

Chapter 6

Flying the Friendly Skies

by Joe Grand

So here I am, sitting in the airport again, waiting for another flight. I should be used to it by now; I fly more often than I see my girlfriend. I know my frequent flyer number by heart and always make sure to ask for a first-class upgrade when I check in. Of course, the gate attendant just smiles at me and shakes her head, every time...

156 Chapter 6 • Flying the Friendly Skies

After breezing through security, I walk down the narrow hallway towards the gate area. My eyes shift around the vast glass-walled room, looking for a place to stake my claim for the next hour before I begin to board my flight. I head for a large window overlooking the tarmac. I plop down in a row of vinyl-covered chairs and proceed to pull out my laptop from my ever-so-obvious laptop bag (it's like having a huge target on my back for thieves). Spreading out my papers on an adjacent seat, I make myself comfortable.

As Windows 2000 loads on my laptop, which sometimes seems like it takes days, I look around the waiting area. I'm always interested in how people pass the time in airports. A few seats down from me, an old man in brown khakis is slouched comfortably, mouth wide open, fast asleep. Behind me is a family with two small kids, loud and whining, running around and knocking over everything in sight. The archetypical businessmen fill many of the chairs, their cell phones glued to their ears. As for me, I look like I practically live in the airport. My shoes are off, kicked to the side on the floor next to my laptop bag. The hooded sweatshirt that I always travel in is unzipped, showing off my red "Lite Beer Athletic Club" T-shirt. I like to travel in comfort.

I've always wondered how some people can just sit in the waiting area...and sit...and sit, not doing anything but staring into space. I can't do that. I need something interesting to fill the time. It usually involves my laptop and an Internet connection.

Wireless networking is wonderful. I don't need to be tethered to anything and can still communicate with the outside world. It works great from home, where I can sit on my porch, overlooking the ocean, and work on circuit designs in the California sun. I'm not constantly tripping over wires when I walk around the house. The one thing I've noticed about wireless is that it's everywhere. It's actually hard not to notice it these days. Residential neighborhoods, hotels, university dorm rooms, the local Starbucks, and the McDonald's down the street—though I don't know why anyone would want to sit in a Mickey D's, eating a Big Mac while using a computer. It would take days just to get the grease smell off the laptop.

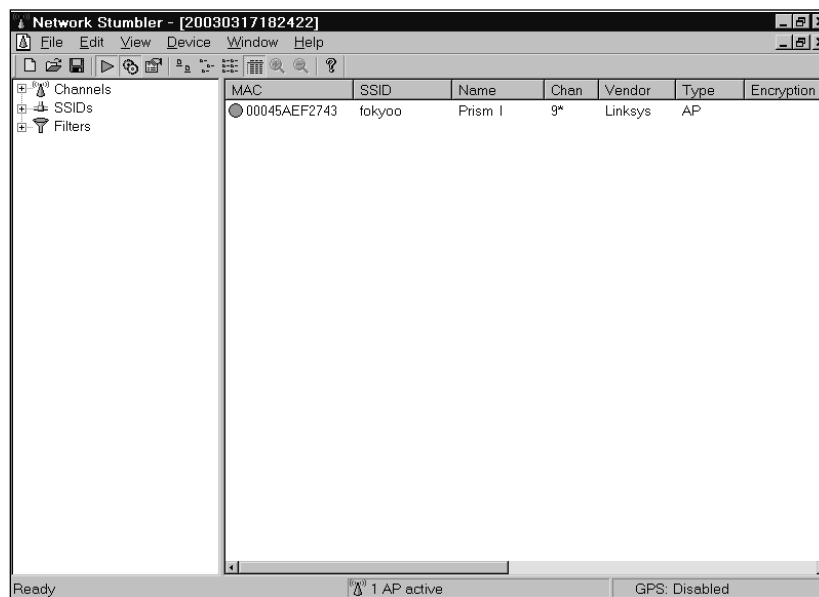
Anyway, I'm relaxed and sprawled out on the airport seats. And I'm itching for a network connection. Actually, I'm just itching for something to do. Boredom is not an option for me.

I decide to first load Network Stumbler to sniff the airwaves for any active 802.11b wireless access points. A single access point pops up in the window. Small airports like this one probably aren't subject to the same strict network security procedures as the larger, urban airports are. So they can get away with wireless local access networks, also known as WLANs, where others might not.

Having wireless capabilities on your corporate network is like putting an Ethernet jack in the company parking lot. Many administrators simply plug in wireless access points and leave the hardware in its default configuration, sometimes opening up their entire corporate network to the public, or at least allowing the public to access the Internet through the corporation's connection. We're at a point where it is so convenient to use wireless technology that people usually just overlook the security problems and pretend they don't exist.

With NetStumbler, I can easily see the media access control (MAC) address, network name (SSID), channel, access point vendor, encryption type, signal and noise values, and some other parameters. To my surprise, there is no encryption used on the wireless network. The network I've detected, labeled "fokyoo," is an open network that simply broadcasts itself to the public.

NetStumbler Showing Active Wireless Access Points



158 Chapter 6 • Flying the Friendly Skies

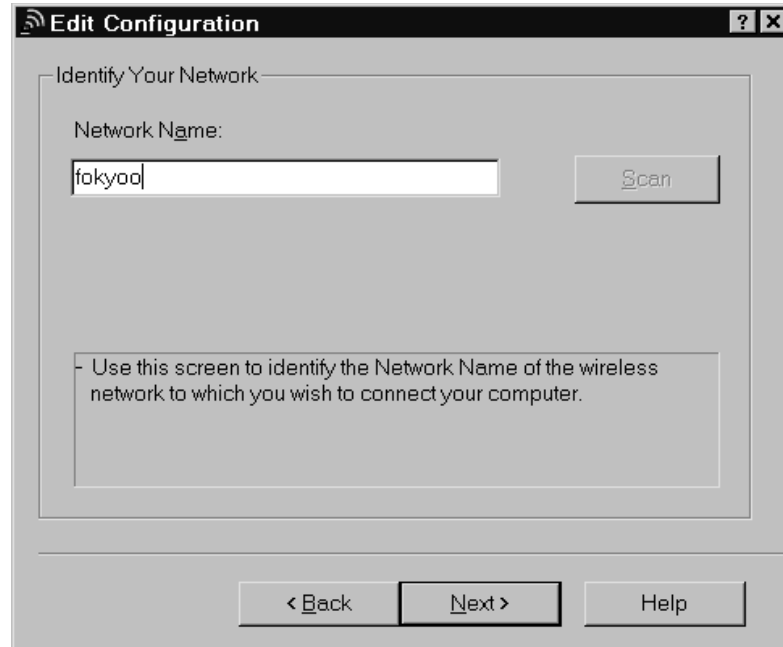
Normally, WEP, the Wired Equivalent Privacy algorithm, is used in 802.11b systems to encrypt and protect wireless traffic. Even though WEP has been found to be extremely flawed, a lot of people still use it to add a (very thin) layer of “security.” I suppose it’s better than nothing, but WEP is breakable by active attacks, passive attacks, and dictionary-based attacks.

Aside from providing encryption on the wireless network, WEP also is used to prevent unauthorized access to the network. WEP relies on a secret key shared between the access point (a base station connected to the wired network) and the mobile station. There are a handful of simple cracking tools, such as AirSnort and WEPCrack, that can determine WEP keys based on analysis of a large number of WEP-encrypted packets. Capturing enough packets to build up a dictionary of WEP initialization vectors that will be used by such a tool might take a dozen hours or a few days, depending on how much traffic is actually flowing over the wireless network. After that, it’s as easy as feeding them into the tool until the WEP key pops out. I recently read about how someone could basically hijack a legitimate user’s wireless connection by kicking the user off the network and quickly hopping on in his place.

Luckily for me, WEP isn’t enabled on this network. I won’t be here for more than an hour, so I probably wouldn’t have enough time to determine the WEP key and associate with the wireless network.

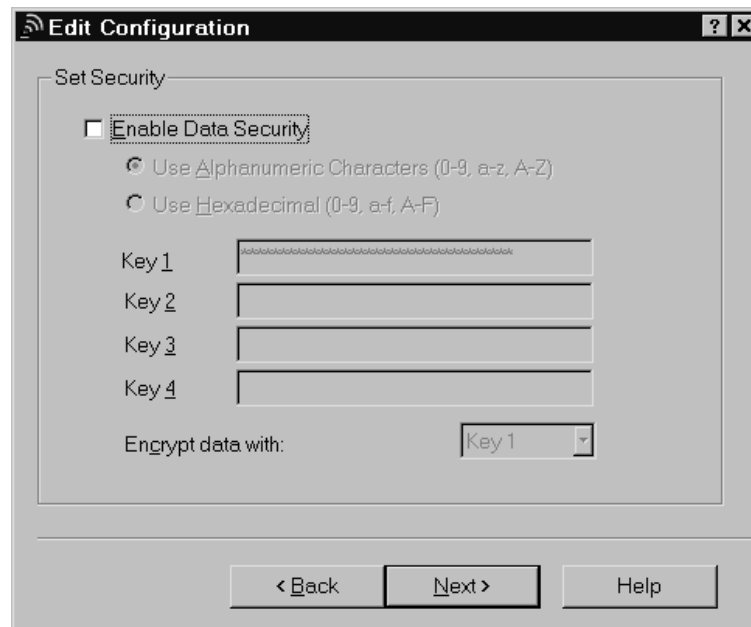
With an unencrypted, open wireless network, all I should need is the SSID in order to associate with the access point and gain access to the network. Simple enough, since the access point broadcasts the SSID—it isn’t meant to be a secret. First, I enter the SSID into my Windows 2000 wireless adapter configuration.

Wireless Network Configuration: Setting the SSID



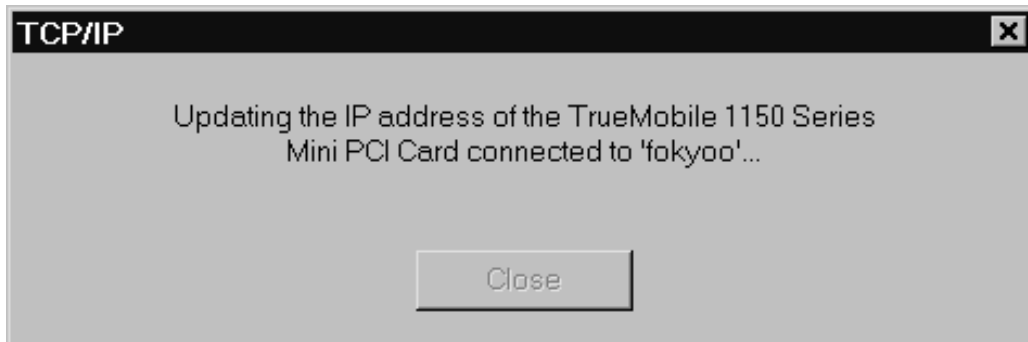
Next, I make sure that WEP is disabled, cross my fingers, and click **Next**.

Wireless Network Configuration: Disabling WEP Security



160 Chapter 6 • Flying the Friendly Skies

If the Dynamic Host Configuration Protocol (DHCP) is enabled on the access point, I will be issued an IP address, gateway information, and access to the network.

Successful Connection to Wireless Network

I'm pleased to see there aren't any errors. I load up the Windows Command Prompt and run `ipconfig` to verify my settings.

```
C:\>ipconfig
```

```
Windows 2000 IP Configuration
```

```
Ethernet adapter Wireless:
```

```
Connection-specific DNS Suffix . : host.atc.state.ca.us
IP Address. . . . . : 192.168.1.103
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

So far, so good! A quick ping to `www.grandideastudio.com` verifies that I am indeed up and running.

```
C:\>ping www.grandideastudio.com
```

```
Pinging www.grandideastudio.com [216.127.70.89] with 32 bytes of data:
```