There are two basic methods of implementing wireless networks based on IEEE 802.11: Ad hoc mode means that the computers will communicate directly, but they must be able to talk to each other constantly to avoid disruptions. You can connect a maximum of 16 computers in this way. The hardware requirements are also quite simple – in fact you only need a WLAN card in each computer.

In access point mode (AP mode), also referred to as a managed infrastructure, one or more access points are used as hubs: The wireless computers transmit data to the access point which in turn will relay the data to the intended recipient. This means that the computers only need to connect to the next access point to log on to the wireless LAN. The access point assumes a role similar to that of an Ethernet switch. Only a couple of years ago access points really could not do anything more fancy that moving data from one WLAN card to another, but now there are devices with integrated network ports, Ethernet switches, or even DSL routers.

Attenuation

You will need to invest a lot more money in hardware to implement an AP network in comparison to an ad hoc network. Of course, each wireless host will still need a WLAN card, but you have the added expense of an access point or access router. For large houses, or houses that are well screened, you may even require multiple access points.

The farther two WLAN computers are apart and the more walls or buildings there are in the way, the poorer and slower the connection will be – until it finally collapses. Even the temperature, humidity, and the weather can affect the connection quality. And so any statement on possible distances would be inconclusive, and this led to our decision to avoid this area. As a basic guideline, access points should be mounted in a high and unobstructed position in the middle of the area you intend them to service.

Illusions of Security

Basically anybody in the proximity of your premises can sniff your wireless LAN, and even log on to your network.

Stepping Up to a Wireless LAN

A LAN Solution for Major Tom

It is so practical to be able to use laptops all over the house without a tangle of cables, or simply not needing to wire up your childrens' bedroom to get them on the net. If you want to know what the requirements for a wireless LAN are, read on. **BY DANIEL COOPER**
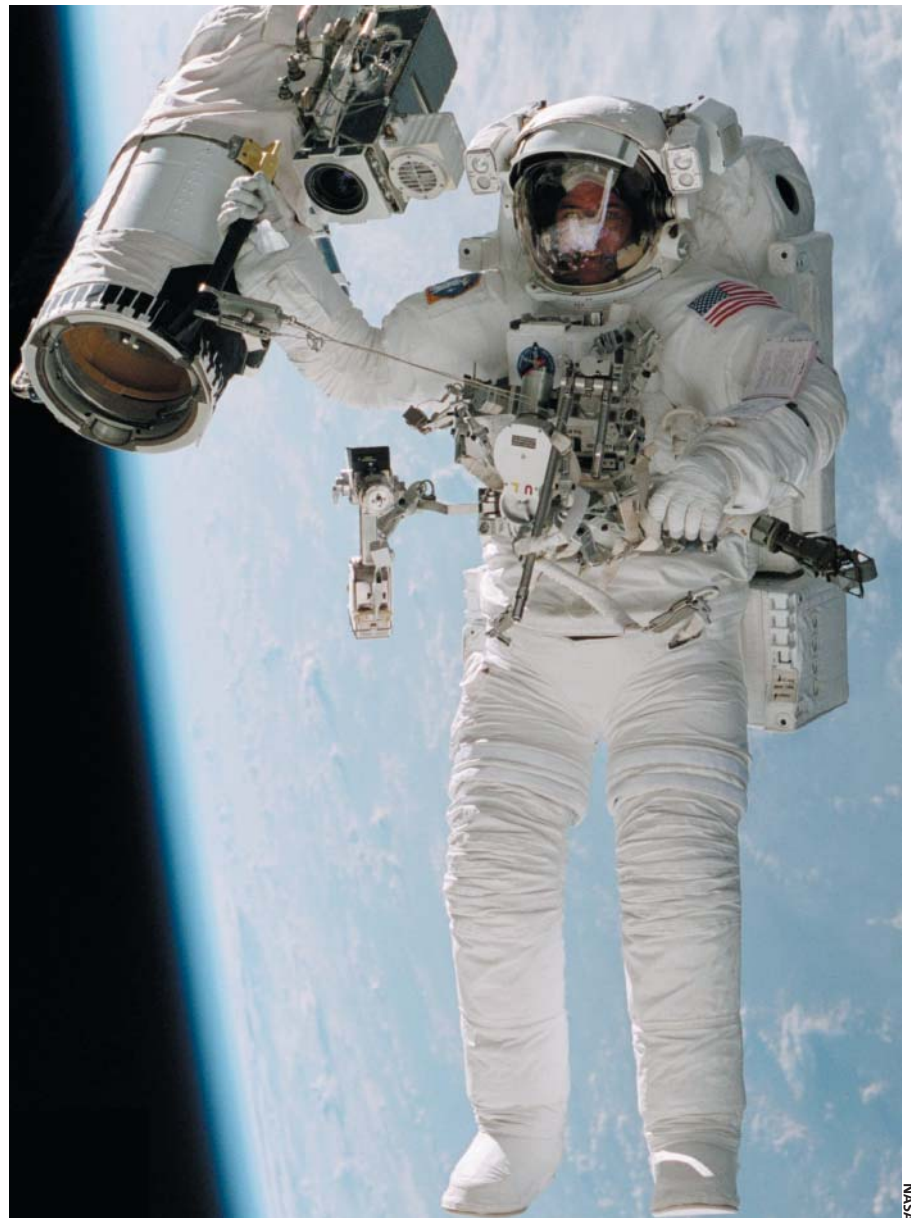
NASA

The WEP (Wireless Equivalent Privacy) encryption standard was thus introduced to prevent misuse. Originally, a 40 bit key (WEP-40) was used, although today's devices nearly all use 128 bit (WEP-128) keys. However, WEP-128 uses 24 bits for the so-called initialization vector (IV), which is simply incremented for each packet, and that leaves only 104 bits for the secret key.

That does not mean you should disable WEP-128 – at least it will keep the script kiddies at bay. Choose your key carefully – the sequence should be randomly generated, if possible. You will need 13 bytes (104 bits) for WEP-128. You will definitely want to avoid using a password for a Windows client as your WEP key. The password is not used directly but truncated to 24 bits in the case of WEP-40, which corresponds to a mere 16.8 million combinations. Considering the fact that a laptop with a 1 GHz CPU can try out about 170,000 keys per second, you do not need to be a genius to work out that your network will be compromized in a matter of minutes. It is preferable to generate the 40 or 104 bits randomly. The following call will provide you with 14 bytes in hexadecimal notation. Now all you need to do is choose 13 of them and use them as your WEP-148 key:

```
dd if=/dev/urandom bs=14 ↵
count=1 | hexdump | cut -c 9-
```

Control Mechanisms

If you want to set up another hurdle for the attacker to take, you can implemement an access conrol list (ACL) on your access point – in our test, the only box offering this feature was the Tellus TWL-R410. This would mean that instead of any card being allowed access, only the hardware addresses (MAC addresses) in the list are allowed to log on to the access point.

Unfortunately, this mechanism is also relatively simple to sidestep, as some card drivers (albeit only via patches in some cases) allow you to edit the MAC address of the card. The attacker only needs to sniff the address of a card with access privileges and spoof that card's MAC address.

We tested a selection of today's wireless LAN products. You can refer to the article "Driver Safari" on page 19 for a description of installing the drivers and details on the configuration of the cards in our test.

Actiontec Wireless USB Adapter 802UI3

The Wireless USB Adapter by Actiontec is particularly useful for desktops or servers. It saves you sacrificing a valuable PCI slot for the adapter you would otherwise require to run laptop cards on your desktop, and even then the position of the wireless LAN card – i.e. under your desk or somewhere in the corner – would not be ideal.

You can use a USB extension lead to attach Actiontec's USB adapter at a distance of up to six meters from the last USB hub and even wall-mount the adapter using the brackets supplied. If you do not feel like drilling holes in the wall, you can always use the sticky pads that complete the package.

The USB adapter is the same size as a standard PC extension card, about one centimeter high and is attached to the USB port by means of a special lead. The device speaks IEEE 802.11b, uses 128 bit encryption and requires the *prism2_usb* module from the "Next-Generation" driver package (see page 19).

There is one issue with the USB adapter: If you remove the *prism2_usb* module without removing *usbcore,* and then detach the USB adapter, you can expect your kernel to crash. You should also avoid unloading the *prism2_usb* module and reloading it without reloading *usbcore.* Practically speaking this means first detaching the device itself, and then removing the drivers – although this is the opposite of what you would normally do.

This driver quirk is no big deal in a static environment as you will not be detaching the USB adapter regularly. The "Driver Safari" on page 19 describes how to add the Actiontec Wireless Adapter to your boot scripts without risking any kernel lockups.

At around £71 the Actiontec wireless USB adapter is cheaper than the price of most other laptop WLAN cards with a PCI adapter, but it is far more flexible for both desktop or server use, because of the USB connectivity. That is why this product gets the Editor's choice award.

D-Link DWL-500 PCI Adapter (Elito-Epox EWL-PCA)

If you want to use a WLAN laptop card in a normal PC, you need a PC card adapter for the PCI bus. The answer is to add a typical laptop CardBus controller – in the case of the DWL-500 by D-Link (around £115) that means the Ricoh RL5c475. Running this device on Linux is simple, as the PCMCIA Card Services support almost all the known chipsets of the WLAN cards.

If you have not already installed the *pcmcia* package, you will need to do so. There are no further configuration steps, as any cards inserted (wireless LAN, or a compact flash module on an adapter card) are recognized and configured by your laptop.

However, do not be surprised when you install your next Linux distribution – Linux will assume that your computer is a notebook, if a CardBus controller is detected, and this can cause SuSE to install a modified KDE desktop with a battery display.
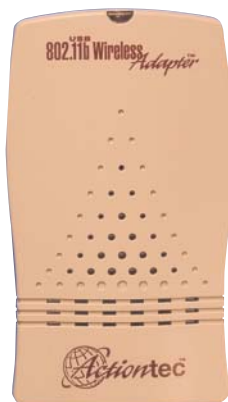
3Com X-Jack Wireless LAN Card

The 3Com 3CRWE62092A Wireless LAN Card with X-Jack antenna is the smallest competitor in our test. The retractable antenna is this card's strong point. This makes the 3Com X-Jack, as the card is normally referred to despite the complex model code, just the same size as a standard Type II card.
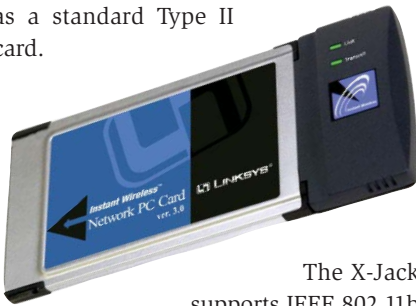
The X-Jack supports IEEE 802.11b with 128 bit encryption, just like the other candidates in our test.

The advantage is self-evident: You do not need to remove the card while transporting your laptop in a bag or case – on the contrary, the card will still work with the antenna retracted, although reception may be poor in this position.

Take care not to bend the antenna when retracting it – only the outside edges of the card lid have been

Figure 1: Cigar cutter included: The upper and lower halves of the lid are so sharp that they strip the plastic coating off the antenna – you can plainly see the plastic shavings and cuts

smoothed, the inside edges are razor-sharp and shave the plastic coating off the antenna. You can plainly see the plastic shavings and cuts in Figure 1.

The 3Com card uses the Poldhu chipset – the driver installation is detailed on page 19. The WLAN card costs somewhere in the region of £100, depending on your dealer, so do your homework before you buy – but that still makes it 20 percent more expensive than its competitors. The extremely practical (and patented) antenna makes this card stand out from the field and is a must for notebooks in daily use. And that's why the 3Com product also gets the Editor's choice award.

Linksys WPC11

The Linksys WPC11 card is based on the Prism 3 chipset, which requires the "Next Generation" driver package. Installing the card was no problem. The Linksys was also the only card in the test with two LEDs on top, one for the transmit and a second LED for the link status. If you are working in access point mode, the LED flashes on and off to indicate that the access point is out of range. The Linksys is a solid workhorse and the price, £70, is reasonable.

ZcoMax AirRunner XL325H

The AirRunner from ZcoMax is based on the Intersil Prism 2.5 chipset and as such requires the use of "Next-Generation" drivers. With the option for an additional antenna. We found this a good quality build product. The transmit power was a respectful 100mW although the XL325HP is reported to be 200mW. The external anntena connected via one of the reverse MMCX sockets. Again with two LEDs for power and transmit. Cost: £90.

Tellus TWL-R410 Wireless AP SOHO Router. (Elito-Epox EWL-R410)

The TWL-R410 by Tellus is a combined DSL router, 4 port switch, wireless access point and modem interface. The device, which costs over £200, to attach a laptop with a wireless card to the inter-net via DSL and / or
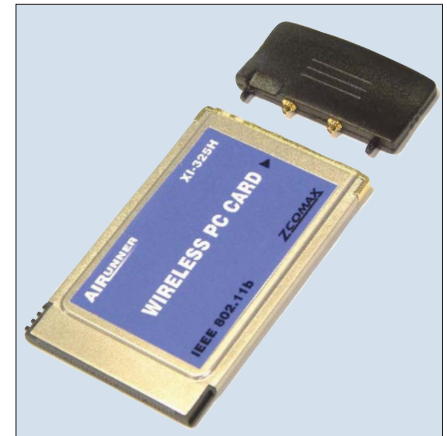
external modem. The TWL-R410's network ports allow you to attach up to four computers or network printers, and depending on the configuration, the access router can be used for seamless access from the wireless to the wired LAN – or it can be used to masquarade easily between the two environments.

The TWL-R410 is easy to configure via the Web frontend provided (Figure 2). One interesting feature is the fact that you can attach a serial modem, besides DSL or network access, thus permitting Internet access if the DSL link fails.

The access router can be secured via a list of permitted or denied hardware addresses and by means of 128 bit encryption.

Of course hardware addresses can always be spoofed, but at least it is an additional hurdle for the attacker to take.

The Tellus TWL-R410 seems to be an extremely well-engineered product. We particularly liked the idea of using an external modem as a backup line for a DSL connection – without the administrator needing to get involved, of course.
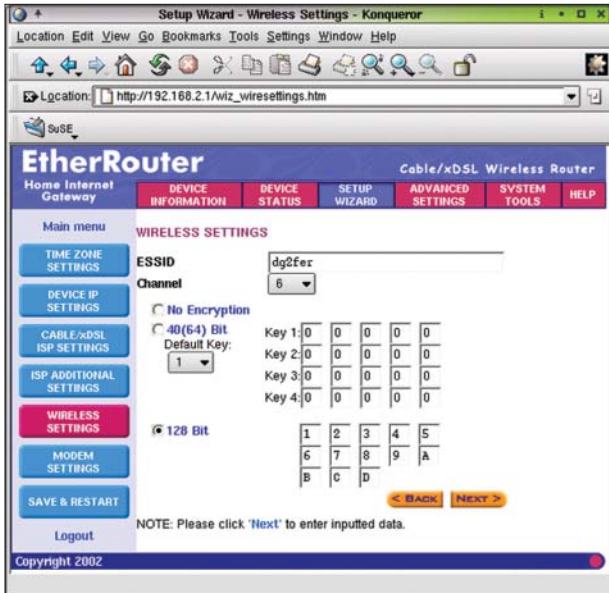
Figure 2: The Web frontend for Tellus' TWL-R410 provides access to a wide range of settings, without being too cluttered
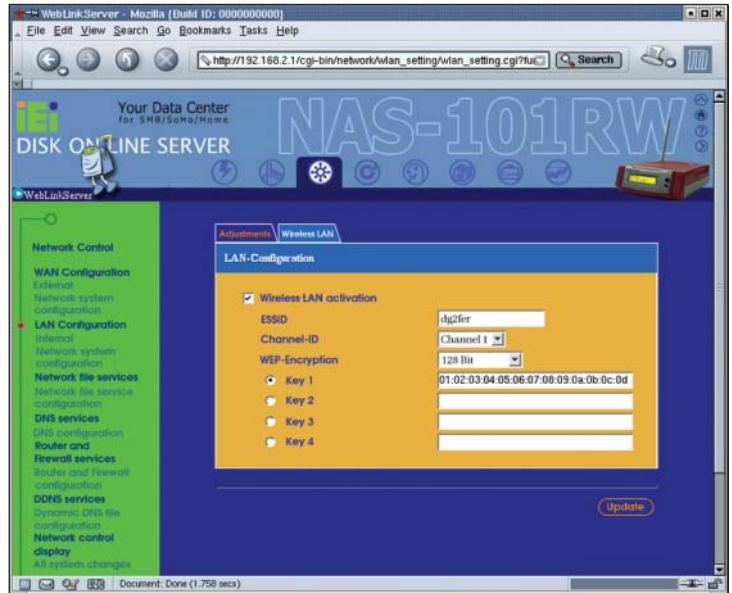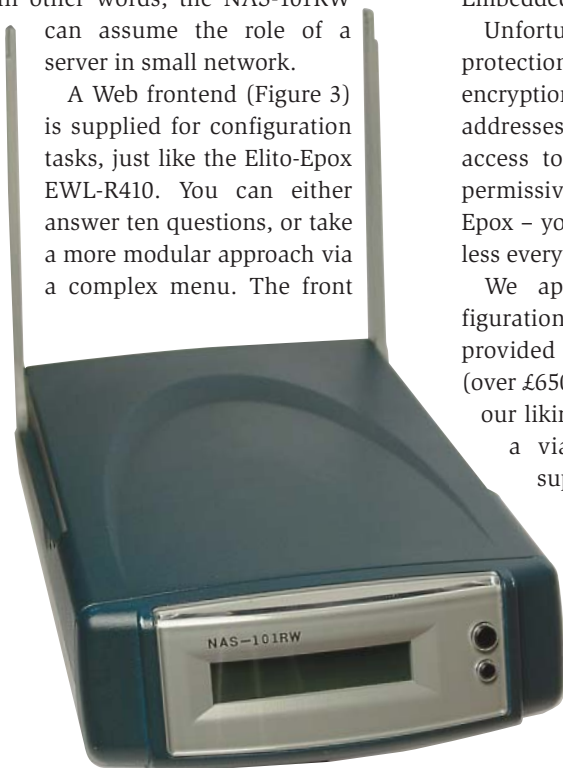

Figure 3: The Web frontend for the NAS-101RW is well-structured. If configured correctly, this allrounder can completely replace a server

IEI NAS-101RW Wireless NAS Access Router

Shortly before this issue went to print, a brand-new product arrived at our offices, IEI Electronics' NAS-101RW. This device can do more or less everything apart from making the coffee and sandwiches: It is at the same time a 4 port switch, a wireless access point, a DSL router, a network bridge, and a network storage device, and has a small footprint to boot. In other words, the NAS-101RW can assume the role of a server in small network.

A Web frontend (Figure 3) is supplied for configuration tasks, just like the Elito-Epox EWL-R410. You can either answer ten questions, or take a more modular approach via a complex menu. The front panel contains a display and various buttons that allow you to query the device's status and perform simple network configuration tasks.

The network drive can be assigned to various user groups, Windows clients, Macs, Novell and of course Linux clients via NFS, HTTP, and FTP.

The NAS-101RW even provides a complete user management module – by the way a look inside the router revealed an Embedded Linux system.

Unfortunately, the NAS-101RW's only protection against attackers is 128 bit encryption – a list of permitted hardware addresses is sadly lacking. However, access to the Web frontend is not as permissive as the R410 router by Elito-Epox – you need a password for more or less everything.

We appreciated the ease of configuration and the intuitive frontend provided by the NAS-101RW. The price (over £650) and the two fans were less to our liking. But still, the NAS-101RW is a viable alternative to providing support for a traditional server in small network environments.

Conclusion

Today's wireless LANs come in all shapes and sizes. Purchasing prices range from £150, for two simple WLAN cards, to £1000 for an access point with network drives and a handfull of WLAN cards. You can take an easy entry approach to wireless networking – start off with two WLAN cards, one in your desktop and the other in your notebook, and then add access points or access routers as your budget allows, until all your computers are on the wireless LAN.

By standardizing on using the IEEE 802.11b protocol it should ensure that wireless LAN devices will have no problem talking to one another now or in the future. ∎

INFO

Howtos and drivers:
http://www.hpl.hp.com/personal/ Jean_Tourrilhes/Linux

Actiontec cards:
http://www.actiontec.com/UK/

D-Link PCI Adapter:
http://www.mobtech.co.uk/ecbmob/ itm00959.htm

3Com XJack card:
http://www.dabs.com/3com/3com. asp?s=404

Linksys card:
http://www.dabs.com/linksys/linksys.asp

ZcoMax card:
http://www.zcomax.co.uk

Tellus Router:
http://www.uk2.21store.com

NAS router:
http://www.iei.com.tw
http://www.nasgenie.com