Wireless Networking in Linux

Look, No Wires

When you're going wireless, it pays to be careful. Get the right hardware, and make sure your network is as secure as you think it is. BY JOE CASAD

Almost everything about the computer industry would amaze our great grandparents, but a wireless network seems especially futuristic.

The task of configuring Linux for wireless has gotten easier over the years. Many distributions include special tools for configuring wireless networks. But wireless networking has never been without its share of headaches. The special needs of a wireless network require some special attention from the user.

One problem with setting up a wireless network is the vast number of differing standards for wireless devices, some of them obsolete or incompatible with contemporary systems, and others so new they have hardly even been implemented. In our cover story, we'll examine the standards of the IEEE 802.11 family, from the venerable 802.11b to more recent variants such as 802.11g and 802.11n. We'll show you which standards provide higher performance and which offer greater compatibility. And we'll describe how the new 802.11i standard addresses some of the privacy issues associated with earlier wireless systems.

The subject of WLAN hardware is always a moving target, with new products and new technologies appearing almost daily. One recent innovation that is becoming increasingly popular is the USB WLAN stick, a compact wireless device that plugs directly into your computer's USB port. In our article "USB Radio: Testing USB WLAN Adapters," we examine some popular USB WLAN devices. We'll show you what works in Linux, and we'll take you through the steps of configuring a USB WLAN adapter.

Of course, one of the biggest problems faced by wireless networks is the question of security. Wireless networks put all the data out in the air, where anyone can read it unless you protect it. Unfortunately, the Wired Equivalency Protocol (WEP), an early security standard for wireless networks, was not so good with protection, giving rise to tools such as AirSnort, which can break the key of a WEP-protected network. If you want real security for your wireless network, you'll need something stronger.

One option is a Virtual Private Network (VPN). A VPN creates a secure tunnel for encrypted communication within an ordinary network. In the article "Wireless Secrets: Safe WLAN Networking with an Encrypted OpenVPN Tunnel," we'll show you how to use the Open Source tool OpenVPN for secure, encrypted communication on a wireless network.

If you have a wireless network now, or if you think you might one day want to go wireless, we hope this month's Wireless Networking cover story gives you lots of ideas for products and technologies you'd like to explore. ■