USRobotics® *Wireless USB Adapter:*

User Guide

Introduction

The Wireless USB Adapter is compatible with a USB port on any standard Windows laptop or desktop computer. Integrated security, including WiFi Protected Access 2 and Wired Equivalent Privacy, assure standards-based, secure access to your wireless network. Upon successful installation, the Wireless USB Adapter can communicate with other home and office wireless networking products.

And to assure a simple, straight-forward installation, USRobotics developed the installation wizard that walks you through the installation of any 54g 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

1	USB connector	Connects to an available USB port
2	Wireless LED	Flashes when the adapter is sending or receiving data

What You Need to Begin

- PC with an available USB port
- PC with Windows Vista™, Windows® XP, or Windows® 2000
- 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

---

© 2005-2007 U.S. Robotics Corporation

R46.1900.00
rev 0 07/07

USRobotics® *Wireless USB Adapter:*

User Guide

Product Specifications

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

Security Features

- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access)
- 802.1x (RADIUS) authentication
- CCX 1.0
- 64/128-bit WEP (Wired Equivalent Privacy) data encryption

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).

Wireless 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 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.

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 5426 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 USB port. This product may be used in a typical laptop (notebook) computer with a USB port. 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

CE0560①

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 5426 Wireless 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 5426 Wireless USB Adapter measured in the conformity test is [INSERT SAR VALUE HERE].

© 2005-2007 U.S. Robotics Corporation

Wireless 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 USB Adapter:*

User Guide

Installation

> **Notice**:
> If you are installing both the Wireless USB Adapter and a Wireless Router or Wireless ADSL2+ Router, go to the *Quick Installation Guide* or *User Guide* for the router and install the router before installing the Wireless USB Adapter.

Install the Wireless 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: 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
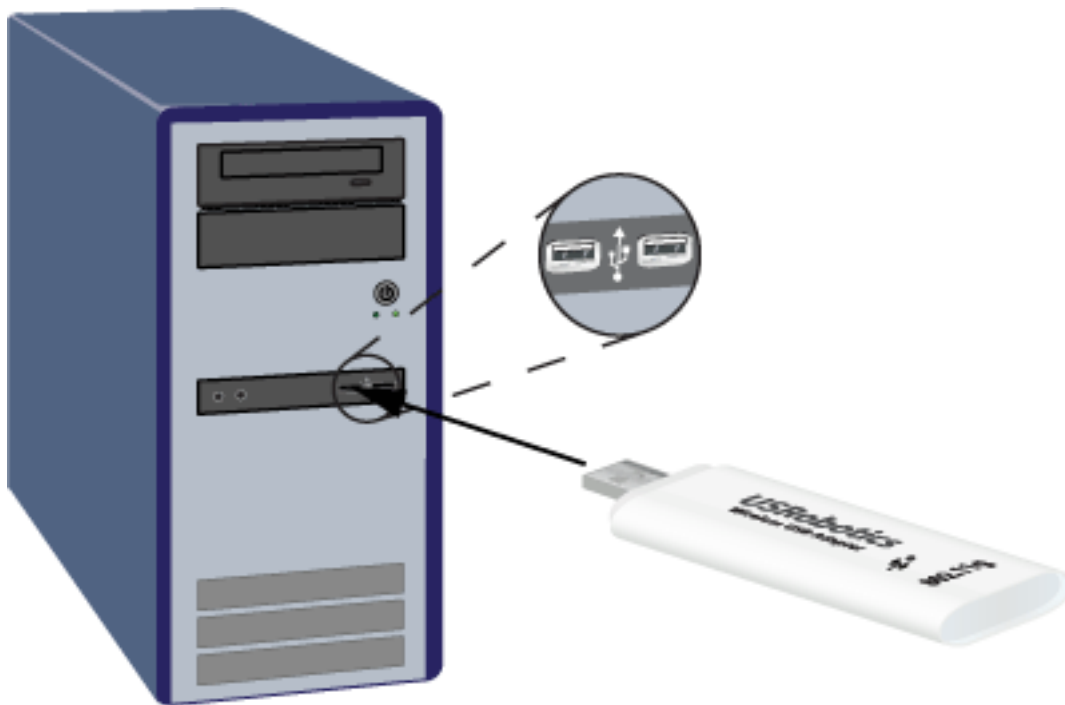
Access Control, click **Continue**.

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, and 2000 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 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

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless USB Adapter:*

User Guide

Connect to a Wireless Network after Installation

Windows Vista

If your computer uses Windows Vista, you must connect to the network manually as follows:

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, manually create a network profile as follows:

   A. Click **Set up a connection or network**.

   B. Select **Manually connect to a wireless network** and click **Next**.

   C. Configure the wireless network with network name (SSID), security type, and encryption type and click **Next**.

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

      If your network requires network authentication:

      i. Click **Change connection settings**.

    ii. Click the **Security** tab.

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

    iv. Complete the settings for the type of authentication you selected and click **OK**.

E. Click Windows **Start** > **Connect To**.

F. Select the network that you just created and click **Connect**.

Windows XP or 2000

If you use Windows XP or 2000, you can connect to the network in one of the following ways:

- 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**.

Wireless USB Adapter: User Guide

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 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**.

© 2005-2007 U.S. Robotics Corporation

USRobotics *Wireless USB Adapter:*

User Guide

Advanced Properties

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

To access the Advanced tab:

- **Windows Vista:** 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.
- **Windows XP:** Right-click the wireless network connection icon in the notification area (also called the *system tray*) and click **Open Network Connections**. Right-click the Wireless USB Adapter and click **Properties**. Click **Configure** and then click the **Advanced** tab.
- **Windows 2000:** Right-click the wireless network connection icon in the notification area (also called the *system tray*) and click **Open Network and Dial-up Connections**. Right-click the Wireless USB Adapter and click **Properties**. Click **Configure** and then click the **Advanced** tab.
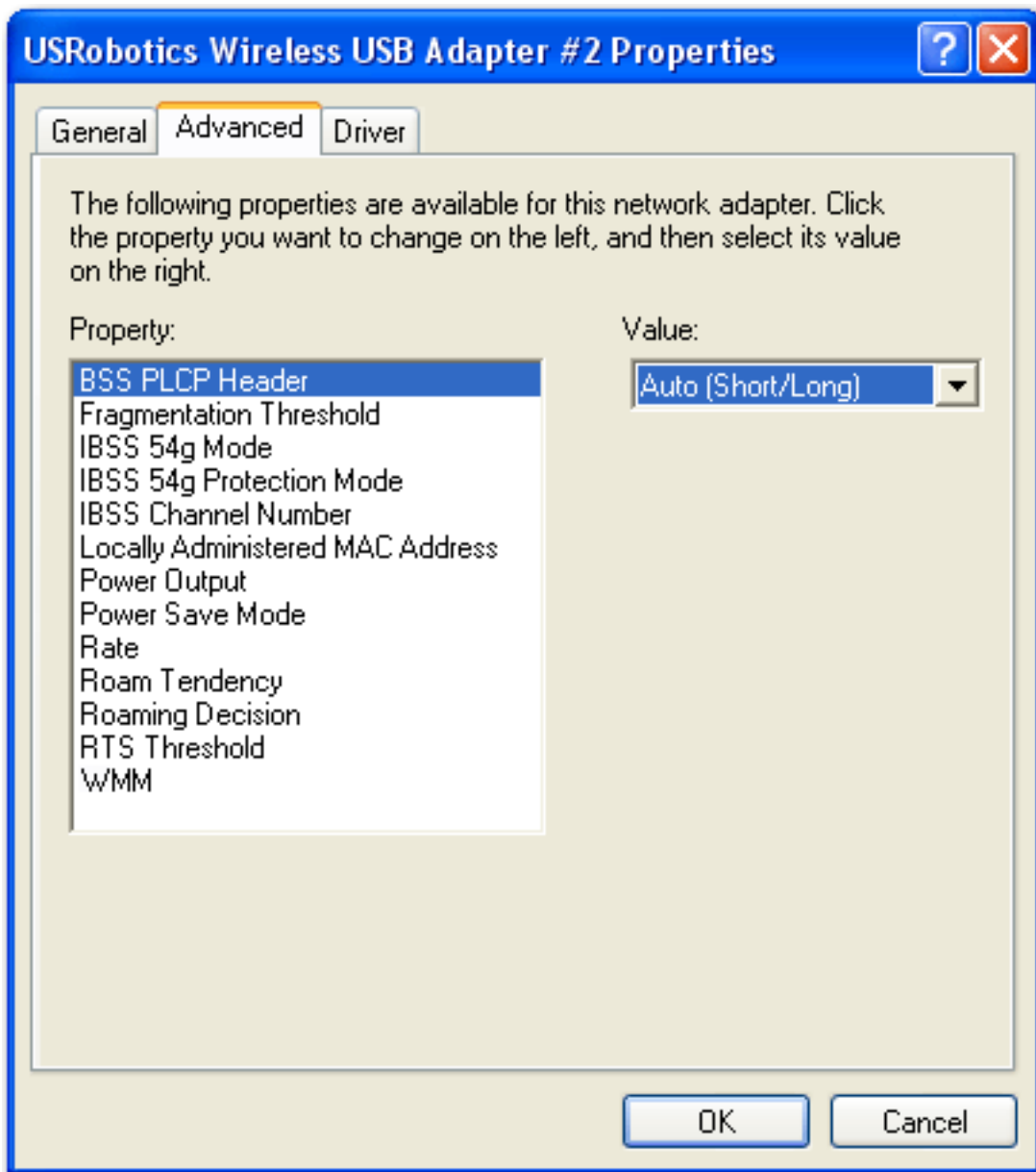
To view the available settings for a given property, click the name of the property in the **Property** list. Then click the down arrow in the **Value** list.

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).

- BSS PLCP Header
- Fragmentation Threshold
- IBSS 54g Mode
- IBSS 54g Protection Mode
- IBSS Channel Number
- Locally Administered MAC Address
- Power Output

- Power Save Mode
- Rate
- Roam Tendency
- Roaming Decision
- RTS Threshold
- WMM

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 (default)

54g - Performance

802.11b Only

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

IBSS Channel Number

The 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.

Locally Administered MAC Address

Locally Administered MAC Address is used to override the MAC address of the Wireless 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.

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%

Power Save Mode

Power Save Mode is used to put the Wireless USB Adapter enabled computer into the IEEE 802.11 Power Save mode. In Power Save mode, the radio is periodically powered down to conserve power. When the radio is in Power Save mode, packets are stored in the access point until the radio comes on. Power Save Fast allows full throughput with power savings.

Disabled

Enabled

Fast (default)

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 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 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 <u>quality of service</u> 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 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 (default) 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.

© 2005-2007 U.S. Robotics Corporation

Wireless USB Adapter:

User Guide

The USRobotics Wireless Utility

Users of Windows XP or 2000 have access to the USRobotics Wireless Utility once the Wireless USB Adapter is installed. With this utility, you can create and edit the settings for wireless connections, view the information regarding your Wireless 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 coloured 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.
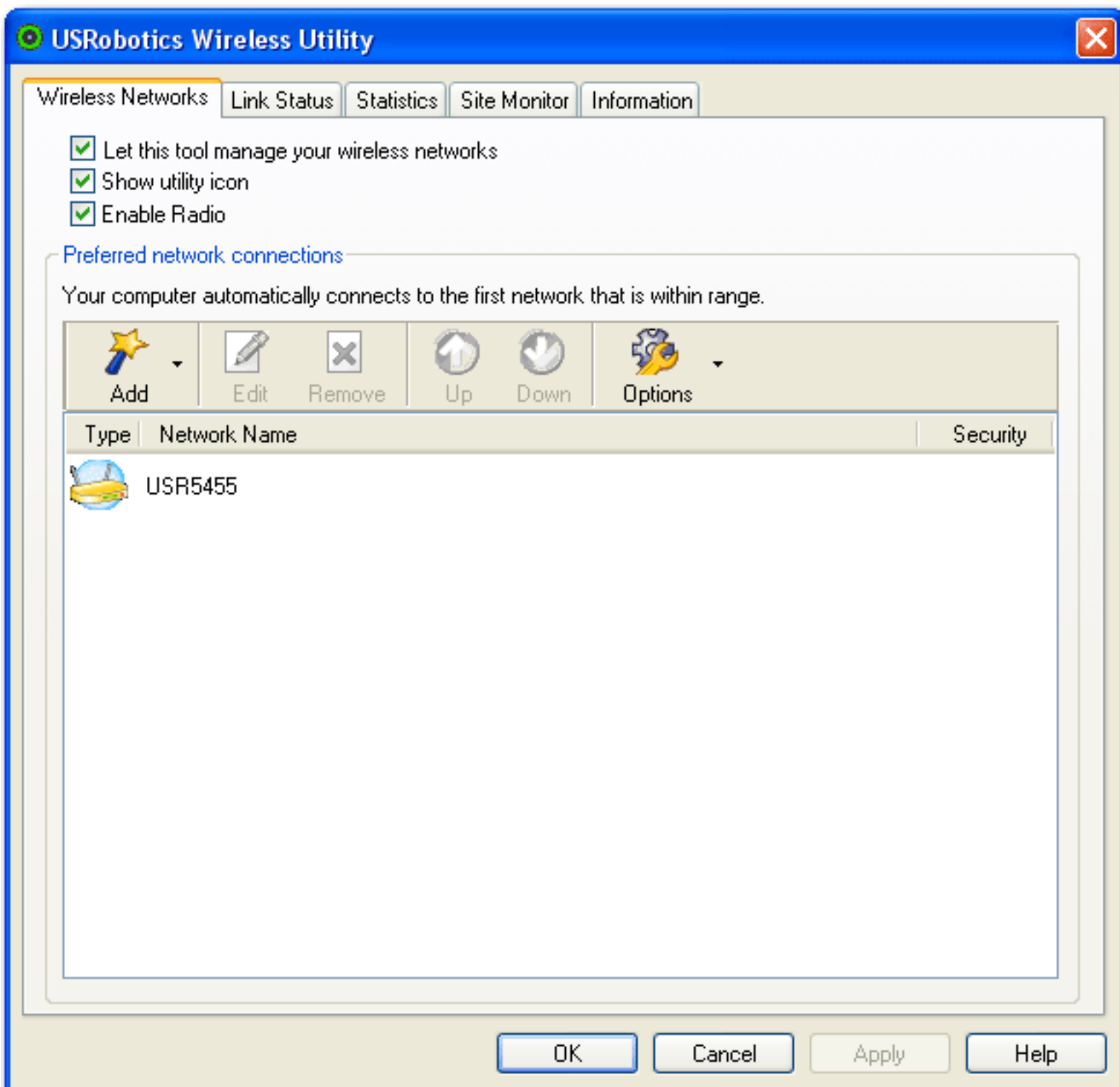
In the **Link Status** area, information regarding your current wireless connection is displayed.
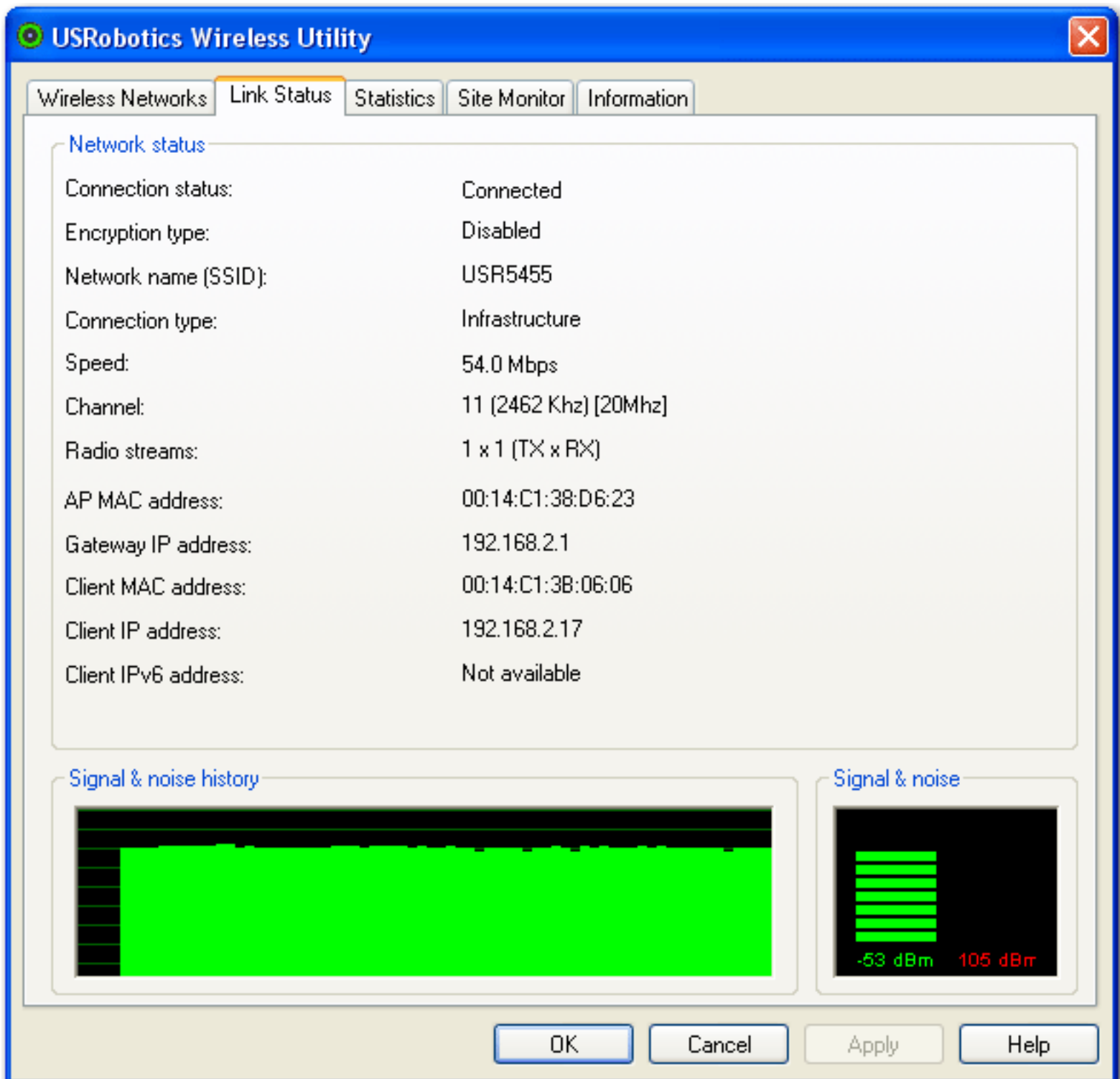
In **Statistics**, you can view the results regarding network traffic over your wireless

connection.
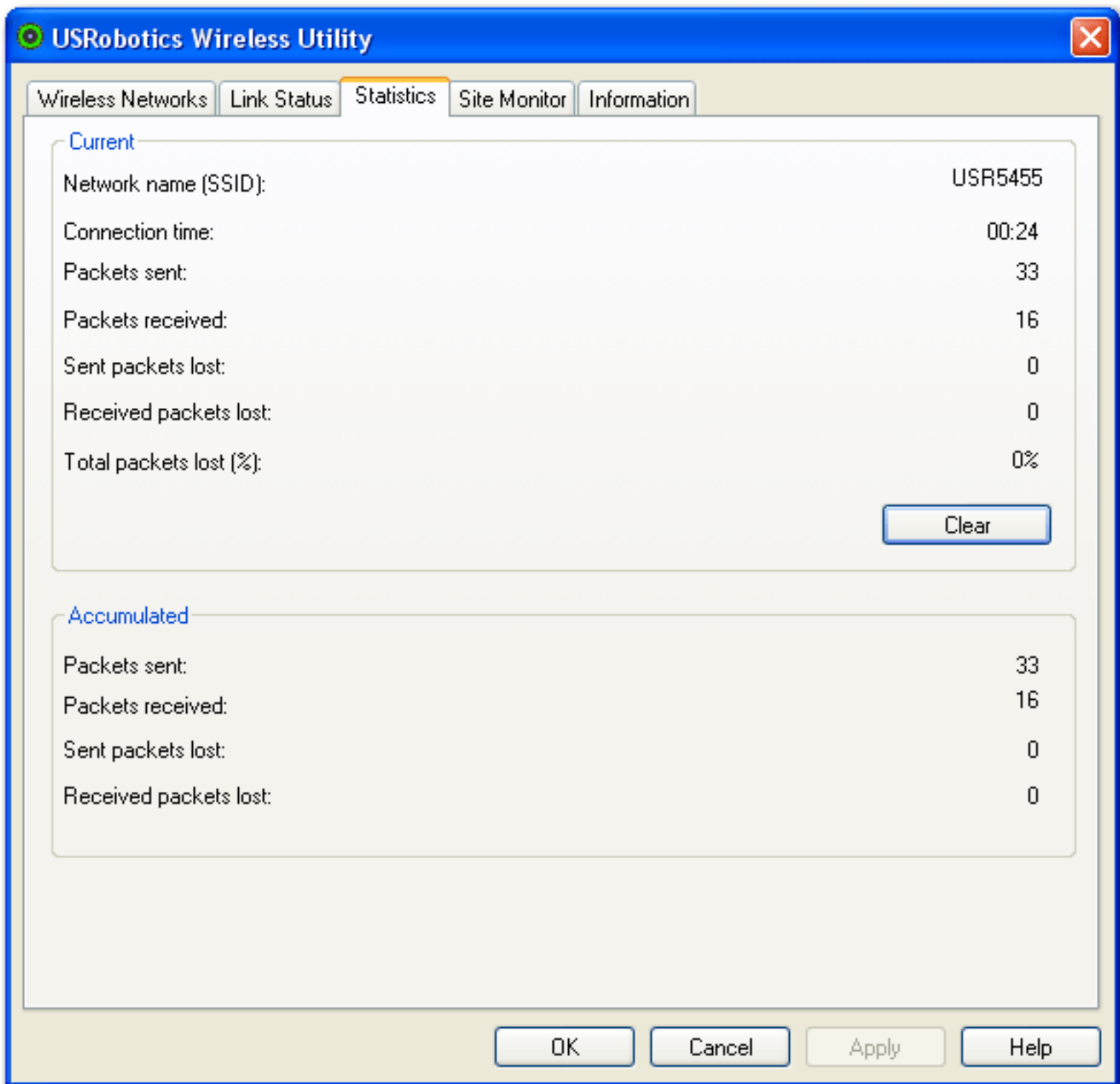
In **Site Monitor**, you can see the wireless network devices that your Wireless USB Adapter could connect to. If you want to connect to a device that you see in this list, go to the Wireless Networks area.
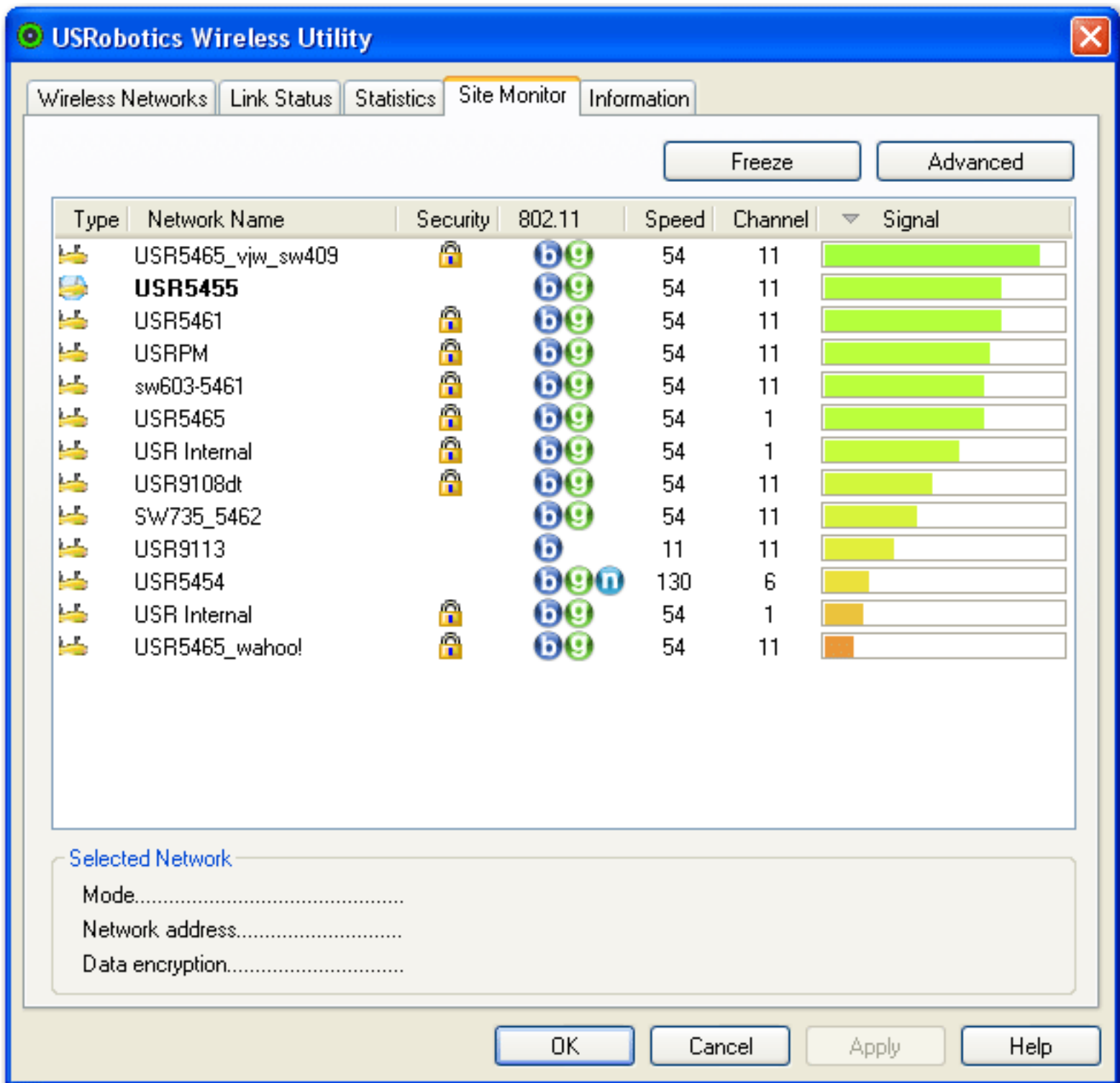
In the **Information** area, you can view the version information for your Wireless USB Adapter.

USRobotics Wireless Utility

| Wireless Networks | Link Status | Statistics | Site Monitor | Information |

Wireless Configuration Utility
Copyright (C) 2004 - 2007, U.S. Robotics Corporation

USRobotics

Software details

Software version:	4.118.1.0	Jun 14, 2007
Driver version:	4.118.1.0	Jun 11, 2007
Supplicant version:	4.118.1.0	Jun 14, 2007

Hardware details

Board:	BCM 0700 Rev 4.2
Chipset:	BCM4318
MAC address:	00:14:C1:3B:06:06

Location details

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

[OK] [Cancel] [Apply] [Help]

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless USB Adapter:*

User Guide

Basic Troubleshooting Procedure

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

1. Verify the physical cable connections between all of your networking devices: access point (if present), router, and modem.

2. Ensure that the power outlets to which these networking devices are connected are live outlets.

3. Check the LEDs on the networking devices 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 stabilise, then reboot your router and wait for the LEDs to stabilise, then reboot your access point (if present) and wait for the LEDs to stabilise. Finally, 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 access point, or reposition the computer or wireless adapter. If possible, ensure that there are no obstructions between the wireless adapter and the router, or if you are using an access point, between the wireless adapter and the access point.

If you still have trouble using the wireless adapter, 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 USB Adapter.

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

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

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 in the Available Networks list in the USRobotics Wireless Utility.

My computer does not create a wireless connection to the wireless router or access point after I changed the settings.

I am experiencing poor link quality.

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless USB Adapter:*

User Guide

My computer does not recognise the Wireless USB Adapter.

Possible Solution:

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

Return to Troubleshooting page

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless USB Adapter:*

User Guide

I am no longer able to access the Internet.

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. Troubleshooting entails checking all of your devices and the connections between them, one at a time. The troubleshooting procedure varies depending the kind of networking device to which you connect your Wireless USB Adapter. Choose the procedure that best fits your network configuration:

- My wireless adapter connects to an access point.
- My wireless adapter connects to a wireless router.
- My wireless adapter connects to a wireless DSL gateway (a device that combines the functions of a wireless router with the functions of a DSL modem).

Return to Troubleshooting page

© 2005-2007 U.S. Robotics Corporation

Wireless USB Adapter:

User Guide

Troubleshooting an Internet Connection through an Access Point

1. Complete the "Basic Troubleshooting Procedure" section on the main Troubleshooting page.

2. 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. The following procedures cover troubleshooting for each of the connections between your computer and the Internet:

    A. Verify wireless adapter's connection to the access point. If your adapter cannot communicate with the access point, 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 the Wireless Adapter's Connection to the Access Point

1. Try to access the access point's configuration interface. If you can access the configuration pages, try again to access the Internet.

   ○ **If you can connect to the access point's configuration pages**: The problem is not in the connection between the wireless adapter and the access point. Go to "Verify the Access Point's Connection to the Router".

   ○ **If you cannot connect to the access point's configuration pages**:

     A. Try a wired connection between the computer and the 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 access point is lit.

        ii. Release and renew your wired adapter's network connection.

        iii. Try to access the access point's configuration pages with the wired connection.
           ■ **If you can connect to the access point's configuration pages**: The problem is in the wireless adapter or its connection to the access point. Go to Step B.
           ■ **If you cannot connect to the access point's configuration pages**: The problem is in the access point. Go to Step E.

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

     C. Make sure that the access point is set to broadcast its Network Name.

     D. Determine whether the access point 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 access point's MAC filtering list.

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

2. Reset the access point. If the access point has a Reset button, follow the

instructions of the access point manufacturer for using the button to reset the access point; otherwise, reboot the access point by disconnecting and then reconnecting its power supply.

A. Wait for the LEDs on the access point to stabilise.

B. [Release and renew the adapter's network connection](#).

3. Try again to access the access point's configuration pages. If you can access the access point's configuration pages, try again to access the Internet.
   - **If you can connect to the configuration pages but not the Internet**: The problem is not in the connection to the access point. Go to ["Verify the Router's Connection to the Cable or DSL Modem"](#).
   - **If you cannot connect to the configuration pages**: Restore the access point to the factory default settings.

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

4. Set the Network Name (SSID) and security settings of the wireless adapter to match the factory default settings of the access point.

5. Try again to access the access point's configuration pages. If you can access the access point's configuration pages, try again to access the Internet.
   - **If you can connect to the configuration pages but not the Internet**: The problem is not in the connection to the access point. Go to ["Verify the Router's Connection to the Cable or DSL Modem"](#).
   - **If you cannot connect to the configuration pages**: Contact the customer support department of the access point'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. Reset the router. If the 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.

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

        ii. Release and renew the adapter's network connection.

    F. If the router cannot obtain a WAN IP address, the problem is most likely in 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 stabilised, 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 stabilised, try to access the Internet again.

   If you still cannot access the Internet: The problem is in the cable or DSL modem or your ISP. Contact the customer support department of your ISP to determine whether there is a problem with your modem or Internet connection.

[Return to Troubleshooting page](#)

USRobotics® *Wireless USB Adapter:*

User Guide

Troubleshooting an Internet Connection through a Wireless DSL Gateway

For the purpose of this troubleshooting procedure, a *wireless DSL gateway* is a device that combines the functions of a wireless router with those of a DSL modem.

1. Complete the "Basic Troubleshooting Procedure" section on the main Troubleshooting page.

2. 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. The following procedures cover troubleshooting for each of the connections between your computer and the Internet:

    A. Verify the wireless adapter's connection to the gateway. If your wireless adapter cannot communicate with the gateway, your computer cannot access the Internet.

    B. Verify the gateway's connection to the Internet. Your Internet connection must be up and functioning.

Verify the Wireless Adapter's Connection to the Gateway

1. Try to access the gateway's configuration interface. If you can access the gateway's configuration pages, try again to access the Internet.

    ❍ **If you can connect to the gateway's configuration pages**: The problem is not in the connection between the wireless adapter and the gateway. Go to "Verify the Gateway's Connection to the Internet".

    ❍ **If you cannot connect to the gateway's configuration pages**:

        A. Try a wired connection between the computer and the gateway:

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

            ii. Release and renew the wired adapter's network connection.

            iii. Try to access the Internet with the wired connection.
                - **If you can connect to the gateway's configuration pages**: The problem is in the wireless adapter or its connection to the gateway. Go to Step B.
                - **If you cannot connect to the gateway's configuration pages**: The problem is in the gateway. You can continue troubleshooting with the wired connection. Go to Step 2.

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

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

        D. Determine whether the gateway 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 gateway's MAC filtering list.

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

        F. Try again to access the gateway's configuration pages.

- **If you can connect to the gateway's configuration pages and still cannot access the internet**: Go to "Verify the Gateway's Connection to the Internet".
- **If you cannot connect to the gateway's configuration pages**: continue with Step 2 of this procedure.

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

   A. Wait for the LEDs on the gateway to stabilise.

   B. Release and renew the adapter's network connection.

3. Try again to access the gateway's configuration pages. If you can access the gateway's configuration pages, try again to access the Internet.
   - **If you can connect to the gateway's configuration pages but not the Internet**: The problem is most likely in the connection to the gateway. Go to "Verify the Gateway's Connection to the Internet".
   - **If you cannot connect to the gateway's configuration pages**: Restore the gateway to the factory default settings.

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

4. Unless you are troubleshooting with a wired connection, set the Network Name (SSID) and security settings of the wireless adapter to match the factory default settings of the gateway.

5. Try again to access the gateway's configuration pages.
   - **If you can connect to the gateway's configuration pages**: Repeat the installation procedure for the gateway.
   - **If you cannot connect to the gateway's configuration pages**: The problem is in the gateway. See the gateway's documentation to correct the problem.

Verify the Gateway's Connection to the Internet

In the gateway's configuration pages, find the WAN status information and verify that the gateway has a WAN IP address. This IP address indicates whether the gateway is communicating with the Internet Service Provider (ISP).

Note: If your ISP uses a static WAN protocol, make sure that the WAN IP address of the gateway 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 gateway.

- **If the gateway has a WAN IP address**: The problem is at the ISP. Contact the customer support department of your ISP to correct the problem.

- **If the gateway does not have a WAN IP address**: Try to acquire a WAN IP address as follows:

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

  2. In the gateway's configuration pages, verify that the gateway has a WAN IP address.

  3. If the gateway still does not have a WAN IP address, verify the gateway's Internet connection information. You may be required to enter the login information your ISP provided.

  4. Refresh the status information and verify that the gateway has a WAN IP address.

     - **If the gateway has a WAN IP address**: If you still cannot access the Internet, the problem is most likely at the ISP. Contact the customer support department of your ISP to correct the problem.

     - **If the gateway's does not have a WAN IP address**: Restore the gateway to the factory default settings.

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

5. If the gateway still cannot obtain a WAN IP address, the problem is most likely at the ISP. Contact the customer support department of your ISP to correct the problem.

[Return to Troubleshooting page](#)

USRobotics® *Wireless USB Adapter:*

User Guide

Troubleshooting an Internet Connection through a Wireless Router

1. Complete the "Basic Troubleshooting Procedure" section on the main Troubleshooting page.

2. 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. The following procedures cover troubleshooting for each of the connections between your computer and the Internet:

   A. Verify the wireless adapter's connection to the router. If your wireless 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 the Wireless Adapter's Connection to the Router

1. Try to 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 the router:

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

         ii. Release and renew the wired adapter's network connection.

         iii. Try to access the Internet with the wired connection.
            - **If you can connect to the router's configuration pages**: The problem is in the wireless adapter or its connection to the router. Go to Step B.
            - **If you cannot connect to the router's configuration pages**: The problem is in the router. You can continue troubleshooting with the wired connection. Go to Step 2.

      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 of the wireless adapter match those 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 the 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 Step 2 of this procedure.

2. Reset the router. If the 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.

   A. Wait for the LEDs on the router to stabilise.

   B. Release and renew the adapter's network connection.

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 you can connect to the router's configuration pages but not the Internet**: The problem is most likely in the connection to the cable or DSL modem. Go to "Verify the Router's Connection to the Cable or DSL Modem".
   - **If you cannot connect to the router's configuration pages**: Restore the 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 the router.

4. Unless you are troubleshooting with a wired connection, set the Network Name (SSID) and security settings of the wireless adapter to match the factory default settings of the 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 pages**: The problem is in the router. See the router's documentation to correct the problem.

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

1. Check the 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 the 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 in the cable or DSL modem or your ISP. Go to "Verify the modem's connection to the Internet".

Verify the Modem's Connection to the Internet

1. Check the LEDs on the 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 the cable or DSL modem is connected to the wall jack.

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

4. After the LEDs on the modem have stabilised, reset the router. If the 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 stabilised, try to access the Internet again.

    If you still cannot access the Internet: The problem is in the cable or DSL modem or your ISP. Contact the customer support department of your ISP to determine whether there is a problem with the modem or Internet connection.

[Return to Troubleshooting page](#)

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless USB Adapter:*

User Guide

I accidentally clicked Cancel during the software installation procedure for the Wireless 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

© 2005-2007 U.S. Robotics Corporation

USRobotics®

Wireless USB Adapter:

User Guide

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

Possible Solution:

If you inserted the Wireless 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

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless USB Adapter:*

User Guide

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

Possible Solution:

For Windows XP and 2000 only: ensure that the USRobotics Wireless Utility is installed for your Wireless USB Adapter and that the USRobotics Wireless Utility detects your Wireless USB Adapter.

Possible Solution:

For Windows XP and 2000 only: 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:

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:

Windows Vista

1. Right-click the USRobotics Wireless Utility in the system tray and select **Connect Using Wizard.**

2. Click **Set up a connection or network**.

3. Select **Manually connect to a wireless network.**

4. Click **Next** and follow the on-screen instructions to connect. You may need the Network name, Security type, Encryption type and Security Key/Passphrase for the router or access point.

Windows XP and 2000

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.

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 USB Adapter must be included in the filtering table of the wireless router or access point.

Possible Solution:

Be sure that each Wireless USB Adapter that you want to connect to the wireless network is set to Infrastructure mode within the USRobotics Wireless Utility. If a Wireless 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](#)

Wireless USB Adapter:

User Guide

My computer does not create a wireless connection to the wireless router or access point after I changed the settings.

Possible Solution:

In the USRobotics Wireless Utility for your Wireless USB Adapter , ensure that you are connecting to the correct wireless router or access point by verifying the WLAN MAC address, Network name (SSID), and security settings. The WLAN MAC address is usually located on the label on the bottom of the wireless router or access point. Ensure that the correct pass phrase and encryption options are being used. If you changed the settings in the configuration of the wireless router or access point, you must also change the settings of every Wireless USB Adapter connecting to this network. The settings of the Wireless USB Adapter must match the new settings of the wireless router or access point.

Return to Troubleshooting page

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless 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 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 router or access point, or 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](#)

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless USB Adapter:*

User Guide

Release and Renew a Network Connection

Windows Vista

1. Click Windows **Start**.

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

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

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

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

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

6. Type **exit** and press ENTER.

Windows XP and 2000

1. Click Windows **Start > Run**.

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

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

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

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

5. Type **exit** and press ENTER.

[Return to Troubleshooting page](#)

© 2005-2007 U.S. Robotics Corporation

USRobotics® *Wireless 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, type **cmd** 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.

© 2005-2007 U.S. Robotics Corporation

Wireless 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 recognise 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 Authentication**A 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 Wireless USB 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 minimise 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 <u>wireless router/AP</u> 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 optimised 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 <u>certificates</u>.
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 <u>IEEE 802.11e</u>.

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 Wireless USB 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 Wireless USB 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 Wireless USB 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 Wireless USB 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.

© 2005-2007 U.S. Robotics Corporation

Wireless USB Adapter:

User Guide

Support

1. Know your model and serial number.

Product	Model Number
Wireless USB Adapter	5426

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

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