Macintosh SIG

May 10, 2011

AirPort (Wireless) Security

Terminology

Client - The computer used to access the wireless network.

Access Point - The AirPort Express/Extreme unit.

The difference between the AirPort Express and the AirPort Extreme:

- The *AirPort Express* supports *AirTunes* with an audio port for connecting to a stereo amplifier or powered-remote speakers and can share a USB printer.
- The *AirPort Extreme* has three wired Ethernet ports and can share a USB printer and/or an external USB hard drive.

Security Objectives

- Prevent unauthorized access to the AirPort settings.
- Prevent access to the network by unauthorized persons.
- Prevent access to data being transmitted between the Client and the Access Point.

AirPort Configuration Utility

Go to:

`/Applications/Utilities/AirPort Admin Utility.app`

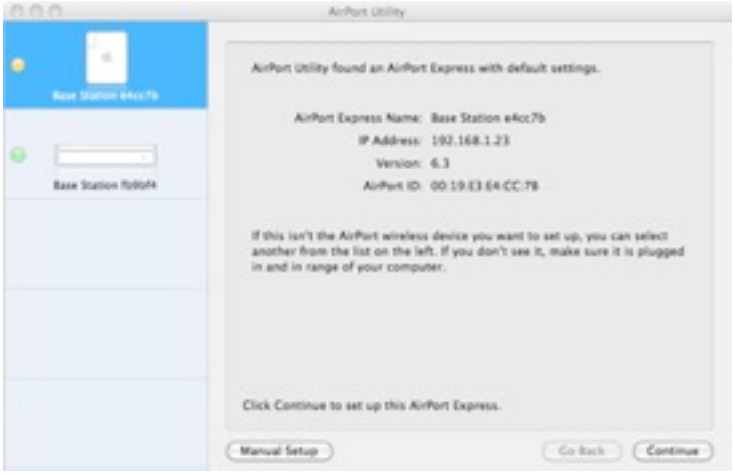

Figure 1, AirPort Utility

Click on *Manual Setup*

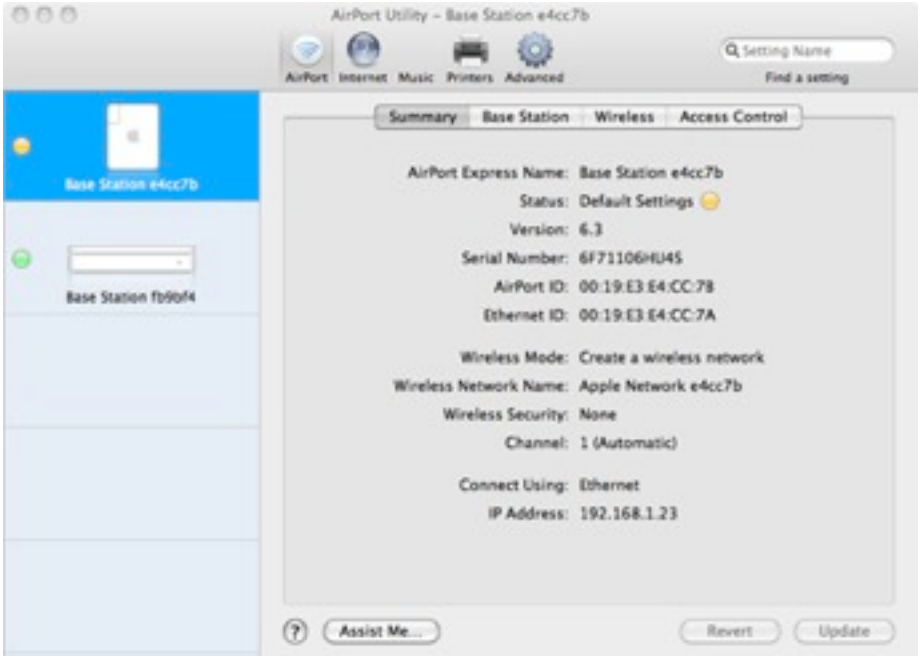

Figure 2, Summary

Click on *Base Station*

AirPort Extreme/Express (Setup) Password

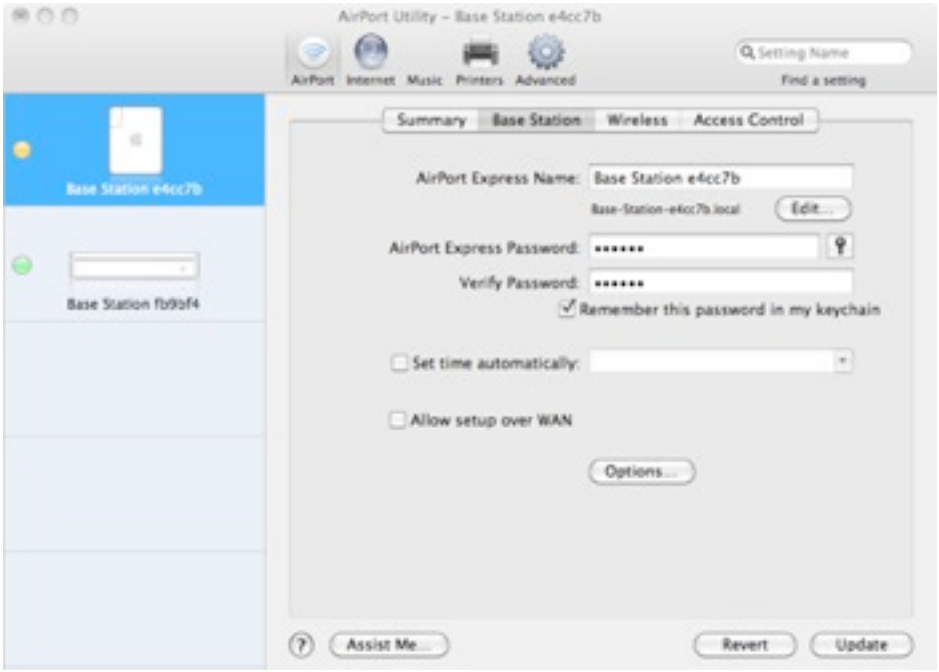

Figure 3, Base Station

The AirPort Express/Extreme Name is the name that will show up when starting the *AirPort Admin Utility*.

- There are two passwords that we will set up.
    - The first is to control access to the AirPort setup. (The default password is *public*.)
    - The second is to control access to the wireless network and encrypt the wireless transmissions.
- On this screen enter the *Password* and the *Verify Password*.
- The password is case-sensitive.
- Uncheck: *Allow setup over WAN*.
- Click on Update.
- After the unit updates, click on: *Wireless*

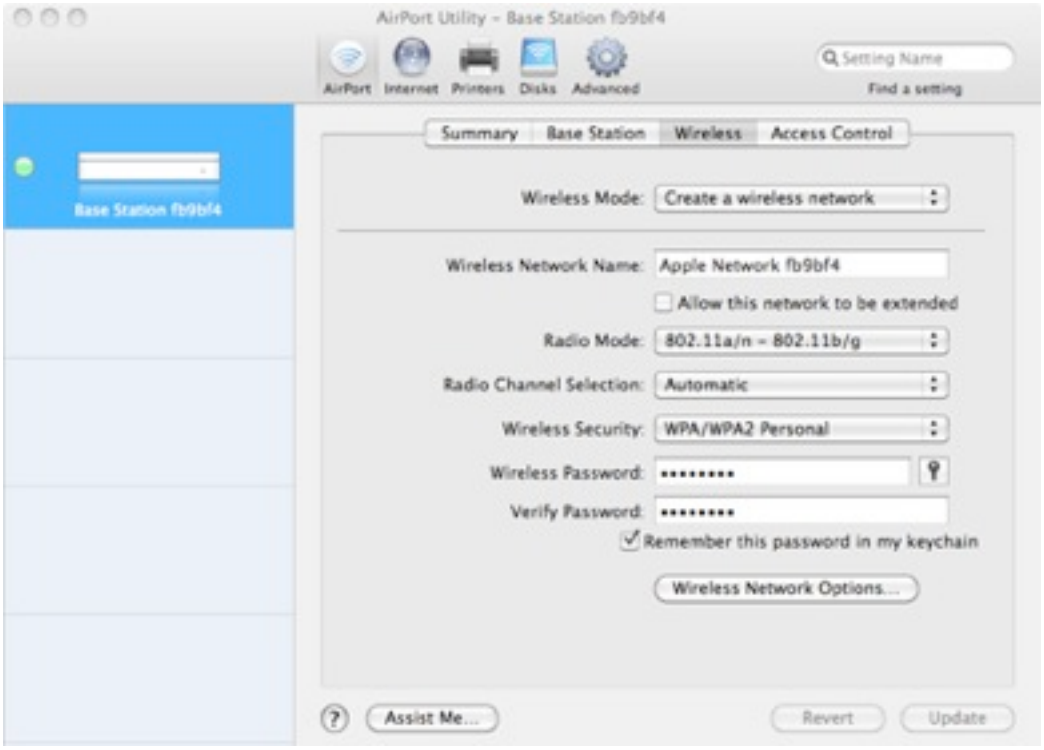

Figure 4, Wireless

Encryption Key (access password)

- In the *Wireless Security* drop-down select *WPA/WPA2 Personal.*

- When the *Wireless Password:* input opens, enter the password to be used to access the network.
- This password is likewise case-sensitive.
- Anytime someone wishes to access your network, they will have to supply this password.
- The text of the password is also used as the encryption key to encrypt the data while is is transmitted between the Client and the Access Point.
- The longer the key (number of characters) the better the encryption (harder to crack).
- Click on *Update*.

For the really paranoid, there are two additional security measures:

- **Create a *Closed Network*.**
- **Create an *Access Control List*.**

Closed Network

A wireless-network Access Point continually broadcasts the *Wireless Network Name*.

When a wireless-equipped computer is within range of an Access Point, the Wireless Network Name will show up in the computer's network-configuration dialog.

From the *Wireless* dialog, click on: *Wireless Network Options*.

Click on *Create a closed network*.

Click on *Done.*

This will turn off the broadcast of the *Wireless Network Name*, effectively hiding the network.

The downside is that to join the network, a user must know the name of the network.

Access Control List (ACL)

Click on *Access Control*.

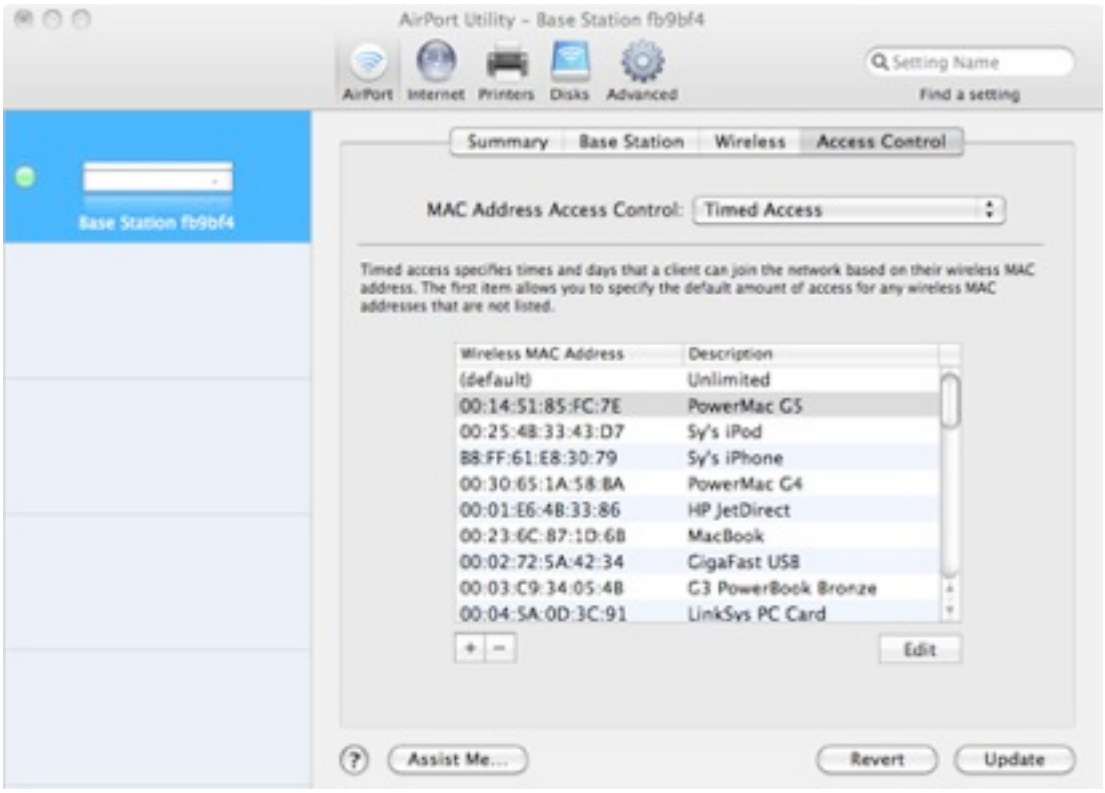

*Figure 5, Access Contro*l

With *Access Control* you can specify which computers can access your network.

Every network interface device has a unique Media Access Control (MAC) address.

To locate the MAC address of your computer:

- Open *System Preferences*.
- Click on *Network*.
- In the left pane click on *AirPort*.
- Click on *Advanced*.
- At the bottom of the dialog is the *AirPort ID* of the computer.

In the Access Control dialog, click on the “+” symbol.

In the *Timed Access Control Setup Assistant*, enter:

- The *MAC Address, and*

- The *Description* (the name of the computer, anything convenient).
- Enter the MAC address and name of any other computers that will access your network.

Click on *Done*.

To temporarily disable Access Control, set the MAC Address Access Control drop-down to: *Not Enabled*.

WiFi *Hotspots*

In order to access a secure -encrypted- network one would need the encryption key. In a business or location that offers free WiFi, they would have to give everybody the encryption key. Which defeats the purpose of the encryption.

Therefore, public Hotspots are NOT ENCRYPTED. Use a public Hotspot with caution.

Finally

Bear in mind that no security system is 100% safe. The best that we can hope for is to make it more difficult for someone to intrude on our system.

Manuals for Apple AirPort devices are here:

http://support.apple.com/manuals#airport

Apple *How To* tutorials are available here:

http://www.apple.com/findouthow/mac/

(Scroll down to Wireless in the left-hand column.)