Tech Moment

Wi-Fi (In)security

By Tom Thorpe

Agenda

Public Wi-Fi

Personal Wi-Fi

Corporate Wi-Fi

6 tips

Public Wi-Fi

Either no security or everyone knows the password

Problem #1 - Bad guys can see what you do online

- Think of your Wi-Fi signal as KNX - everyone within range can tune in and listen
- Your only protection is data encryption

Problem #2 - Bad guys can put up a phony network

- Looks like the real thing, but all traffic goes through it

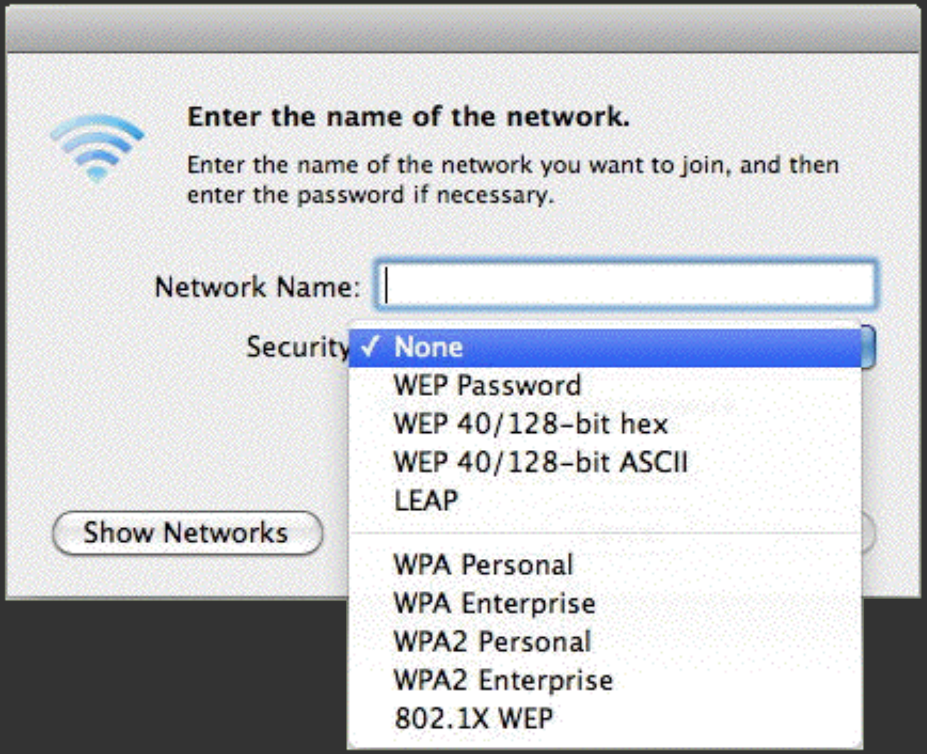
Personal Wi-Fi

You have several security options at home:

- Pick the wrong one and you have a Starbucks situation at your house
- Pick the right one and you can rest easy your data is secure

Q. How is your Wi-Fi configured?

MacOS choices



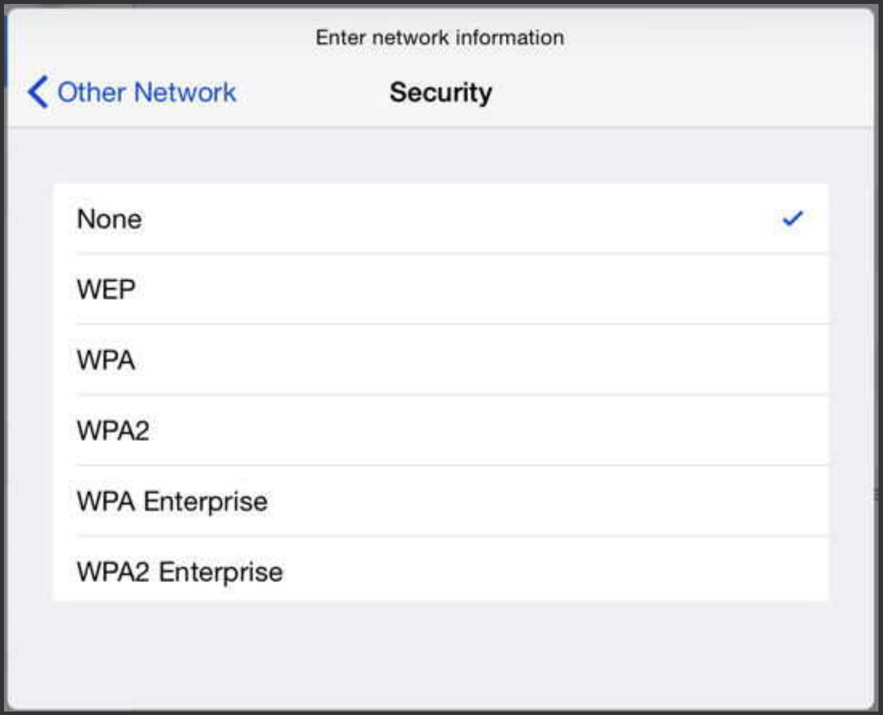
Enter the name of the network.

Enter the name of the network you want to join, and then enter the password if necessary.

Network Name:

(Apple/System Preferences…/Network/AirPort/Network Name…/Join Other Network…)

iOS choices



Enter network information

< Other Network

Security

- None ✓
- WEP
- WPA
- WPA2
- WPA Enterprise
- WPA2 Enterprise

(Settings/ Wi-Fi / Choose a network… / Security)

“None”

- No security at all
  - i.e. really public Wi-Fi

“WEP”
“WEP Password”

1997-2004

WEP = Wired Equivalent Privacy

Flavors:

	Key in bits	Hex digits	ASCII characters
WEP-40	40	10	5
WEP-104	104	26	13
Non standard	128	32	16
Non standard	232	58	29

“WEP”
“WEP Password”

pass phrases

- Everyone uses the same pass phrase
- A regular text phrase is converted to a key
- Phrases are 8-63 printable ASCII characters
  - “Hello” → 48656C6C6F
  - “Hello SBAMUG” → 48656C6C6F205342414D5547

pass phrase to key conversion

- One way process
- It may not be consistent between manufacturers
- Option: Enter as hex digits or the equiv. ASCII characters

“WEP 40/128-bit hex”

WEP with the key entered in hexadecimal

“WEP 40/128-bit ASCII”

WEP with the key entered in ASCII format

WEP in general

There are major flaws in the design of WEP technology

Cracking software is able to break it within minutes

“WPA”
“WPA-PSK”
“WPA Personal”

2003 - 2004, Interim solution

WPA = Wi-Fi Protected Access

256 bit key

- 64 hexadecimal digits
- or, as a pass phrase of 8 to 63 printable ASCII characters
- pass phrase to key conversion is now consistent between manufacturers

“WPA”
“WPA-PSK”
“WPA Personal”

WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets

- TKIP = Temporal Key Integrity Protocol
- It dynamically generates a new 128-bit key for each packet

There are known security holes in TKIP

WPA is much harder to crack than WEP

- It is still possible with the use of more advanced tools

“WPA2”
“WPA2-PSK”
“WPA2 Personal”

2004 - present

WPA2 = Wi-Fi Protected Access II

Wi-Fi devices certified since 2006 support both WPA and WPA2

If you see the Wi-Fi trademark Wi Fi™ it supports both WPA and WPA2

“WPA2”
“WPA2-PSK”
“WPA2 Personal”

Instead of TKIP, WPA2 uses a more advanced AES algorithm

- pass phrases created with AES are virtually uncrackable
- AES is so secure that it could potentially take millions of years for a supercomputers' brute-force attack to crack its encryption

WPA2 is also capable of using TKIP instead of AES

- But then it basically becomes WPA!

You should be using WPA2 (AES)

Corporate Wi-Fi

So far, all users of a network shared a common pass phrase

For corporate Wi-Fi each person has his/her own user name and password

- Requires a server with a database of users
- Administrative hassle
- Not normally used at home

“802.1X WEP”

Like WEP but the key can change every session

“LEAP”

LEAP = Lightweight Extensible Authentication Protocol

Like WEP but the key can change dynamically

Cisco proprietary

“WPA Enterprise”
“WPA2 Enterprise”

Like WPA or WPA2 but the key can change every session

6 tips

Tip #1

Be very careful at a public Wi-Fi

Or use a VPN (more next month)

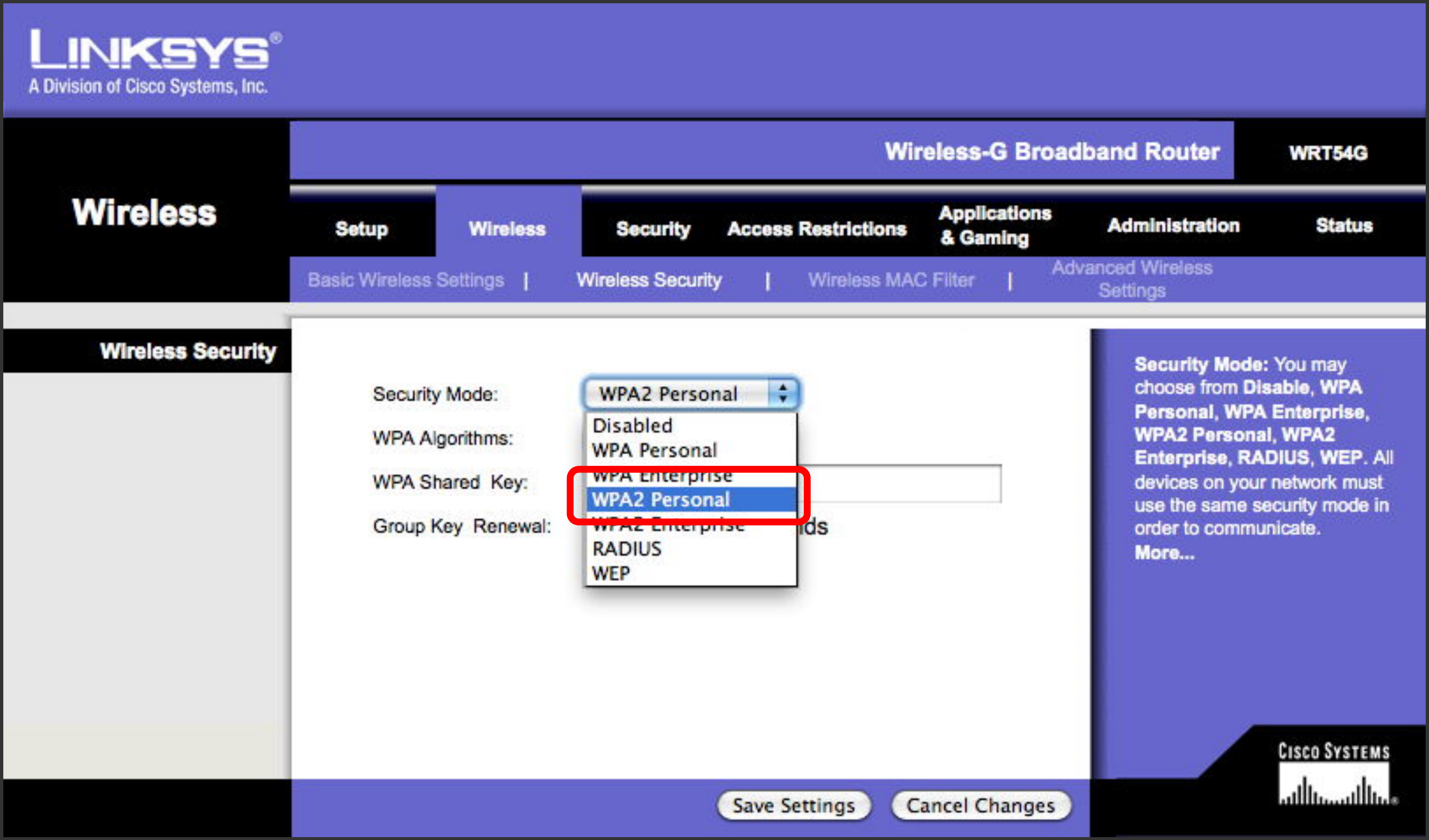
Tip #2

Use WPA2 (AES) at home

Not set by your computer, iPad, or iPhone

Determined by your Wi-Fi access point (wireless router)

Example



Security Mode: WPA2 Personal

WPA Algorithms:

WPA Shared Key:

Group Key Renewal: ...ds

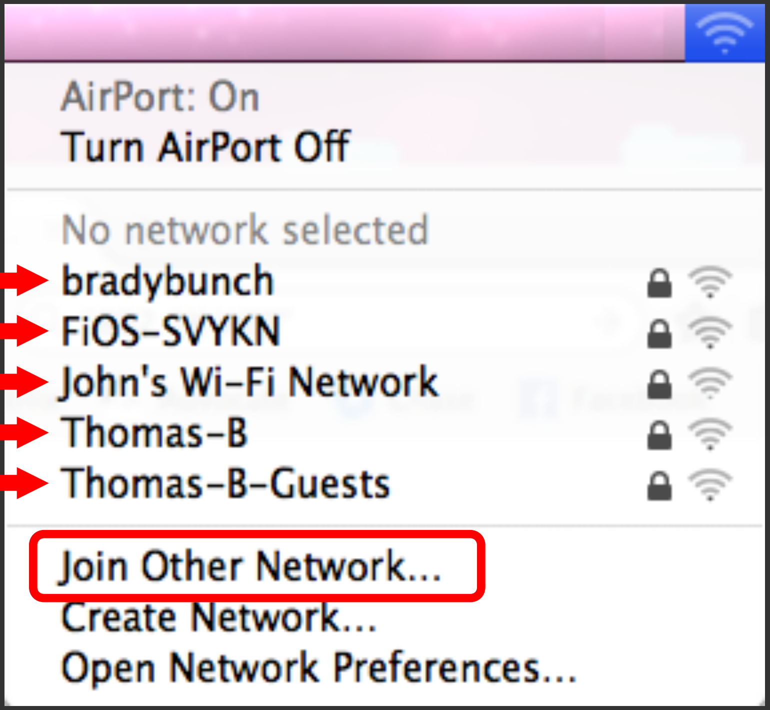
Security Mode: You may choose from **Disable, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, WEP**. All devices on your network must use the same security mode in order to communicate.
More...

Tip #3
Turn off your SSID broadcast

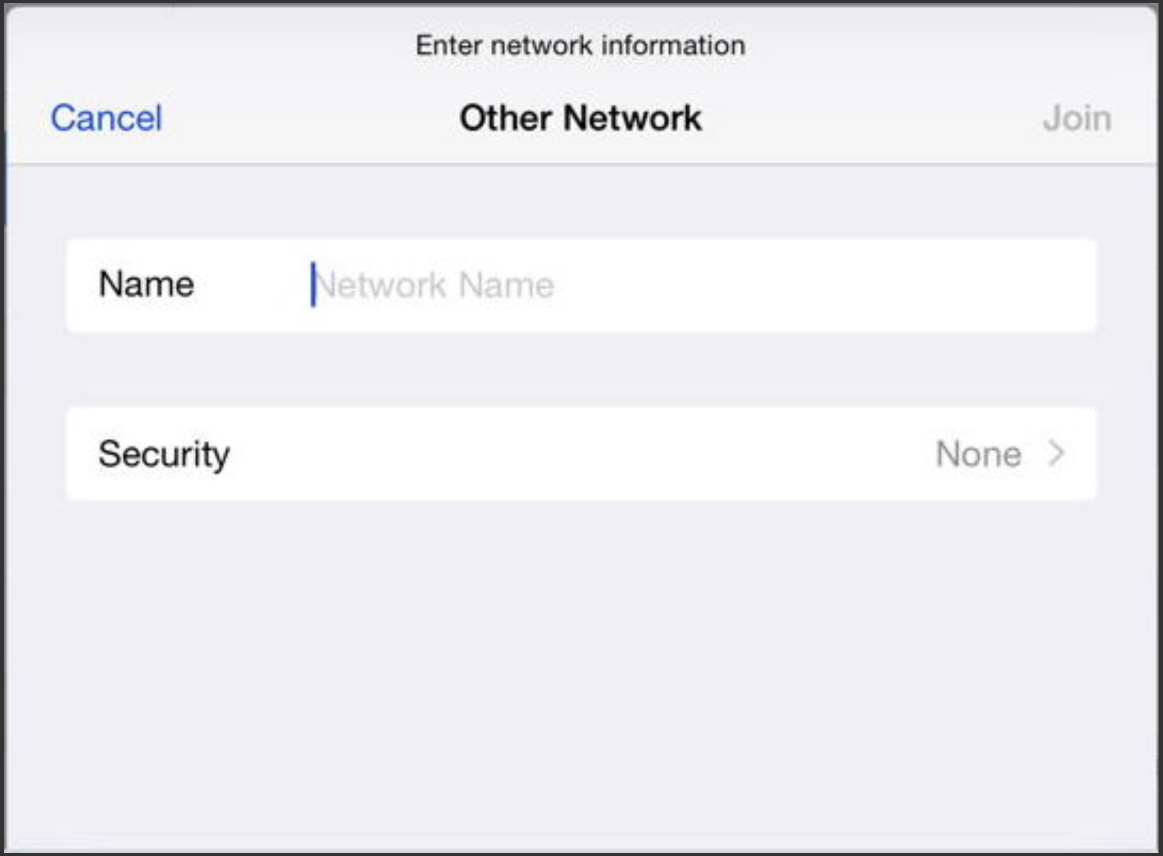
SSID = Service Set Identifier

32 alphanumeric character unique identifier attached to the header of packets

- Your access point transmits it every few seconds
- It makes finding the network easy
- The SSID here is “SBAMUG”


AirPort: On
Turn AirPort Off
No network selected
bradybunch
FiOS-SVYKN
John's Wi-Fi Network
Thomas-B
Thomas-B-Guests
Join Other Network...
Create Network...
Open Network Preferences...

SSID's



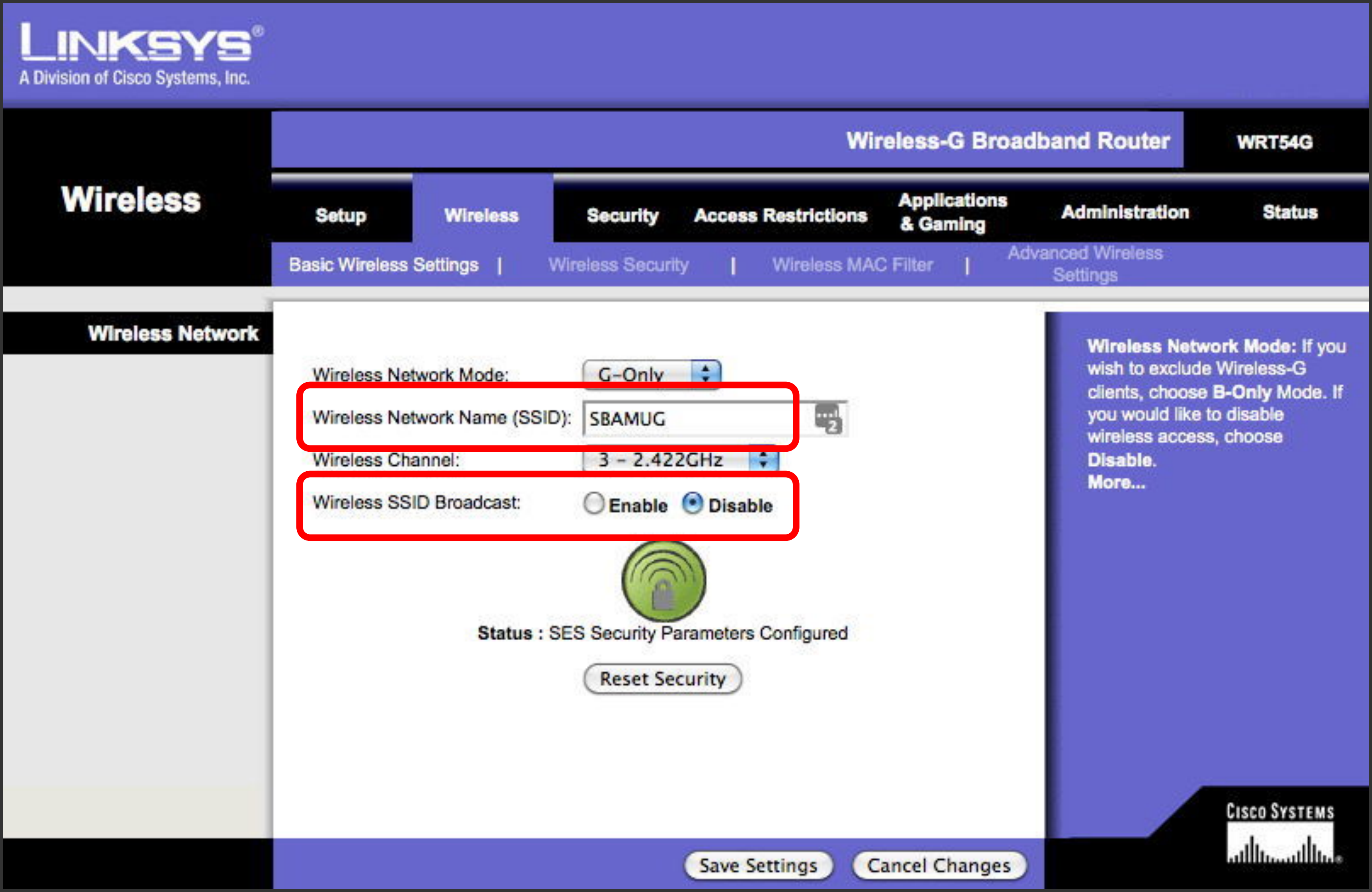
Enter network information

Other Network

Name Network Name

Security None

Example



Wireless Network Mode: G-Only

Wireless Network Name (SSID): SBAMUG

Wireless Channel: 3 - 2.422GHz

Wireless SSID Broadcast: ○ Enable ● Disable

Status : SES Security Parameters Configured

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...

Good news:

The average person won’t know your network exists

Bad news:

Wi-Fi signals are still present and a determined bad guy can still find your network

Also, you’ll have to manually enter your SSID to initially join the network.

Tip #4

Don’t use the manufacturer’s SSID

The bad guys have recomputed tables to crack them for a multitude of common passwords

Make up your own weird network name (SSID)

Tip #5

Use an Ethernet cable

Connect via a cable and forget Wi-Fi

Tip #6

Use a good strong pass phrase

The most important tip!

Bonus Charts

Network Security

There is no such thing as a “secure Wi-Fi network” - only secure communications over it

Any Wi-Fi connected device (iPhone, iPad, computer, laptop, etc.) can be attacked

Using Public Wi-Fi

Double check that you are connecting to the right network

Bad guys can snag anything that is not secured:

- HTTP web pages
- Popular websites like Google, Facebook, etc. are ok, watch it on others
- Careful with user names and passwords
- Instant-messaging service (Yahoo Messenger)
- Incoming and/or outgoing email including your email passwords

Rule: If it isn’t encrypted assume someone else is looking at it

Using Public Wi-Fi [cont’d[

Only encrypted connections are safe

- Every time you log in to a website, make sure that your connection is encrypted (https)
- Make sure that the connection stays encrypted for all of your online session
  - e.g. Facebook will encrypt your log-in and then may return you to an unsecured session. (To avoid this problem enable Secure Browsing in the Security settings.)

Using Public Wi-Fi [cont’d[

Only encrypted connections are safe [cont’d]

- – For email clients like Apple Mail, make sure both your POP3 or IMAP (incoming) and SMTP (outgoing) connections have encryption turned on
  - • As an alternate to Apple Mail, login to your email via a secure (https) web browser connection
- – Never use FTP (File Transfer Protocol) or other services that aren’t encrypted
- – To encrypt most activity, use a virtual private network (VPN)

Using Public Wi-Fi [cont'd]

Avoid financial transactions

If you do accidentally login to someplace unsecured, go home and immediately change the password

Disconnect when not in use

Double Bonus Charts

Laptops/Computers on Wi-Fi

Pertains to:

- Laptops in all public places
- Computers at home if you have bad neighbors

If a bad guy can get on the network then he can send packets and get replies

- There is nothing you can do to stop them
- Therefore your laptop/computer might be hacked

Laptops/Computers on Wi-Fi [cont'd]

Are any of your user accounts vulnerable?

- Logout of your normal user account
- You'll see the login screen that shows user accounts that could be hacked
- Do they all have good passwords?

Have you enabled file sharing, remote login or any other "sharing" option?

- Are they properly protected?

THOUGHT: What could happen if you logged out and handed your laptop/computer to a stranger. What could they do?