 2005) is a draft standard that defines a set of Quality of Service enhancements for LAN applications, in particular the IEEE 802.11 Wi-Fi® standard. The standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless IP and Streaming Multimedia.

IEEE 802.11g

The 54 Mbit/s, 2.4 GHz standard (backwards compatible with IEEE 802.11b) (2003)

IEEE 802.11h

A supplementary standard to IEEE 802.11 to comply with European regulations. It adds transmission power control and dynamic frequency selection.

IEEE 802.11i

IEEE 802.11i (also known as WPA2™) is an amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks. The draft standard was ratified on 24 June 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses.

IETF

Internet Engineering Task Force A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

infrastructure network

A network in which there is at least one wireless router/AP and one wireless client. The wireless client uses the wireless router/AP to access the resources of a traditional wired network. The wired network can be an organization intranet or the Internet, depending on the placement of the wireless AP.

Initiator ID

The peer identity bound to a PAC.

intermediate certificate

A certificate issued by an intermediate certification authority (CA). See also root certificate.

Internet Protocol (IP) address

The address of a computer that is attached to a network. Part of the address designates which network the computer is on, and the other part represents the host identification.

IPv6

Internet Protocol Version 6 IPv6 is the next generation protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 (IPv4).

ISM frequency bands

Industrial, Scientific, and Medical frequency bands in the range of 902–928 MHz, 2.4–2.485 GHz, 5.15–5.35 GHz, and 5.75–5.825 GHz.

ITU-T X.509

In cryptography, ITU-T X.509 is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard for public key infrastructure (PKI). Among other things, ITU-T X.509 specifies standard formats for public key certificates and a certification path validation algorithm.

L

LAN

local area network A high-speed, low-error data network covering a relatively small geographic area.

LEAP

Light Extensible Authentication Protocol A version of Extensible Authentication Protocol (EAP). EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.

M

m

meter

MD5

Message Digest 5 An algorithm that takes an input message of arbitrary length and produces an output in the form of a 128-bit fingerprint or message digest. It is intended for digital signature applications where a large file must be compressed in a secure manner before being encrypted with a private key under a public-key algorithm such as RSA.

MHz

megahertz A unit of frequency equal to 1 000 000 cycles per second.

Mbit/s

megabits per second Transmission speed of 1 000 000 bits per second.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol MS-CHAP uses the Message Digest 4 (MD4) hashing algorithm and the Data Encryption Standard (DES) encryption algorithm to generate the challenge and response and provides mechanisms for reporting connection errors and for changing the user's password.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2 This protocol provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving. To minimize the risk of password compromise during MS-CHAP exchanges, MS-CHAPv2 supports only a newer, more secure, version of the MS-CHAP password change process.

N

network key

A string of characters that the user must type when creating a wireless network connection profile that uses WEP, TKIP, or AES encryption. Small office/home office users can obtain this string from the wireless router/AP installer. Enterprise users can obtain this string from the network administrator.

nonbroadcasting network

A network that is not broadcasting its network name. To connect to a nonbroadcasting network, you must know the network name (SSID) and search for the network name.

ns

nanosecond 1 billionth (1/1 000 000 000) of a second.

O

OFDM

orthogonal frequency division multiplexing A frequency division modulation technique for transmitting signals by splitting the radio signal into various frequencies that are then transmitted simultaneously, rather than sequentially.

P

PAC

Protected Access Credential Credentials distributed to a peer for future optimized network authentication. The PAC comprises, at most, three components: a shared secret, an opaque element, and optionally, other information. The shared secret part contains the preshared key between the peer and authentication server. The opaque part is provided to the peer and is presented to the authentication server when the peer wishes to obtain access to network resources. Finally, a PAC may optionally include other information that may be useful to the client.

PAP

Password Authentication Protocol A method for verifying the identity of a user attempting to log on to a Point-to-Point server.

PEAP

Protected Extensible Authentication Protocol A version of Extensible Authentication Protocol (EAP). EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.

PKI

public key infrastructure In cryptography, a public key infrastructure (PKI) is an arrangement that provides for third-party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates.

Power Save mode

The state in which the radio is periodically powered down to conserve power. When the radio is in Power Save mode, receive packets are stored in the AP until the radio comes on.

preferred network

A network connection profile created using Windows WZC. Such profiles are listed under **Preferred networks** on the **Wireless Networks** tab in Windows **Wireless Network Connection Properties**.

preferred network connection

A network connection profile created using the USRobotics Wireless Utility.

provisioning

Providing a peer with a trust anchor, shared secret, or other appropriate information necessary for establishing a security association.

Q

QAM

quadrature amplitude modulation A modulation technique that uses variations in signal amplitude and phase to represent data-encoded symbols as a number of states.

Quality of Service

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. See IEEE 802.11e.

R

RADIUS	Remote Access Dial-In User Service
residential gateway	A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. A residential gateway is also referred to as an access point (AP).
RF	**radio frequency**
roaming	A feature of the USRobotics Wireless *MAX*g adapter that enables wireless clients to move through a facility while maintaining an unbroken connection to the wireless network.
root certificate	Internet Explorer divides certification authorities (CAs) into two categories, root certification authorities and intermediate certification authorities. Root certificates are self-signed, meaning that the subject of the certificate is also the signer of the certificate. Root CAs have the ability to assign certificates for intermediate CAs. An intermediate CA has the ability to issue server certificates, personal certificates, publisher certificates, or certificates for other intermediate CAs.
RTS threshold	The number of frames in the data packet at or above which an RTS/CTS (request to send/clear to send) handshake is turned on before the packet is sent. The default value is 2347.

S

scanning	An active process in which the USRobotics Wireless *MAX*g adapter sends Probe-Request frames on all channels of the ISM frequency range and listens for the Probe-Response frames sent by wireless routers/APs and other wireless clients.
single sign-on	A process that allows a user with a domain account to log on to a network once, using a password or smart card, and to gain access to any computer in the domain.

smart card

Smart cards are small portable credit-card shaped devices with internal integrated circuits (ICs). The combination of the small size and IC make them valuable tools for security, data storage, and special applications. The use of smart cards can improve user security by combining something a user has (the smart card) with something only the user should know (a PIN) to provide two-factor security that is more secure than passwords alone.

SSID

service set identifier A value that controls access to a wireless network. The SSID for your USRobotics Wireless *MAX*g adapter must match the SSID for any access point that you want to connect with. If the value does not match, you are not granted access to the network. You can have up to three SSIDs. Each SSID can be up to 32 characters long and is case-sensitive. Also referred to as the network name.

STA

Station A computer that is equipped with a wireless LAN network adapter (see also wireless client). A station can be stationary or mobile.

T

TKIP

Temporal Key Integrity Protocol An enhanced wireless security protocol that is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP provides per-packet key mixing, a message integrity check (MIC), and a rekeying mechanism.

TLS

Transport Layer Security The successor to Secure Sockets Layer (SSL) protocol for ensuring privacy and data integrity between two communicating applications.

TTLS

Tunneled Transport Layer Security These settings define the protocol and the credentials used to authenticate a user. In TTLS, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol (typically password-based protocols, such as MD5 Challenge) over this encrypted channel to enable server validation. The challenge and response packets are sent over a nonexposed TLS encrypted channel.

TPM

Trusted Platform Module A security hardware device on the system board that holds computer-generated keys for encryption. It is a hardware based solution that can help avoid attacks by hackers looking to capture passwords and encryption keys to sensitive data.

The security features provided by the TPM are internally supported by the following cryptographic capabilities of each TPM: hashing, random number generation, asymmetric key generation, and asymmetric encryption/ decryption. Each individual TPM on each individual computer system has a unique signature initialized during the silicon manufacturing process that further enhances its trust/security effectiveness. Each individual TPM must have an owner before it is useful as a security device.

U

UAPSD

Unscheduled Automatic Power Save Delivery An enhanced power-save mode for IEEE 802.11e networks.

W

WEP

Wired Equivalent Privacy A form of data encryption. WEP is defined by the IEEE 802.11 standard and is intended to provide a level of data confidentiality and integrity that is equivalent to a wired network. Wireless networks that use WEP are more vulnerable to various types of attacks than those that use WPA.

wireless client

A personal computer equipped with a wireless LAN network adapter such as the USRobotics Wireless *MAX*g adapter.

wireless router/AP

A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. The wireless router/AP has at least one interface that connects it to an existing wired network. See also access point.

WLAN

wireless local area network A local area network (LAN) that sends and receives data by way of radio.

WMM™

Wi-Fi Multimedia WMM™ improves user experience for audio, video, and voice applications over a wireless network by prioritizing streams of content and optimizing the way the network allocates bandwidth among competing applications.

WPA2

Wi-Fi Protected Access Wi-Fi Protected Access™ (WPA2™) is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wirelessLAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is based on the final IEEE 802.11i amendment to the IEEE 802.11 standard. WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm. WPA2 is backward compatible with WPA.

WPA-PSK	**Wi-Fi Protected Access Preshared Key**. A network authentication mode that does not use an authentication server. It can be used with AES or TKIP data encryption types. WPA-Personal (PSK) requires configuration of a preshared key (PSK). You must type a text phrase from 8 to 63 characters long, or a hexadecimal key 64 characters long for a preshared key 256 bits in length. The data encryption key is derived from the PSK. WPA2-PSK is a more recent version of this authentication mode based on IEEE 802.11i.
WPN	The file name extension of a wireless preferred network connection profiles file.
WZC	**Wireless Zero Configuration Service** The Windows service for connecting to a wireless network.

USRobotics **Wireless MAXg USB Adapter: User Guide**

Support

1. Know your model and serial number.

Product	**Model Number**
Wireless *MAX*g USB Adapter	5425

   You can find your serial number on the side of the package and on the back of the switch.

2. Go to the Support section of the USRobotics Web site at www.usr.com/support

   Many of the most common difficulties that users experience have been addressed in the FAQ and Troubleshooting Web pages for your switch.

   The Support Web pages also contain information on the latest firmware and documentation updates.

3. Submit your technical support question using an online form, or contact the USRobotics Technical Support Department.

Country	**Webmail**	**Voice**
United States & Canada	http://www.usr.com/emailsupport	(888) 216-2850

Country	Webmail	Voice
Austria	www.usr.com/emailsupport/de	07110 900 116
Belgium (Flemish)	www.usr.com/emailsupport/nl	070 23 35 45
Belgium (French)	www.usr.com/emailsupport/be	070 23 35 46
Czech Republic	www.usr.com/emailsupport/cz	
Denmark	www.usr.com/emailsupport/ea	38323011
Finland	www.usr.com/emailsupport/ea	08 0091 3100
France	www.usr.com/emailsupport/fr	0825 070 693
Germany	www.usr.com/emailsupport/de	0180 567 1548
Greece	www.usr.com/emailsupport/gr	
Hungary	www.usr.com/emailsupport/hu	0180 567 1548
Ireland	www.usr.com/emailsupport/uk	1890 252 130
Italy	www.usr.com/emailsupport/it	39 02 69 43 03 39
Luxembourg	www.usr.com/emailsupport/be	342 080 8318
Middle East/ Africa	www.usr.com/emailsupport/me	+44 870 844 4546
Netherlands	www.usr.com/emailsupport/nl	0900 202 5857

Norway	www.usr.com/ emailsupport/ea	23 16 22 37
Poland	www.usr.com/ emailsupport/pl	
Portugal	www.usr.com/ emailsupport/pt	0 21 415 4034
Russia	www.usr.com/ emailsupport/ru	8 800 200 20 01
Spain	www.usr.com/ emailsupport/es	902 117964
Sweden	www.usr.com/ emailsupport/se	08 5016 3205
Switzerland	www.usr.com/ emailsupport/de	0848 840 200
Turkey	www.usr.com/ emailsupport/tk	0212 444 4 877
United Arab Emirates	www.usr.com/ emailsupport/me	0800 877 63
United Kingdom	www.usr.com/ emailsupport/uk	0870 844 4546

For current support contact information, go to: www.usr.com/emailsupport