

The AP/router being used to setup WPA Personal is the WRT54GL, as shown below.

The following assumptions are being made:

- The AP/router is out of the BOX or it has been reset to factory settings (The administration tab has the configuration management options, or press the reset button located in the back of the router's case)
- The latest AP/Router firmware revision is being used (in our case it is 4.30.5 for the WRT54GL V4)
- The wireless NIC in the PC/laptop card can handle WAP encryption, Windows XP is patched to SP2 level, or Windows 2000 is patched to SP4.
- All the instructions pertain to the WRT54GL, all Cable/aDSL routers have similar settings.
- The PC used to configure the router can link to it using the wireless media, hence first we configure the router first, we will loose connectivity but when we will reconnect to it one the wireless NIC is configured. If more than one PC is being used. The PC responsible for configuring the router must be plugged in to the LAN side.

Two steps are involved:

- Setup the AP
- Setup the Wireless NIC

Setup the AP

The router by default has the DHCP server function enabled, and it will automatic setup your NIC to an address starting at 192.168.1.100

The screenshot shows the Linksys WRT54GL configuration interface. The top navigation bar includes 'Wireless', 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Wireless Security' section is active, showing the following settings:

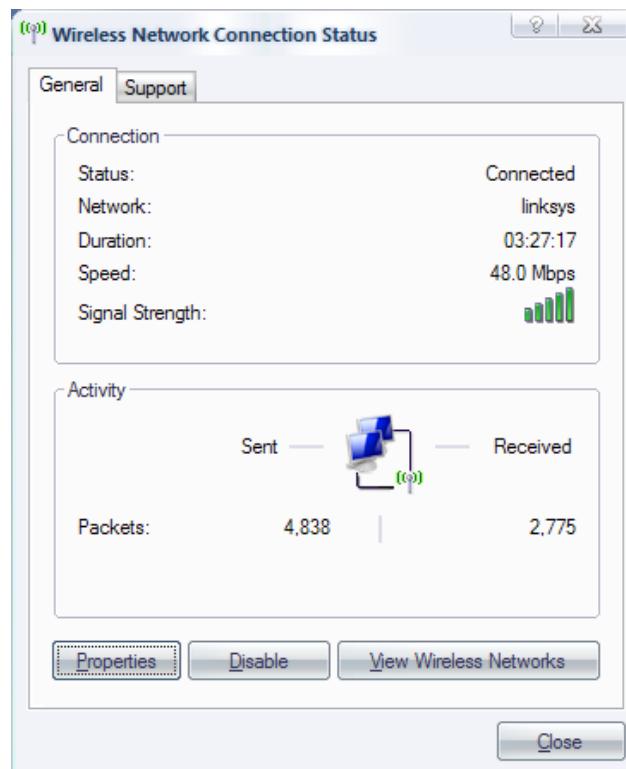
Security Mode:	WPA Personal
WPA Algorithms:	AES
WPA Shared Key:	1234567890
Group Key Renewal:	3600 seconds

At the bottom of the configuration area are 'Save Settings' and 'Cancel Changes' buttons. A sidebar on the right contains a 'Security Mode' warning: 'You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate. More...'. The Cisco Systems logo is visible in the bottom right corner.

Open your browser, point it to 192.168.1.1, login to the router, click on Wireless, then wireless security. Use the values shown in the image above. Once you click on "Save Settings", you might loose connectivity over the wireless connection. The WPA Shared key is only a suggestion, it is not to be used for production purposes.

Setup the Wireless NIC

Open your wireless connection status, you can go to control panel, or find the small wireless connection icon located in the information area (the PC clock at the right side of the task bar). Double click on the small icon. In either case, a window similar to the one shown on the right should come up. Click on “Properties”

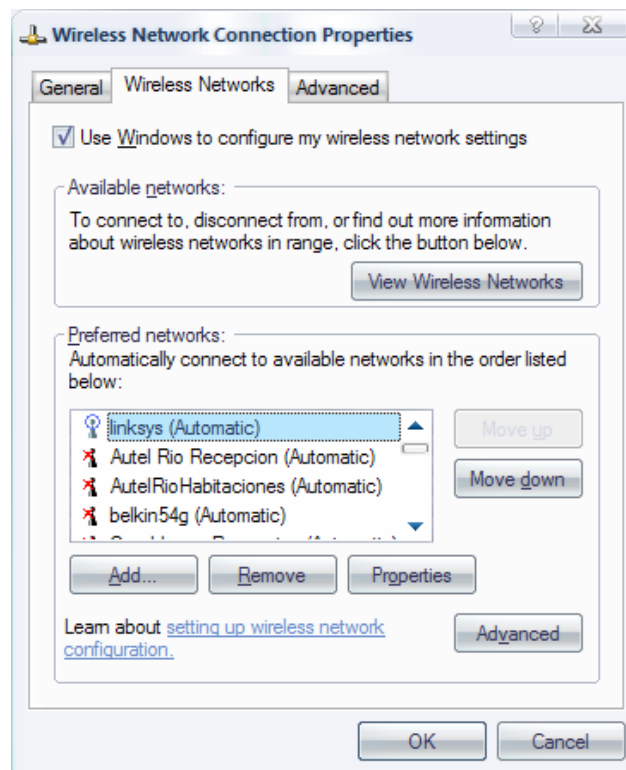


There are two choices here:

You can choose add.

You can click on linkys, shown within the list of “Preferred networks”, then click on “Properties”

If you use the second choice, the next screen come up.



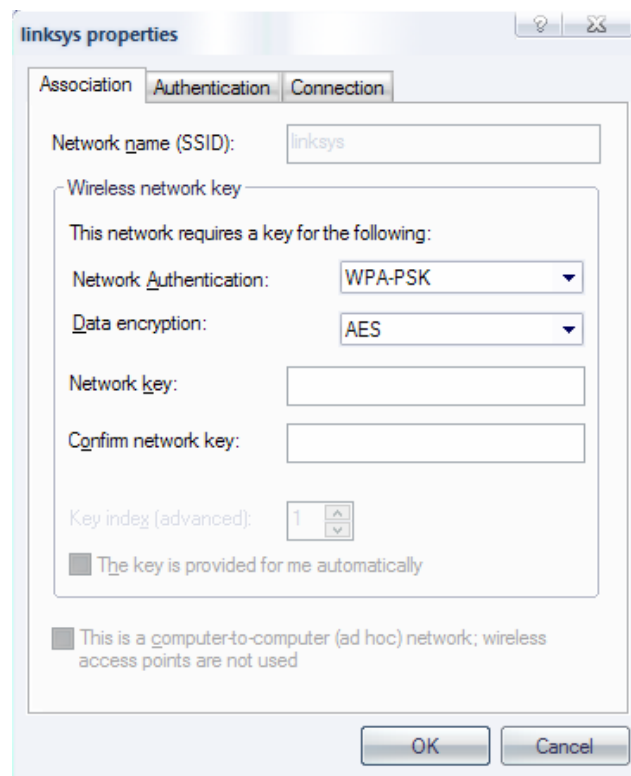
For the network name (SSID) make sure you type (or see linksys), this will depend on the settings of your router.

For network authentication, choose WPA-PSK (pres-shared key)

The data encryption is set to AES, AES is used by the US government.

The network key is the same as the one used in the router {1234567890}

After this, all is ready, click on OK on all the screens, and you are ready to connect!!!!



In summary, WAP accomplishes several goals:

- Ensures only authorized users connect to the AP, although it is susceptible to dictionary attacks.
- Ensures nobody can view the contents of the frames being transmitted between the AP and your PC.

What is not being accomplished:

- The connection is not secured from eavesdropping as it travels through other network segments unless the packets are encrypted by other means (such as a VPN)
- The computer must be protected in regards to virus, web surfing habits, and other related precautions.