Lose the wires, keep the security

Until recently, it's been difficult to use the words "secure" and "wireless" in the same sentence. Recent developments mean that's no longer the case. We look at six different options.

By Matt Tett, RMIT IT Test Labs

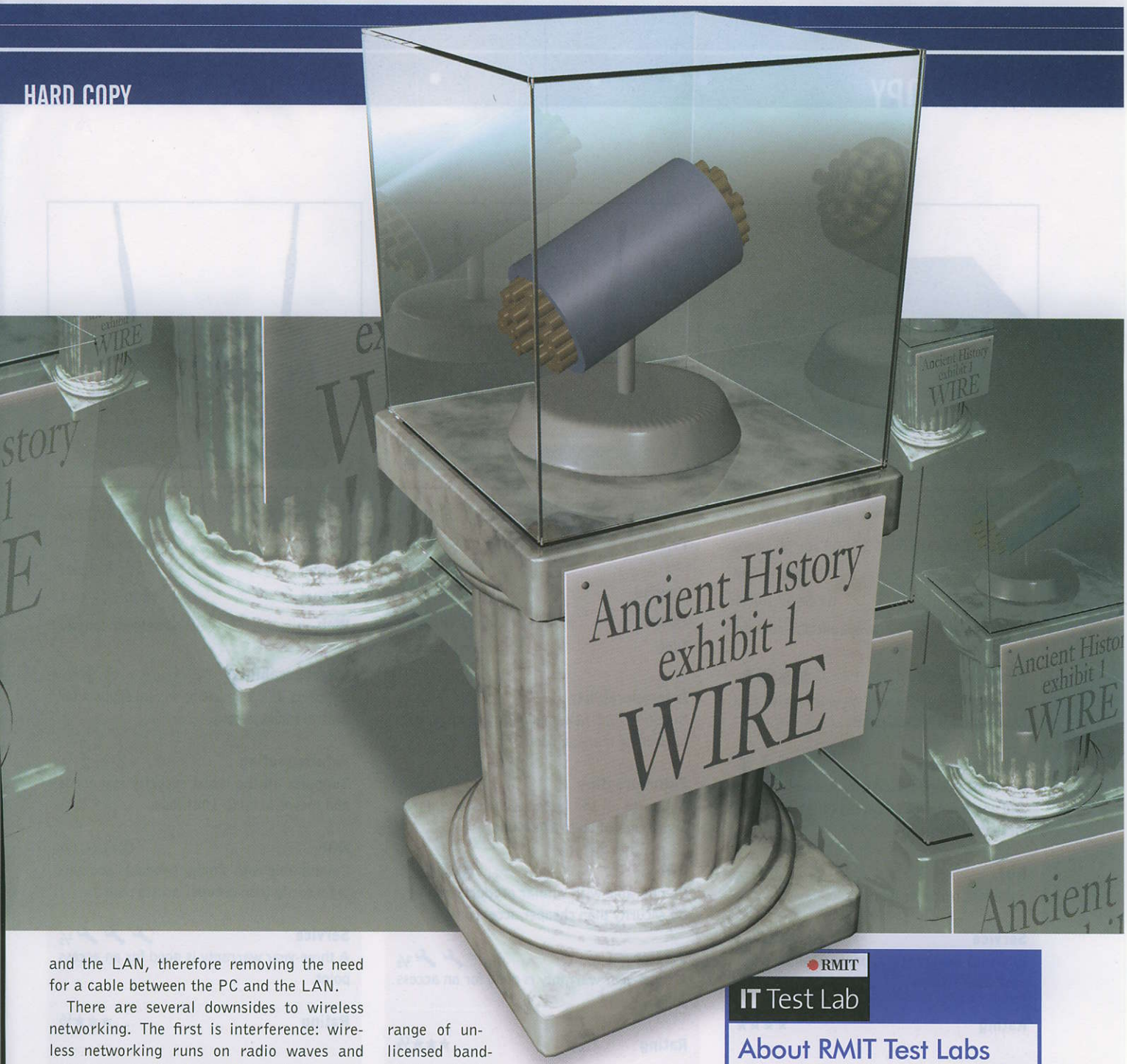
November 2003 was the last time the Test Lab had a look at wireless networking devices for *Technology & Business.* In that review we placed some emphasis on the security attributes of the wireless networking equipment. In March 2003, we looked at products designed to increase the security of wireless networks; these were virtually the first generation of products specifically designed for that purpose. They came in several flavours, including beefed-up access points, a dedicated hardware gateway, and a security software suite. In fact, the Editor's Choice winner of both those reviews was Netgear, with the FVM-318 in March 2003 and then the FWAG114 in November 2003. Lets see if Netgear can fend off another onslaught of wireless security opponents in this review and complete the hat trick.

Things have certainly heated up in the wireless security arena since both those reviews were published. Increasingly, enterprises are seeing wireless as a viable data delivery method to enable their staff more freedom around the office. This can increase productivity, reduce capital expenditure, as well as reducing deployment, licensing, and support costs by providing employees with a single notebook or tablet PC, instead of a desktop PC as well as a notebook/tablet.

Many businesses may have shelved their wireless plans previously due to well-publicised security concerns around the wired equivalent privacy (WEP) standard and the 802.11 technology concept, or because their already overburdened IT department simply did not have the resources to place into learning, developing, deploying, and supporting yet another IT system. However, many of these businesses are now sitting up and paying closer attention to the developments and benefits that wireless can provide.

Intel through its Centrino badge has done a great deal of marketing over the past eighteen months, prompting home users to create 802.11 wireless networks and also raising the awareness and profile of public wireless hotspots. Virtually all notebooks these days—and even some PC system motherboards—now come with wireless built in.

This review assumes that the reader is already familiar with wireless local area networks (WLAN). Suffice it to say, a basic wireless network consists of a wireless-enabled client PC (generally a notebook or tablet) and a wireless access point (AP)—most often a small box with one or two antennae that resides somewhere on the local area network (LAN), and enables the operator to connect wirelessly between their PC, the AP,



and the LAN, therefore removing the need for a cable between the PC and the LAN.

There are several downsides to wireless networking. The first is interference: wireless networking runs on radio waves and unless an operator has a licence to transmit in specific protected or licensed radio bands they must use the unlicensed spectrum. This means the more wireless equipment out there, the more the airwaves will become polluted. This is OK in a relatively remote location, but in crowded office buildings with many separate companies, it could become a lot more of a problem. Interference degrades the signal which leads to slower speeds or, in some cases, the total inability to operate. Most wireless equipment these days is capable of automatically hopping up and down a few channels to find the clearest link, however this is still very limited due to the small range of unlicensed bandwidth available.

The second downside to wireless LAN has been maximum data speed, however this is slowly improving. Early WLAN equipment ran at 2Mbps, then 11Mbps, followed shortly by 22Mbps and then 54Mbps. Recent developments from vendors like D-Link and Netgear have seen that now pushed to 108Mbps by combining two 54Mbps channels. However, this is still fairly proprietary, requiring particular brand APs and matched network interface cards (NICs).

Maximum data speed is of course theoretical. Real-life deployments must contend with both radio interference and physical

RMIT
IT Test Lab

About RMIT Test Labs

RMIT IT Test Labs is an independent testing institution based in Melbourne, Victoria, performing IT product testing for clients such as IBM, Coles-Myer, and a wide variety of government bodies. In the Labs' testing for *T&B*, they are in direct contact with the clients supplying products and the magazine is responsible for the full cost of the testing. The findings are the Labs' own—only the specifications of the products to be tested are provided by the magazine. For more information on RMIT, please contact the Lab Manager, Steven Turvey, at stevet@rmit.edu.au.

Product	ANTlabs ezXcess
Price	Gateway from $3500 for 50 users
Vendor	InTechnology
Phone	07 5657 5050
Web	www.antlabs.com.au

Interoperability ★★★★
Excellent interoperability; works with any wireless LAN access point.

Futureproofing ⌛⌛⌛⌛
Provides gateway security between wired and wireless networks, a task that will be in increasing demand.

ROI $$$$½
Excellent price for features.

Service 🔧🔧🔧½
One-year warranty appears standard for gateway devices.

Rating ★★★★

Product	D-Link DWL-7100AP
Price	Access point $549.95, NIC $154.95
Vendor	D-Link
Phone	02 8899 1800
Web	www.dlink.com.au

Interoperability ★★★½
Supports 802.11a,b, and g; no real support for central management.

Futureproofing ⌛⌛⌛½
Supports all the latest security standards and speeds of up to 108Mbps.

ROI $$$$
Comparable with similar products and better security than cheaper access points.

Service 🔧🔧🔧½
A three-year warranty is good for an access point.

Rating ★★★½

Product	Netgear WG302
Price	Access point $579
Vendor	Netgear
Phone	1800 502 061
Web	www.netgear.com.au

Interoperability ★★★
Supports 802.11b and g; no real support for central management.

Futureproofing ⌛⌛⌛½
Supports all the latest security standards and speeds of up to 108Mbps.

ROI $$$$
Comparable with similar products and better security than cheaper access points.

Service 🔧🔧🔧½
A three-year warranty is good for an access point.

Rating ★★★½

TEST BENCH

Interoperability
What wireless protocols does the device support? Can it be managed centrally to reduce admin work?

Futureproofing
Does the device include recent security standards? Will it grow with your needs?

ROI
Does the enhanced level of security the device provides justify the price?

Service
What is the warranty? What service and maintenance contracts are available?

Product Nortel Wireless LAN 2200 Series
Price Gateway US$10,999, access point US$599
Vendor Nortel Networks
Phone 02 8870 5000
Web www.nortelnetworks.com

Interoperability
Supports 802.11a,b, and g. Access points rely heavily on proprietary technology.

Futureproofing
Very secure, very scalable.

ROI
Very expensive but very secure.

Service
One-year warranty appears standard for gateway devices.

Rating ★★★½

Product SonicWALL Distributed Wireless
Price Gateway from US$1434, access point US$744, NIC from US$114
Vendor SonicWALL
Phone 03 9699 1978
Web www.sonicwall.com

Interoperability
Supports 802.11a,b, and g. Access points rely heavily on proprietary technology.

Futureproofing
Very secure, very scalable, supports speeds of up to 108Mbps.

ROI
Very good pricing for an integrated one-stop wireless network security system.

Service
One-year warranty appears standard for gateway devices.

Rating ★★★★

Product 3Com Wireless LAN Access Point 8250
Price Access point $700, NIC $99
Vendor 3Com
Phone 1800 678 515
Web ap.3com.com

Interoperability
Upgradable to support 802.11a,b, and g standards; works well in a managed environment.

Futureproofing
Good support for current WLAN security standards.

ROI
A little on the expensive side.

Service
One-year warranty is a little below the average for an access point, but an extended warranty is available.

Rating ★★★★

interference (physical objects, distance, etc), the bandwidth overheads of maintaining the wireless link itself, implementing security across the link (eats bandwidth), the number of users on the system, (including the amount of data they are likely to be shunting back and forth and the number of users performing simultaneous data transactions across the network), and the distance between the users and the access points.

The basic premise in corporate WLAN security deployment is similar to the concept of a Virtual Local Area Network (VLAN) available in most modern network switches; the WLAN should be as separate as possible from the rest of the LAN. This has several benefits. Firstly, this makes it easier to manage and contain threats should a problem arise on the WLAN. Secondly, it provides a single point of connection between the WLAN and the wired network, enabling the security team to monitor that single connection for any suspicious behaviour and to deploy adequate equipment such as internal firewalls and dedicated wireless security gateways.

VLAN is not only a comparable technology, it is also a complementary one. Instead of investing in brand-new infrastructure such as dedicated cabling and switches to support the new wireless deployment, many companies are simply enabling a VLAN on their existing network switches and separating the ports that have the APs plugged into them onto their own VLAN. This VLAN is then a virtual separate network (it can even have different IP ranges etc) and a gateway can

Product	ANTlabs ezXcess	D-Link DWL-7100AP	Netgear WG302	Nortel Networks Wireless LAN 2200 Series	SonicWALL Distributed Wireless	3Com Wireless LAN Access Point 8250
Vendor	InTechnology	D-Link	Netgear	Nortel Networks	SonicWALL	3Com
Phone	07 5657 5050	02 8899 1800	1800 502 061	02 8870 5000	03 9699 1978	1800 678 515
Web	www.antlabs.com.au	www.dlink.com.au	www.netgear.com.au	www.nortelnetworks.com	www.sonicwall.com	ap.3com.com
Price of gateway (RRP inc GST)	50 users from $3500 to 2000 users for $16,500	N/A	N/A	Security Switch 2270 US$10,999	TZ170 US$1434, Pro 2040 US$2394	N/A
Price of access point (RRP inc GST)	N/A	DWL-7100AP $549.95	$579	Access Port 2230 US$599	SonicPoint US$774	3CRWE825075A $700
Price of PC-Card network interface (RRP inc GST)	N/A	DWL-AG660 $154.95	N/A	N/A	802.11b US$114, dual band US$179	Xjack $99
Warranty	1 year with service level agreement	3 years	3 years	1 year	1 year	1 year hardware, 90 days software
Extended warranty available	✓	✘	✘	✓	✓	✓
Wireless network standards supported	All	802.11a, b, g, 108Mbps	802.11b, g, Super G 108Mbps	802.11a, b, g	802.11a,b,g, 108Mbps	802.11b, g; 802.11a upgrade available
Recommended users per access point	N/A	40	32	30	25	253
Outdoor range with included antenna(s) (m)	N/A	100m	200m	600m	N/A	100m
Supports wireless-to-wireless bridging	N/A	✓	✓	✘	✘	✓
Removable antennas	N/A	✘	✓	✓	✘	✓
Can act as DHCP server	✓	✓	✓	✘	✓	✓
Can disable SSID broadcasting	N/A	✓	✓	✓	✓	✓
NAT support	✓	✘	✓	✘	✓	✘
WEP support	✘	✓ 152-bit	✓ 152-bit	✓	✓ 128-bit	✓ 154-bit
WPA support	✓	✓ WPA(TKIP), 802.1x, AES	✓ TKIP, AES, WPA-PSK	✓	✓ TKIP, AES, 3DES	✓ 256-bit AES, TKIP
802.11i support	✓	✓	✓	✘	✓	N/A
MAC address filtering and authentication	✓	✓	✓	✓	✓	✓
IP address authentication	N/A	N/A	✓	✓	✓	✘
External authentication	✓	✓	✓	✓	✓	✓
Inbuilt firewall	N/A	N/A	✘	✓	✓	✓
Inbuilt intrusion detection	N/A	N/A	✘	✘	✓ (optional service)	✘
IPSec VPN WLAN connectivity	✓	N/A	✓	✓	✓	✘
Supports central management of multiple access points	N/A	✘	✓	✓	✓	✓

then be plugged in between that VLAN and the rest of the corporate network.

The main benefit of the truly enterprise-level wireless equipment now on the market is centralised management. While many other technologies have needed to be redesigned with this concept in mind, these wireless systems seem to have been developed at the right time to take advantage of centralised management immediately without needing any fiddly upgrades or add-ons to enable it. Most are still proprietary to each vendor, however this factor is more than offset by the savings made in deployment, management, and support costs by deploying a single-vendor solution, particularly if used by a larger enterprise requiring many distributed access points.

There are also two other developments in wireless security, that have only recently begun to be incorporated into the equipment, namely Wi-Fi Protected Access (WPA) and 802.11i. Many vendors started to offer WPA—which is basically a subset of some of the proposals found in the 802.1i specification—as an interim security measure before the 802.11i standard was passed. We will most likley see WPA falling into the background as vendors move to 802.11i.

Both use AES encryption, however there are a a few minor differences, mainly in the way keys are handled. WPA mostly uses the temporary key integrity protocol (TKIP) and 802.11i uses AES-CCMP (CCMP somehow

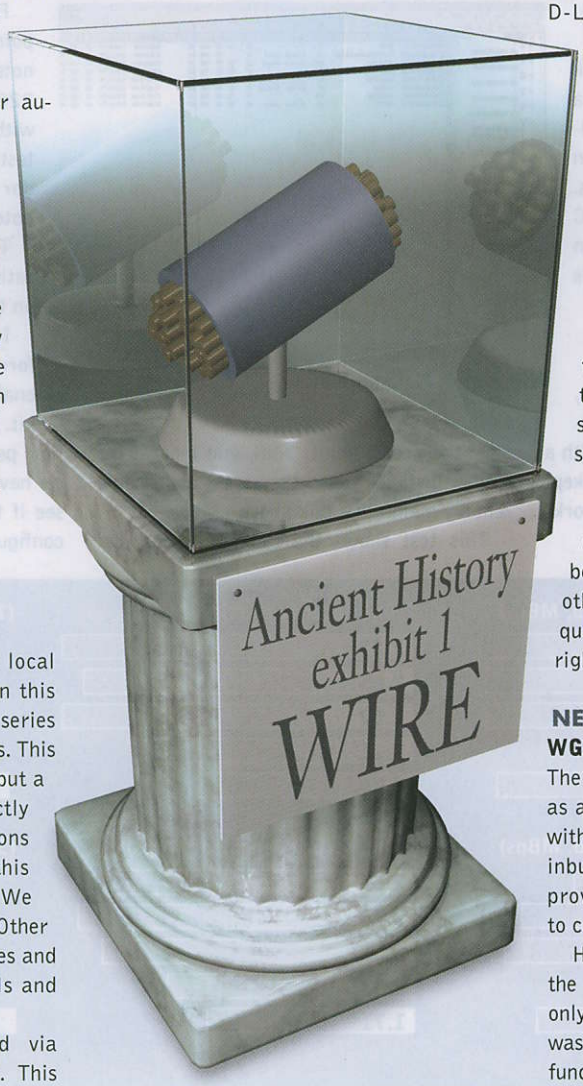
stands for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). CCMP is technically the stronger of the two, however it would still take several hundred years to crack encrypted data using TKIP's data encryption enhancements. This is a very interesting debate and I would enourage anyone with more than a passing interest in this subject to do some further research. A good starting point is *www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf*

WPA uses the 802.1x standard for authentication and requires a separate RADIUS authentication server. (RADIUS stands for remote authentication dial-in user service, but it's not only used for dial-in connections.) If a small business does not have the resources to deploy a RADIUS server, an alternative is to run WPA-PSK— a shared passkey system. When using WPA-PSK, the administrator must be careful though because it introduces some potential vulnerabilities. If the option exists to run a RADIUS server then that path is definitely the more secure option.

ANTLABS
ezXcess SG Standard
Funk Software Steel Belted RADIUS

InTechnology is better known as the local supplier of Funk software, however on this occasion the vendor delivered one of a series of products from ANTlabs called ezXcess. This product is not a wireless access point, but a gateway device. This device is not strictly limited to wireless network applications either, however for the purposes of this review we will limit it to this task. We looked at the entry-level SG Standard. Other models have different network interfaces and can support larger numbers of VLANs and concurrent users.

Initial configuration is performed via a Web interface on the Trusted port. This enables the adminstrator to set up all the predefined ranges such as IP addresses, IP leases, and access modes. There are so many configuration options available it just is not funny; the designers have really left no stone unturned when looking at the functionality of this device. All this complexity provides the back-end for users to connect seamlessly with zero config. As soon as users connect to the AP and open a Web browser, they are presented with a login page from the ezXcess appliance. Administrators can select to authenticate users via 802.1x or RADIUS server. This is where Funk software's Steel Belted RADIUS comes in. There is even an option to use the system to generate billing data and information.



Once set up and running, the day-to-day administration is minimal, in fact we would assume that the administrators would have more regular interaction with the RADIUS server than the ezXcess appliance itself.

For businesses looking to provide users with temporary hassle-free access to their network resources, this solution is definitely something to consider. For businesses wanting to separate their WLAN network infrastructure and authenticate the users separately from other network connections, this is the appliance for them.

D-LINK
DWL-7100AP

D-Link's DWL-7100AP access point is an access point supports the 802.11a, b, and g standards and can run up to 108Mbps in D-Link's 108AG Turbo Mode. As for security, it has options to run either 152-bit WEP or WPA with AES encryption. The 7100 also can operate as a point-to-point (PtP) bridge, as well as a point-to-multipoint (PtMP) bridge with other access points based on their MAC addresses.

Configuration and administration of this access points is very straightforward through a Web interface. The initial basic configuration is handled by a simple step-by-step wizard.

Overall this D-Link access points shows a great move forward in both security and features. While 108Mbps may be a proprietary speed for the time being, other features such as the 7100's dual-frequency support are a definite move in the right direction.

NETGEAR
WG302 ProSafe

The WG302 from Netgear initially struck us as a basic 802.11g standalone access point with no redeeming security features. The only inbuilt security was WEP, which has been proven time and time again to be very easy to compromise.

However, we discovered the firmware on the unit we had been shipped for testing was only version 1.0.2, while the latest version was 2.0.3. This firmware adds a lot of security functionality such as WPA, WPA-PSK, RADIUS server support, and Netgear's 108Mbps top speed (Super-G).

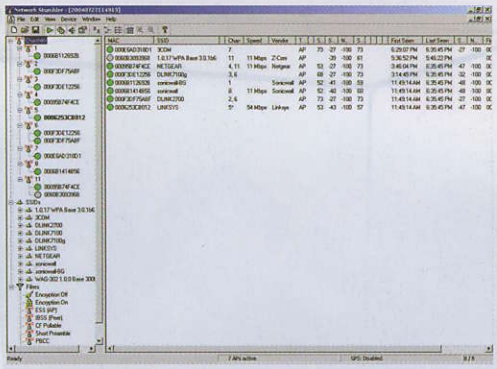
Updating the firmware was no walk in the park, however credit must be given to Netgear's online instructions that were relatively simple to follow for someone who is technically literate. There were a few potential pitfalls, but luckily we avoided these and

HOW WE TESTED

We constructed a series of tests to determine the effectiveness of each package's ability to secure a wireless connection, and if there was any reduction in performance as a result of enabling this security.

TEST 1: NETSTUMBLER

We ran Netstumbler, a wireless network discovery, mapping, and logging tool on a generic clone notebook fitted with a dual-mode network card to see what information was being broadcast from the access points. NetStumbler logs information such as MAC addresses, SSIDs, and possible encryption such as WEP. All the access points in this review could hide their SSIDs effectively.



Testing with NetStumbler.

TEST 2: PERFORMANCE

We developed an in-house test procedure, using a local FTP server connected directly to the LAN port of the access point with a crossover RJ45 network cable. This was kept totally separate from all other wired networks to ensure no wired LAN interference.

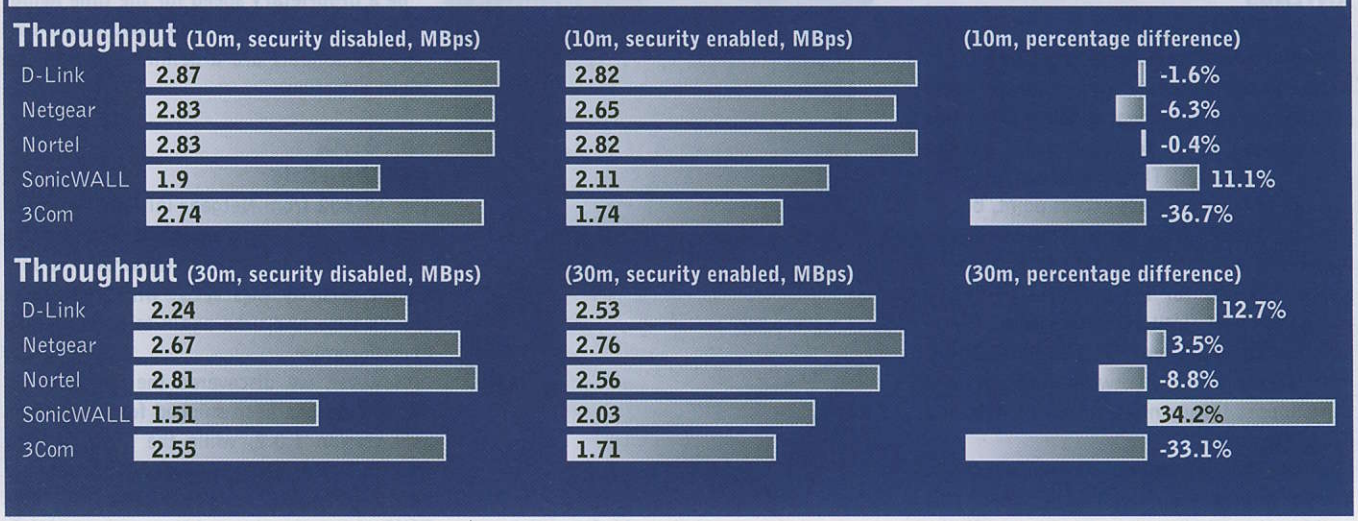
We then ran a simple script at measured intervals within the corridors of our building. The script downloads a file from a server to the mobile device five times and records the average throughput. This test we ran at 10m from the access point, 30m, and then at the further distance where the access point could reliably maintain a link above 1Mbps.

This test shows the maximum physical distance achieved between the client and the access point. We ran the test both with WPA security disabled and enabled, to see if there was a noticeable difference in performance as a result of using the security features.

First we tested each vendor's access point using an Acer Travelmate 8000 notebook with an Intel Pro Wireless 2200BG integrated network interface with no wireless security set up. This test provided a baseline result of a vendor non-specific connection between the notebook and the vendor's access point.

The second test used the same configuration with WPA-PSK encryption enabled on the wireless network.

Interestingly some of the devices performed better with WPA-PSK encryption enabled while others took a performance hit. This goes to show it is worthwhile running performance tests against a baseline as we have done before deploying equipment to see if there are any overheads with various configurations or vendors.



managed to get the updates completed with the minimum of fuss. The rest of the configuration was fairly straightforward using the well designed Web interface.

Overall this unit has very similar features to the D-Link DWL-7100AP, however the Netgear WG302 lacks the dual-band capability.

NORTEL
Wireless LAN Security Switch 2270
Wireless LAN AP 2230

Nortel provided a very impressive distributed wireless LAN security device with its own uniquely shaped access points. The APs support 802.11a, b, and g. They have an internal antenna as well as room for three external antennae, two for 2.4GHz and one for 5GHz.

Initial configuration is via the console (serial) port. Basic console configuration takes the administrator through a guided series of questions to set IP configurations, DHCP pool server addresses, RADIUS server ad-

Things to look out for . . .

- **Ease of management.** If you are looking to deploy more than three or four access points in the company, then a centrally managed system may be worth looking at. Even if you plan to start off small but may be expanding the wireless network in the future, a centrally managed system is worth considering.
- **Support for security standards.** Some wireless systems require proprietary cards or client software to run securely. This can lead to added support costs involved in setting up clients and supporting them. Also, if the system requires proprietary vendors cards, these may be expensive or may not interoperate well with the equipment that they are being installed into. They do not provide very good futureproofing.
- **Support for different standards.** Not knowing what equipment your users may wish to connect to the wireless network could potentially cause troubles. Try to ensure that the access points you select support both 802.11a and 802.11g. Remember g is backward compatible with b, so basically you would be covering all current standards. (Don't worry about 108Mbps for the time being, this is not a "standard" speed yet and is proprietary to a few vendors.)
- **Ease of deployment.** Power over Ethernet (PoE) is a technology fast becoming popular now for a variety of applications from VoIP to WLAN, this eases the deployment by having to only provide a single RJ45 cable to the access point. This provides both data and power needs. Configuration should also be considered when deploying a solution, so those larger deployments should really consider centralised management solutions, as these generally enable the administrator to set policies and configuration options for the access points and then push them out to the hardware. This also enables centralised reconfiguration, updates, redundancy, and reporting.

dresses, and so on. Note that to get the APs running, you must have a DHCP server running on the network. After the system reboots, the administrator can then access the device via a Web interface.

Security is the primary design of the Nortel solution and there are many security features incorporated into the device. It only took 10 to 15 minutes to set up initially for a relatively technically literate person. The system appears potentially to be very hard to work with, however after spending an hour or two setting up various policies, an administrator can begin to appreciate both the functionality and the relative ease of use, considering the quite complex tasks being performed.

The Nortel solution is very expensive, but is still possibly the best integrated wireless-only security product in this review. Nortel has certainly made an effort to address every detail when designing this kit. If you are in the market for a secure, powerful, centralised, distributed wireless LAN solution, the Nortel package is a definitely worth a look.

SONICWALL
SonicWALL Pro 4060
SonicPoint AP
TZ170 AP
SonicWALL PCMCIA Card

Vigilant readers will have realised that SonicWALL submitted exactly the same piece of kit for the intrusion detection and prevention review in last month's edition of *Technology & Business* magazine (August 2004), the Pro 4060. This time, the folks at SonicWALL also supplied us with two SonicPoint access points, which connect to any of the Pro-series appliances to provide a centrally managed distributed wireless access and security system. This has the added benefits of being able to operate as a firewall and IPS. SonicWALL also supplied a TZ170 wireless access point for smaller businesses.

Installation and configuration for the SonicPoints is through the SonicOS interface, which is accessed via a browser on the internal port of the appliance.

The SonicPoints are specifically designed to connect to one of the network ports on any of the Pro series of appliances. The administrator creates the configuration settings for the devices, then the firewall/IPS appliance searches the network for SonicPoints, registers them, and updates their configuration accoording to its records.

The beauty of this system is that it also enables the administrators to search for and identify rogue access points on the network. It also greatly reduces the management of the wireless network and enables updates and changes to the AP configurations to be pushed out from one central location. And since it is on a separate logical network interface, the data can be screened and processed separately by the appliance.

SonicWALL can offer "wireless guest services", which enables a company to provide a short-term username and password to visitors or anyone who is not regularly expected to need access to information or services on the network.

Administration of the system is definitely more overwhelming than just a simple wireless gateway system, because the appliance can incorporate firewall and IDS/IPS functionality as well. Compared to running separate firewalls, intrustion detection and prevention systems, and wireless security systems, it is not really that complex at all . . . provided you need all that functionality.

Overall the SonicPoint solution would have to be the most integrated security solution we have seen in the lab to date, incorporating wireless security, firewall, and intrusion detection/prevention in the one appliance. If this is the way of the future, the security administrator's job is definitely going to get a lot better. Who knows, there may even be time to write policies and deploy them rather than spend all day maintaining the disparate security components to ensure that they are all working well.

3COM
AP8250
802.11 a/b/g Wireless PC Card

The 3Com AP8250 is one of the most futuristic shapes of AP we have seen. Once the unit has been plugged in and powered on, configuration is done using the 3Com Wireless Infrastucture Device Manager, which is bundled on the included CD with various other tools and utilities. This device manager takes a few seconds to install on a host PC, and allows the administrator to configure any 3Com APs it detects. Once the initial pre-IP configuration has been completed, the operator is then launched straight into a browser-based configuration screen that offers the choice of advanced setup or a setup wizard for the remainder of the configuration.

On the security side, 3Com supports RADIUS authentication, 802.1x authentication, and MAC address filtering. 3Com even supports Windows user authentication as well as WEP (in legacy mode too for older clients), WPA (AES & TKIP), and WPA-PSK.

Overall this is a very neat enterprise-orientated product with a excellent feature set, particularly in security. It's very easy to deploy and looks good too.

3Com also sent a dual-frequency (2.4GHz and 5.0GHz) network interface card, allowing the user to connect to any hotspot or wireless network they encounter. 3Com has also included features such as WPA, autonomous load balancing (ALB), and 802.1x support. There are also proprietary 3Com security features too, such as 3Com's Serial authentication (using EAP-TLS and EAP-MD5) and Dynamic Security Link, both of which require compatible 3Com APs to work. If you are deploying all 3Com-branded wireless equipment into a new site or looking to replace all existing wireless cards and APs, these products may deliver a edge above and beyond the wireless security standards that exist today. But don't forget you would be locked into a single vendor environment for the life of the technology.

FINAL WORDS

Wireless security has finally come of age and can only from here on in begin to provide better peace of mind for CTOs and security admins.

A word of warning: don't rely on WPA-PSK unless you must; if the wireless budget can accommodate, it is definitely better to run a RADIUS server. If the cost cannot be justified, ensure the PSK passkey is greater than 20-bits and preferably a random alphanumeric string, not an easy-to-guess series of characters.

With a range of products reviewed here providing a well planned, robust, and secure wireless LAN solution should not be as formidable as it once was. As long as the network planners take into account all the factors involved with WLAN technology and don't try to overextend the WLAN capabilities, it should be plain sailing. ■

EDITOR'S CHOICE

Scenario 1

Company: Honest John's Mobile Phones
This company wants to install a wireless network in its office, but has serious concerns about the security of wireless.
Approximate budget: Open
Requires: Wireless access points sufficient for 150 mobile users, with strong security and management features.
Concerns: The make-or-break feature will be the built-in security; consumer-level security such as WEP or a basic firewall will not be sufficient. Likewise, the management features of the access points must be up to enterprise standards, and the ability to manage the access points centrally will be a major consideration.
Best solution: For comprehensive wireless security and management features, Nortel provides an excellent system, at a price. Companies should never spend more on protecting an asset than the asset itself is worth, so Nortel's package will suit the requirements of larger businesses. For a fully-featured security solution at a more SME-friendly price, the SonicWALL range also helps busy admins reduce the amount of work they need to do configuring their various security systems.

TECHNOLOGY & BUSINESS EDITORS CHOICE AS TESTED BY RMIT LABS

Editor's Choice: SonicWALL SonicPoint

Many administrators may fear installing a wireless network because of the extra work required to keep it secure. By integrateing wireless security with its current firewall and intrusion detection/prevention infrastructure, SonicWALL is likely to do very well by minimising the additional work required. We think this points the way for a future direction in security.

Unleashes Your Day.

Distributed Wireless Solution

Comprehensive Security for both your Wired and Wireless Networks!

- **Integrated secure WLAN makes adding wireless easy and affordable**
- **Dual-radio 802.11a/b/g SonicPoints enable wireless roaming, guest services, rogue AP detection and more**
- **Low total cost of ownership; easily scales from 2 to 128 SonicPoints**
- **Standards-based: WEP, WPA, IPSec and future 802.11i for airtight wireless security**

SonicWALL

Distributed Wireless Solution

Busi-soft COMPUTERS
Busi-Soft - 1300 888 602

NETWORX AUSTRALIA
Networx Australia - (02) 8383 5223

ACTIV AUSTRALIA
Activ Australia - (02) 9284 4200

BASS COM "Enjoy life"
BassCom - (08) 9474 2455

SONICWALL