

# Developments in Network Technology



Faculty of  
Information Technology



Chartech books

# DEVELOPMENTS IN NETWORK TECHNOLOGY

by  
Tony Jeffree

*This report is published by the Faculty of Information Technology of the Institute of Chartered Accountants in England and Wales. The views expressed do not necessarily reflect those of the Council of the Institute.*

*Copyright © 2003 The Institute of Chartered Accountants in England & Wales.*

*All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission of the publisher.*

*No responsibility for the loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by the publisher.*

*ISBN 1-84152-201-5*

---

# **CONTENTS**

<b>PREFACE</b>	<b>4</b>
<b>1. MANAGEMENT SUMMARY</b>	<b>6</b>
<b>2. FLEXIBLE NETWORKING</b>	<b>8</b>
<b>3. HIGH SPEED INTERNET ACCESS</b>	<b>15</b>
<b>4. SECURE WIDE AREA COMMUNICATION</b>	<b>22</b>
<b>5. FUTURE DEVELOPMENTS</b>	<b>27</b>
<b>Appendix 1 USEFUL WEB RESOURCES</b>	<b>28</b>

---

# PREFACE

The use of computer networking has seen an explosive growth over the past two decades, developing from a set of expensive, specialised technologies used by a small number of large organisations, to its present-day state, where networking products and services have become ‘off-the-shelf’ commodities available to business and home users alike.

The networking technologies themselves are also developing at a rapid pace. To take a simple example, the data transmission rates achievable in Local Area Networking technologies (LANs) have increased by a factor of 1000 since the early 1980s; at that time, the state-of-the-art in LANs was around 10 megabits per second, whereas now, LAN technologies can offer data rates in excess of 10 gigabits (ten thousand megabits) per second. As with the developments in PC technology, the increase in power and speed has come with a corresponding decrease in size and cost; an Ethernet networking card for a PC can now be had for less than £20, and occupies a few square inches of card area, compared with £200 or more in the early 1980s for a card up to five times as large.

With the advances in networking technology, as with other aspects of IT, come opportunities for the business user. These opportunities can offer improvements to current ways of doing business (e.g., doing what you do now, but better and faster), or they can offer new ways of doing business that could not have been contemplated before. An obvious example here is the advent of the Internet, and with it, the World Wide Web, which has made e-commerce a realistic possibility, and some would argue, an essential offering, for modern businesses in the 21st Century. Hence, as well as looking at technology from the point of view of what it can do to serve existing businesses, it is also important to look at what new business opportunities might exist as a consequence of what the technology now allows you to do.

While it is unrealistic for the non-IT professional to become an expert in the emerging technologies in networking, it is nevertheless useful to have some level of understanding of the direction in which technology is currently

---

developing, and what the implications might be for today's businesses, as a precursor to deciding what to buy and install in order to meet the specific needs of a business. Given the expected readership of this guide, awareness of such technologies may be important, not only for their potential use within the reader's own organisation, but also within client organisations that the reader may work with in an advisory role. This guide is therefore aimed at introducing some of these emerging technologies and to show the benefits they can deliver to a business, rather than explaining the fine details of the technology. It will be of particular interest to readers who:

- have an old network which is in need of replacement;
- have an existing network but are not up to date of what is now possible with emerging network technologies;
- need to upgrade their network.

# 1. MANAGEMENT SUMMARY

There are two basic families of networking technologies in use today within businesses of all sizes, and also, increasingly, within the home environment:

- Networks that are primarily used to interconnect computer systems and their peripherals within a building or campus are referred to as Local Area Networks or LANs. Generally speaking, a LAN is under the control of a single organisation, usually the organisation to which it provides its networking services.
- Networks that are used to interconnect computer systems over longer distances are referred to as Wide Area Networks, or WANs. WANs are generally operated as public services; in other words, the network is controlled and operated by one supplier organisation, and its services are offered to interconnect multiple user organisations.

Unlike LANs, whose origins are to be found in the computer industry, WANs have historically been closely related to the telephony industry; in fact, many of today's digital telephone networks use essentially the same technology as wide area data networks.

The wide area network that is undoubtedly the most familiar today is the Internet, whilst the most widely known LAN technology is probably Ethernet.

From the above description, it is clear that WANs and LANs exist in two quite distinct environments, each with its own set of problems:

- LANs exist within the relatively 'safe' environment of a single organisation, and are used mostly for communication between individuals and systems within that environment.
- WANs are generally networks that, to a greater or lesser degree, interconnect multiple organisations, and are used for communication either between geographically distributed parts of one organisation, or between two or more distinct organisations. This environment is clearly not as 'safe' as the

LAN environment; for example, WANs immediately introduce the opportunity for one organisation's data to be monitored by another, unless steps are taken to prevent this.

As an organisation's use of networking becomes more sophisticated, it will often find that there is a need to integrate its LAN and WAN use, in order to gain the most out of the technology that it employs. This in turn highlights three specific problems that are key to the way in which today's businesses are able to successfully exploit network technology:

1. How to make access to the corporate LAN as flexible as possible, particularly as the growth of a remote workforce who are not based in the main office continues apace.
2. How to integrate the LAN with a WAN in a way that gives high speed access to services attached to the WAN.
3. How to ensure that communication over the WAN is not compromised by the fact that your data may be passing through equipment owned and operated by other companies or organisations.

The following sections take a look at emerging network technologies that directly address these key problems. Each section is organised along the following lines:

- A description of the network technology and how it interacts with other technologies.
- A discussion of the implications for business, why the technology is important, what types of applications might it support, and what kinds of business opportunities might emerge through using it.
- A discussion of some of the practical issues and factors to be considered in deploying the technology.

## 2. FLEXIBLE NETWORKING

### The technology

The majority of LAN installations to date have been based on fixed cabling of one kind or another. Early LANs used coaxial cables; more recently, twisted pair cabling has taken over from coax, with some use of optical fibre where particularly high data transfer rates are required. The problem with cable-based networking infrastructures is just that – they are cable-based, and so every device that needs to connect to the LAN has to have a cable trailing from it.

Two relatively new networking technologies aim to change the way we think about constructing and using LAN installations:

- 802.11 Wireless LANs, sometimes known as ‘Wi-Fi’ (an adaption of the popular home entertainment term ‘Hi-Fi’);
- Bluetooth.

### *Wireless LAN*

A wireless LAN, as the name implies, offers a wireless connection between a computer system and the LAN, via a *wireless access point*. The data transmission rates that can be achieved are relatively low when compared to the performance of the early Ethernet LANs, but are more than adequate for connecting the average PC or laptop to a LAN, unless applications that demand high data rates are being used.

Wireless access points generally have an Ethernet port that allows them to be connected to a conventional wired LAN (see Figure 1), but for small business use, it is possible to network a number of PCs together using only a wireless access point.

Connecting a PC or laptop to the wireless LAN involves the use of a wireless LAN interface that will slot into a laptop, or plug into a desktop PC. Increasingly, modern laptop computers are being manufactured with inbuilt wireless LAN capability, in anticipation that they will be used in this way. Assuming that the

security features of the technology have been correctly set up, the wireless 'connection' between the computer and the wireless access point is established automatically when the two devices are within radio range. The range of transmission is variable, depending on the construction of the building that it is used in, but can cover distances of up to 100 metres under the right conditions. If it is necessary to use more than one wireless access point to achieve the necessary coverage within a building, a wireless-enabled PC will automatically connect to the access point that offers the best signal.

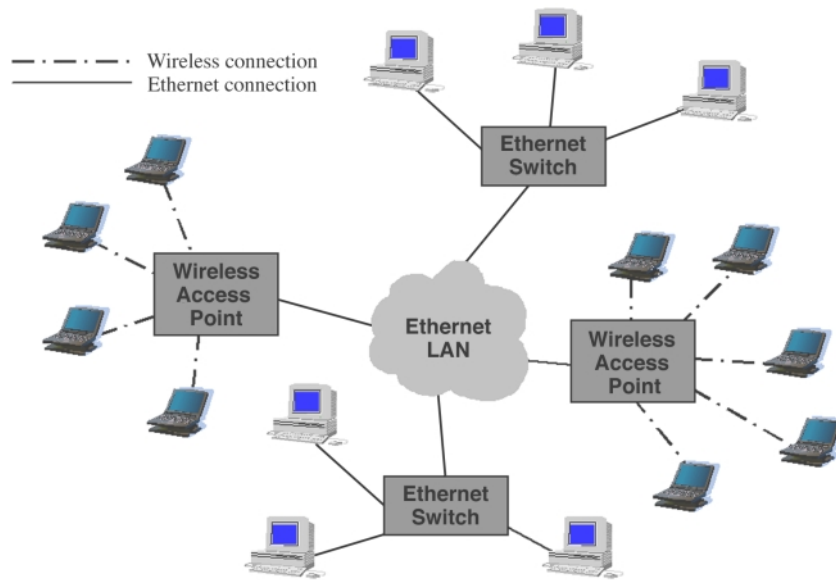


Figure 1: Wireless access points with Ethernet port

### *Bluetooth*

Bluetooth is a technology that was originally conceived as a means of replacing the cables between a computer and its peripherals – for example, printers, scanners, and so on. The data transfer rates that it can achieve are adequate for this kind of use, but not for connecting a PC to a LAN. It is now starting to appear in conjunction with other kinds of devices as well – for example, to connect a palmtop computer to a host PC, or to connect a hands free kit to a mobile phone. The transmission range for Bluetooth is significantly shorter – tens rather than hundreds of metres, and as less power is needed to drive the radios in Bluetooth devices, this technology is more appropriate than Wi-Fi for use in smaller, low power devices.

## **Implications for business**

### *Wireless LAN opportunities*

After a fairly slow start, the use of wireless LAN technology is increasing rapidly at the moment, as more organisations begin to appreciate the potential benefits.

The first and most obvious benefit for business is that the use of wireless technology can considerably simplify the job of ‘wiring up’ a building for LAN access. The simple fact that it is not necessary to provide each individual machine with its own network cable can result in cost savings, especially in older buildings where installing new cabling is difficult, or where it is desirable not to interfere with the architectural or decorative features of the property. Cable installation can be kept to the minimum required to establish the interconnections between the access points.

The second significant area of benefit concerns the opportunities that the technology offers to change the way that we work and the way we organise the place of work. The flexibility that can be gained through the fact that a laptop PC no longer has to be used in a fixed place in order to be connected into a

corporate network can be considerable. In organisations that have a number of staff that are ‘migrant’ in one way or another (for example, sales teams or consultants that spend much of their time off the premises, or employees that spend part of their working week working from home) then the potential benefits can be significant. The use of wireless-enabled laptop computers would allow them to connect to the corporate LAN when they visit the office, but without the need to provide them with a fixed base where they would plug their PC into the LAN. The fact that the wireless coverage potentially extends to all rooms in a building means that anywhere that is large enough to house a table and chair is potentially usable as a temporary office. In fact, as the wireless coverage may well extend beyond the confines of the office building itself, it may well be possible to access the corporate network in this way while enjoying a Cappuccino at the café next door to the office (though it should, of course, be noted that there are security implications in doing so).

This last point introduces a third significant aspect of wireless LAN technology – that increasingly, it is possible to connect to the Internet in public places by using services offered via so-called ‘hot spots’ in airport departure lounges, public buildings, cafés, and so on. For people who may need to work while on the move, and for whom the ability to connect back to their home office might be important (to pick up email, synchronise diaries, send reports, and so on), these kinds of services will become very popular.

A further benefit of the wireless approach is that it allows the rapid installation of networking capability in temporary sites – in exhibition venues, or on construction sites, for example.

### *Bluetooth opportunities*

Bluetooth, while potentially finding a useful niche in reducing the number of cables that we have to carry around to make modern technology work conveniently, does not look like it will have the same degree of impact that wireless LANs

---

will have. However, it definitely has its place – for example, allowing hand-held palmtop computers to be used for recording appointments, and making it possible to coordinate them with a centralised appointment system simply by bringing the device within range of a PC with a Bluetooth adapter.

Work is currently progressing on standards for a very much lower power consumption wireless ‘personal area network’ or ‘PAN’ technology that is aimed at enabling simple, low-power devices to exchange small amounts of information. For example, this kind of technology would make it possible to create smart business cards that could exchange contact information with similarly enabled devices, or smart conference admission tickets that would control the operation of the entry/exit barriers to the venue.

## **Deployment issues**

Wireless technologies, by their very nature, introduce issues with regard to security and privacy. For example, the old analogue mobile telephone network was notoriously insecure, as it was possible to tune in to conversations using easily obtainable radio scanners. With wireless LANs, this problem was recognised early in their development, and the technology was developed with an in-built security mechanism known as ‘WEP’ (which stands for Wire-Equivalent Privacy). The concept was that the communication would be made as secure as would have been the case if the network connection had been made via a cable.

Unfortunately, the original WEP technology was found to have flaws in its security. While offering some degree of protection, WEP is by no means secure against the attacks that might be made by a determined hacker. Consequently, the standards body responsible for developing the 802.11 Wireless LAN standards is currently developing a replacement for WEP that will not suffer these problems.

In the meantime, various proprietary improvements to WEP exist in the Wi-Fi

products currently available in the marketplace, and stop-gap measures can be taken to make the technology more secure.

A major problem with wireless LAN technology is that users often do not even bother to invoke the security features that WEP (and its proprietary enhancements) can provide, and there is a tendency to start using wireless access points without changing the settings from their factory defaults. This leads to the potentially dangerous situation where someone sitting in a car outside an office building could access a corporate LAN with very little difficulty, simply by knowing what the default security settings are for the major manufacturers' access points. This highlights one of the most crucial aspects of security; that access controls and encryption mechanisms are no use whatsoever if you make it possible for attackers to discover what security settings (passwords, user names, encryption keys, etc.) you are using.

### **Case study**

Laing O'Rourke, one of the UK's leading construction companies, will become one of the first enterprises to adopt Intel® Centrino™ mobile technology company-wide. The link-up with Intel is part of Laing O'Rourke's strategy to introduce the benefits of wireless computing to its staff and customers in order to dramatically improve communications. Specifically built for wireless mobility, the mobile technology features integrated wireless LAN capabilities and offers improved mobile performance while enabling extended battery life in thinner, lighter notebook PC designs.

Laing O'Rourke plans to provide many of its 4,000 staff with notebook PCs based on mobile technology that features built-in wireless LAN capabilities. The company is also installing wireless local area network

*continued*

(WLAN) hotspots at its offices, including its headquarters in Dartford, and at various construction sites. The combination of the mobile technology and the wireless hot spots will enable staff to easily access email and their corporate network from their offices and construction sites. Additionally the company intends to build WLAN hotspots into major new developments it is working on such as Heathrow Terminal 5 and other high profile commercial projects throughout the country.

“Our vision is to exploit the benefits of wireless Internet access in every aspect of our work and to bring the benefits to our customers too,” explained Ray O’Rourke, chief executive, Laing O’Rourke. “We believe that wireless computing can dramatically improve our ways of working.”

“Equipping our staff with notebook PCs based on Intel Centrino mobile technology will radically improve construction site communications and the productivity of our engineers who spend much of their time at different offices and construction sites,” explained Sam Simons, director of strategy at Laing O’Rourke. “We believe the impact of wireless computing on the construction industry will be far-ranging. From the engineer who will be able to view and change digital plans on a notebook PC on-site, even at the top of scaffolding, to the architect who will be designing buildings in a different way in order to facilitate wireless working.”

### **3. HIGH SPEED INTERNET ACCESS**

#### **The technology**

Traditionally, businesses that had a need to use wide area networking would either make use of dial-up connections using modems and telephone lines, or would have a leased line installed – a permanent data connection leased to them by a telecommunications provider. Dial-up connections are limited in terms of the data transmission rates achievable (56 Kilobits/second under ideal conditions using the current modem technology, but often not as good as that) and are slow to establish a connection. However, what they lack in speed they gain in flexibility, as they can be used on any normal phone line, and can connect to any destination that has a telephone number. Leased lines offer much higher data rates, but tend to be expensive, partly because they involve the dedicated use of a line between two locations, plus guaranteed access to the transmission equipment in between.

Integrated Services Digital Network (ISDN) services offered a slight improvement over dial-up; making a data connection over ISDN is almost instantaneous, and gives a fixed data rate of 64 Kilobits/second. The popular Highway services offered by BT provided two 64 Kilobit/second channels, which could be bonded together to give a single 128 Kilobits/second channel. However, ISDN is still essentially a dial-up service, and each channel is charged at normal telephone call rates, so using both channels becomes twice as expensive as conventional dial-up services. For users that make significant use of wide area connectivity, this can prove quite expensive.

Recently a number of new services that come under the general heading of ‘Broadband Internet access’ have started to emerge in the UK. Broadband services are based on a variety of transmission technologies:

- DSL (Digital Subscriber Line) services, that make use of existing telephony infrastructure;
- Cable Modem services, that make use of cable TV infrastructure;

- Metropolitan Area Ethernet services, that generally require the installation of new cable infrastructure, often based on fibre optic cabling, although some variants of this technology make use of DSL technology.

One thing that all of these technologies have in common is that they offer a permanent, ‘always on’ connection to the Internet; you pay a fixed monthly rental for the service, regardless of how much use you make of it. However, it should be pointed out that the costs of such a fixed monthly rental are in fact relatively inexpensive, and are becoming even cheaper as competition between the service providers heats up.

### *ADSL*

The most common DSL service available in the UK is the ADSL service provided by BT (and re-sold by a number of other service providers too). The ‘A’ stands for ‘Asymmetric’, which means that the data transfer rates are not the same in both directions. The transmission rate from the subscriber to the Internet is lower than in the reverse direction; the idea here is that downloading large web pages will account for a high proportion of the use, whereas the volume of data that needs to be transmitted from the user to the network is generally smaller. The data rates available with ADSL, and in fact the actual availability of ADSL, depend critically on the distance between the subscriber and the nearest digital telephone exchange, and also on the number of subscribers that are using the service. Typically, the service now offers up to 2 Megabits/second for downloads, and up to 250 Kilobits/second for uploads (though download speeds of 8 Megabits/second are beginning to emerge). So, unlike leased lines, ADSL gives no guarantee as to the actual transmission rates that will be made available.

### *Cable Modems*

The Cable Modem services offered by the cable TV companies (mostly NTL

---

these days in the UK) are only available in parts of the country already served by a cable TV network. The data transmission rates available with these services are similar to ADSL, and as with ADSL, the number of subscribers sharing the infrastructure affects the transmission rates that are actually delivered.

With both ADSL and Cable Modem services, it is a simple matter to connect the cable modem or the ADSL filter into an existing LAN, allowing the external Internet connection to be accessed by all of the PCs connected to the LAN. A router is used to achieve this. One side of the router connects to the LAN, and the other side to the cable modem or the ADSL filter, as illustrated in Figure 2.

### *Metropolitan Area Ethernet services*

Where significantly higher data transmission rates are needed, Metropolitan Area Ethernet services are emerging that will allow data rates of up to 10 Gigabits/second to be achieved between the customer premises and the service provider, if suitable fibre optic cabling is available (or can be installed) in order to make this possible. This kind of approach might be used in order to allow a large company that was spread across a number of sites to interconnect their LANs, making them look like one single LAN from the point of view of the users.

## **Implications for business**

With the growth of e-commerce, the importance of wide area networking for all sizes of business is increasing. For small businesses, an Internet presence can simplify their route to market, and can put them in touch with a wide range of supplier organisations. For larger businesses, the ability to work across a number of different sites, but have the corporate network behave as if it was a single integrated LAN, can considerably improve their operating efficiency

without the expense, for example, of consolidating the business on a single site. Broadband services nicely fill the gap between dial-up services and the traditional leased line services, offering a good level of performance for relatively modest cost, making them a realistic proposition for all sizes of organisation.

The availability of broadband services makes it possible to seriously consider other approaches to working, such as home working. A home worker with a broadband connection back to the office can operate much more effectively

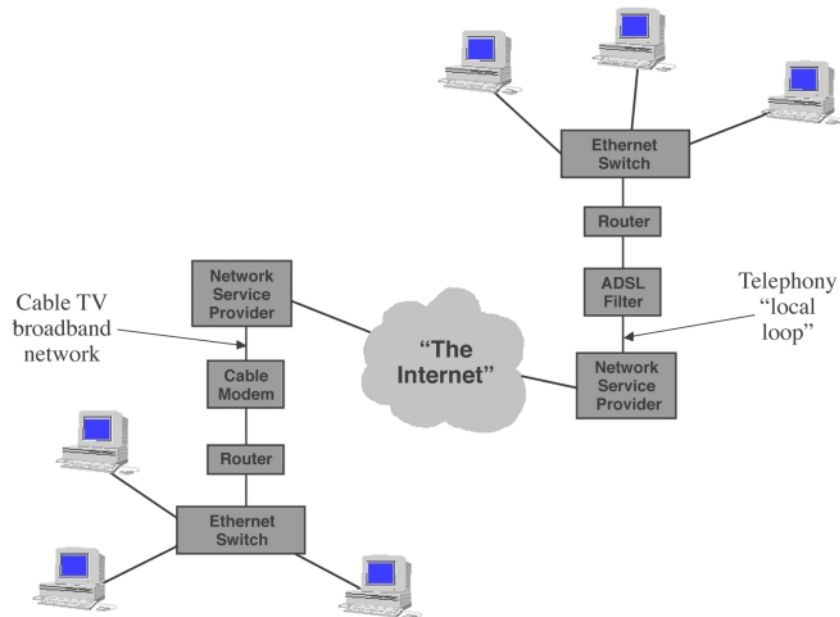


Figure 2: Networked PC s accessing the Internet via broadband services

---

than would have been possible using only a dial-up service. A good example of this is BT's own directory enquiries service, which is partly staffed by home workers; in fact, more than 3,500 of their staff are now home workers, and in all cases, high speed access to the corporate network is a key factor in making this possible.

Broadband has the potential to breathe new life into the economies of some of the more remote parts of Britain. For example, Internet-based businesses are starting to appear in the Hebridean islands, where their remoteness is no longer a barrier to offering services, such as graphic design.

Perhaps the most significant factor for small businesses is that the development of a professional Internet presence can create the illusion that the company is much larger than it actually is. The reality may be that the company consists of two people working from a spare bedroom, whilst the Internet presence gives the impression of a large, established company.

## **Deployment issues**

The availability of Cable Modem and to some extent, ADSL services is patchy at the moment. Cable Modem services are confined to a small number of UK towns and cities, whilst some areas of the country do not yet have access to ADSL. However, this situation is improving considerably with time.

The Metropolitan Area Ethernet services are currently in their infancy, and it may be some while before products and services based on this technology are widely available.

With any permanent connection to the Internet, security once again becomes a concern, and particularly so when connecting a corporate LAN to the Internet. At the very least, the use of a firewall between the LAN and the WAN is a necessity. In some cases, it may also be appropriate to consider further measures, such as data encryption techniques, in order to protect the data contained in the

---

corporate network, and to prevent ‘eavesdropping’ of information transmitted externally. The inadvertent transmission and reception of computer viruses becomes much more of a concern in such circumstances too, so the importance of proper anti-virus measures is critical. Some of these security issues may be addressed using the technology introduced in Section 4 of this guide.

### **Case study**

Formed in 1997, QualityTime Software operates from the Ealing home of its director Mark Tompsett. It has developed and sells two Internet or Intranet-based time management tools; QualityTime Time Reporting and QualityTime Staff Movements. The company has two staff based in the office with two others teleworking from other parts of London.

The company used to be dependent on several 56k dial-up modems. “We had a website that used the free web space service that came with our PIPEX account,” Tompsett said. “It was not interactive and if a potential client visited our site we had no way of knowing anything about them.” Suppliers, trainers and partners wanted to use real time web cast presentations, which is nearly impossible using a 56k modem. “To save time and money we used to download big files after-hours, when connection times were cheaper and it would not interfere with the rest of the business.”

Teleworking was a major part of the life of the business, but dial-up meant that every time someone wanted to request information or update a database they had to send an email to the Head Office staff who had to do all the work. “After a while it became clear that we needed an always-on connection and with ADSL becoming more widely available, we thought that would be our best option,” Tompsett said.

*continued*

QualityTime Software opted for Pipex's Xtreme Business 500 service to connect a server in their office to an ADSL line. This acted as a mail server, a website, a database server and a firewall. This server was linked to the office's local area network, giving teleworkers direct access to the company database. By using ADSL, this solution was significantly cheaper than a leased line.

QualityTime now have a more interactive website which enables it to track its customers; data is recorded directly into the business's database. Customers can download product information in convenient printable formats, evaluation versions of the products for testing, and the latest software updates as they appear. In the office, there is now immediate and high-speed access to the Internet saving both time and money.

Not only can the staff now watch web casts in full motion video, they can also download presentations and documentation to review at the same time. "ADSL has put us on the same footing as a much bigger company. Anyone connecting to us would think that we were the same as any other big software house."

In the future, Tompsett is planning to expand the capabilities of the website to enable customers to demo its products on-line without having to download them and run them in their systems first. This is something that would have been unthinkable without an ADSL connection.

## 4. SECURE WIDE AREA COMMUNI- CATION

### The technology

The first two areas of technology development described in this guide have both raised issues of security. Wireless networks potentially allow hackers access to a network because it is impossible to limit the propagation of the radio signals used by the technology. Connecting a LAN to a wide area network, and particularly, to the Internet, raises security issues by virtue of the fact that data is propagated through equipment owned and operated by other organisations, and can potentially be disrupted, scrutinised or modified en route.

Historically, organisations that needed to construct networks that would serve multiple sites, or maybe allow communication with their clients or suppliers, would achieve this by constructing a *virtual private network*, or VPN, using data lines leased from telecommunications service providers. The term virtual is used here because the network is not truly privately owned and operated; it relies for its wide area connections on the service provider's lines and equipment. Because the privacy offered by such a network is based on a service agreement between the client and the service provider, stating that the service provider will not look at or modify the data on the network, such networks are known as *trusted* VPNs.

With the advent of the Internet, along with relatively cheap broadband access technologies, the concept of constructing VPNs across the Internet has become of interest, as it has the potential to offer a VPN service at significantly lower cost than would be the case with networks constructed from dedicated leased lines. However, the very public nature of the Internet means that, although it is possible still to construct trusted VPNs in this environment, many users require a higher degree of assurance that their communications over the VPN will be secure. Hence, this has given rise to the use of technologies that allow *secure* VPNs to be constructed.

The basic concept behind a secure VPN is that all communications taking place across the VPN are encrypted, thus preventing the data from being read in

any meaningful form, even if a potential eavesdropper is able to examine the data packets being transmitted on the network. The devices communicating over the network, or the network users, or both, may well also need to be *authenticated*, to ensure that only trusted individuals or equipment can be attached to the network.

Most current implementations of secure VPNs are based on a family of encryption technologies known as IPSec (IPSecurity), which is used to construct a secure ‘tunnel’ across the Internet that can carry the client’s data.

### **Implications for business**

VPN technology is accessible to business users in a variety of forms. The telecommunications service providers have offered trusted VPN services for a number of years and, increasingly, are also offering secure VPN services. In both cases, the offering is a managed service, having the advantage of off-loading the maintenance and management of the network from the user.

Perhaps the most interesting aspect of secure VPNs is that it is possible for these services to be provided and managed by the businesses that use them. As they rely on encryption technology that can be installed either as software in a PC or as add-ons to existing LANs, VPN services can potentially be used by all sizes of business user, from the SME up to the multi-national.

In conjunction with some of the ‘broadband’ access technologies mentioned earlier, secure VPNs can significantly improve the security of communication within a distributed organisation. This may be important both for internal communications within the organisation, but also for communications with client or trading partners, where confidentiality of commercially sensitive information may be a requirement. The potential for providing secure networking for home workers may also be important.

The same secure VPN technology can also be applied as a means of overcoming the present shortcomings in wireless LAN security; if all information transmitted

over the wireless LAN is properly encrypted using the IPSec mechanisms, it is no longer a concern that an eavesdropper might be able to 'see' the data packets being communicated, since it will be very difficult to decrypt the data.

Secure VPNs can, in many ways, be viewed as a means of making the other networking technologies safer to use in a commercial environment; hence, coupled with the other technologies mentioned in earlier sections, VPNs become an essential factor in delivering the benefits that can accrue from these technologies.

A major benefit with managed VPN services is that they significantly reduce the costs associated with constructing and managing a wide area data network. This can be significant for all sizes of business. Even the larger multinationals often cannot afford the expense of running a truly private WAN, whereas the established telecommunications suppliers can offer a managed service at a much more affordable cost.

## **Deployment issues**

With managed VPN services, the very nature of the managed service removes many of the support issues that may otherwise have existed, such as provisioning the network, managing its growth to meet changes in demand, and handling fault detection and correction. However, it is important to make sure that the service level agreement with the service provider gives the right level of guarantees, not only with regard to the data transfer performance that the network will offer, but also in relation to the level of confidentiality and security with which the data will be transferred across the network.

With secure VPNs, the security delivered depends not only upon making use of the right technologies, but also on adopting the right procedures for managing and using them. Encryption is a complete waste of time unless it is backed up with the necessary procedures to keep it secure; for example, regularly changing the encryption keys. The level of security afforded by encryption can be

improved by using bigger encryption keys. However, the bigger the keys, the greater the processor power needed to encrypt and decrypt the data (though with today's powerful computer processors, this is unlikely to be a major practical issue).

For the smaller companies, the use of managed VPN services may prove to be expensive, as service providers will obviously charge a premium for the provision of service level guarantees on a VPN. It may be more cost-effective for them to use a 'normal' broadband connection, with no special service level guarantees, and overlay IPSec-based encryption in order to create their own secure VPN service. However, this brings with it the added complication of the need to manage the security mechanisms employed, so the cost of this needs to be factored into the equation.

### **Case Study**

International food manufacturer HJ Heinz wanted to restructure its operations, but soon recognised the need for enhanced communications if the restructuring was to be successful. The company chose Cable & Wireless to help plan and implement its solutions. The result has achieved a significant reduction in operational costs, and has provided a communications solution that is robust and flexible enough to handle future changes.

Heinz has approximately 44,000 employees at 200 locations worldwide. Traditionally, Heinz manufactured its products locally. Following a review of its structure, it decided to centralise its operations into five manufacturing centres. Simon Shaw of Cable & Wireless explained the challenge. "In order to coordinate production and distribution under the new model, the entire organisation needed to work more closely together. This meant greater

*continued*

dependence on inter-office communication systems via WANs, with a dramatic increase in their usage.” Additionally, their local and international voice and data systems had to be flexible enough to accommodate planned geographical expansion.

A key challenge that they had to overcome was a lack of consistency in local provision for voice networking and LAN services in each country. The multiplicity of disparate legacy systems would have led to increased maintenance costs and high workload on a small in-house staff. Chris Middlehurst of Heinz said “We were looking to establish a single, coherent communications strategy that would reduce costs and enable rapid integration of new systems.”

Cable & Wireless designed a solution using IP convergence technology – the use of a single unified network for voice, data, and video traffic. 14 sites throughout Europe were fitted with Cable & Wireless IP-LAN, a managed LAN service. The sites are connected over the wide area using Cable & Wireless IP-VPN QoS, a fully managed VPN service that allows the user to define priorities for certain classes of traffic with guaranteed performance targets. The solution can support any type of data by encapsulating it in IP, and supports three classes of service, so time-sensitive traffic such as voice calls are not held up by low priority data such as emails.

The solution has enabled Heinz to make an overall operational saving of 10%. Middlehurst said “Because the solution is a managed service, we didn’t need to invest in specialist staff to maintain it.”

## **5. FUTURE DEVELOPMENTS**

It has been said that prediction is terribly difficult, especially about the future, and predicting the future of networking technologies is no exception. However, it is evident that, at the moment, we are in the middle of the same kind of revolution that we underwent with the advent of the mobile phone a decade or so ago. Only this time, the revolution is centred around mobile data transmission technologies, and the integration of voice and data technologies. We are beginning to see this happening in a small way with the recent release of mobile phones that can send and receive pictures. This may be something that is more appealing to the individual user at present, and which may not have many applications in the business arena, but it is nonetheless a good example of what is possible using today's mobile networking technology. In particular it shows the way that the digital mobile phone network, which is essentially just another form of data network, can be used to carry both voice and data.

The next few years will bring further developments that are of more interest to the business environment, and will make the use of technology 'on the move' much simpler and, at the same time, better integrated with the traditional business applications used on PCs today. The truly integrated 'Personal Digital Assistant' or PDA, which combines the functions of a portable PC with those of a mobile voice and video phone, securely networked using wireless networking technologies to the parent company (which of course may itself be geographically dispersed across other mobile users, home offices, and corporate offices), is a goal that is being brought steadily closer by these kinds of developments.

## **APPENDIX 1 USEFUL WEB RESOURCES**

The *Virtual Private Network consortium*, an industry consortium of VPN equipment and software vendors, maintain a website at:

<http://www.vpnc.org/>

The '*Wi-Fi Alliance*' maintains a website at:

<http://www.weca.net/OpenSection/index.asp>

BT's ADSL business offerings are described on their website:

<http://www.btopenworld.com/broadband/forwork/>

This website also has further information on networking services and security services.

*NTL's broadband* and other business networking services are described on their website:

<http://www.business.ntl.com/>

## THE AUTHOR

Tony Jeffree has been involved in the computer industry since 1975, initially in the process control field with Kent Process Control Ltd, but more recently as a consultant in various aspects of IT, networking and data communications. He has managed IT consultancy practices in Sema Group Consulting Ltd and the National Computing Centre.

Since the start of 1996, he has operated as an independent consultant, specialising in delivering consultancy services related to LAN technologies, management and team building training, and the development of IT course materials.

He is also heavily involved in standardisation activities in IEEE 802 and ISO, relating to the development of standards for network management and local area networking technologies. He is currently the Chairman of the IEEE 802.1 Working Group, which is responsible for the development of standards for LAN Bridging, management, and security.

His contact details are as follows:

Tel: 0161 973 4278

Email: [tony@jeffree.co.uk](mailto:tony@jeffree.co.uk)

Faculty of Information Technology  
ICAEW  
PO Box 433  
Chartered Accountants' Hall  
Moorgate Place  
London  
EC2P 2BJ

Tel 020 7920 8481  
Fax 020 7920 8657  
E-mail [itfac@icaew.co.uk](mailto:itfac@icaew.co.uk)  
URL <http://www.icaew.co.uk/itfac>

Price **£12.50**

Issued free to members of the  
Faculty of Information Technology

ISBN 1-84152-201-5

September 2003