Wireless-N USB Adapter

USER GUIDE

Contents

Overview

What's in the Package

The adapter package includes the following:

- Wireless-N USB adapter
- CD containing the Installation Wizard and documentation
- USB extension cable
- Quick Start manual

What's in this User Guide

The chapters in this **User Guide** describe how to:

- Install the Zoom Wireless-N USB adapter on a Windows® PC and Mac
- Connect your computer to a wireless network
- Enable security on the Wireless-N USB adapter
- Use the advanced features of the Wireless-N USB configuration software

Chapters 1 and 2 cover the basics – what you need to get connected and to enable security.

If you are interested in the more advanced features of the Wireless-N USB adapter, please see Chapter 3. This chapter explains how to create profiles so you can switch your connection from one network to another, monitor the strength of your network connection, scan a list of available networks, and switch to Soft AP mode.

1

Installation Instructions

This chapter provides simple instructions for installing the Wireless-N USB adapter on a Windows PC (for Windows 7, Vista, XP, and 2000). If you have already installed the adapter on a computer (by using the separate Quick Start guide, for instance), you can skip this chapter. If you have a Mac, please go to Chapter 4 on page 35.

Before You Begin

If you want to install the Wireless-N USB adapter on a Windows PC, your PC needs the following:

- Available USB port
- Windows 7, Vista, XP, or 2000
- CD or DVD drive
- 6 MB of free hard drive space

Installing and Connecting the Adapter on a Windows PC

Important: Do not plug the Adapter into your computer yet. We will tell you when to plug it in.

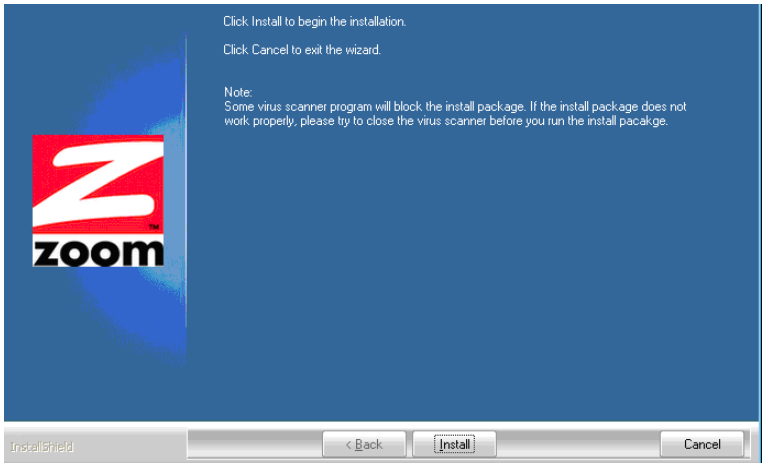
1 Insert the Wireless-N USB CD into the CD or DVD drive. The CD should start automatically.

For Windows Vista and Windows 7 only:

If the **AutoPlay** dialog box appears, click **Run Setup.exe**.

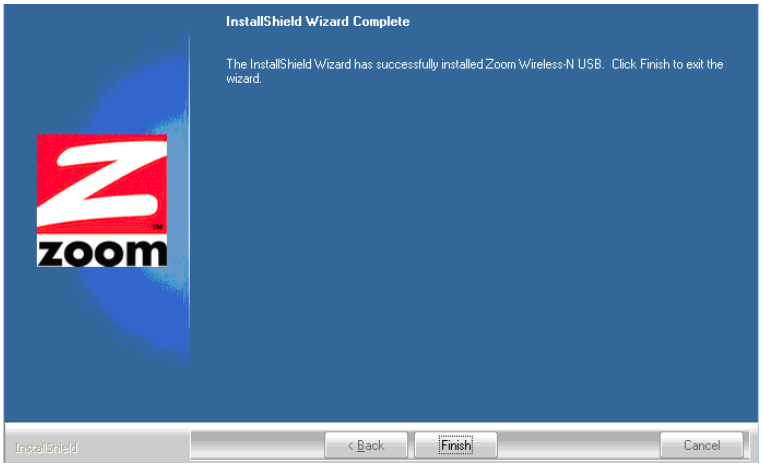
If a message appears saying *An unidentified program wants access to your computer or Do you want to allow the following program from an unknown publisher to make changes to this computer?*, click **Allow or Yes**.

2 On the next screen, select **Install**.



3 A Zoom Wireless-N USB Setup screen is displayed for a few seconds while the installation proceeds.

4 On the **InstallShield Wizard Complete** screen, click **Finish** and remove the CD.



5 Plug the USB Adapter into one of the available USB slots on your computer. (If it is difficult to insert the USB Adapter directly into the USB slot because there isn't enough space near the slot, first plug the USB Adapter into the **extension cable** included in the package and then plug the other end of the extension cable into the USB slot in your computer. Since the extension cable is semi-rigid, you can twist the extension cable to orient the USB Adapter for best reception. Usually a vertical orientation is best.)

To connect to a network

Now you are ready to connect to a network. Wireless networks typically have a wireless access point, router, or gateway at the heart of the wireless network. Wireless networks sometimes use wireless security and sometimes do not. What you do next depends on your network's wireless security. You have several options:

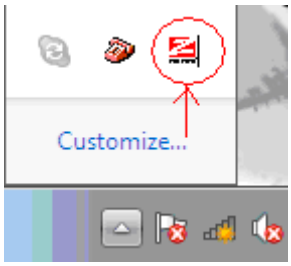
1 If your access point or router supports **WPS**, we highly recommend that you **connect to a network using WPS**. See WiFi™ Protected Setup (WPS) on page 12.

2 If your access point or router does not support WPS or you prefer not to connect this way, you can **connect to a network without security** as described below.

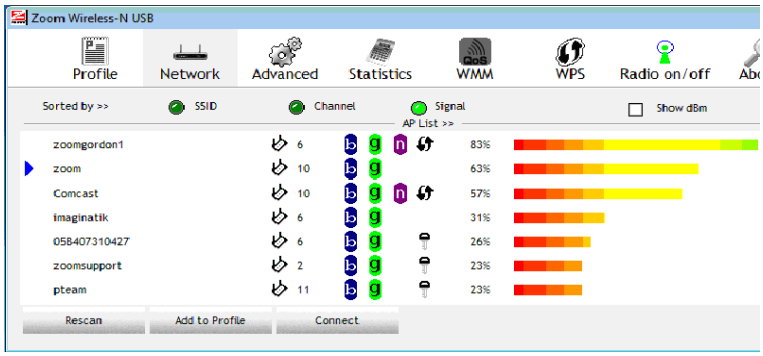
3 If you decide that you want to **join a wireless network that has security**, scroll down to **Section 2: Setting Security** and follow the instructions.

To connect to a network without security

1 Double-click the **Zoom** icon on your taskbar to open the configuration software.



2 In the **Zoom** Wireless-N USB **Network** window, look through the list of available wireless networks and highlight the network you want, and then click **Connect**.



3 If you join a wireless network that **does not have security**, you should now be connected. To check your connection, open your Web browser and go to your favorite site.

> ⓘ If the network you select has security configured, you must enable and configure security on your Zoom Wireless-N USB Adapter before you can connect. See Chapter 2, **Setting Security**.

We highly recommend security. Chapter 2, Setting Security on page 10 has descriptions of the available security options and setup instructions.

If you have difficulty accessing the Internet, follow the suggestions in the Troubleshooting section in Appendix B at the end of this User Manual.

The Adapter LED

The state of the LED on the Wireless-N USB adapter is explained below.

LED Status	Meaning
Flashing	The Wireless-N USB adapter is attempting to or has connected to a wireless network and is transmitting or receiving data.

2

Setting Security

We strongly recommend security, although you do not need to use it to get your wireless connection working.

Important! You must first enable security on the wireless access point or router. You then enable security on the adapter using the same configuration that you used for the access point or router. For example, if the wireless access point or router is configured for WEP, you must select WEP security in the Wireless-N USB configuration software and enter the same encryption key.

Accessing security options

1. On your taskbar, double-click the **Zoom Wireless-N USB** icon to open the **Zoom Wireless-N USB** configuration software.
2. Make sure that the desired wireless network is displayed in the **Profile** and **SSID** text boxes (the term **<Infra>** designates an Infrastructure network) and that the **Network Type** is correct.

   There are two types of wireless networks: *Infrastructure* and *Ad Hoc*.

   - In an **Infrastructure** network, wireless devices communicate with each other via a wireless access point, router, or ADSL modem with built-in wireless technology.
   - In an **Ad Hoc** network, a group of wireless devices communicate directly with other “client” devices that are using wireless adapters. The network does not include a wireless access point or wireless router.

- In the unlikely event that you use an **Ad Hoc network**, you must set up **Static IP addressing**.
  See **Appendix A: TCP/IP Settings**.

3 For configuration instructions for the different types of available security options, consult this table:

To configure	Go to page
WPS	12
WEP / WEP-Shared	14
WPA2	15
WPA	16
802.1x	16

- **WiFi™ Protected Setup (WPS)**: This is the option we recommend, if it is supported by the wireless access point or router and the other devices in your network. This protocol can greatly simplify the process of configuring WPA2 or WPA security.
- **WEP** (**W**ired **E**quivalent **P**rivacy): Both the **WEP** and WEP-**Shared** Authentication modes set WEP security. WEP is the preferred setting, WEP–Shared should only be used when connecting with certain Mac products that do not support standard WEP. If the devices in your network do not support WPA2 or WPA, select **WEP** data encryption.

  This method requires you to enter an encryption key. The keys can be 64 or 128 bits in length.
- **WPA2:** Select WPA2 if all of the devices in the network support WPA2, or if your access point or router offers both WPA2 and WPA. To use this option, you will need to enter the WPA Preshared Key in the text box.
- **WPA:** To use this option, you will need to enter the WPA Preshared Key in the text box.
- **802.1x:** With 802.1X authentication, each wireless device (client) sends a signal to the wireless access point or router, which in turn sends the signal to the RADIUS server. The server determines whether or not the client is allowed to join

the network. You can access 802.1x option from WEP, WPA2, or WPA.

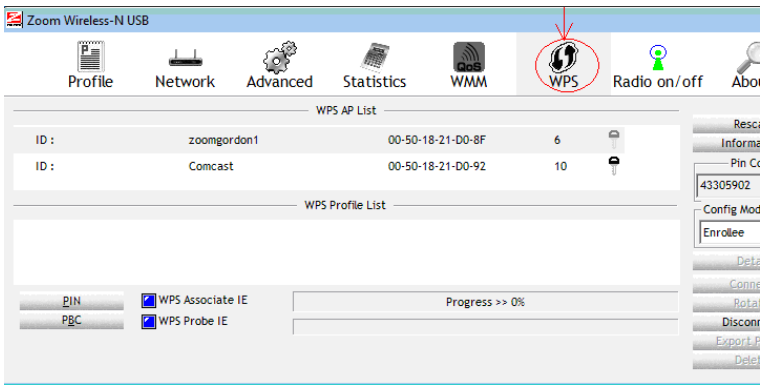
WiFi™ Protected Setup (WPS)

To connect to a network using WPS

If your wireless access point or router supports **W**iFi™ **P**rotected **S**etup (WPS), this protocol can greatly simplify the process of configuring WPA2 or WPA security. If your wireless access point or router supports WPS it typically has a WPS button built into its case.

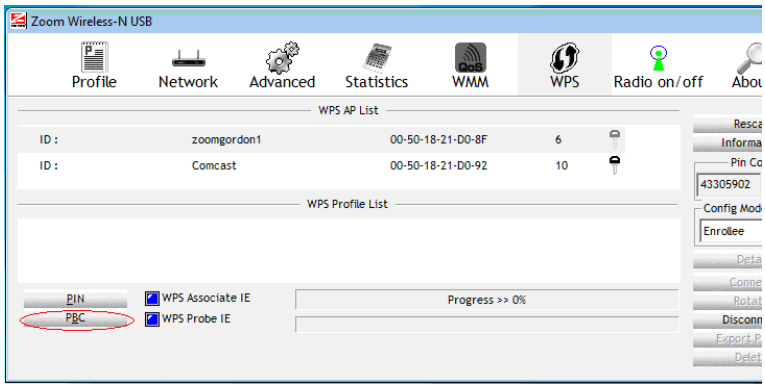
1 Start by double-clicking the **Zoom** icon on your taskbar to launch the **Config Utility**.

2 On the **Configuration** tab, click the **WPS** button to open the **WPS Config** screen.



3 Go to the wireless access point or router and activate the **WPS** pushbutton (or *Secure Setup* or similarly named button, or a virtual pushbutton on the software display of the access point). You may have to hold down the **WPS** button for several seconds or until the WiFi™ indicator light on the access point starts flashing. The access point will now begin accepting **WPS** connections. (If security has not been set on the access point, a random SSID and WPA key will be used.)

4 Now, click on **PBC** (Push Button configuration) on Zoom's **WPS Config** screen.

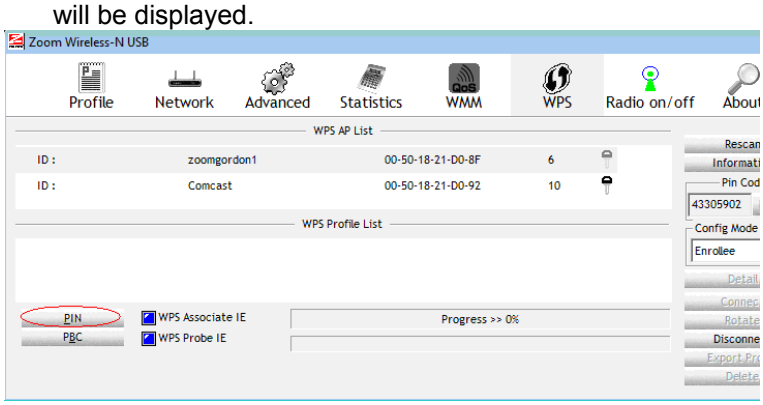


You should now have a secure connection. Open your Web browser and go to your favorite site.

PIN option:

1 If the access point does not have a hard or soft security pushbutton, you can use the **PIN** option.

2 In the text box, the Adapter's randomly generated **PIN** number will be displayed.



3 Go to the access point or router, enter the Adapter's **PIN** number in the appropriate place on the access point's configuration interface, and click a button -- called **Start PIN**

or something similar -- to activate a search for the Adapter. When the access point or router identifies the Adapter, it will automatically configure security.

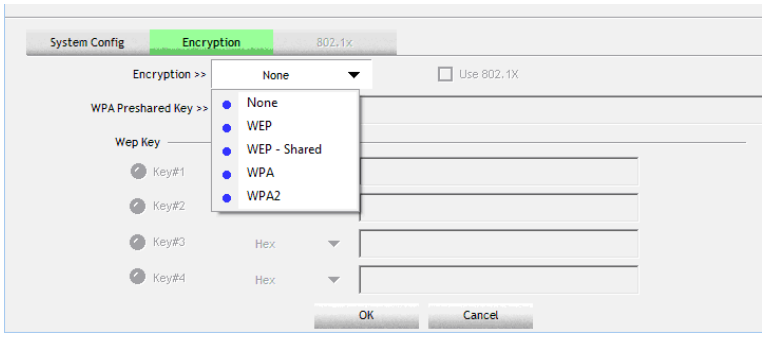
You should now have a secure connection. Open your Web browser and go to your favorite site.

That's it! You have configured WPS security for your wireless connection, and you're ready to use the Internet.

WEP (Wired Equivalent Privacy) / WEP-Shared

1 In the **Network** window select the wireless network you want to join and click Connect.

2 In the **Encryption** tab, click the Encryption drop-down arrow and select **WEP** (recommended) or **WEP-Shared**.



3 In the **WEP Key** area**,** do the following:

a In the first drop-down list select:

- **Hexadecimal digits**

or

- **ASCII characters**

b In the (Network) **Key** text box, enter a key using the table below as a guide.

The key must be the same for all the devices on your network.

If you selected key type…	Enter exactly…
Hexadecimal digits – 128 bits	26 characters A–F, a–f and 0–9. For example, 00112233445566778899AABBCC.
Hexadecimal digits – 64 bits	10 characters. The characters can be A-F, a-f, and 0-9. For example, 11AA22BB33.
ASCII – 128-bits	13 characters. The characters can be any upper- or lower-case letters and numbers. For example: MyKey12345678.
ASCII – 64 bits	5 characters. The characters can be any upper- or lower-case letters and numbers. For example, MyKey.

4 Click **OK** to save your settings and return to the **Configuration** tab.

5 Click the **Close** box to exit the configuration software.

That's it! You have configured WEP security for your wireless connection, and you're ready to use the Internet.

WPA2

Select **WPA2** if all of the devices in the network support WPA2.

1 In the **Network** window select the wireless network you want to join and click Connect. In the **Encryption** tab, click the Encryption drop-down arrow and select **WPA2**.

2 Enter the WPA Preshared Key in the text box.

3 Click **OK** to save your settings and return to the **Configuration** tab.

4 Click the **Close** box to exit the configuration software.

That's it! You have configured WPA2 security for your wireless connection, and you're ready to use the Internet.

WPA

1 In the **Network** window select the wireless network you want to join and click Connect. In the **Encryption** tab, click the Encryption drop-down arrow and select **WPA**.

2 Enter the WPA Preshared Key in the text box.

3 Click **OK** to save your settings and return to the **Configuration** tab.

4 Click the **Close** box to exit the configuration software.

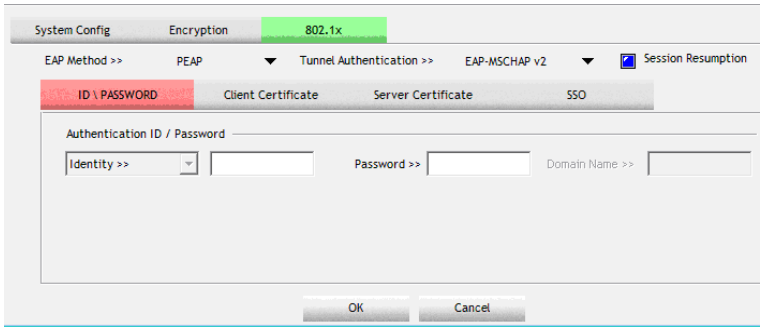
That's it! You have configured WPA security for your wireless connection, and you're ready to use the Internet.

802.1x

With 802.1X authentication, each wireless device (client) sends a signal to the wireless access point or router, which in turn sends the signal to the RADIUS server. The server determines whether or not the client is allowed to join the network. You can access 802.1x option from WEP, WPA2, or WPA.

1 At the **Encryption tab**, click the **Use 802.1x** box to enable it.

2 Click on **802.1x** tab.



3 Click the **EAP** (**E**xtensible **A**uthentication **P**rotocol) **Method Type** drop-down list and select an authentication protocol:

- **PEAP** (**P**rotected **E**xtensible **A**uthentication **P**rotocol). This is the default. With PEAP, you can select from four authentication extensions:
  - **Tunnel Authentication>>** (**TTLS**: **T**unneled **T**ransport **L**ayer **S**ecurity). With TTLS, you can select from three authentication extensions:
    - **EAP-MS-CHAPv2** Microsoft's version of CHAP (Challenge-Handshake Authentication Protocol (default)
    - **EAP-TLS** (**T**ransport **L**ayer **S**ecurity) / **Smart Card**. There are no authentication extension options with TLS.
    - **Generic Token Card**
  - **TLS / Smart Card**
  - **EAP-FAST**
  - **LEAP**

4 Click **OK** to save your settings and return to the **Configuration** tab.

5 Click the **Close** box to exit the configuration software.

That's it! You have configured **802.1x** security for your wireless connection, and you're ready to use the Internet.

Changing your Security Setting

If the type of security on your wireless network changes, you need to modify your security settings. To do this, follow the instructions in **Section 2: Setting Security** on page 10.

3

Advanced Options

*The **Zoom Wireless-N USB** utility provides options so you can create profiles, monitor the signal strength of your network connection, scan available networks, and specify advanced settings. This chapter tells you when and how to use each of these options.*

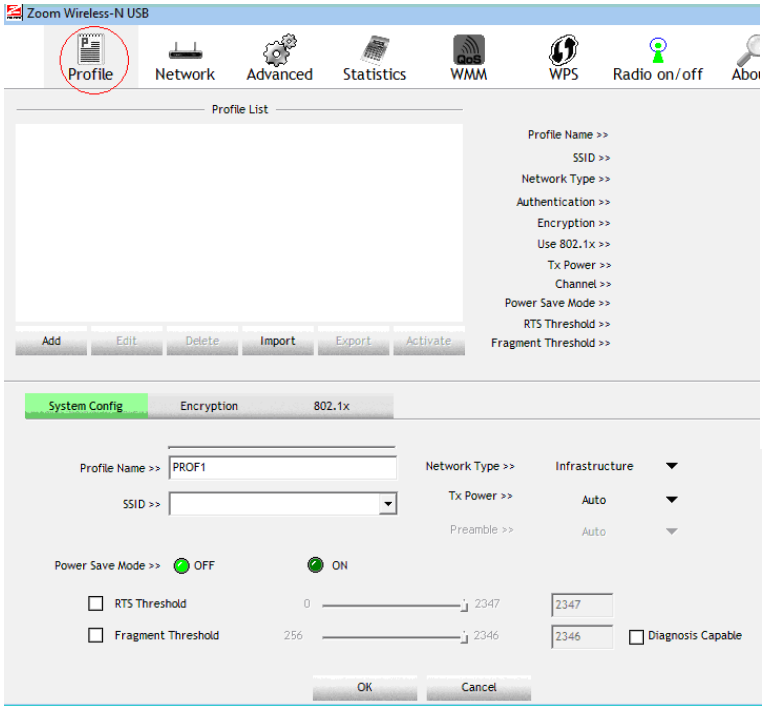
Creating Profiles

A profile is a collection of settings needed for a particular wireless connection. If you plan to use more than one network, you can create a profile for each one and then switch to its profile when you want to connect to that particular network.

For example, you may want to set up profiles for a work network and a home network, each of which has different configuration settings. By creating two profiles, you can store the settings for each network and then switch quickly and easily from one network to the other by selecting the appropriate profile.

1. On your taskbar, double-click the Zoom **Wireless-N USB** icon.

2 On the **Configuration** tab, click on **Profile.** Then click on **Add.** In the text box **Profile Name>>** enter a name for the profile you want to create.



For example, let's say you have a small home network to which you want to be able to switch quickly when you arrive home. Give the profile the name "Home":

3 Then enter the following settings:

- **SSID** – Select the network name. In the example above, the SSID is **Home**.
- **Network Type** – From the drop-down list, select **Infrastructure.**
- **Enable Security** by selecting the Encryption tab. Then, from the menu, select the type of security you wish to enable.

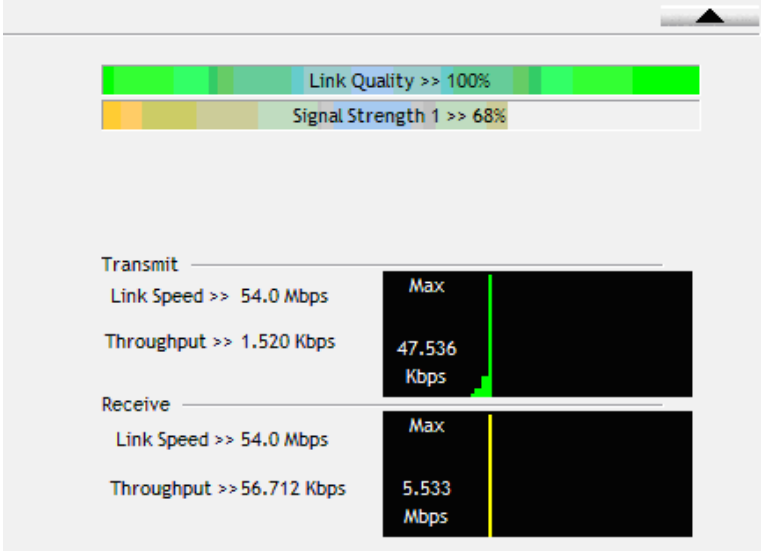
Note: If you are setting up an ad hoc network, as in this example, only WEP security is available to you.

After you enter your security settings, click **OK** to return to the **Configuration** tab.

4 In the **Configuration** area, click the **OK** button to save the settings.

Monitoring Link Status

To access the **Status** area, click on the arrow on the bottom right corner of the Zoom utility screen.



The **Status** area on the **Configuration** tab displays the following information about your wireless connection:

- **Status**>> In an *Infrastructure* network, the name and the MAC address of the wireless access point or router to which your computer is connected.

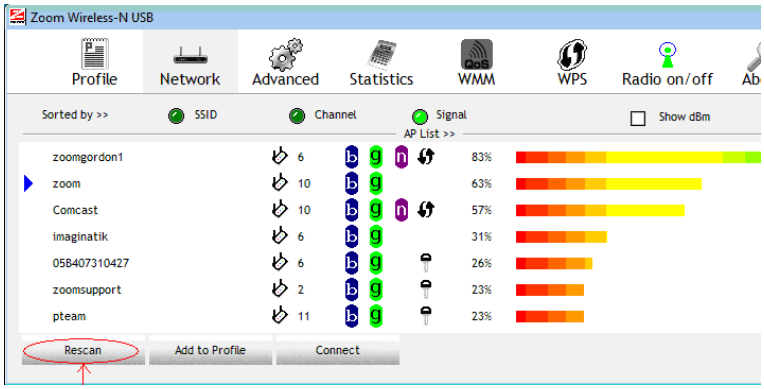
  In an *ad hoc* network, the virtual MAC address used by computers in the network.
- **Channel**>> The Wi-Fi frequency channel.
- **Link Speed**>> Highest transmission speed in **M**ega**b**its **p**er **s**econd of the last received packet.
- **Throughput (K**ilo**b**its**/sec)**>> TX = number of packets transmitted per second without errors.
  RX = number of packets received per second without errors.
- **Link Quality** (Infrastructure only): The transmission quality of the last received packet.
  80 – 100% = Excellent
  60 – 80% = Good
  40 – 60% = Fair
  Under 40% = Poor or no connection
- **Signal Strength** (Infrastructure only): The transmission signal strength of the last received packet, expressed as a percent of maximum allowable power.
  Note: you may be able to improve the signal strength by plugging the USB adapter into the extension cable (included in the package) and plugging the extension cable into the computer to position the adapter in a more favorable location.
  80 – 100% = Excellent
  60 – 80% = Good
  40 – 60% = Fair
  Under 40% = Poor or no signal strength

Using Network and Rescan

Use the **Network** window and the **Rescan** button when you need to do any of the following:

- Find a list of network names (SSIDs) so you can connect to a network
- Check the channel difference between your network and other networks within range
- Check the network type (infrastructure or ad hoc) of your network
- Verify whether security is enabled for your network

To use this window, click the **Network** tab, then click the **Rescan** button to refresh the list.

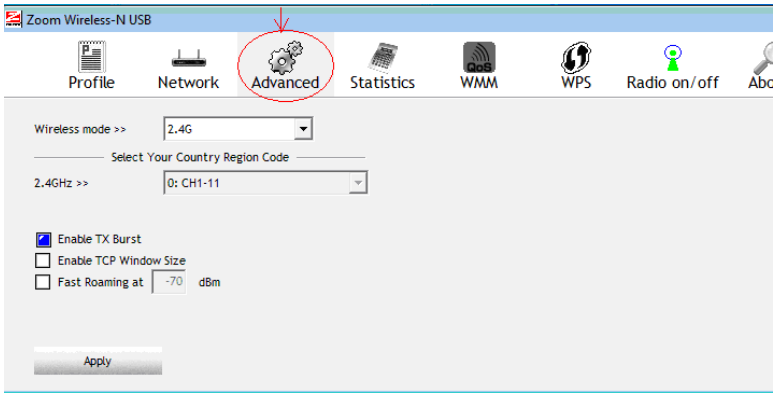


The information displayed on the **Network** tab is as follows:

- **SSID** (**S**ervice **S**et **Id**entifier): An SSID, also known as Network Name, is chosen by the person who sets up the network. The SSID is a code attached to all packets sent over an infrastructure wireless network. The code can contain up to 32 alphanumeric characters. All devices in the network must share the same SSID.
- **Network Type:** Infrastructure or Ad Hoc.
- **Channel**: The Wi-Fi frequency channel.
- **802.11n/g/b:** Indicates which of the following (n, g, b) standards are supported.
- **Security**: The type of security configured for the network.
- **Signal**: The strength and quality of your transmissions.

Advanced Configuration

To access this window, click the **Advanced** button on the **Configuration** tab.



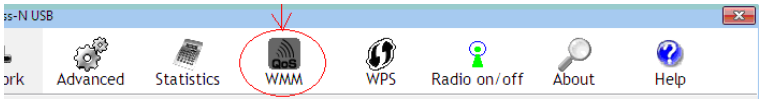
Here you can view and set the following parameters:

- Wireless Mode
- Country Region Code
- Enable TX Burst
- Enable TCP Window Size
- Fast Roaming at -70 dBm

When you are finished, click on the **Apply** button.

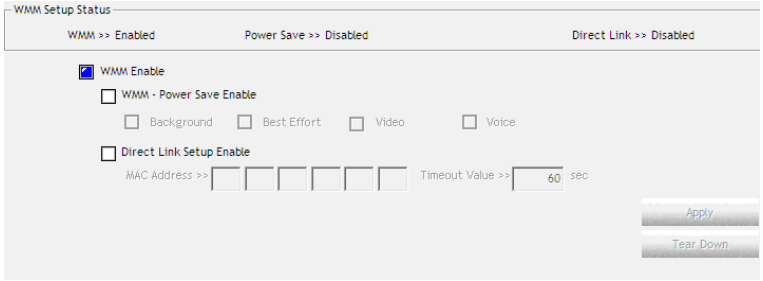
WMM (WiFi™ Multimedia)

To access this window, click the WMM button on the Configuration tab.



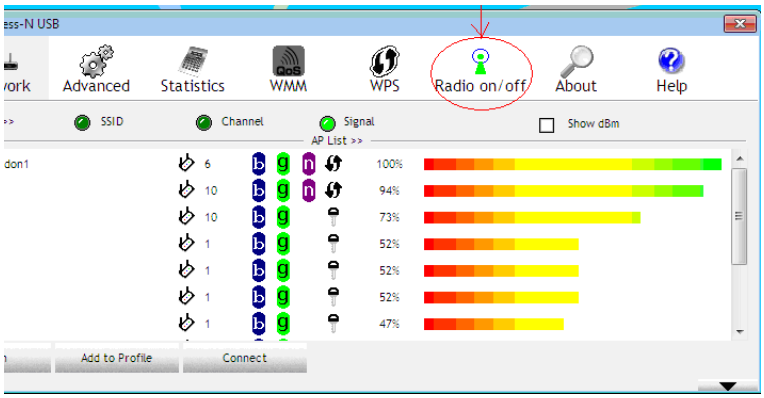
Here you can view and set the following parameters:

- WMM – Power Save Enable
- Direct Link Setup Enable



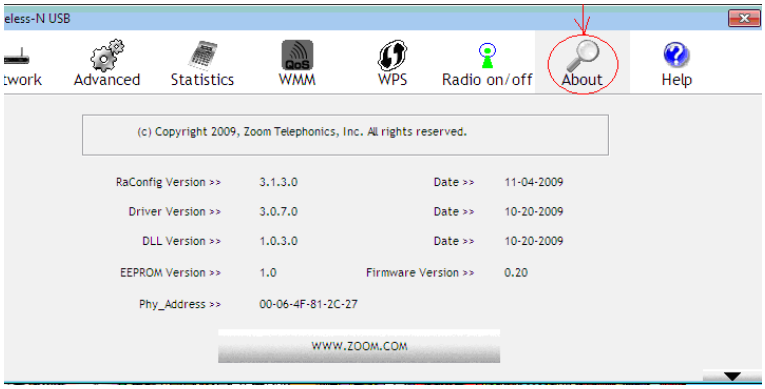
Radio On / Off

Instead of unplugging the USB Adapter when you want to turn the wireless connection off, you can click the **Radio On/Off** button on the **Configuration** tab. To reconnect, click the **Radio On/Off** button which will turn the connection on again.



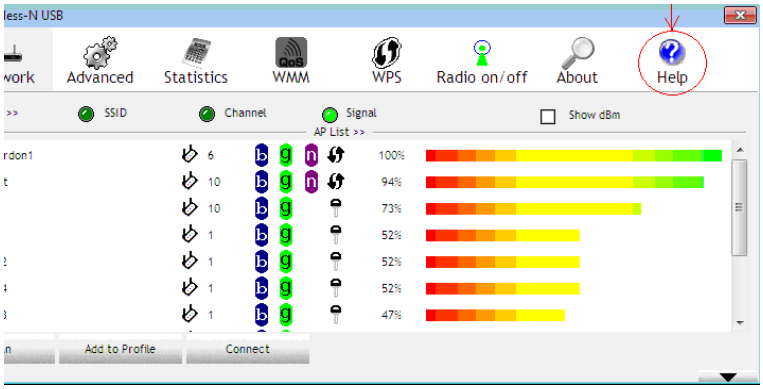
About tab

To access this window, click the **About** button on the **Configuration** tab. Here you can view information about the Driver version, DLL version, and EEProm version.



Help tab

To access this window, click the **Help** button on the **Configuration** tab. Here you can access online help for the Wireless-N USB Adapter.

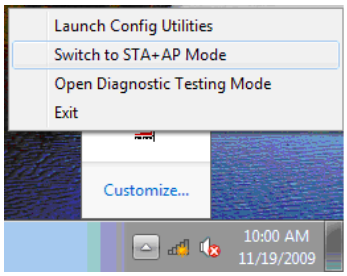


Soft AP Mode

For Windows 7:

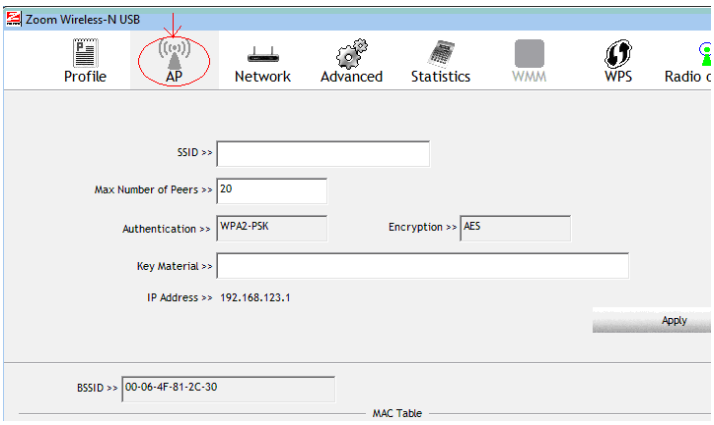
Right-click the **Zoom icon** on the taskbar and select "**Switch to STA+AP Mode**" to make your wireless USB adapter act as a wireless AP.

For example if you had a cable or ADSL modem directly attached to your PC, you can use your wireless USB adapter as an AP to allow other wireless devices to access the cable or ADSL modem.



1 Click **OK.**

2 In the **Zoom Utility** window that opens up, click on the **AP** icon at the top.



3 In the **SSID** textbox, type in the name you would like to assign to your network.

4 In the **Max Number of Peers** textbox, the maximum number of clients that are allowed access is 20. You can choose any number below 20 if you prefer.

5 The **Authentication** is set by default to WPA2-PSK and cannot be changed.

6 The **Encryption** is set by default as AES and cannot be changed.

7 In the **Key Material** textbox, enter the Preshared Key you would like to assign to the network.

8 The IP Address is automatically generated.

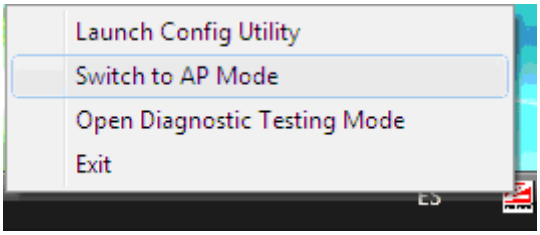
9 Click **Apply**.

Note: Clients that need to connect to this network should use the same SSID and Preshared Key assigned here.

For Windows Vista, XP, and 2000:

Right-click the **Zoom icon** on the taskbar and select "**Switch to AP Mode**" to make your wireless USB adapter act as a wireless AP.

For example if you had a cable or ADSL modem directly attached to your PC, you can use your wireless USB adapter as an AP to allow other wireless devices to access the cable or ADSL modem.

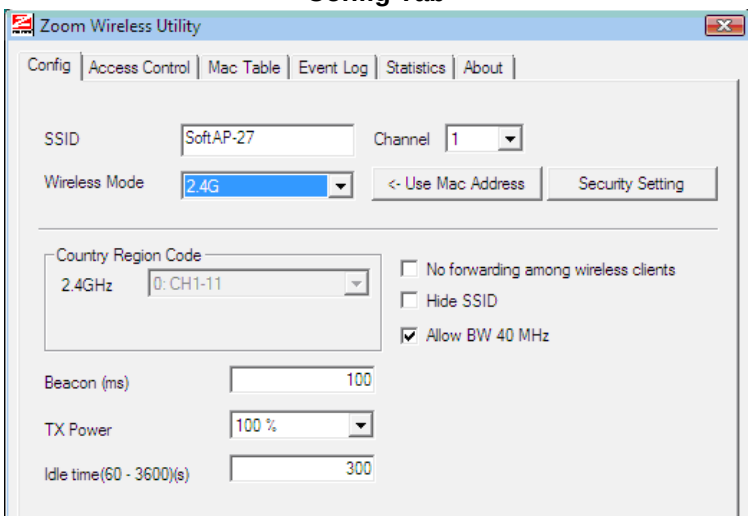


1 Click **OK.**

2 The **Zoom Utility** software opens up.

3 In the dialog box that opens, you can access and change **Soft AP** information.

Config Tab



SSID: AP name of user. You can also click Use MAC Address button to display it.

Channel: Manually select the AP using the channel. The system default is CH 1.

Wireless Mode: This currently supports 2.4G (included 802.11b/g/n) wireless mode.

Use MAC Address: Click this button to replace SSID by the MAC address.

Country Region Code: The available channel differs from different countries.

No forwarding among wireless clients: No beacon among wireless client, clients can share information each other. The system default is no forwarding.

Hide SSID: Do not display AP name. System default no hide.

Allow BW 40MHz: Click to disable this function. Default is enabling.

Beacon (ms): The time between two beacons. The system default is 100 ms.

TX Power: Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and Lowest. The system default is 100%.

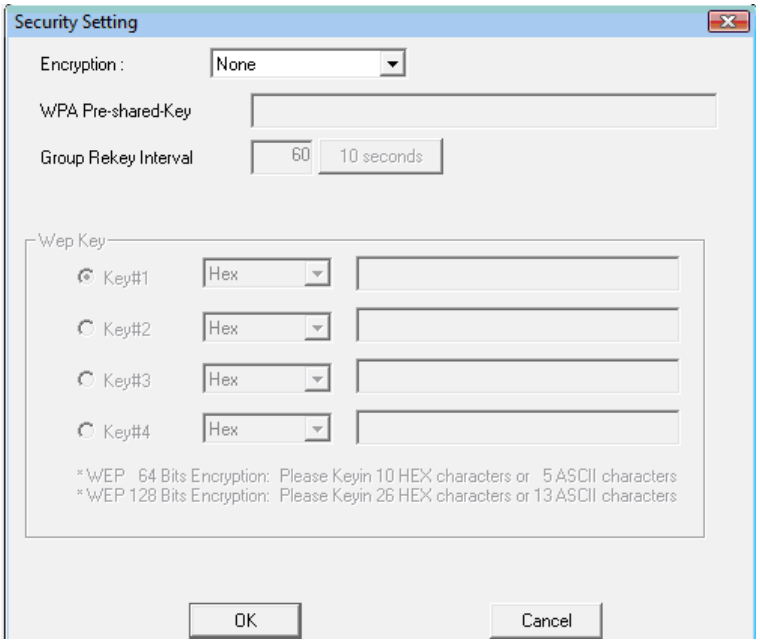
Idle time (60-3600)(s): It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. Default value of idle time is 300 seconds.

Default: Use the system default value.

Apply: Click to apply the above settings.

Security Setting Tab

The Security Setting tab displays the Authentication Type and Encryption Type used within the AP. The system default is no authentication and encryption.



Encryption Type: From here, you can select: None, WEP, WEP-Shared, WPA, or WPA2.

WPA Pre-shared Key: Enter the Pre-shared key here.

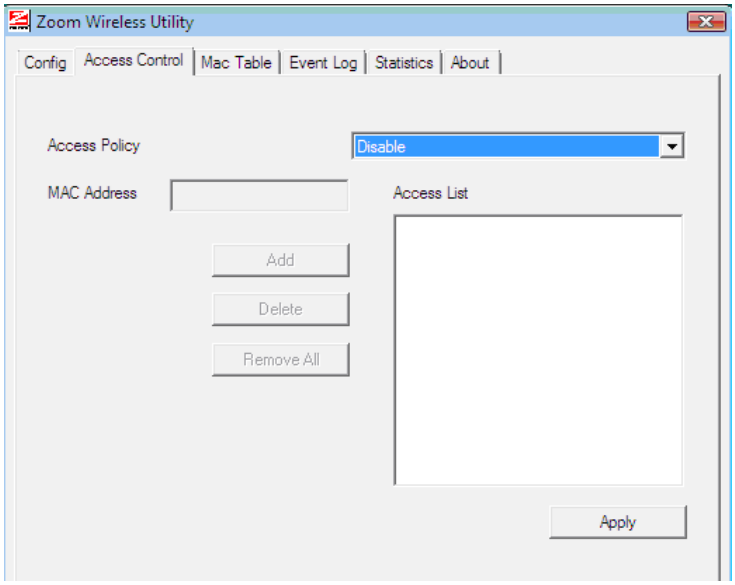
Group Rekey Interval: Default is 60 seconds.

WEP Key: Only valid when using WEP encryption. The key must match with the AP's key. There are several formats to enter the keys.

• Hexadecimal (128bits): 26 Hex characters.

• ASCII (128bits): 13 ASCII characters.

Access Control Tab



Access Policy: User chooses whether AP start the function or not. System default is Disable.

-- Disable: Do not use this access control function.

-- Allow All: Only the MAC address listed in the Access List can connect with this soft AP.

-- Reject All: Only the MAC address listed in the Access List can NOT connect with this soft AP.

MAC Address: Manually force the MAC address using the function. Click Add and the MAC address will be listed in the Access List pool.

Access List: Display all MAC Address that you have set.

Add: Add the MAC address that you would like to set.

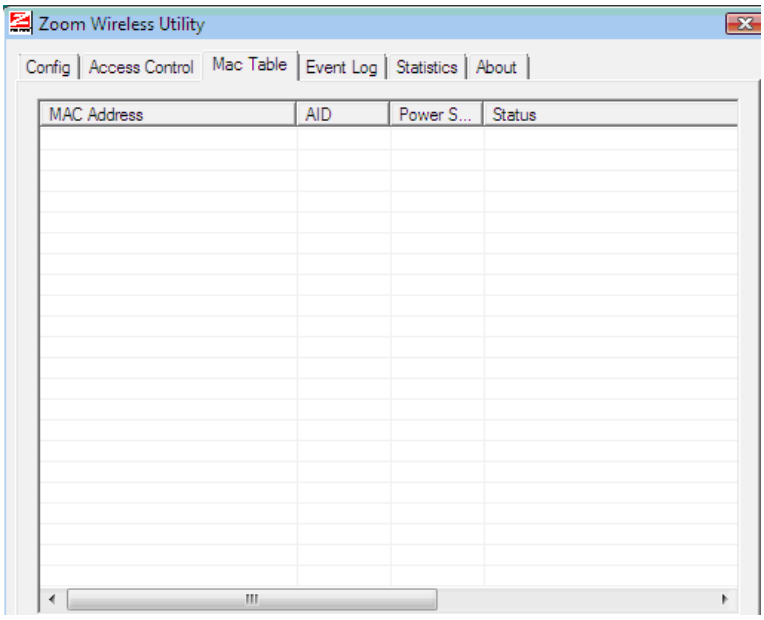
Delete: Delete the MAC address that you have set.

Remove All: Remove all MAC address in the Access List.

Apply: Apply the above changes.

MAC Table Tab

The MAC Table displays detailed station information of current connection.



MAC Address: The station status. (MAC address of current connection.)

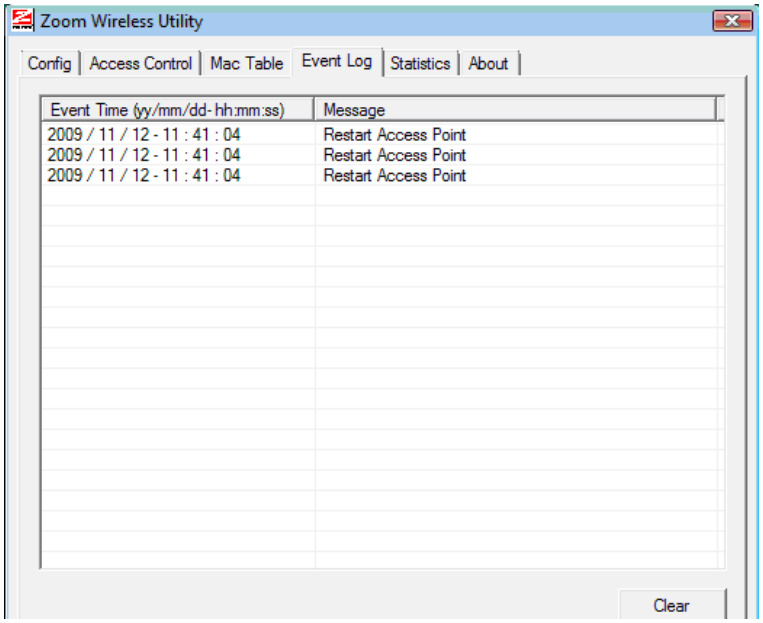
AID: Raise value by current connection.

Power Saving Mode: This section displays whether the current connection supports Power Saving.

Status: The status of the current connection.

Event Log Tab

This tab records all of the event times and messages.



Event Time (yy/mm/dd-hh:mm:ss): Records the event time.

Message: Records all the event messages.

Statistics Tab

The Statistics tab displays detailed counter information based on the 802.11 MIB counters. The information is translated into a format that is easier to understand.

Transmit Statistics

Frames Transmitted Successfully: Frames successfully sent.

Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.

Frames Transmitted Successfully After Retry: Frames successfully sent with one or more reties.

Receive Statistics

Frames Received Successfully: Frames Received Successfully.

Frames Received With CRC Error: Frames received with CRC error.

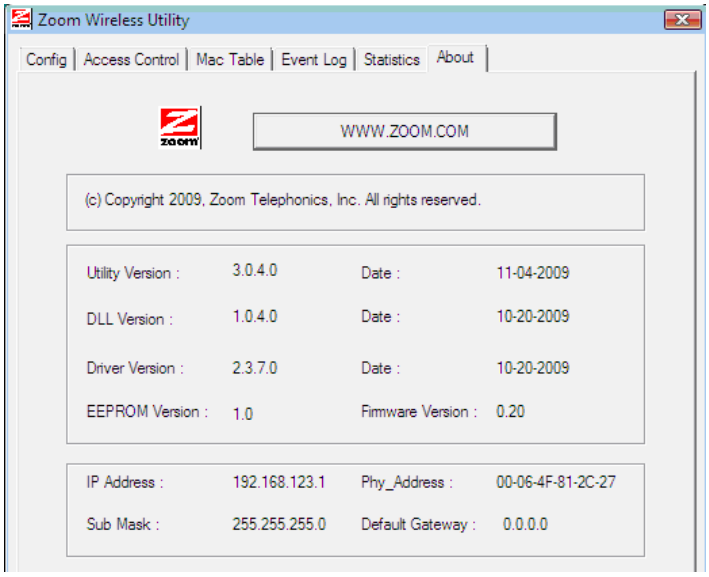
Frames Dropped Due To Out-of-Resource: Frames dropped due to resource issue.

Duplicate Frames Received: Duplicate received frames.

Reset Counter: Reset counters to zero.

About Tab

This tab displays the wireless card and driver version information.



4

Installation Instructions for Mac OS X 10.3, 10.4, and 10.5

This chapter provides instructions for installing the Wireless-N USB adapter on a Mac (OS X 10.3, 10.4, and 10.5).

Installing and Connecting the Adapter

Important: Do not plug the Adapter into your computer yet. We will tell you when to plug it in.

1 Insert the Wireless-N USB CD into the CD or DVD drive.

2 Double-click the Zoom installer to open. Click on the Mac folder.

3 In the folder, select your OS X version and double-click to open.

4 You will see two files: one for installation and one for uninstallation. Select the file for installation.

5 Double-click the installer and then click **Continue**.

6 Click **Install**.

7 In the dialog box, you will see a text box for Name and a text box for Password. Use the name and password of your Mac OS X user account (the same information you use to login to your computer) and click **OK**.

8 Click **Continue Installation**.

9 Click **Restart**.

10 Wait until you see the desktop. Then, plug the USB Adapter into one of the available USB slots on your computer. (If it is difficult to insert the USB Adapter directly into the USB slot because there isn't enough space near the slot, first plug the USB Adapter into the **extension cable** included in the package and then plug the other end of the extension cable into the USB slot in your computer. Since the extension cable is semi-rigid, you can twist the extension cable to orient the USB Adapter for best reception. Usually a vertical orientation is best.)

11 The USB Wireless Utility should appear on the taskbar.

12 If you see the message "A new network interface has been detected" select Network Preferences. Click Apply.

13 If you do not see the message “A new network interface has been detected” go to the Apple logo and select System Preferences. Then select Network. If you do not see the USB ethernet adapter on the list, click the + button. Go to the Interface drop-down menu and select USB Ethernet (en3) in OS X 10.5 or Ethernet Adapter (enx) in OS X 10.4 & 10.3 and click **Create**. Then click **Apply**. Go to Site Survey and select the Network you prefer by highlighting it and click **Connect**.

14 To verify the IP, go to the Apple logo on your computer’s menu bar. Select System Preferences. Select Network. You should be able to see USB Ethernet network connection (USB Ethernet (en3) in OS X 10.5 or Ethernet Adapter (enx) in OS X 10.4 & 10.3).Click on it and the IP Address should be displayed in the dialog box.

15 You should now be connected. To check your connection, open your Web browser and go to your favorite site.

To connect to a network

Now you are ready to connect to a network. Wireless networks typically have a wireless access point, router, or gateway at the heart of the wireless network. Wireless networks sometimes use wireless security and sometimes do not. What you do next depends on your network’s wireless security. You have several options:

1 If your access point or router supports **WPS**, we highly recommend that you **connect to a network using WPS**.

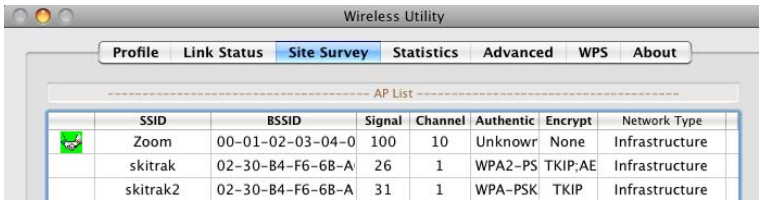
2 If your access point or router does not support WPS or you do not know what it is or you choose not to connect this way, you can **connect to a network without security**.

3 If you decide that you want to **join a wireless network that has security**, scroll down to **Section 5: Setting Security** and follow the instructions.

To connect to a network without security

1 From the **Go** menu on your Mac Finder's menu bar, select Applications. To open the configuration software, double-click the USB Wireless Utility icon.

2 In the Wireless Utility **Site Survey** window, look through the list of available wireless networks and highlight the network you want and click **Connect**.



3 If you join a wireless network that **does not have security**, you should now be connected. To check your connection, open your Web browser and go to your favorite site.

> If the network you select has security configured, you must enable and configure security on your Zoom Wireless-N USB Adapter before you can connect. See Chapter 5, **Setting Security for Mac**.

If you have difficulty accessing the Internet, follow the suggestions in the Troubleshooting section in Appendix B at the end of this User Manual.

The Adapter LED

The state of the LED on the Wireless-N USB adapter is explained below.

LED Status	Meaning
Flashing	The Wireless-N USB adapter is attempting to or is connected to a wireless network and is transmitting or receiving data.

5

Setting Security for Mac

We strongly recommend security, although you do not need to use it to get your wireless connection working.

Important! You must first enable security on the wireless access point or router. You then enable security on the adapter using the same configuration that you used for the access point or router. For example, if a wireless access point is configured for WEP, you must select WEP security in the Wireless-N USB configuration software and enter the same encryption key.

Accessing security options

1. From the **Go** menu on your Mac Finder's menu bar, select Applications. To open the configuration software, double-click the USB Wireless Utility icon.
2. In the **Site Survey** window, make sure that the desired wireless network is displayed in the **SSID** text box (the term **<Infra>** designates an Infrastructure network) and that the **Network Type** is correct.

   There are two types of wireless networks: *Infrastructure* and *Ad Hoc*.

   - In an **Infrastructure** network, wireless devices communicate with each other via a wireless access point, router, or ADSL modem with built-in wireless technology.

- In an **Ad Hoc** network, a group of wireless devices communicate directly with other “client” devices that are using wireless adapters. The network does not include a wireless access point or wireless router.
- In the unlikely event that you use an Ad Hoc network, you must set up Static IP addressing. See **Appendix A: TCP/IP Settings**.

3 For configuration instructions for the different types of available security options, consult this table:

To configure	Go to page
WPS	42
WEP / WEP-Shared	44
WPA2	45
WPA	46

- **WiFi™ Protected Setup (WPS)**: This is the option we recommend if WPS is supported by all the devices in your network. This protocol can greatly simplify the process of configuring WPA2 or WPA security.
- **WEP** (**W**ired **E**quivalent **P**rivacy): Both the **WEP** and WEP-**Shared** Authentication modes set WEP security. WEP is the preferred setting, WEP–Shared should only be used when connecting with certain Mac products that do not support standard WEP. If the devices in your network do not support WPA2 or WPA, select **WEP** data encryption.

  This method requires you to enter an encryption key. The keys can be 64 or 128 bits in length.
- **WPA2:** Select **WPA2** if all of the devices in the network support WPA2. To set this type of security, you will need to enter the WPA Preshared Key in the text box.
- **WPA:** To set this type of security, you will need to enter the WPA Preshared Key in the text box.

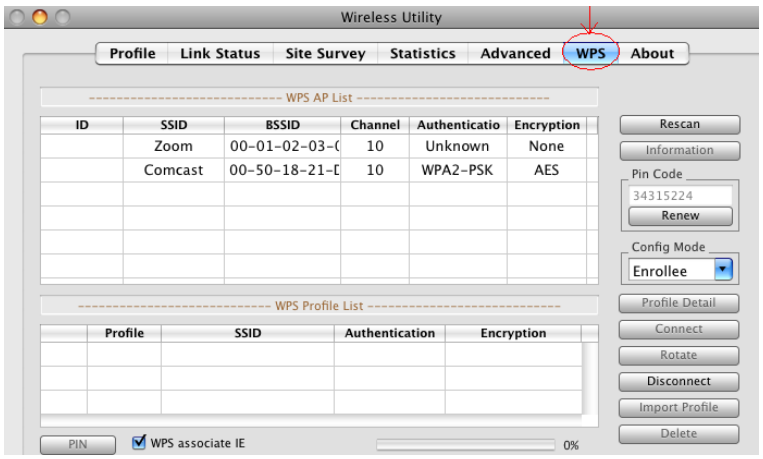
WiFi™ Protected Setup (WPS)

To connect to a network using WPS

If your wireless access point or router supports **W**iFi™ **P**rotected **S**etup (WPS), this protocol can greatly simplify the process of configuring WPA2-PSK or WPA-PSK security. If your wireless access point or router supports WPS, it typically has a WPS button built into its case.

1 From the **Go** menu on your Mac Finder's menu bar, select Applications. To open the configuration software, double-click the USB Wireless Utility icon.

2 On the **Wireless Utility** screen, click the **WPS** button to open the **WPS Config** screen.



3 Go to the wireless access point or router and activate the **WPS** pushbutton (or *Secure Setup* or similarly named button, or a virtual pushbutton on the software display of the access point). You may have to hold down the **WPS** button for several seconds or until the WiFi™ indicator light on the access point starts flashing. The access point or router will now begin accepting **WPS** connections. (If security has not

been set on the access point or router, a random SSID and WPA key will be used.)

4 Now, click on **PBC** (Push Button configuration) on Zoom's **WPS Config** screen.

You should now have a secure connection. Open your Web browser and go to your favorite site.

PIN option:

1 If the access point or router does not have a hard or soft security pushbutton, you can use the **PIN** option.

2 Click on **PIN** on Zoom's **WPS Config** screen. In the text box, the Adapter's randomly generated **PIN** number will be displayed.

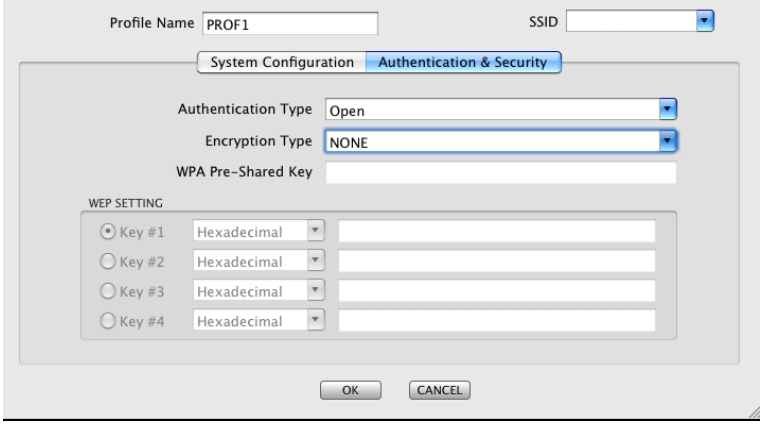
3 Go to the access point or router, enter the Adapter's **PIN** number in the appropriate place on the access point's configuration interface, and click a button -- called **Start PIN** or something similar -- to activate a search for the Adapter. When the access point or router identifies the Adapter, it will automatically configure security.

You should now have a secure connection. Open your Web browser and go to your favorite site.

That's it! You have configured WPS security for your wireless connection, and you're ready to use the Internet.

WEP (Wired Equivalent Privacy) / WEP-Shared

1 In the **Site Survey** window highlight the wireless network you want to join and click Connect. For the **Encryption** type, click the Encryption drop-down arrow and select **WEP** (recommended) or **WEP-Shared**.



2 In the **WEP Setting** area**,** do the following:

a In the first drop-down list select:

- **Hexadecimal digits**

or

- **ASCII characters**

b In the **Key #1** text box, enter a key using the table below as a guide.

The key must be the same for all the devices on your network.

If you selected key type…	**Enter exactly…**
Hexadecimal digits – 128 bits	26 characters A–F, a–f and 0–9. For example, 00112233445566778899AABBCC.
Hexadecimal digits – 64 bits	10 characters. The characters can be A-F, a-f, and 0-9. For example, 11AA22BB33.
ASCII – 128-bits	13 characters. The characters can be any upper- or lower-case letters and numbers. For example: MyKey12345678.
ASCII – 64 bits	5 characters. The characters can be any upper- or lower-case letters and numbers. For example, MyKey.

3 Click **OK** to save your settings and return to the **Configuration** tab.

4 Click the **Close** box to exit the configuration software.

That's it! You have configured WEP security for your wireless connection, and you're ready to use the Internet.

WPA2

Select WPA2 if all of the devices in the network support WPA2.

1 In the **Site Survey** window select the wireless network you want to join and click Connect. For the **Encryption** type, click the Encryption drop-down arrow and select **WPA2**.

2 Enter the WPA Preshared Key in the text box.

3 Click **OK** to save your settings and return to the **Configuration** tab.

4 Click the **Close** box to exit the configuration software.

That's it! You have configured WPA2 security for your wireless connection, and you're ready to use the Internet.

WPA

1 In the **Site Survey** window select the wireless network you want to join and click Connect. For the **Encryption** type, click the Encryption drop-down arrow and select **WPA**.

2 Enter the WPA Preshared Key in the text box.

3 Click **OK** to save your settings and return to the **Configuration** tab.

4 Click the **Close** box to exit the configuration software.

That's it! You have configured WPA security for your wireless connection, and you're ready to use the Internet.

Changing your Security Setting for Mac

If the type of security on your wireless network changes, you need to modify your security settings. To do this, follow the instructions in Section 5: **Setting Security for Mac** on page 40.

6

Advanced Options for Mac

*The **Zoom Wireless-N USB** utility provides options so you can create profiles, monitor the signal strength of your network connection, scan available networks, and specify advanced settings. This chapter tells you when and how to use each of these options.*

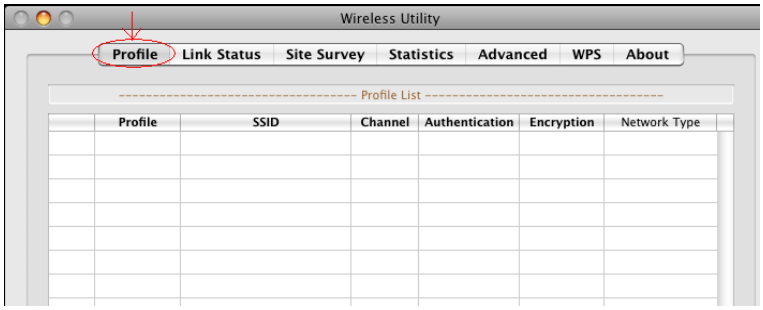
Creating Profiles

A profile is a collection of settings needed for a particular wireless connection. If you plan to use more than one network, you can create a profile for each one and then switch to its profile when you want to connect to that particular network.

For example, you may want to set up profiles for a work network and a home network, each of which has different configuration settings. By creating two profiles, you can store the settings for each network and then switch quickly and easily from one network to the other by selecting the appropriate profile.

1. From the Go menu on your Mac Finder's menu bar, select Applications. To open the configuration software, double-click the USB Wireless Utility icon.

2. On the Wireless Utility screen, click on **Profile.** Then click on **Add.** In the text box **Profile Name** enter a name for the profile you want to create.



For example, let's say you have a small home network to which you want to be able to switch quickly when you arrive home. Give the profile the name "Home":

3 Then enter the following settings:

- **SSID** – Select or type in the network name. In the example above, the SSID is **Home**.
- **Power Saving Mode** – Select the radio button for either:
  - **CAM** (Constantly Awake Mode) or
  - **Power Saving Mode**
- **Network Type** – From the drop-down list, select either **Infrastructure** or **Ad Hoc** (802.11)**.**
- **Ad Hoc channel** – (Note: You will only need to follow this section for the Ad Hoc channel if you selected the Ad Hoc network type.) From the drop-down list, select the channel used by the other device(s) in the network. If you are setting up the first computer in the network, select a channel.

  Also, to avoid interference, it is desirable to have a 5-channel difference between your channel and the channel being used by another network within range.

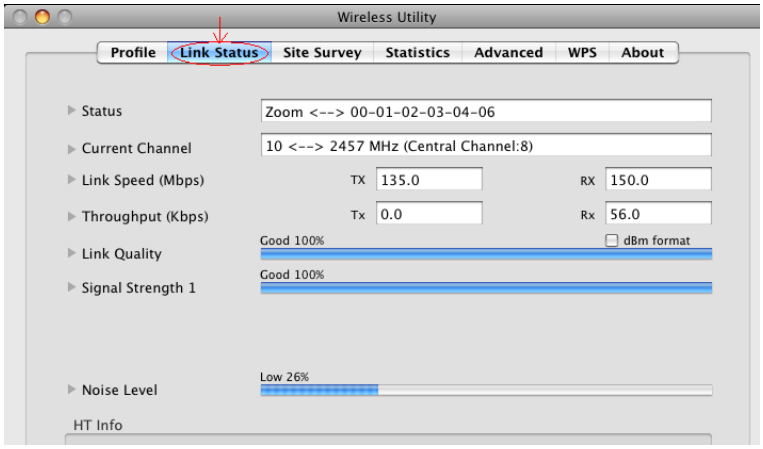
  If you are unsure of which channel to use, select Channel 6.
- **Enable Security** by selecting the **Authentication & Security** tab. Then, from the menu, select the type of security you wish to enable.

Note: If you are setting up an ad hoc network, as in this example, only the WEP Encryption Type is available to you.

After you enter your security settings, click **OK** to return to the Profile window.

4 In the Profile window, highlight the profile you created and click **Activate**..

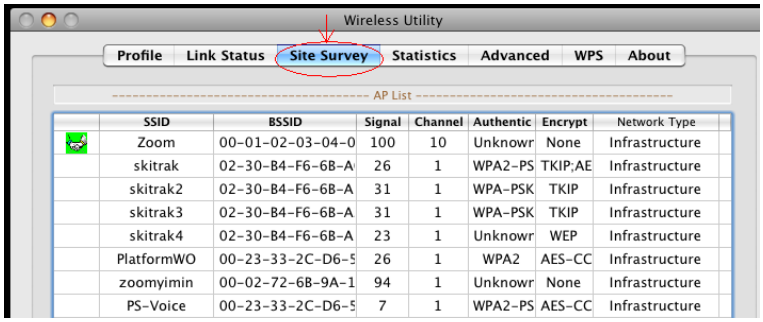
Monitoring Link Status for Mac



- **Status**>> In an *Infrastructure* network, the name and the MAC address of the wireless access point or router to which your computer is connected.

  In an *ad hoc* network, the virtual MAC address used by computers in the network.
- **Current Channel**>> The Wi-Fi frequency channel.
- **Link Speed**>> Highest transmission speed in **M**ega**b**its **p**er **s**econd of the last received packet.
- **Throughput (K**ilo**b**its**/sec)**>> TX = number of packets transmitted per second without errors.
  RX = number of packets received per second without errors.
- **Link Quality** (Infrastructure only): The transmission quality of the last received packet.
  80 – 100% = Excellent
  60 – 80% = Good
  40 – 60% = Fair
  Under 40% = Poor or no connection
- **Signal Strength** (Infrastructure only): The transmission signal strength of the last received packet, expressed as a percent of maximum allowable power.
  Note: you may be able to improve the signal strength by plugging the USB adapter into the extension cable (included in the package) and plugging the extension cable into the computer to position the adapter in a more favorable location.
  80 – 100% = Excellent
  60 – 80% = Good
  40 – 60% = Fair
  Under 40% = Poor or no signal strength
- **Noise Level**>> Indicates the noise activity out of 100%.

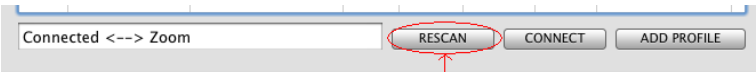
Using Site Survey and Rescan for Mac



Use the Site Survey window and the Rescan button when you need to do any of the following:

- Find a list of network names (SSIDs) so you can connect to a network
- Identify the MAC address (BSSID) of your wireless access point or router
- Check the channel difference between your network and other networks within range
- Check the network type (infrastructure or ad hoc) of your network
- Verify whether security is enabled for your network

To use this window, click the Site Survey tab, then click the Rescan button to refresh the list.



The information displayed on the Site Survey tab is as follows:

• SSID (Service Set Identifier):SSID or Network Name, is chosen by the person who sets up the network. The SSID is a code attached to all packets sent over an infrastructure wireless network. The code can contain up to 32 alphanumeric characters. All devices in the network must share the same SSID.

• BSSID (Basic Service Set Identifier): A Basic Service Set consists of a wireless access point or router connected to wired network and a set of wireless devices. In an infrastructure network, the BSSID is the MAC address of the wireless router or wireless access point. In an ad hoc network, the BSSID is the MAC address of the first computer in the network to be powered up.

• Signal: The strength and quality of your transmissions.

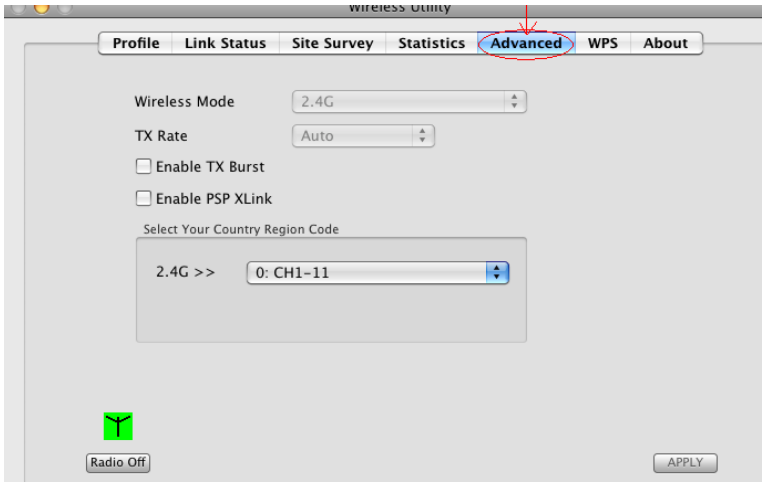
• Channel: The Wi-Fi frequency channel.

• Authentication and Encryption: The type of security configured for the network.

• Network Type: Infrastructure or Ad Hoc.

Advanced Configuration for Mac

To access this window, click the **Advanced** button on the **Configuration** tab.



Here you can view and set the following parameters:

- Wireless Mode
- TX Rate
- Enable TX Burst
- Enable PSP XLink
- Select Your Country Region Code
- Radio On / Radio Off button

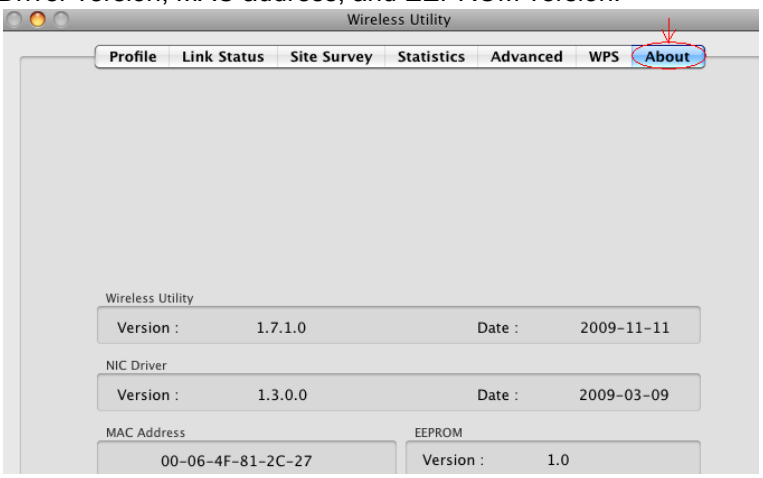
When you are finished, click on the **Apply** button.

Statistics tab for Mac

To access this window, click the **Statistics** button on the **Configuration** tab. Here you can view Transmit and Receive statistics.

About tab for Mac

To access this window, click the **About** button on the **Configuration** tab. Here you can get view information about the Driver version, MAC address, and EEPROM version.



Appendix A

TCP/IP Settings

There are two types of wireless networks: *Infrastructure* and *Ad Hoc*.

- In an **Infrastructure** network, wireless devices communicate with each other via a wireless access point, router, or ADSL modem with built-in wireless technology.
- In an **Ad Hoc** network, a group of wireless devices communicate directly with other "client" devices that are using wireless adapters. The network does not include a wireless access point or router.

By default, Windows is set for **dynamic addressing (DHCP)**. This is typically the correct setting for an Infrastructure network, but needs to be changed to **static IP addressing** if you are using an Ad Hoc network. (Note: Use our instructions as a basic guide. Advanced users will know other ways to set up their networks.)

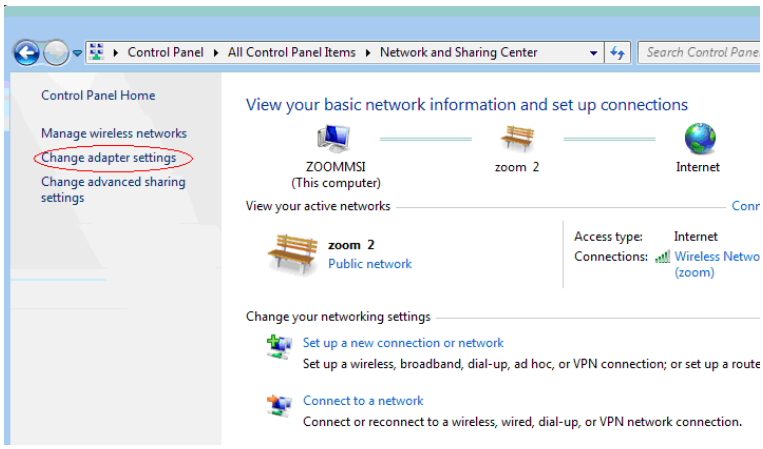
To set up TCP/IP, please go to the section that corresponds to your Windows or Mac operating system. Note that you normally only set up TCP/IP in the unlikely event that you have an Ad Hoc network.

Windows 7

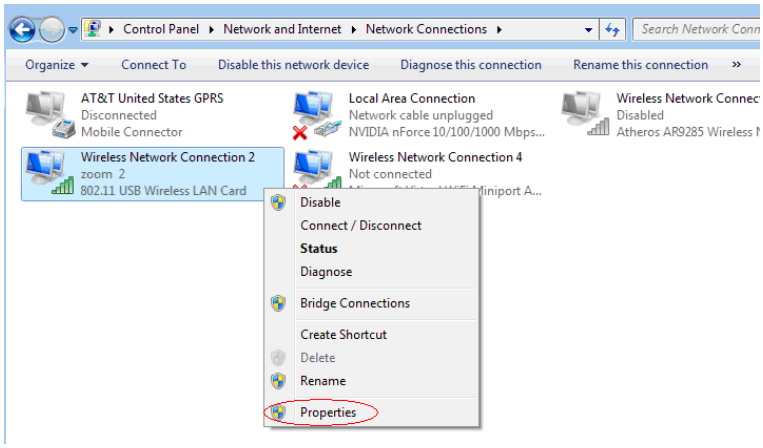
1. Follow these steps to open the **TCP/IPv4** or **TCP/IPv6 Properties** dialog box.

   a. From the desktop, click the **Start** button, select **Control Panel**.

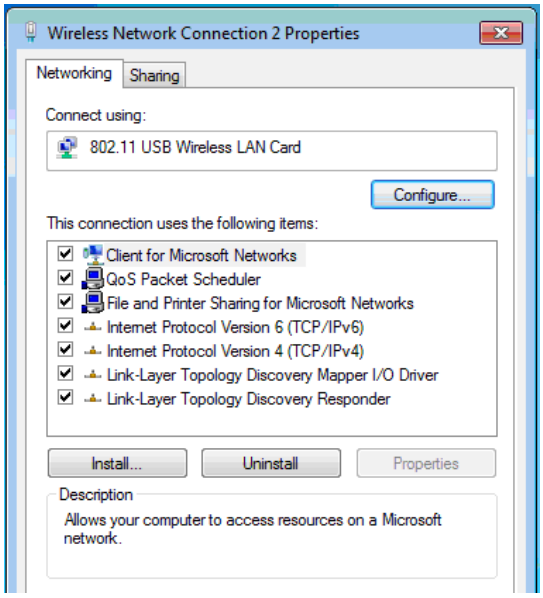
b Under **Network and Sharing Center**, select **Change adapter settings** from the menu on the left side of the screen.



c Right-click on the **Wireless Network Connection** icon and select Properties:



d In the **Wireless Network Connection Properties** dialog box, highlight the version of TCP/IP (Transmission Control Protocol/Internet Protocol) that you are using and click the **Properties** button.



e To set static IP addressing, continue with Step 2 below. For dynamic addressing (DHCP), continue with Step 3 below.

2 **To set static IP addressing:** In the **TCP/IPv4** or **TCP/IPv6 Properties** dialog box, on the **General** tab, complete the following:

a Ensure that Obtain an IP address automatically is not selected. Then select the buttons labeled: Use the following IP address and Use the following DNS server addresses.

b If this is the first computer to be set up in the ad hoc network, enter **10.0.0.5** for an **IP address**. If you are adding it to an existing ad hoc network, increment the last digit by one, for example, **10.0.0.6**, **10.0.0.7**

c Enter **255.255.255.0** for **Subnet mask**. The **Subnet mask** should be the same for each computer in your ad hoc network.

d Enter **10.0.0.5** for **Default gateway** and **Preferred DNS server**. (This is the IP address of the first computer that was set up in your ad hoc network.) The **Default Gateway** and **Preferred DNS server** should be the same for each computer in your ad hoc network.

e Click **OK** twice.

That's it! You have set static IP addressing for a Windows 7 computer in an ad hoc network.

3 **For dynamic addressing (DHCP):** To verify your DHCP settings, complete the following:

a Ensure that **Obtain an IP address automatically is** selected.

b Select either Obtain a DNS server address automatically or Use the following DNS server addresses. All text boxes for static IP addressing should be blank.

If you select **Use the following DNS server addresses**, enter your preferred and alternate server addresses.

c Click **OK** twice to exit.

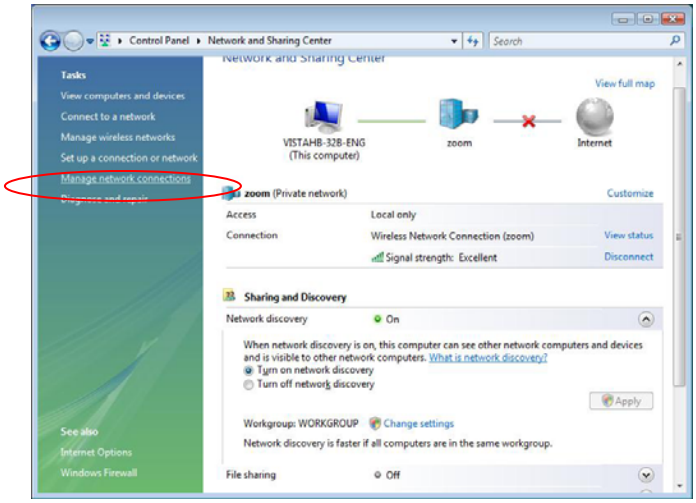
That's it! You have verified your DHCP settings for a Windows 7 computer in an infrastructure network.

Windows Vista

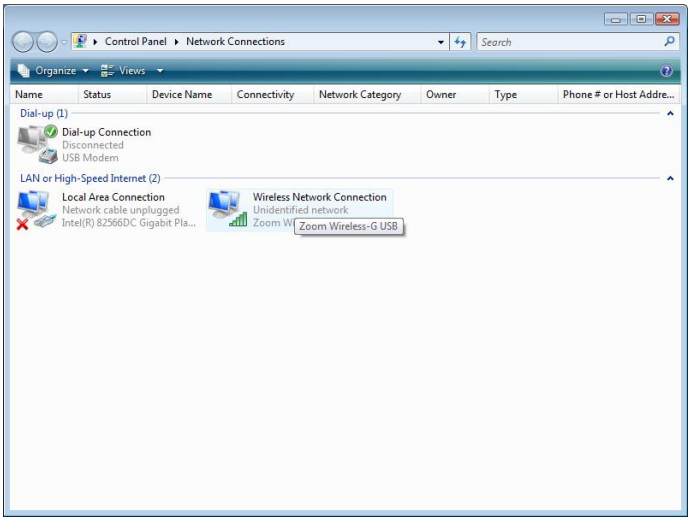
1 Follow these steps to open the **TCP/IPv4** or **TCP/IPv6 Properties** dialog box.

a From the desktop, click the **Start** button, select **Control Panel**, and then double-click **Network and Sharing Center**.

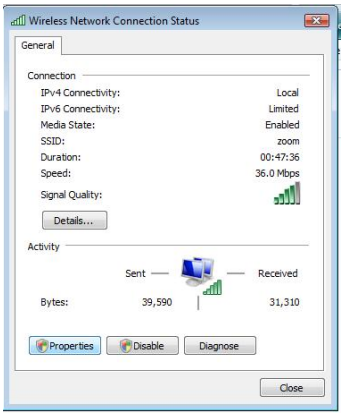
b In the **Network and Sharing Center** window, under **Tasks**, select **Manage Network Connections**:



c In the **Network Connections** window, double-click the **Wireless Network Connection** option:



d In the **Wireless Network Connection Status** dialog box, click the **Properties** button:



e In the **Wireless Network Connection Properties** dialog box, highlight the version of TCP/IP (Transmission

Control Protocol/Internet Protocol) that you are using and click the **Properties** button.

f To set static IP addressing, continue with Step 2 below. For dynamic addressing (DHCP), continue with Step 3 below.

2 **To set static IP addressing**: In the **TCP/IPv4** or **TCP/IPv6 Properties** dialog box, on the **General** tab, complete the following:

a Ensure that Obtain an IP address automatically is not selected. Then select the buttons labeled: Use the following IP address and Use the following DNS server addresses.

b If this is the first computer to be set up in the ad hoc network, enter **10.0.0.5** for an **IP address**. If you are adding it to an existing ad hoc network, increment the last digit by one, for example, **10.0.0.6**, **10.0.0.7**

c Enter **255.255.255.0** for **Subnet mask**. The **Subnet mask** should be the same for each computer in your ad hoc network.

d Enter **10.0.0.5** for **Default gateway** and **Preferred DNS server**. (This is the IP address of the first computer that was set up in your ad hoc network.) The **Default Gateway** and **Preferred DNS server** should be the same for each computer in your ad hoc network.

e Click **OK** twice.

That's it! You have set static IP addressing for a Windows Vista computer in an ad hoc network.

3 **For dynamic addressing (DHCP)**: To verify your DHCP settings, complete the following:

a Ensure that **Obtain an IP address automatically is** selected.

b Select either **Obtain a DNS server address automatically** or **Use the following DNS server addresses**. All text boxes for static IP addressing should be blank.

If you select **Use the following DNS server addresses**, enter your preferred and alternate server addresses.

c Click **OK** twice to exit.

That's it! You have verified your DHCP settings for a Windows Vista computer in an infrastructure network.

Windows XP

1 Follow these steps to open the **Internet Protocol (TCP/IP) Properties** dialog box.

a From the desktop, click the **Start** button, select **Control Panel**, and then click **Network Connections**.

b Right-click the **Wireless Network Connection** icon, and select **Properties**.

c In the **Wireless Network Connection Properties** dialog box, select **Internet Protocol (TCP/IP)** from the list, and click the **Properties** button.

d To set static IP addressing, continue with Step 2 below. For dynamic addressing (DHCP), continue with Step 3 below.

2 **To set static IP addressing**: Complete the following:

a Ensure that **Obtain an IP address automatically** is not selected. Then select the buttons labeled: **Use the following IP address** and **Use the following DNS server addresses**.

b If this is the first computer to be set up in the ad hoc network, enter **10.0.0.5** for an **IP address**. If you are

adding it to an existing ad hoc network, increment the last digit by one, for example, **10.0.0.6**, **10.0.0.7**

c Enter **255.255.255.0** for **Subnet mask**. The **Subnet mask** should be the same for each computer in your ad hoc network.

d Enter **10.0.0.5** for **Default gateway** and **Preferred DNS server**. (This is the IP address of the first computer that was set up in your ad hoc network.) The **Default Gateway** and **Preferred DNS server** should be the same for each computer in your ad hoc network.

e Click **OK** twice.

That's it! You have set static IP addressing for a Windows XP computer in an ad hoc network.

3 **For dynamic addressing (DHCP):** To verify your DHCP settings, complete the following:

a Ensure that **Obtain an IP address automatically** is selected.

b Ensure that either **Obtain a DNS server address automatically** or **Enable DNS** is selected. All text boxes for static IP addressing should be blank.

c Click **OK** twice to exit.

That's it! You have verified your DHCP settings for a Windows XP computer in an infrastructure network.

Windows 2000

1 Follow these steps to open the **Internet Protocol (TCP/IP) Properties** dialog box.

a From the desktop, click the **Start** button, point to **Settings**, then click **Network and Dial-up Connections**.

b Right-click the **Local Area Connection** icon, and select **Properties**.

c In the **Properties** dialog box, in the **Connect Using** box, make sure the **Zoom Wireless-N USB adapter** is displayed.

From the **Components** list, select **Internet Protocol** (**TCP/IP)** and click the **Properties** button.

d To set static IP addressing, continue with Step 2 below. For dynamic addressing (DHCP), continue with Step 3 below.

2 **To set static IP addressing**: Complete the following:

a In the Internet Protocol (TCP/IP) Properties dialog box, ensure that Obtain an IP address automatically is not selected. Then make sure the buttons labeled Use the following IP address and Use the following DNS server addresses are selected.

b If this is the first computer to be set up in the ad hoc network, enter **10.0.0.5** for **IP address**. If you are adding it to an existing ad hoc network, increment the last digit by one, for example, **10.0.0.6**, **10.0.0.7**

c Enter **255.255.255.0** for **Subnet mask**. The **Subnet mask** remains the same for each computer in your ad hoc network.

d Enter **10.0.0.5** for **Default gateway** and **Preferred DNS server**. (This is the IP address of the first computer that was set up in your ad hoc network.) The **Default Gateway** and **Preferred DNS server** should be the same for each computer in your ad hoc network.

e Click **OK** twice.

That's it! You have set static IP addressing for a Windows 2000 computer in an ad hoc network.

3 **For dynamic addressing (DHCP):** To verify your DHCP settings, complete the following:

a Ensure that Obtain an IP address automatically is selected.

b Ensure that either **Obtain a DNS server address automatically** or **Enable DNS** is selected. All text boxes for static IP addressing should be blank.

c Click **OK** twice to exit.

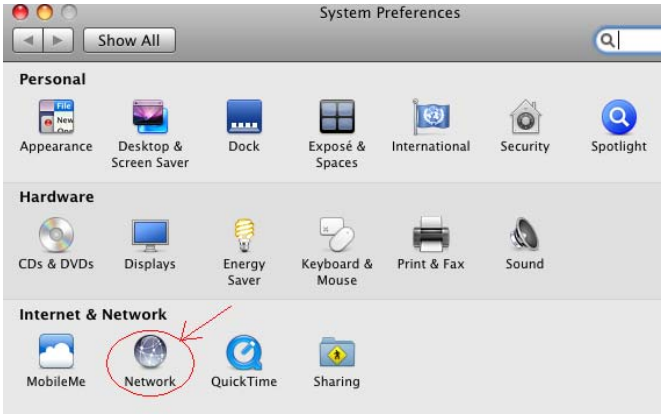
That's it! You have verified your DHCP settings for a Windows 2000 computer in an infrastructure network.

Mac

1 Follow these steps to open the **Network** dialog box.

a From the desktop, click the **Apple** logo, select **System Preferences**.

b Click on **Network**.



c Select the adapter icon from the menu on the left side of the screen.

d In the Network dialog box, the default setting is DHCP.

e To set static IP addressing, continue with Step 2 below. For dynamic addressing (DHCP), continue with Step 3 below.

2 **<u>To set static IP addressing</u>:** In the **Network** dialog box, complete the following:

a Click on the **Advanced** button. Make sure you are on the TCP/IP tab. In the **Configure 1Pv4** drop-down menu, select **Manually**.

b If this is the first computer to be set up in the ad hoc network, enter **10.0.0.5** for an **IP address**. If you are adding it to an existing ad hoc network, increment the last digit by one, for example, **10.0.0.6**, **10.0.0.7**

c Enter **255.255.255.0** for **Subnet mask**. The **Subnet mask** should be the same for each computer in your ad hoc network.

d Click on the DNS tab.

e Click on the plus sign (+) at the bottom of the box. Enter **10.0.0.5** in the text box **(**for **Router** and **DNS server)**.

(This is the IP address of the first computer that was set up in your ad hoc network.) The **Router** and **DNS server** should be the same for each computer in your ad hoc network.

f Click **OK**. Then click **Apply**.

That's it! You have set static IP addressing for a Mac computer in an ad hoc network.

3 **For dynamic addressing (DHCP):** To verify your DHCP settings, complete the following:

a In the **Configure IPv4** drop-down menu, ensure that **Using DHCP** is selected.

b The **Status** at the top of the window should say **Connected.**

c Close the dialog box by clicking on the red button (x) at the top left of the box.

d Click **Apply**.

That's it! You have verified your DHCP settings for a Mac computer in an infrastructure network.

Appendix B

Troubleshooting

➢ ***If your Zoom Wireless-N USB adapter is not working properly, try these steps:***

- Make sure the adapter is not damaged and that it is securely connected to the computer, either directly or through its short USB extension cable (which is included in the package).
- Perform a power cycle – take the following steps in the order given:
  1. Turn off the computer.
  2. Turn off your wireless access point or router, and wait a few seconds.
  3. Turn the access point or router back on.
  4. Turn on the computer.

     Windows Vista users: Try again to connect your wireless adapter to a network using Windows Networking.
- If you are using the USB extension cable, try changing the orientation of the adapter by twisting the semi-rigid USB extension cable to angle it toward the direction of the access point or router.
- Try the adapter in another USB port.
- Unplug other USB devices from your computer one at a time and see if that allows the adapter to work.
- If possible, try installing the adapter on another computer.

*If the problem does not seem to be hardware-related, click the Zoom icon on your taskbar to run the **Wireless-N USB** software.*

1. Check the **Configuration** tab to make sure that the **SSID** and **Network Type** settings for the adapter are the same as these settings for the other devices in your wireless network.
2. Then check the security settings to make sure that the adapter is configured for the same security system as the other devices in your

wireless network. Make sure that your security key is the same – remember that the keys are case-sensitive.

3 Check your TCP/IP settings by scrolling down to **Appendix A** and following the instructions.

4 If the adapter still does not work, uninstall the software and then re-install it. To do this, first go to the notification area of the taskbar (commonly found on the bottom right corner of your desktop), right-click and select the **Safely Remove Hardware** icon. Highlight **USB Mass Storage Device** and click **Stop**. In the next screen, click **OK**. Then click **OK** again and then click **Close** to exit the window. Now, you can physically remove the USB adapter from the USB port. Then select **Start**, **All Programs**, **Zoom Wireless-N USB**, **Uninstall Zoom Wireless-N USB**. Now you can re-install the Wireless-N USB software by following the instructions at the beginning of this manual by starting from **To install the Adapter** on page 6.

***Mac* users:** To uninstall, follow the instructions below.

- Insert the CD that came with the package into your CD or DVD drive. Open the folder associated with your Mac OS X (either 10.3, 10.4, or 10.5)
- Select the **Uninstall** icon and double-click to open the file. Follow the instructions on the screen.
- Restart your computer.
- Now, unplug the Adapter.
- If you want to reinstall, follow the installation instructions in Section 4:on page 35.

If the above solutions do not work, consult Technical Support. Please see **Appendix C: Zoom Technical Support Services** on page 71.

Appendix C

Zoom Technical Support Services

Zoom has a variety of technical support services available to our customers. We strive to provide convenient, professional support responsive to our customers' needs and capabilities. If you find yourself unable to get your Zoom product to operate, and you have thoroughly reviewed your owner's manual and all relevant documentation, please feel free to contact us for help.

For your records, and to facilitate Technical Support from either your equipment supplier or Zoom, please record the following information when you receive your Zoom product.

Product Information

Product Name

_____

Product Model Number

_____

Product Serial Number

_____

Date Installed

_____

The serial number (S/N) is located on the adapter next to the S/N barcode. Please be sure to write the number down. This will greatly speed up your service and insure that the service representative is addressing the proper Zoom product.

Calls to Zoom's voice technical support staff are the most time consuming, and at times you may find it difficult to get through. We do not want you left on hold for long periods of time, so we limit the queue length. We recommend that you take the time to familiarize yourself with the other services described in this section before calling. Many questions can be answered more quickly using e-mail or our World Wide Web Home page.

World Wide Web

Zoom's Web page lets you send email for assistance, register on-line, access product reviews and descriptions, and do a whole lot more. Visit the Zoom Technical Support area for the latest Flash Files and Drivers for your Zoom Product. To access Zoom's Web page, please log onto your local Internet Service Provider, then go to the Web browser and select: **www.zoom.com**

From Zoom's home page you can easily go to Technical Support or many other useful areas.

Smart Facts™ Q&A Search Engine (English Only)

Smart Facts™ is an automated intelligent database of Frequently Asked Questions (FAQ's) about Zoom products. It allows you to search for solutions to your Technical Support questions, by product or via a powerful Keyword Search Engine. If you still cannot find a solution to your question, SmartFacts lets you access our Technicians via email for a personalized response. SmartFacts provides you with a way to track the history of your problem and to add or change the description without having to enter any information that was previously sent. SmartFacts can even contact you automatically if there is an update to your hardware or software that helps to address the question you had. You can access SmartFacts from **www.zoom.com/techsupport**

Contact Zoom by Email

You can email Zoom with any tech support questions you might have and one of our Technical Support Engineers will respond by email within 2 business days. You may request personal assistance via email at www.zoom.com/techmail. When emailing Zoom, be sure to include the following:

- Serial number of your adapter
- Your full name and address
- A detailed description of your problem

Contact Zoom by Phone

You can reach Technical Support by calling these numbers:

In the United States, call **(617) 753-0961**.

In the UK, call

London: +44 2033180660 **or**

Manchester: +44 1618840074

Certain other countries can dial an in-country number to reach Zoom Technical Support:

Portugal: **+35 1221451012**

Spain: **+34 911516304**

Switzerland: **+41 435000369**

Return of Defective Units

Please contact your local distributor or reseller for Factory Authorized Repair or Replacement of your **In-Warranty Defective Product**. If you are unable to reach your distributor, you can contact the Zoom Factory Customer Service by calling:

US: (617) 753-0023

UK: *London:* +44 2033180660

UK: *Manchester:* +44 1618840074

Please note that the customer is responsible for any charges (including brokerage or customs and duties) associated with shipping the defective unit to Zoom for repair. During the first year Zoom will pay return shipping to the customer by common carrier. After the first year the customer may be required to pay a shipping and handling fee. Any applicable customs, duties and brokerage charges to import the product are the responsibility of the customer. Zoom encourages all customers to return defective units to their respective reseller whenever possible.

Appendix D

Regulatory Information

U.S. FCC Part 15 Emissions Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

IMPORTANT NOTE:

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Industry Canada Emissions Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device.

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community.

Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

Note: The user must ensure that the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

- This device will automatically limit the allowable channels, as determined by the setup program during installation, by examining the operating system's current country of operation. If the country of operation is not determined, the device will default to US settings. Use of the incorrect country of operation may result in operation not in accordance with local regulations, and may cause harmful interference to other systems. The user is obligated to ensure that the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document. If configured incorrectly, you can contact technical support for instructions on changing the device's spectrum usage.
- This device may be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1 - 13, except where noted below.
  - In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
  - In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
  - In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

Electrostatic Discharge Statement

The unit may require resetting after a severe electrostatic discharge event.

Declaration of Conformity

Declaration of Conformity
Déclaration de conformité
Konformitätserklärung
Dichiarazione di conformità
Declaração de Conformidade
Konformitetsdeklaration

Overensstemmelseserklæring
Conformiteitsverklaring van de EU
Δήλωση Συμμόρφωσης
Deklaracja zgodności
Declaración de conformidad
Cam kết về sự tuân thủ ở Châu Âu

Manufacturer/Producent/Fabrikant/ Constructeur/Hersteller/Κατασκευαστής/ Fabbricante/ Fabricante/Tillverkare/ Nhà sản xuất	**Zoom Telephonics, Inc.** **207 South Street** **Boston, MA 02111 USA / 617-423-1072** **www.zoom.com**
Brand/Varemærke/Merk/Marque/Marke/ Μάρκα/Marchio/Marka/Marca/Thương hiệu	**Zoom Wireless-N USB Adapter**
Type/Typ/Μάρκα/Tipo/Kiểu mẫu	**Model 4411 Series 1077**

The manufacturer declares under sole responsibility that this equipment is compliant to Directive 1999/5/EC (R&TTE) via the following. This product is CE marked.

Producenten erklærer under eneansvar, at dette udstyr er i overensstemmelse med direktivet 1999/5/EC (R&TTE) via følgende. Dette produkt er CE-mærket.

De fabrikant verklaart geheel onder eigen verantwoordelijkheid dat deze apparatuur voldoet aan Richtlijn 1999/5/ EC op grond van het onderstaande. Dit product is voorzien van de CE-markering.

Le constructeur déclare sous son entière responsabilité que ce matériel est conforme à la Directive 1999/5/EC (R&TTE) via les documents ci-dessous. Ce produit a reçu le marquage CE.

Hiermit erklärt Zoom die Übereinstimmung des Gerätes modem mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EC (R&TTE). Dieses Produkt ist das gekennzeichnete CE.

Ο κατασκευαστής δηλώνει με αποκλειστική του ευθύνη ότι αυτό το προϊόν συμμορφώνεται με την Οδηγία 1999/5/EC μέσω των παρακάτω. Αυτό το προϊόν φέρει τη Σήμανση CE.

Il fornitore dichiara sotto la sola responsabilità che questa apparecchiatura è compliant a 1999/5/EC (R&TTE) direttivo via quanto segue. Questo prodotto è CE contrassegnato.

Producent stwierdza że to urządzenie zostało wyprodukowane zgodnie z Dyrektywą 1999/5/EC (R&TTE). Jest to potwierdzone poprzez umieszczenie znaku CE na urządzeniu.

O fabricante declara sob sua exclusiva responsabilidade que este equipamento está em conformidade com a Directiva 1999/5/EC (R&TTE) através do seguinte. Este produto possui Marcação CE.

El fabricante declara bajo su exclusiva responsabilidad que este equipo satisface la Directiva 1999/5/EC (R&TTE) por medio de lo siguiente. Este producto tiene marca CE.

Nhà sản xuất cam kết với trách nhiệm của mình là thiết bị này tuân theo Hướng dẫn 1999/5/EC (R&TTE) thông qua các mục sau. Sản phẩm này được đánh dấu là CE.

EN 60950-1:2001/A11:2004 /IEC 60950-1:2001 /
EN 301 489-1, v1.61: 2005-09; EN 301 489-17, v1.2.1: 2002-08 /
EN 61000-4-2 : 1995 + A1 : 1998 + A2 : 2001 / EN 61000-4-3 : 2002 + A1 :2002/ EN 61000-4-4 :2004 / EN 61000-4-5 : 1995 + A1 : 2001 / EN 61000-4-6 :1996 + A1 : 2001/
EN 61000-4-11 : 2004 /
EN 300 328, v1.7.1: 2006 / EN50385:2002/ EN 55022:2006/EN 61000-3-2:2006 / EN 61000-3-3:1995 + A1 : 2001 + A2 : 2005 /

Paul Prohodski
25 November, 2009
1077/TF, Boston, MA, USA

Director, /Direktør, /Director, /Directeur /Direktør, /Διευθυντής, /Direttore, /Dyrektor /Director, /Director, Đốc

NOTICE

The manufacturer does not warrant that the hardware will work properly in all environments and applications, and makes no warranty or representation, either expressed or implied, with respect to the quality, performance, merchantability, or fitness for a particular purpose of the software or documentation. The manufacturer reserves the right to make changes to the hardware, software, and documentation without obligation to notify any person or organization of the revision or change.

All brand and product names are the trademarks of their respective owners.

Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.