PixelPoint®

WiFi Networking

Best Practices

Initial Release 07/16/2014

Powering Better Guest™ Experiences

Publication Details

Trademarks
PixelPoint, ParTech, and their respective logos are all trademarks of PAR Technology Corporation.

PAR may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document.

Except as expressly provided in any written license agreement from PAR, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft® and Window s® are registered trademarks of Microsoft Corporation in the United States and/ or other countries. Other product names may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Disclaimer
PAR has thoroughly reviewed this document and believes it to be reliable. However, this document is provided for informational purposes only and PAR makes no warranties, either expressed or implied, in this document. Information in this document is subject to change without notice. Risk of use and responsibility for the results of use of this document lie with the user.

Patents
The following patents apply to some areas of functionality within the PixelPoint software suite: Pat. 6,384,850; 6,871,325; 6,982,733; 8,146,077; 8,287,340

Table of Contents

Overview

WiFi Networks can pose a serious security risk even when correctly configured. Because of wireless devices offering simplified setup methods for easy use and wizard setup programs, WiFi networks can become a target for intrusion.

This quick guide is intended to minimize intrusion risk through common wireless security configuration best practices.

This document refers to configuration setting within a D-Link wireless router as an example only. Configuration interfaces may vary by wireless networking device.

WiFi Networking Best Practices

- Use WPA2 Personal Wireless passwords
- Hide the SSID name
    - Avoid Obvious SSID names such as "D-Link" or "Cisco"
- Disable Guest Mode
- Use MAC Filtering
- Enable Access Point firewall
- Update firmware
- Change the default WAN IP address
    - Avoid the standard. For example: 192.168.0.1
- Change the Access Point admin password to a complex password
- Avoid standard ports
    - RDP uses port 3389
    - Sybase uses port 2638

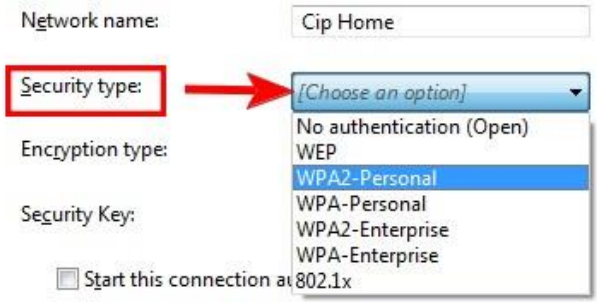
Mobile Device (Handheld or Tablet)

- In power settings, disable sleep mode
- Disable Bluetooth
- Modify low battery settings to not disable wireless below a usable threshold
- NIC Adaptor Settings
- Disable "Look for other networks while connected"
- Activate "Connect even if SSID not broadcasting name"
- Disable "Minimum Power Consumption"
- Disable "Afterburner"
- Reduce "Fragmentation Threshold"
- Set Roam Tendencies to Conservative
- Set Roam Decision to Optimum Distance
- Set Power Output to 100

Secure Setup

Wifi networks can be setup with three common security protocols: WEP, WPA, and WPA2. WEP is now a deprecated protocol as the systems using this network type are easily compromised. WEP Networks are no longer to be considered secure.

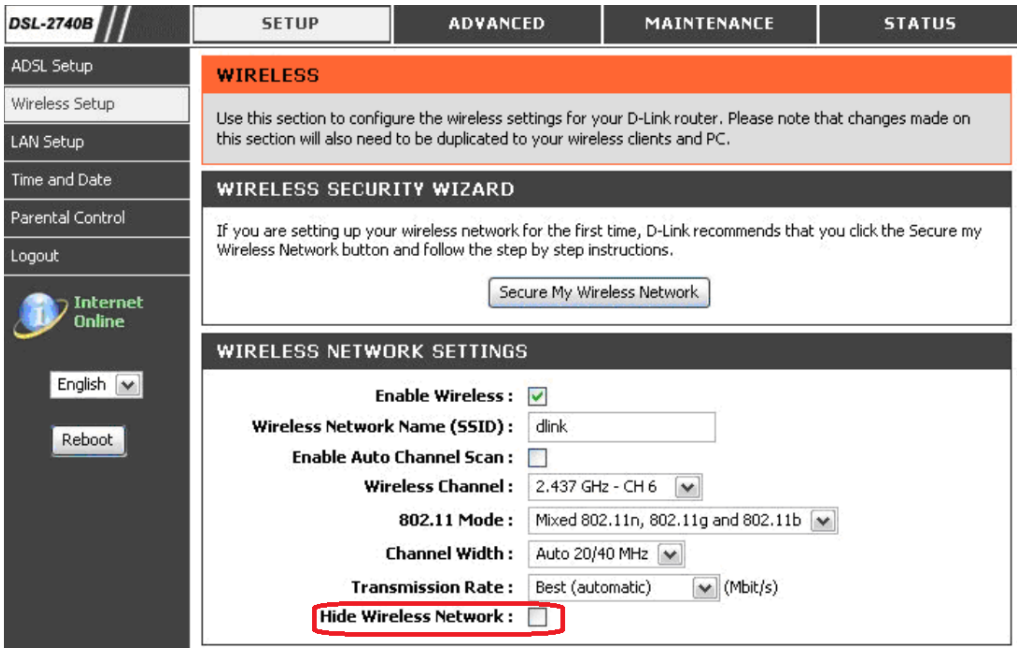
As such, all networks should be setup with a WPA2 security protocol, using WPA2-Personal Wireless passwords.



Additionally, if the router or access point has a built-in firewall, enable it.

Hide the SSID Name

For additional security, disable to visibility of your Wifi network, by hiding the SSID. Do this by entering the router menu in a browser window. Enter the Router's IP address in the address bar (Router IPs are displayed on the side or bottom of the router unit.) In the menu, under "Setup", "WirelessSetup" or "Settings" should be a check box option for "Hide Wireless Network." Check the box and click [Save], or [Apply], and restart the router.

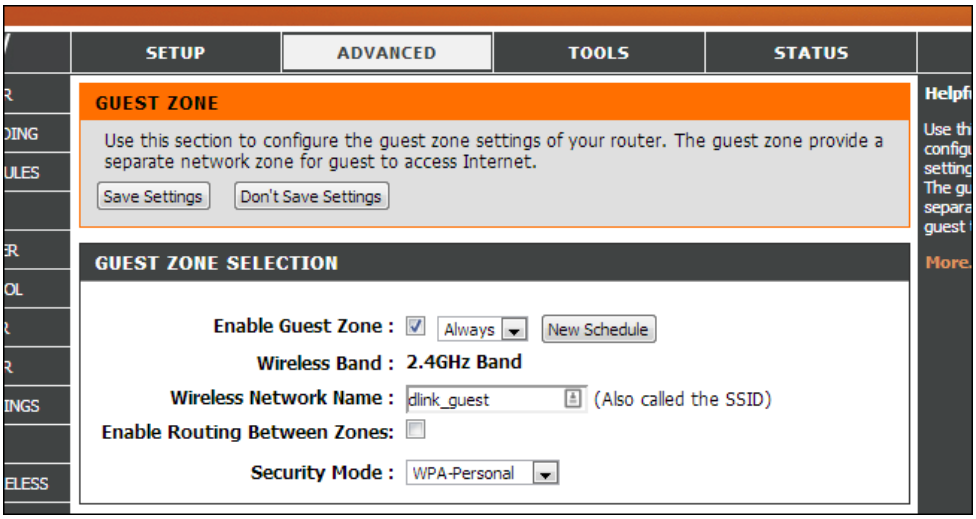


Note: The examples pictured show settings for a D-Link wireless router. Configuration interfaces may vary by wireless networking device.

Wireless networks will typically be assigned a default name by the router. Names like "D-link', "Cisco", or "Linksys" are very common and should be changed to avoid being guessed. Any access to a router, even limited access, can present a potential security threat.

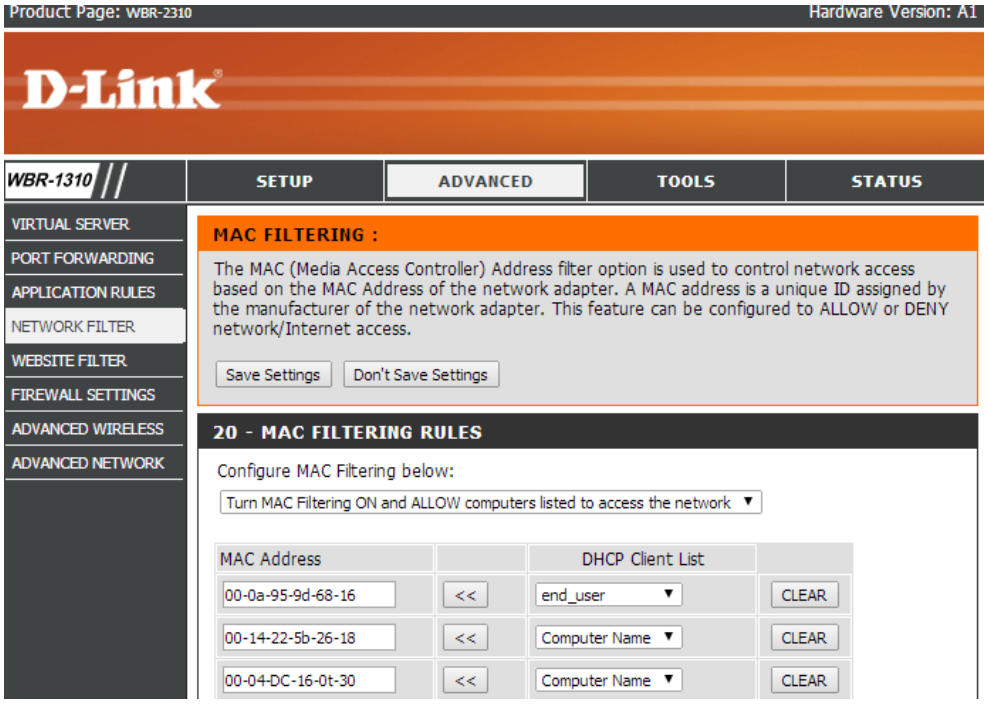
Disable Guest Mode

Some routers may be configured with a Guest Mode, a separated WiFi network with limited access. This mode should be disabled for greater security. In most cases, the option is located in the router menu under "Advanced", or "Admin Settings."



Use MAC Filtering

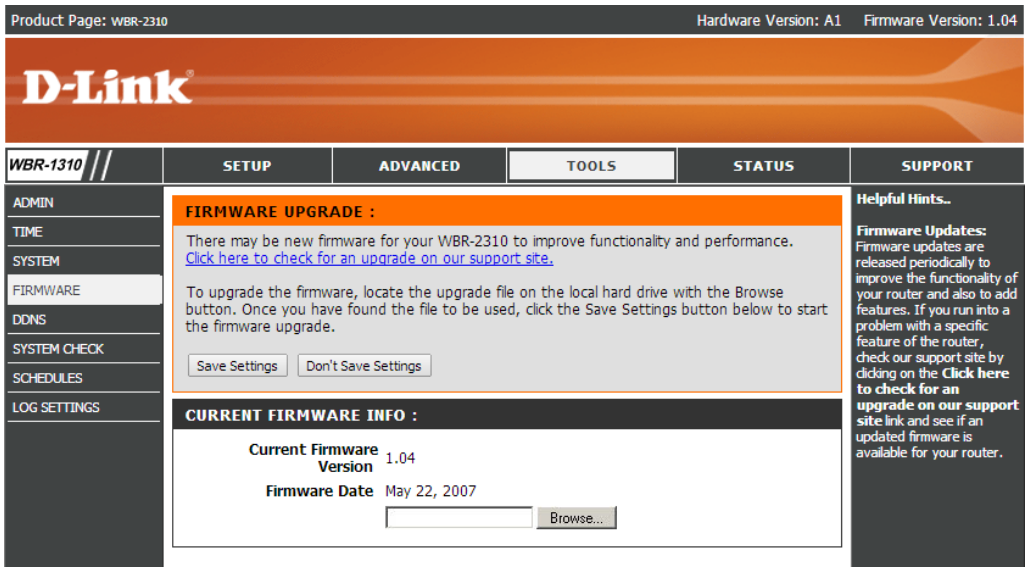
MAC Filtering allows a network to allow only computers, which are specifically authorized to access the network. Alternatively, MAC Filtering may deny a specific MAC Address from accessing the network.



Router Settings

Update Firmware

Once the network is setup, update the router's firmware. Most makes and models should have a simple wizard to check the current version and download updates, if necessary.



Change the Default WAN IP Address

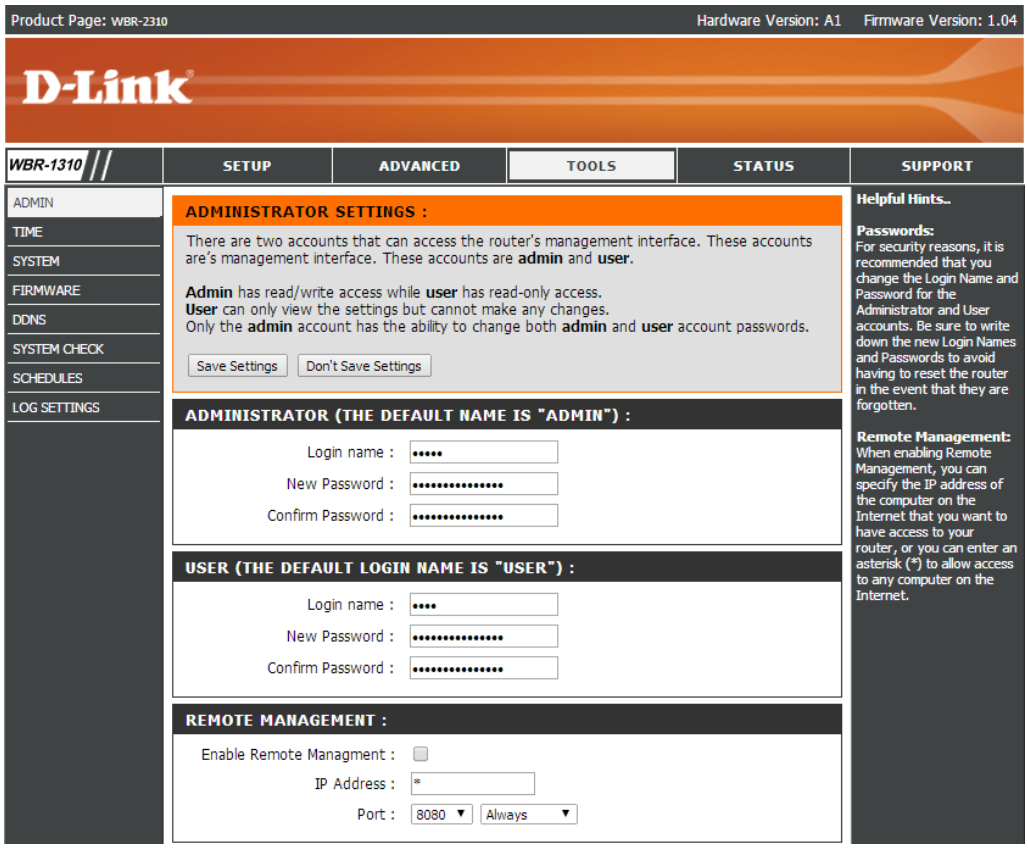
Avoiding the standard IP address on routers (for example 192.168.0.1) can help prevent unwanted intrusion into your router, even if your network is otherwise protected. Altering your router's IP address will likely require you to alter the IP address of the computers connecting to it. IP address must be set with a certain parameters:

- Four sets of three numbers
- Number sets are separated by a period
- The highest possible value for one number set is 255
- Zeroes before a number can be excluded (eg. 001=1)
- Computers on the network use the same first three sets of numbers and a fourth set between 0 and 255

Valid	Not Valid
138.5.22.746	199.182.876.1

Change the Access Point Admin Password

Routers have standard login information for altering settings. This login info is usually a login name of "Admin" and often a blank password or a password that is easily guessed, such as "Admin" or "Dlink".



Avoid standard ports

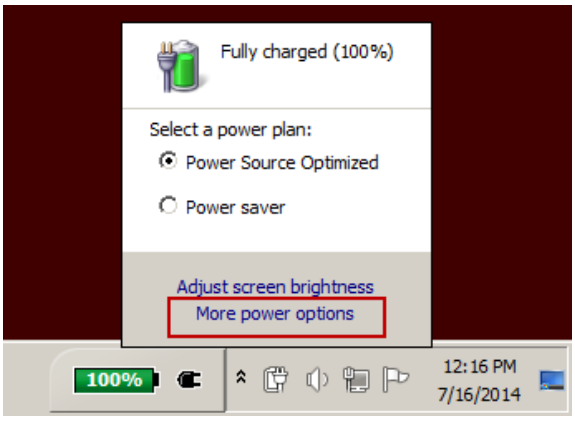
Some regularly used programs are configured to use the same port; for example: Remote Desktop uses port 3389, and Sybase uses port 2368. By reconfiguring these programs to use a different port a network can be made more secure. This dissuades outside devices from scanning for openings in these common ports. The installation wizards of these programs will likely allow for customization of the ports the program uses. If the wizard does not allow to change ports or if the program is already installed, ports should be changed in the settings or properties menu of those programs.

Mobile Device Settings

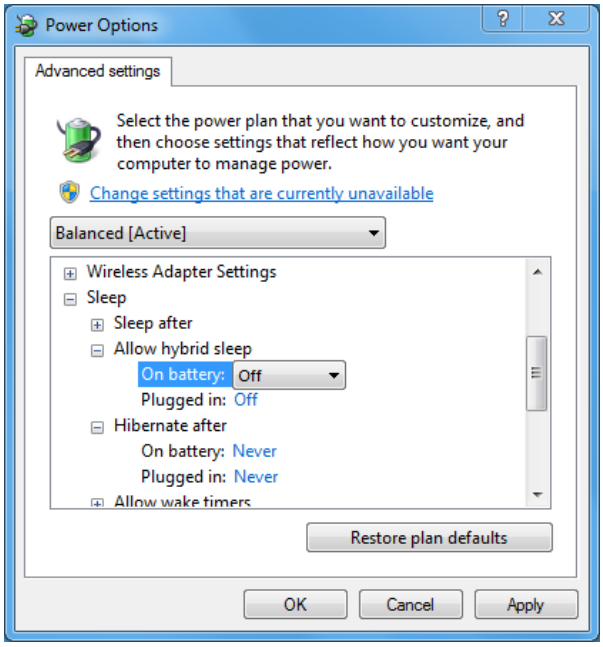
Mobile devices such as tablets and wireless handhelds should be configured with specific settings to help avoid unwanted intrusion to a network through the mobile device if an authorized user. Different devices may have different methods for changing these settings, but most should be close to the processes below.

Power Settings

Access the power settings on notebook computers through the battery icon in the start menu and select More Power Options.



Look through the power settings and change the options to avoid sleep while the unit is in use, even if the lid is closed.



For a mobile phone or tablet, modify battery settings, so the phone does not disable wireless. This is usually accomplished in the Advanced section of the WiFi Settings of the mobile device.

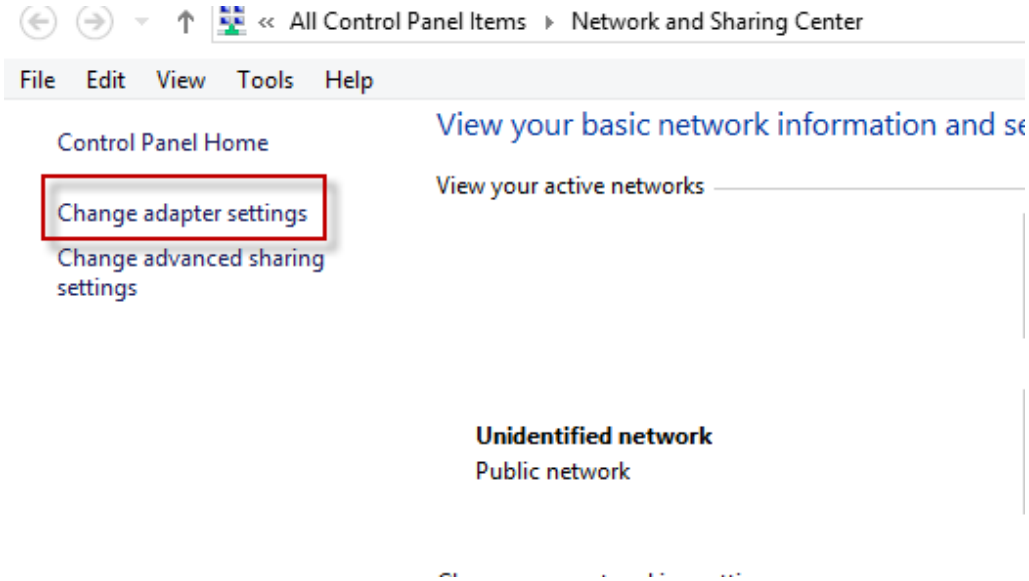
Disable Bluetooth

Phones and mobile devices with Bluetooth enabled provide a means of intrusion by other Bluetooth enabled devices. Disable Bluetooth by going into the Wireless & Network Settings menu and ensuring the Bluetooth setting is unchecked. Different phones and devices may have slightly different names for the menu and the display may vary slightly. Alternatively, some devices will have an icon setting in the main screen for enabling or disabling device settings. Ensure this setting is disabled.

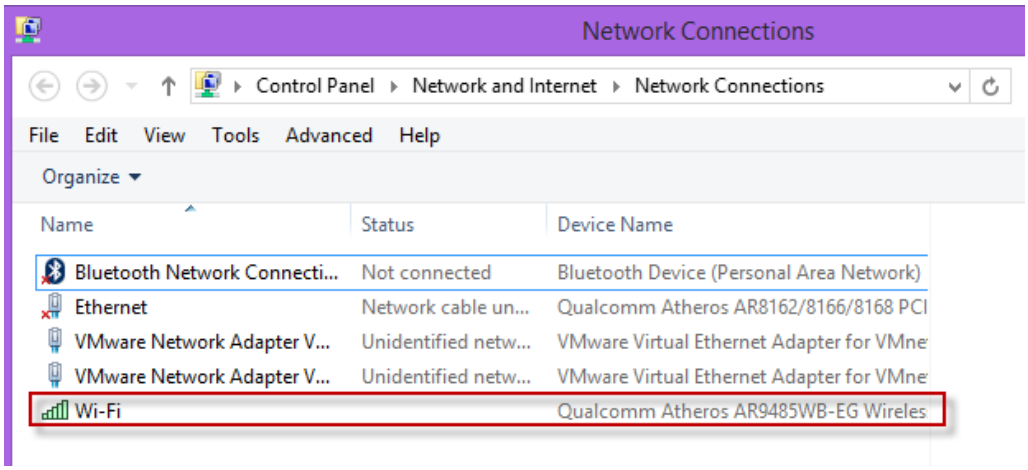
Note: The above example shows settings within an Android-based device. Settings menus may vary by wireless device.

NIC Adapter Settings

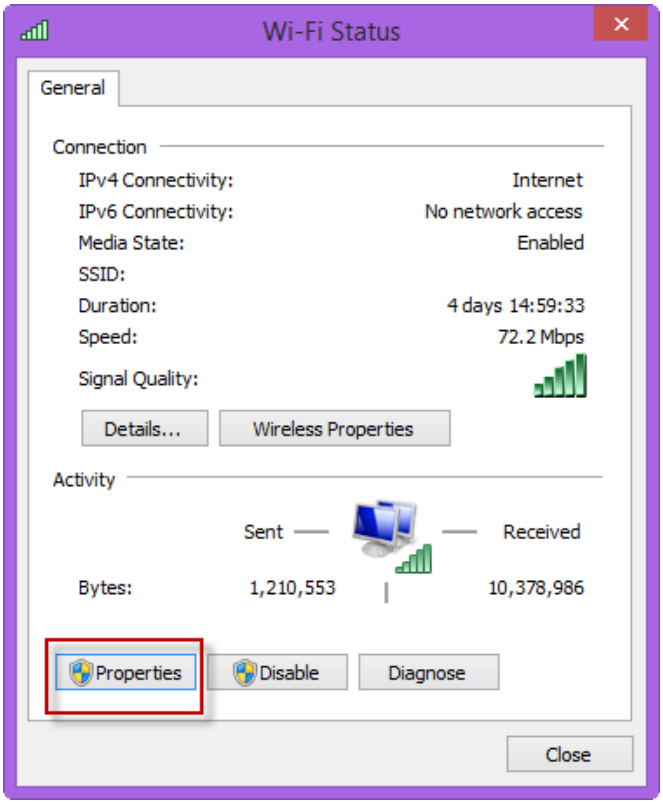
1. In the Network and Sharing Center, click Change adapter settings.



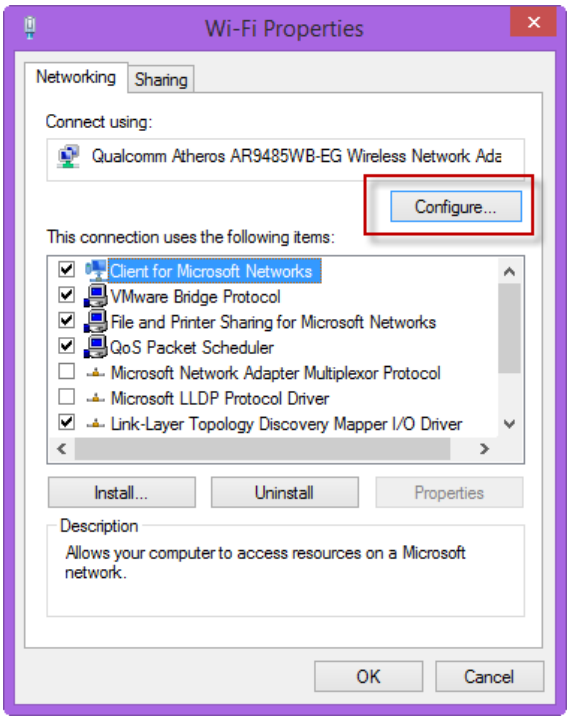
2. Select your WiFi Adapter.



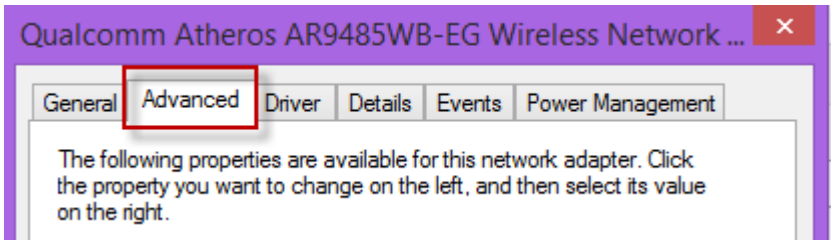
3. Click [Properties].



4. Click Configure.



5. Click the Advanced tab.



While in the advanced tab look for the following settings and modify them as indicated:

- Disable "Look for other networks while connected"
- Activate "Connect even if SSID not broadcasting name"
- Disable "Minimum Power Consumption"
- Disable "Afterburner"
- Reduce "Fragmentation Threshold"
- Set Roam Tendencies to Conservative
- Set Roam Decision to Optimum Distance
- Set Power Output to 100