Securing your Linksys WRT54G

Abstract

Current implementations of the 802.11b and 802.11g wireless LAN standards have several potential pitfalls for security. However, built in security mechanisms in these protocols can be used to mitigate most security risks for SOHO users.

Out of the box, the Linksys Wireless Router default configuration is insecure. However functionality built into the product can be used to greatly enhance the security of this device. This paper examines how to configure the Linksys Wireless Router, WRT54G, in a manner which will maximize the security of your Wireless LAN

©2005 Richard Wanner. All rights reserved.

Table of Contents

Table of Figures

©2005 Richard Wanner. All rights reserved.

Introduction

Wireless networks are becoming increasingly common due to the ease and cost of deployment of the LAN using wireless technologies. Wireless networks provide different challenges than wired networks, especially in securing data in transit between the client and the wireless access point. The common wireless standards, provide mechanisms for securing wireless data, and despite the limitations of the wireless, when the provided mechanisms are deployed and maintained in a systematic manner data can be secured against all but the most determined and patient attacker.

This paper describes security strategies for the Linksys Wireless Router, model WRT54G, Version 2. Specifically the WRT54G running firmware version 3.03.6. Other firmware versions may have slight variances in functionality, but the general principles should apply.

This paper assumes the user is familiar with the Linksys web-based management interface, and how to use a web browser.

Configuration Recommendations

For the Linksys Wireless Router WRT54G I recommend the following configuration settings to secure your wireless LAN.

1. Configure Management Parameters
2. Configure Basic Wireless Parameters
3. Reset default SSID
4. Disable SSID Broadcast
5. Change from default channel
6. Enable MAC Address Filtering
7. Enable Encryption

The following sections will describe why and how you should do these steps.

Configure Management Parameters

The changes in this section are all performed from the “Administration” tab under “Management”. The following steps are in this section:

1. Reset administration password
2. Enable secure management
3. Disable management via wireless
4. Disable Remote Management
5. Disable UPnP (Universal Plug and Play)

Reset Admin Password

From the factory the Linksys Routers with a default password of “admin”. The Linksys Wireless Router uses a web based interface, and this interface is

©2005 Richard Wanner. All rights reserved.
For information contact cerberus@whitehats.ca or rwanner@pobox.com.

accessible to anyone on your network. Because this is a wireless network, anyone who can access your network may be able to access the GUI interface and attempt to make changes. By setting the password we will at least be able to prohibit unwelcome users from reconfiguring the device. The password can be up to 63 characters.

Enable Secure Management

Shortly before the release of this firmware a new management feature was added, which at the time of writing was still undocumented. All previous Linksys have only supported web management via HTTP. A welcome addition in this version is the ability to manage the router securely via HTTPS. To enable this functionality simply click the check mark beside HTTPS. Please note that the management URL will change from http://access-point-ip/ (http://192.168.1.1 by default) to https://access-point-ip/ (https://192.168.1.1/ by default).

Disable Management via Wireless

Another new feature in the 3.0+ firmware is the ability to disable management of the router via wireless devices associated with the access point. By default if someone manages to associate with your access point and login to your router (difficult if the device is securely configured), they can change the configuration of the router. My recommendation is that you have a web-enabled computer hardwired to the router, then disable this and use that machine only for management. If you don’t have any hardwired devices then leave “Wireless Access Web” enabled.

Disable Remote Management

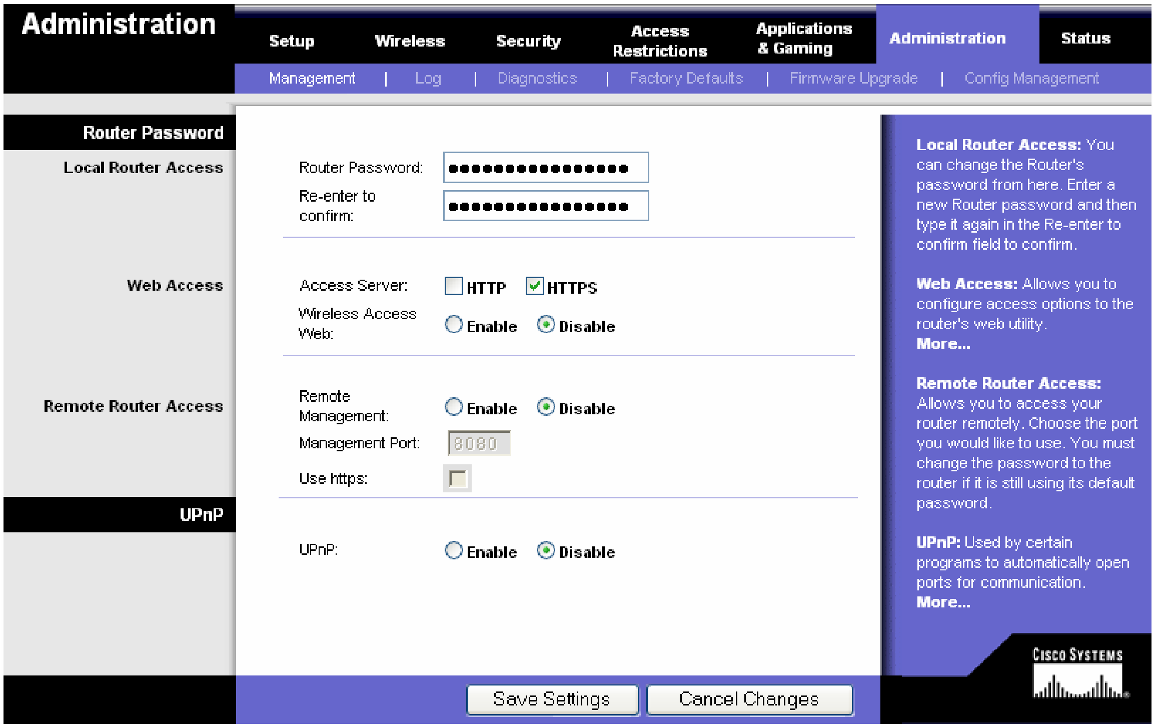
Remote Router Access permits web-based management of the wireless router from external networks such as the Internet. By default this feature opens port 8080/TCP on the external side of the router. This feature provides significant risk to the device, by permitting an attack vectorand more importantly your internal network. It should be disabled unless remote management is absolutely required.

Disable UPnP (Universal Plug and Play)

UPnP stands for Universal Plug and Play. I cannot think of a valid reason why UPnP functionality would be required on when this device is used as a perimeter router.

The screen below shows the configuration of this screen with all changes applied. Don’t forget to click “Save Settings” to apply your changes.

©2005 Richard Wanner. All rights reserved.



Local Router Access

Router Password: ●●●●●●●●●●●●●●●●

Re-enter to confirm: ●●●●●●●●●●●●●●●●

Web Access

Access Server: ☐ HTTP ☑ HTTPS

Wireless Access Web: ○ Enable ● Disable

Remote Router Access

Remote Management: ○ Enable ● Disable

Management Port: 8080

Use https: ☐

UPnP: ○ Enable ● Disable

Local Router Access: You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

Web Access: Allows you to configure access options to the router's web utility. **More...**

Remote Router Access: Allows you to access your router remotely. Choose the port you would like to use. You must change the password to the router if it is still using its default password.

UPnP: Used by certain programs to automatically open ports for communication. **More...**

Figure 1 – Management Screen

While you are on this screen, ensure that Remote Router Access and UPnP are disabled.

Configure Basic Wireless Parameters

The changes in this section are all performed from the "Wireless" tab under "Basic Wireless Settings". The following steps are in this section:

1. Configure Network Mode
2. Set SSID from default
3. Set Wireless Channel from default
4. Disable SSID Broadcast

Configure Network Mode

The "Wireless Network Mode" details what type of wireless NICs, more specifically what wireless protocols, are permitted to connect to the router. The choices are "Disabled", "Mixed", "B-only", and "G-only". "Disabled" disables the wireless access point built into the router. "Mixed" permits both 802.11b and 802.11g NICs to associate to the access point. "B-only" restricts access to just 802.11b NICs. "G-only" does the same thing only for 802.11g NICs.

My recommendation is that you pick the option that is most restrictive for your environment. In my case all of my wireless NICs are 802.11g, so I have set the access point to "G-only".

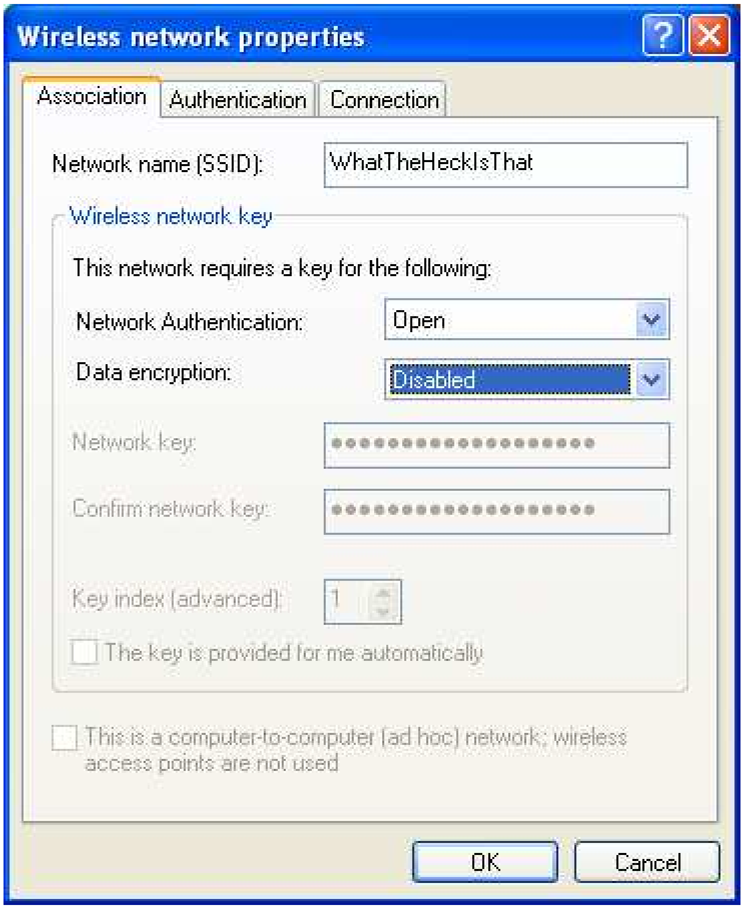
©2005 Richard Wanner. All rights reserved.

Set SSID from default

The service set identification (SSID) defines a network name for your wireless network. In order to communicate the access point and the client's wireless interface must specify the same SSID. The Linksys wireless access points ships with a default SSID of "linksys" The SSID is easily sniffable, but changing it will at least deter the casual attacker.

The SSID can be up to 32 characters in length.

Be sure to change the SSID in all of your computers to match the new one in the router. It can be set on the Wireless Network Properties Screen.



Network name (SSID): WhatTheHeckIsThat

This network requires a key for the following:

Network Authentication: Open

Data encryption: Disabled

Network key: ••••••••••••••••••••

Confirm network key: ••••••••••••••••••••

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Figure 2 – Wireless Network Properties Screen

Set Wireless Channel from default

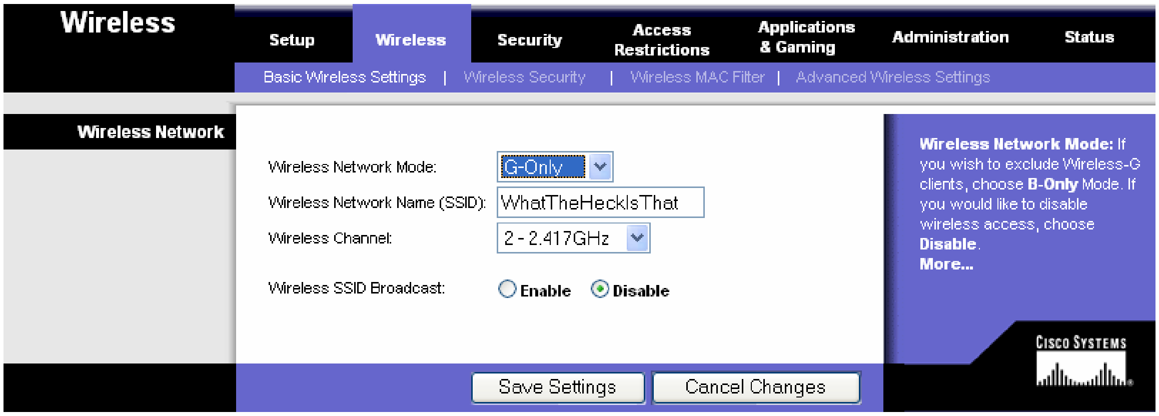
By default the radio in the Linksys wireless access point is set to channel 6. Although it is a minor bit of obscurity it is a good idea to switch to a different channel so a wireless interface in the default configuration cannot automatically associate to your network.

©2005 Richard Wanner. All rights reserved.

Disable SSID Broadcast

When wireless NICs are enabled they survey the local area for wireless networks that they potentially can connect to. One way that wireless access points indicate their presence is to periodically broadcast their SSID. If your wireless NIC already knows about your network it does not need the SSID broadcast to find the network, so you can reduce the visibility of your network by disabling SSID Broadcast. Please note that just because you disable SSID broadcast, doesn't mean that someone cannot detect the SSID of your wireless network. When you use your wireless network the SSID is attached to each wireless frame. All that this means is that the SSID of your network will not be visible when the network is not in use.

The screen below shows the configuration of this screen with all changes applied. Don't forget to click "Save Settings" to apply your changes.



Wireless Network Mode: G-Only

Wireless Network Name (SSID): WhatTheHeckIsThat

Wireless Channel: 2 - 2.417GHz

Wireless SSID Broadcast: ○ Enable ● Disable

Wireless Network Mode: If you wish to exclude Wireless-G clients, choose **B-Only** Mode. If you would like to disable wireless access, choose **Disable**.
More...

Figure 3 – Basic Wireless Settings Screen

Enable MAC Address Filtering

The MAC (Media Access Control) address is a physical address which is assigned to every network interface card (NIC). Ultimately this address is what is used by Ethernet to deliver frames to your computer. The WRT54G provides the ability to permit or deny the ability to access the wireless network based on MAC address of the NIC. My recommendation is that this feature be enabled to only permit the wireless NICs that are present in your environment, and should be associating with the access point.

The changes in this section are all performed from the "Wireless" tab under "Wireless MAC Filter". The following steps are in this section:

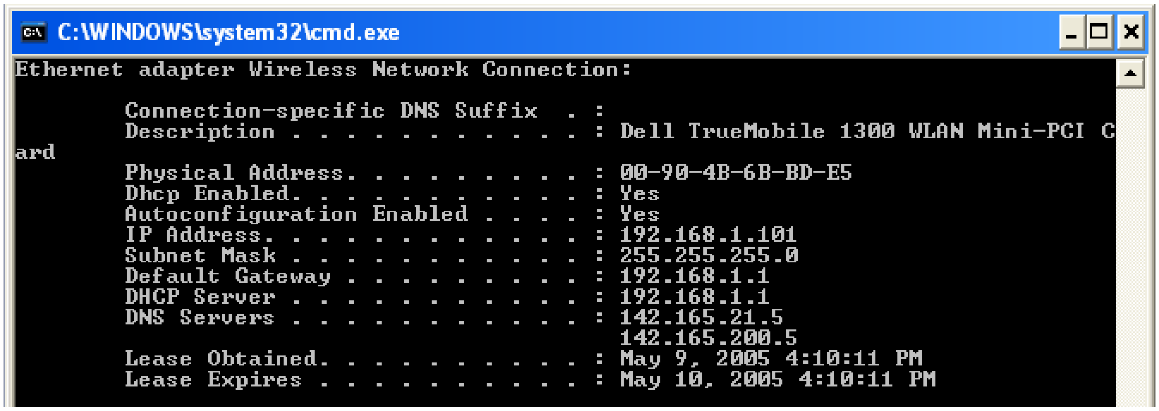
1. Configure NIC Address in MAC Filter
2. Enable Wireless MAC Filter

The order of these two steps is significant. If you are doing the configuration from your wireless enabled computer… If you enable the MAC filter without telling the filter which MACs to permit you will lock yourself out of configuration.

Configure MAC Address Filter

First things first we need to add our MAC address to the list of acceptable MACs. You open this screen by clicking on the “Edit MAC Filter List” button.

Before we can add a MAC address, you need to figure out the MAC addresses of all of the wireless NICs in use in your network. In a Windows environment that is done by opening a command prompt window (Start->Run->cmd) and running the “ipconfig /all” command. Examine the output until you find the data for your wireless NIC. It almost always is the one with “wireless” in the name. The figure below shows sample output for the wireless NIC in my laptop.



C:\WINDOWS\system32\cmd.exe

```
Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Dell TrueMobile 1300 WLAN Mini-PCI C
ard
        Physical Address. . . . . . . . . : 00-90-4B-6B-BD-E5
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 142.165.21.5
                                            142.165.200.5
        Lease Obtained. . . . . . . . . . : May 9, 2005 4:10:11 PM
        Lease Expires . . . . . . . . . . : May 10, 2005 4:10:11 PM
```

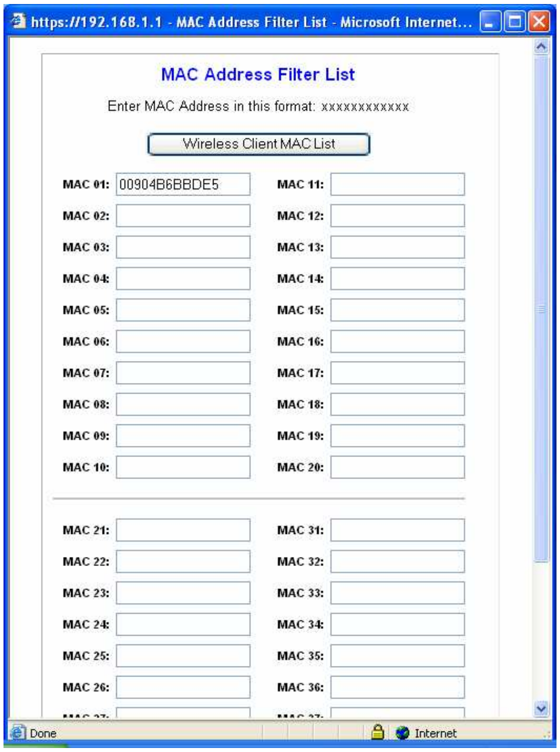
Figure 4 – ipconfig /all output

The MAC address is the one labelled “Physical Address” in this case 00-90-4B-6B-BD-E5.

If the machines you want to add to this list are already using the wireless network, there is an easier way to look up the MAC addresses. The MAC Address Filter List screen provides a “Wireless Client MAC List” button which conveniently pops up a window which provides the MAC of all currently associated systems.

The MAC Address Filter List screen takes the MAC address without dashes or spaces or any other kind of separator, in this case 00904B6BBDE5. The figure below shows the screen with a MAC address filled in. Once you have filled in your relevant wireless MACs don’t forget to scroll down to the bottom of the screen and click “Save Settings”. Then you can close the window and return to the main Wireless MAC Filter configuration screen.

©2005 Richard Wanner. All rights reserved.



https://192.168.1.1 - MAC Address Filter List - Microsoft Internet...

MAC Address Filter List

Enter MAC Address in this format: xxxxxxxxxxxx

Wireless Client MAC List

MAC 01:	00904B6BBDE5	MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	
MAC 07:		MAC 17:	
MAC 08:		MAC 18:	
MAC 09:		MAC 19:	
MAC 10:		MAC 20:	
MAC 21:		MAC 31:	
MAC 22:		MAC 32:	
MAC 23:		MAC 33:	
MAC 24:		MAC 34:	
MAC 25:		MAC 35:	
MAC 26:		MAC 36:	

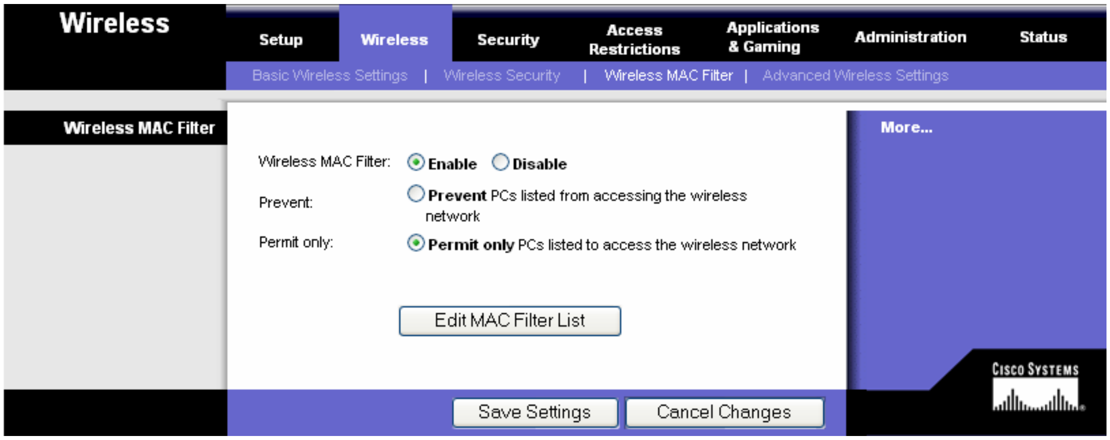
Done | Internet

Figure 5 – MAC Address Filter List Screen

Enable Wireless MAC Filter

To enable the wireless MAC filter so it will only permit approved MAC addresses to access the wireless network click on "Enable" beside Wireless MAC Filter and click on "Permit only PCs listed to access the wireless network".

The screen below shows the configuration of this screen with all changes applied. Don't forget to click "Save Settings" to apply your changes.



Wireless MAC Filter: ● Enable ○ Disable

Prevent: ○ **Prevent** PCs listed from accessing the wireless network

Permit only: ● **Permit only** PCs listed to access the wireless network

Edit MAC Filter List

Save Settings | Cancel Changes

Figure 6 – Wireless MAC Filter Screen

©2005 Richard Wanner. All rights reserved.

Enable Encryption

I intentionally left this configuration for the end. We could have applied it earlier, but to do this you will lose connectivity with the clients, so it is best left to the end.

The WRT54G provides several different choices for encryption. In a SOHO environment I recommend you use WPA with a pre-shared key. WPA stands for WiFi Protected Access. It utilizes a pre-shared key to initially set up an encrypted session, and then renegotiates the key at pre-defined interval.

The changes in this section are all performed from the “Wireless” tab under “Wireless Security”. The following steps are in this section:

1. Set Encryption parameters on the router and client

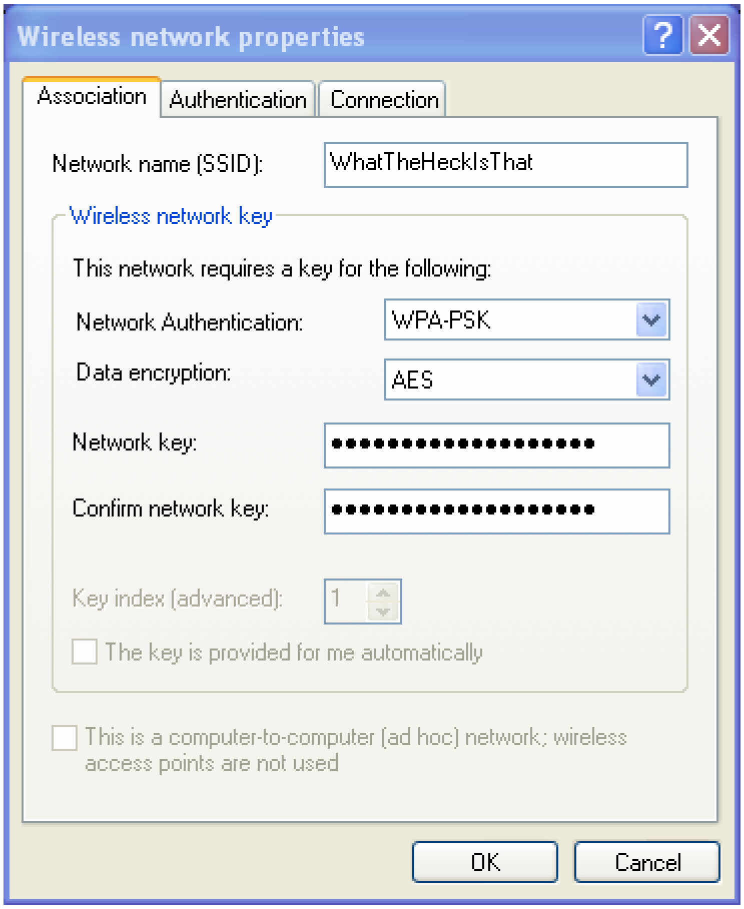
Set Encryption parameters

First things first, you need to pick a pre-shared key. It can be any string up to 32 characters in length. This key will need to be entered on the router, and in each client NIC which will connect with the router.

First step, enter the chosen pre-shared key into the wireless network properties screen on the client NIC. You can access the Wireless Network Properties screen though Start->Settings->Control Panel->Network Connections and opening your wireless network connection. Click Properties and then choose the “Wireless Networks” tab. Select your wireless network (or define a new one if you haven’t set it up yet). Then click Properties.

From the “Network Authentication” pull-down select “WPA-PSK”, PSK stands for pre-shared key. The two choices for “Data Encryption” are “TKIP” or “AES” either is an acceptable choice from a security point of view, but I prefer to use “AES” because it is a industry standard encryption algorithm with a few years of validation behind it. Then enter your chosen pre-shared key in the “Network key:” and Confirmation boxes. Don’t click “OK” yet. First we have to configure the router. The figure below shows the client side when it is all configured.

©2005 Richard Wanner. All rights reserved.



Network name (SSID): WhatTheHeckIsThat

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: AES

Network key: ●●●●●●●●●●●●●●●●●●●

Confirm network key: ●●●●●●●●●●●●●●●●●●●

Key index (advanced): 1

□ The key is provided for me automatically

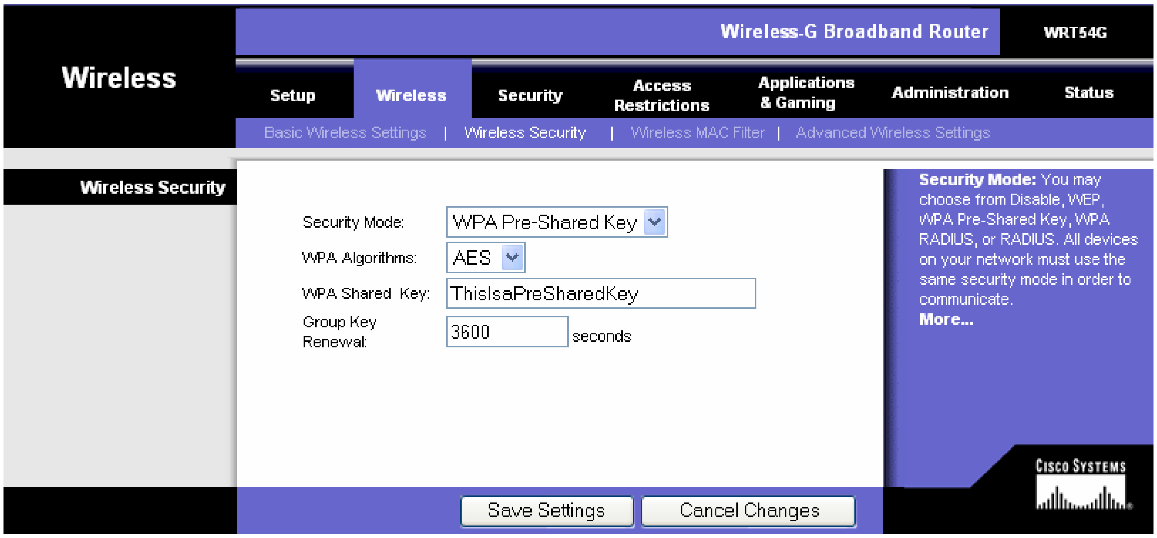
□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Figure 7 – Wireless Network Properties Screen

On the router side, choose "WPA Pre-Shared Key" from the "Router Mode" pull-down. Select "AES" from the "WPA Algorithms:" pull-down and enter your chosen pre-shared key into the "WPA Shared Key:" box. The "Group Key Renewal" field defines how often the key is renegotiated in seconds. The default is one hour (3600 seconds). This is adequate, but if you want to be extremely paranoid you can adjust the interval down accordingly.

The figure below shows the configuration of this screen with all changes applied.

©2005 Richard Wanner. All rights reserved.



Security Mode: WPA Pre-Shared Key

WPA Algorithms: AES

WPA Shared Key: ThisIsaPreSharedKey

Group Key Renewal: 3600 seconds

Security Mode: 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...**

Figure 8 – Wireless Security Screen

Now click “Save Settings” on the router side, wait a few seconds and click “OK” on the client side. That will apply the changes and get the wireless network back in sync. Of course if you have more clients you will need to apply the same settings to them as well.

Maintenance

What we have covered in the rest of this document will provide you with a very stable and secure wireless setup. However there are some things you should still do periodically. The most important is to periodically check for and apply new firmware versions as they become available. Linksys releases new firmware for several reasons. The most important is to fix security vulnerabilities in the product. New firmware versions will appear at http://www.linksys.com/download/firmware.asp?fwid=201

References

Linksys Corporation, WRT54G User Guide, 2003

Craiger, Phillip J., 802.11, 802.1x, and Wireless Security, June 23, 2002, URL: http://rr.sans.org/wireless/802.11.php

©2005 Richard Wanner. All rights reserved.