Mobile VPNs

Converting technological promise into revenue streams for operators and vendors

BWCS

Mobile VPNs

Author: Ken Wieland

First Edition
ISBN 1-903758-41-6

Published by BWCS Ltd
6 Worcester Road, Ledbury, HR8 1PL, United Kingdom.
Tel +44 1531 634 326, Fax +44 1531 631 443
Email: info@bwcs.com
Website: http://www.bwcs.com

About BWCS

BWCS is the publisher of this report. Other recent market reports include *Wi-Fi, WiMAX and 802.20 – The disruptive potential of wireless broadband; Railway W-LAN Services*; *Mobile Proximity Payment Services*; and *I-Mode 2007*. We also publish a series of expert handbooks for the telecoms industry, including *Service Design, Implementation and Management* by Paul Whitlock and Chris Wright; *Achieving Excellent Customer Relationships* by Philip Grant; *IP in Mobile Networks – A Guide to Operations and Management* by Dr Tony Judge and Luca Burroughs; *Interconnect Costing (2nd Edition)* by Peter Cartwright; and *Carrier Services Contracts* and *Global Telecommunications Contracts: A Handbook for Customers and Suppliers* by David W. Bartell.

BWCS is a specialist consultancy set up to help telecommunications companies sell their products and services more effectively. We advise many of the world's leading telecommunications companies on all aspects of sales, marketing, competitor analysis, business development, business planning and market research. If you would like to know more about the services we offer, please contact us.

Tel: +44 1531 634 326
Fax: +44 1531 631 443
E-mail: info@bwcs.com

When you need to:	BWCS can help you by:
Bring new technologies to market	Analysing how they will be received by customers. Analysing how they fit with other technologies and in the marketing mix
Know more about your competitors	Performing detailed competitor analyses
Prospect for new business	Profiling individual customers and markets, plus lead generation and lead qualification
Understand user requirements and attitudes	Designing and managing market research programmes
Put together your business plan	Developing revenue and market share models, opex and capex models, performing sensitivity analyses, and valuing your business or project on discounted cash flows
Measure customer satisfaction	Designing and managing market research programmes, interviewing individual customers
Learn about principles of interconnection costing	Providing interconnect costing training courses

Contents

Tables and Figures

1 Executive Summary

1.1 Everything to play for

Mobile VPNs have yet to be widely embraced by SMEs and corporates. Vodafone, which launched its Mobile Connect Card (MCC) in November 2002, had sold only 167,000 units by the end of 2003. Despite the mobile operator's claim that the sales figure was 'in line with expectations', no amount of spin can disguise the fact that this is a poor take-up rate. The Vodafone MCC, which allows GPRS connectivity to the public Internet and the corporate LAN from the laptop, has largely failed to capture the imagination of the enterprise community. The mobile operator will be hoping that its GPRS/3G data card, launched in February and March 2004 across Europe, will enjoy greater success.

And it isn't just Vodafone which has found the going hard. Mobile operators across the board – as well as fixed-line operators who resell cellular capacity to add a mobile VPN option to their suite of remote access services – report a similar story of patchy interest.

To put a brave face on their inability to crack the enterprise market with mobile data services, operators have a tendency to euphemistically describe this period as 'early days'. Operators, however, have not been as blameless as this innocent expression may imply. A disconnect has emerged between what operators are offering and what customers want.

The net result is the overwhelming majority of mobile operators' data revenue comes from consumer SMS. To take Vodafone as an example again, 15.9% of its service revenue during 2003 was derived from data: 11.8 % from messaging and only 4.1% from non-SMS/MMS traffic. While these statistics reveal a depressing picture of apparent enterprise resistance to mobile data use, it also illustrates an opportunity – it's still an untapped market.

1.2 Why have mobile VPNs failed to take off?

From a technological point of view, the ability to transmit data securely between a mobile device and the corporate LAN or Web-based application is the essence of what a mobile VPN is all about. That being the case, it can address one of the main concerns that IT managers have when it comes to mobilising the workforce – maintaining the security of enterprise resources when accessed remotely. The comfort factor on security is particularly strong when IT managers opt for an 'end-to-end' mobile VPN implementation, which comprises an unbroken 'tunnel' between the end-user device and corporate LAN.

But addressing network security concerns will not be enough to stimulate the mobile VPN market. Operators and their strategic partners will, first and foremost, need to put the technology into a business context for that to happen. Unless it is demonstrated clearly to the enterprise what the benefits are of deploying a mobile VPN – increased productivity, improved market competitiveness, more job satisfaction (and perhaps even new revenue streams, which would really catch the attention of the CEO) – there will be a continued resistance to adoption.

In that regard, Lucent deserves credit for trying to kick-start the market with numerous mobile VPN pilots designed specifically around the business processes of the enterprise itself. If more case studies of successful mobile VPN implementations could be circulated from a variety of sources – with examples taken from different vertical industry sectors – then it would help create a market momentum.

In addition to a lack of education on the possible business benefits associated with mobile VPNs, other factors have hindered their adoption in Europe. These include:

- Unreliability and poor throughput performance of GPRS, especially for transmitting large volumes of data.
- Excessive mobile data tariffs combined with the difficulty of accurately predicting monthly costs when using the per-megabyte charging model.
- High total cost of ownership. Ongoing technical and administrative costs need to be added to upfront capital requirements for mobile VPN adoption. These costs could be considerable for IT managers responsible for installing, configuring and upgrading VPN clients on a large number of end-user devices. The task is made more difficult (and expensive) if there is a diversity of OS (operating system) software versions in use across the laptop workforce.
- Lack of trust in the mobile operator. For organisations that don't have sufficient IT resources to implement and manage an 'end-to-end' mobile VPN for themselves, they may consider opting for a network-based mobile VPN. This hands over the responsibility of managing the data traffic between the end-user device and the corporate LAN to the mobile operator. However, mobile operators would need to assure IT managers that there would be no security threat to their business in such a set-up. This is a big hurdle for mobile operators to overcome if they are to move beyond the role of pipe provider.

1.3 What do enterprises want?

By identifying key barriers to mobile VPN adoption – as well as speaking to CEOs, CIOs, IT managers and field workers about their particular requirements – it becomes possible to draw up a list of what the enterprise wants from a mobile VPN implementation.

Items on this list will include:

- easy-to-understand tariff structures that make it possible to accurately predict monthly costs
- service level agreements on GPRS and 3G connections
- uniform and simple log-on procedures across all access technologies, including 2.5G, 3G and WiFi
- access to the fastest possible wireless connection wherever possible, from the one device, and the preservation of the VPN connection when roaming across different access networks
- one bill from one service provider
- simple and quick provision and upgrade of mobile VPN clients
- for IT managers to have clear visibility of remote workers' access patterns (which files are being accessed and from where) along with details of network performance
- unmonitored access to the Internet to be restricted if required
- the mobile VPN implementation should be compatible with existing fixed-line VPN infrastructure (VPN gateways, for example) and have minimal impact on business continuity during the set-up process
- clear business benefits.

Those who can deliver on most of these requirements the soonest will have the best chance of making inroads into the mobile VPN market. The focus of this report is to examine ways in which these requirements can be fulfilled.

2 Defining Mobile VPNs

2.1 A need for clear definitions

The purpose of this chapter is twofold:

- to identify and define the different mobile VPN flavours that are available in the marketplace; and
- to highlight the pros and cons of each type of mobile VPN from the perspective of both the mobile operator and the enterprise end-user.

BWCS acknowledges from the outset that it would be a mistake for a mobile operator – or anyone else for that matter – to try and sell a 'mobile VPN' *per se* to an enterprise customer. That would be to fall into the trap of selling a technology over a service or a business solution.

Even so, there is still a need for mobile operators (or their resellers and systems integrator partners) to be able to define clearly their mobile VPN product portfolio – with sparing use of jargon – to IT managers. If not, then another barrier to their adoption is erected.

To achieve that clarity, a common agreement is first required on what the terminology surrounding mobile VPNs actually means. In conducting research for this report, BWCS found that even among mobile operator product managers, there isn't a general consensus over the meaning of key terms. While one talked happily about 'network-based' mobile VPNs and 'end-to-end' mobile VPNs, another seemed unclear as to what those two terms actually meant. That's not to say that the first had a better mobile VPN understanding than the second but rather reveals a wider problem of conveying clear messages and having meaningful debate in what is, potentially, a complex subject.

Because of this scope for confusion, a section devoted to defining mobile VPN terms is necessary. This is not an attempt to be the last word on the subject, nor is it meant to be prescriptive. However, at the very least, this chapter will provide a common framework of reference for the reading of this report. And, particularly for the non-technical reader, it will hopefully throw some light on the terms commonly associated with mobile VPNs.

As part of that process, it is worth looking first at the rise of fixed-line VPNs and remote corporate LAN access. This will provide a context for the later development of mobile VPNs and a clearer understanding as to why they are becoming increasingly important.

2.2 VPNs and remote access: a brief history

2.2.1 The birth of VPNs: ATM and Frame Relay

Prior to the rise of virtual private networking more than ten years ago, enterprises that wanted to establish data connectivity between office sites used dedicated leased lines. As this was an expensive overhead, these links were usually restricted to between headquarters and the most important branch offices. Being dedicated links, however, they did provide the highest level of network security.

With the emergence of public ATM and Frame Relay wide area networks (WANs) during the 1990s, service providers had a way to lower their own costs and those of their enterprise customers. By emulating dedicated and secure private connections over a shared packet-switched infrastructure using so-called PVCs (permanent virtual circuits), virtual private networks (VPNs) were born.

The network is ‘virtual’ because enterprises share infrastructure rather than own it; it is ‘private’ because they still enjoy the security associated with dedicated connections.

2.2.2 Remote access over dedicated links: PSTN and ISDN dial-up

Before the widespread growth of the Internet, enterprises wishing to provide their travelling workers with access to the corporate LAN (local area network) had to rely on PSTN and ISDN dial-up. Such a system comprises a remote access server (RAS) – usually based within the enterprise domain – with phone lines attached to it. Employees working off-site call into the RAS to access the corporate LAN.

To protect against unauthorised access and to give the IT manager a way to monitor who is accessing which file and from where, the RAS carries out the so-called ‘triple A’ function:

- Authentication: ensures no unauthorised person can access the corporate LAN (user names and passwords is one method).
- Authorisation: the access policies adopted by the IT manager. A salesperson will most probably be denied access to the server containing the salary details of the CEO, for example.
- Accounting: the IT manager can access the call usage details (duration and location) of each remote worker calling into the RAS. He also can see details of which files are being accessed.

While the PSTN/ISDN dial-up system provides high levels of network security (PSTN and ISDN networks use circuit-switched connections, which provide dedicated links), it is neither a cheap nor a very scaleable

way for enterprises to manage their remote workers. The drawbacks of PSTN/ISDN dial-up networking are:

- Expensive hardware requirements: enterprises need to invest in RAS equipment, modem banks and phone line installation. Every phone line added is an extra investment.
- High phone bills: international calls, particularly from hotel rooms, can still be expensive. Although enterprises can use toll-free numbers and calling cards to reduce these long-distance charges, that could still mean a considerable up-front cost, particularly if IT managers use multiple suppliers of RAS numbers to add resiliency.
- High operational costs: by maintaining a dial-up infrastructure within the enterprise, additional costs will include network support engineers, testing equipment, and the training to provide adequate help-desk facilities. The greater the number of phone lines, the higher these costs will be.
- Inconvenience for the remote worker: to access different PSTN points around the world, remote workers will have to carry various adapters. Moreover, access to the corporate LAN will be limited to the location of the PSTN access point.
- It does not support home or remote workers using DSL (digital subscriber line) access. Basic DSL packages can offer 500Kbps downstream speeds compared with the theoretical maximum of 56Kbps via a PSTN modem.

2.2.3 The next phase: IP VPNs

ATM and Frame Relay VPNs, although cheaper than private leased lines, have their own limitations. LAN applications running over these two WAN packet-switched protocols have to be specially formatted, which is an added expense. The number of branch offices that the headquarters can connect to is also restricted to those sites that have ATM of Frame Relay customer premise equipment (CPE).

To overcome these limitations, the public Internet, with its ubiquitous presence, is now being increasingly used by enterprises as a medium for virtual private networking – the so-called IP VPN. By using ‘tunnelling’ and encryption protocols, data can be transmitted securely across the public Internet.

The most widely-used protocol to set up site-to-site links across the public Internet is Internet Protocol security, more commonly referred to as IPSec. Ratified by the IETF (Internet Engineering Task Force) and supported by a wide range of vendors – including Cisco and Nortel – IPSec offers a high level of cryptography, as well as authentication. It can also work in conjunction with digital certificates, which strengthens the authentication process.

The main advantages of IP VPNs are:

- LAN-based applications can pass over the WAN without the need for special formatting (since the early 1970s, IP/ethernet has been the dominant protocol within the LAN).
- There is no need to install ATM or Frame Relay equipment on each site requiring connectivity to headquarters, nor is there the need to set up and manage multiple PVCs across the WAN (which can be time-consuming and expensive). Instead, an IP router can be installed quickly on site giving immediate connectivity to all other sites attached to the Internet.
- Extranets – where companies access shared databases with their suppliers or business partners – become easier and cheaper to set up.
- They pave the way for IT managers to lower the total cost of ownership (TCO) for remote access support compared with PSTN/ISDN dial-up.

2.2.4 Remote access over a VPN: leveraging the public Internet

The most obvious benefit of remote access over the public Internet is reduced phone bill costs: workers travelling abroad can make local calls to Internet service providers (ISPs) rather than paying international call rates. There is also less hardware maintenance required compared with PSTN dial-up infrastructure.

Nevertheless, VPN remote access does require some IT investment, not least in the shape of VPN concentrators (otherwise referred to as VPN servers) and the installation and management of IPSec clients. An IPSec client is a piece of software residing on an end-user device, which sets up a ‘tunnel’ across the public Internet to the VPN server at the corporate LAN; it then encrypts data it sends and de-encrypts data it receives. The VPN concentrator is responsible for terminating the tunnels at the corporate LAN.

IT managers will be more inclined to make the investment in Internet-based VPN remote access as the popularity of teleworking and DSL (digital subscriber line) access increases. Traditional PSTN dial-up infrastructure cannot support DSL-based teleworking, but an increasing number of companies are recognising the need to provide their employees with the opportunity to work from home – which usually requires intranet access – should they request it.

With a growing acceptance by enterprises that the public Internet can be a safe medium for the transport of corporate data, mobile operators have a big opportunity to drive more data across their packet-switched cellular networks, not least when those networks support IP. As any service used on the wireline Internet can now be accessed by devices attached to these

'next-generation' wide area cellular networks, mobile operators can do the following:

- Complement existing IT investment in fixed-line VPN infrastructure to offer 'always on' connectivity to information resources on the LAN – anytime, anywhere. (Like PSTN dial-up, remote access over a fixed-line VPN is still limited to finding a suitable access point, which might not always be conveniently located.)
- Promote the use of a secure, 'mobile office' to all enterprises connected to the Internet. There is no longer the need to run private, leased line connections from the mobile operator's network to the corporate premises.

In short, they can offer mobile VPNs.

2.3 What is a mobile VPN?

2.3.1 Overview

We have already established what a VPN is – that is, a shared or public infrastructure that can provide the security and performance levels required of a truly private network.

A mobile VPN can similarly be defined as the use of a public cellular network to provide secure connectivity to enterprise information resources. These resources will either be based on the corporate LAN or at an extranet site. They could also exist in the form of a web-based application, such as MS Outlook, as we shall see later.

For the purposes of this report, a remote worker will not be deemed 'mobile' if accessing corporate information over a fixed-line VPN infrastructure. Although the remote worker accessing the corporate LAN from a hotel room is 'mobile' in the sense that he or she is not restricted to being in the office to have access to information, there is no 'mobility' at the point of access.

This will also rule out corporate LAN access via wireless LAN (WLAN) or Wi-Fi 'hotspots' as an example of a mobile VPN. Although the scope for 'mobility' is greater than with the hotel room example, the remote worker is still restricted to the limited radius of the WLAN hotspots themselves.

For true mobility – the 'anytime, anywhere' level of access to corporate information – remote workers must turn to wide area cellular networks and it is here where the focus of this report lies. Whether it is via handheld devices or laptops, BWCS defines a mobile VPN user as someone accessing corporate information – securely – over a public, wide area cellular network.

BWCS does recognise the trend, however, of closer interworking between cellular and WLAN networks, as well as industry moves to integrate both types of access on handheld devices. This trend will be explored more fully in the profiles on mobile and 'fixed' operators (Chapters 5 and 6 respectively).

2.3.2 Different mobile VPN categories

Mobile VPNs can be split into four main categories:

- end-to-end
- network-based;
- application-specific
- voice.

Each category of mobile VPN is broadly applicable to both the GSM and CDMA cellular platforms, including their respective 'next-generation' packet-switched iterations: GPRS (2.5G) and UMTS (3G) on the GSM side; CDMA2000 1X, CDMA2000 1xEV-DO (data optimised) and CDMA2000 (3G) on the CDMA side.

For the purposes of this report, we will focus on the GPRS and UMTS network architectures to illustrate each main mobile VPN category – and their sub-categories – available today.

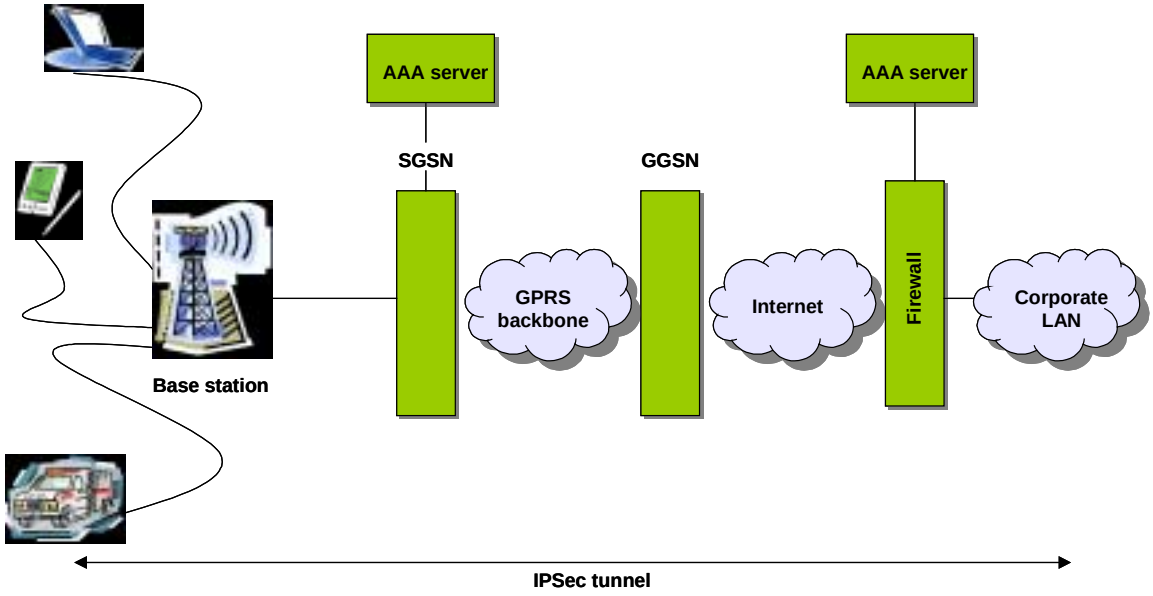
2.4 End-to-end mobile VPNs

2.4.1 Network architecture

The 'end-to-end mobile VPN', sometimes referred to as 'voluntary tunnelling', will have the greatest appeal to enterprises that have their own IT resources and place a high premium on security. The reasons for that can be found in the way the end-to-end mobile VPN is configured.

As can be seen in Figure 2.1, a secure IPSec tunnel (which passes encrypted data) extends from the end-user device straight through to the corporate gateway without interruption – it is end-to-end. In such a scenario, the IT manager will usually take on the task of installing, configuring and managing the IPSec clients on the end-user devices; he or she will also have to ensure interoperability between the end-user and the VPN corporate gateway. Since the IPSec client establishes the tunnel link to the corporate gateway, this explains the 'voluntary' tag – IT managers have chosen to take on the responsibility themselves of providing end-to-end security.

Figure 2.1 Voluntary tunnelling architecture



Source: BWCS

Note: IPSec-based VPN solutions use IKE (Internet key exchange) to authenticate end-users to the corporate network automatically, which is usually based on the 'pre-shared key' method. For this method to work, the AAA server in the mobile operator's network needs to know the end-user's IP address and the secret key associated with it to interact with the AAA server in the customer's network – the converse is also true. As such, a degree of co-operation is required between the mobile operator and the enterprise, even in a voluntary tunnelling environment: the mobile operator and the customer have to agree on the IP addresses of the VPN gateways and the security policies to be used.

Although end-to-end encryption gives a high degree of security comfort to enterprises, there are clear administrative costs to bear and a need for in-house IT expertise. Only large organisations, generally speaking, will have the necessary IT and financial resources to opt for this type of mobile VPN.

It has to be noted that a number of other protocols, besides IPSec, can be used to implement the end-to-end secure connection. These include L2F (Layer 2 Forwarding), Microsoft's PPTP (point-to-point tunnelling protocol) and L2TP (Layer 2 tunnelling protocol). However, due to IPSec's dual function of authentication and high levels of cryptography, it is generally the preferred choice by IT managers for corporate LAN access via laptops and PCs.

For PDAs running on Microsoft's Pocket PC operating system, mmO2 reports that a better user experience can be had if the in-built PPTP client, supported by Microsoft, is used instead of the IPSec client. One reason for that is – due to the greater mobility of the handheld device – there is a tendency for the IPSec tunnel to 'break'. As the VPN tunnel is session-

based (which means it is only active during use), the mobile user will have to initiate the whole set-up procedure from scratch once the tunnel breaks.

2.4.2 'Encryption tax' on bandwidth

By using end-to-end encryption, a major drawback of voluntary tunnelling is the negative impact it has on GPRS performance. To enable encryption, IPSec VPN clients require a data 'overhead' of about 12 bytes per packet. So, depending on the packet size the application is using – which can range between 32 and 576 bytes (according to Cellcom, an Israeli mobile operator) – the end-user, effectively, can experience data throughput decreases by as much as 40 percent.

Lucent says that IPSec VPN users will experience, on average, application performance deterioration of around 25 per cent. Even so, as GPRS enables downstream data rates of between 20-40Kbps, this level of bandwidth 'tax' for the benefit of IPSec encryption is significant. Application throughput, in a worst-case scenario, could be little more than 10Kbps using an end-to-end mobile VPN.

There are cost implications to consider, too. If enterprises are paying for data usage on a per megabyte basis, they will be paying extra for the traffic overhead to enable security. Mobile operators will also need to invest more in their GPRS networks if they cannot take advantage of software compression techniques. (Software compression reduces the amount of data required by an application but, if the traffic is encrypted, compression cannot be applied.)

2.4.3 How can mobile operators differentiate themselves?

At first sight, mobile operators may appear restricted to playing a passive role of pipe provider within the end-to-end mobile VPN environment. However, BWCS has identified five key areas in which mobile operators can raise their profile in the eyes of CEOs and CIOs within the voluntary tunnelling framework.

A: Managed services

Large organisations, with their own IT resources, will most likely select, install and manage the VPN components for themselves or in partnership with systems integrators (SIs). These components comprise VPN clients, data cards (for laptop use), VPN gateways and IP routers. If, however, the mobile operator can manage some or all of those components on the enterprise's behalf, then this is a value-added service with the potential to increase margins.

(For the sake of establishing coherent mobile VPN definitions, BWCS argues that if the mobile operator's managed service package extends towards hosting the VPN gateway – perhaps at a data centre located near the customer premise – then this is a variant of a network-based mobile

VPN (see Section 2.5). Although this type of mobile VPN is still based on voluntary tunnelling (where the end-user has initiated the tunnel on his or her device) the hosting and management of infrastructure by the mobile operator turns it into a network-based mobile VPN.)

While it will be difficult for mobile operators to muscle into the managed services space – and some (like mmO2) may even come to the conclusion that the high level of competition among SIs to deliver managed VPN services is such that the margins are not sufficiently attractive to try and compete – it does represent a strategic opportunity for the mobile operator to become more customer-facing. A closer working relationship with the enterprise should make it easier for the mobile operator to sell more mobile data services in the future.

In November 2002, the Vodafone Group launched its remote corporate LAN connectivity service across its European networks – known as Vodafone Remote Access – with a managed service option for IT departments wishing to outsource the configuration and management of the various VPN components.

In partnership with Cisco, Vodafone (via its reseller channels) provides the IPSec clients, VPN gateways and routers that business customers require. It also packages into the service its own branded GPRS data card – the Vodafone Mobile Connect Card – which allows SIM-based authentication for plain Internet access. In addition, Vodafone offers device-based software to make the establishment of a GPRS connection as easy as possible. According to Vodafone, plain Internet access and VPN connectivity (which is integrated into corporate IT systems) can take ‘as little as five hours to set up’ with the Vodafone Remote Access managed option.

Other ‘professional’ products that mobile operators can offer include a managed firewall service. Although firewalls can’t do any deep packet inspection on encrypted traffic to determine the presence of any ‘invaders’, a firewall placed in the mobile operator’s network can still perform the important function of blocking any non-IPSec traffic (which may contain viruses) from reaching the end-user device. Mobile operators can also provide further firewall protection for plain Internet access.

As important as these security measures are, they have their limitations. For mobile operators to protect their own networks and those of their customers from denial of service (DoS) attacks, they continually need to update their anti-virus software to try and stay ahead of ever more ingenious ways to disrupt software. This is clearly not a fully secure method, as the havoc unleashed by the MyDoom virus in early 2004 demonstrates.

One method designed to complement network-based attempts to prevent DoS attacks comes from Cisco in the shape of its Cisco Security Agent (CSA), which is software that can be downloaded onto a laptop . The first

version of the CSA is compatible with the following operating systems: Windows (NT, 2000 and XP) and Solaris. It does not run on handheld devices, including smartphones and PDAs.

CSA works by identifying viruses through the way they behave ('abnormal' requests to the operating system, for example) and then prevents them from exerting damage. By not relying on anti-virus software that continually needs to be updated, the CSA can act as a standalone layer of security defence. In February 2004, Cisco said it was talking to fixed and mobile operators in the EMEA region with a view to offering the CSA as a managed service to enterprise customers.

Another service that mobile operators can offer is software compression. However, this will be offered as either a 'box' to be placed behind the corporate firewall or come as part of the CPE-based VPN components themselves (as opposed to being a network-based service in the voluntary tunnelling set-up). With end-to-end encryption, the only opportunity to compress data is within the corporate LAN, before it is encrypted.

B: Different public APN attributes

To access the Internet or any other 'external' packet data network via the GPRS network, the end-user device needs to be allocated an APN (Access Point Name). This enables the GGSN (Gateway GPRS Service Node) – which acts as a gateway between the GPRS network and public data networks – to appropriately route traffic between the end-user device and its intended destination.

Rather than having to manage multiple APNs (that is, one per user) over their networks, mobile operators are opting to provide a single, public APN that can be applicable to all customers. Lucent points out that some vendors have a very limited number of APNs that can be provisioned on their Home Location Registers (HLRs), which makes the dedicated APN approach difficult to scale.

By using a public APN (which the IT manager or end-user provisions onto the laptop, PDA or smartphone), the GGSN identifies which VPN network the customer belongs to based on the domain component of the user name (expressed in the format, *user@domain*).

In such a configuration, it is possible for mobile operators to provide different tariff levels: one for plain Internet access and another for VPN tunnel traffic that travels directly to the corporate VPN gateway from the end-user device. Mobile operators can offer this two-tier tariff structure through 'deep packet inspection' techniques to determine whether the traffic is IPSec or Web-based.

Mobile operators can also give IT managers greater control over employees surfing the Web for personal use by offering a different public APN with different attributes. For example, if the APN is specially

configured, it is possible to force all Internet access requests to go via the corporate VPN gateway. Only if the mobile worker has the appropriate level of access rights associated with his or her user name can Internet browsing then take place (with the IT manager being able to monitor which websites are being visited).

O2 launched such a service in Germany and the UK in July 2003 in response to a growing desire by CIOs to control Internet use. Called Mobile Web VPN, the public APN (*vpn.o2.co.uk* in the UK) allows Internet access only through the corporate VPN gateway. By contrast, O2's Mobile Web service, which uses the *mobile.o2.co.uk* public VPN, allows full Internet access (which is not routed through the corporate VPN gateway) plus VPN connectivity.

C: Public and private IP addresses (and NAT)

When a mobile user initiates an Internet access or VPN session, the end-user device will use either a private or public IP address, depending on the service offered by the mobile operator. If it is a private IP address, the device will not be able to connect across the Internet without NAT (network address translation).

Unlike public IP addresses, a private IP address cannot be routed across the Internet, but mobile operators commonly use them to get round the growing problem of public IP address shortage. By allocating mobile devices from a pool of private IP addresses as and when they are requested, mobile operators can support a larger number of Internet users than otherwise possible with the limited number of public IP addresses that are available. The private IP address system can only work, however, if NAT takes place, which has the effect of converting the private IP address into a public one that can be routed across the Internet.

Unfortunately for IT managers using end-to-end VPN encryption, NAT has the effect of modifying packets of data on the IPSec Authentication Header (AH). This is interpreted as a security violation and the VPN tunnel is not created. Similar tunnel 'disruption' can also occur within the ESP (encapsulating security payload) mode of IPSec if NAT is inserted between the end-user device and its destination point.

There is an established way to get round this problem and that is to use NAT Traversal (sometimes referred to as UDP encapsulation), a technique developed by the IETF. In effect, NAT Traversal 'protects' the IPSec – in both AH and ESP modes – when NAT is used and so preserves the integrity of the VPN tunnel.

But not all VPN clients support NAT, which is a potential stumbling block to IT investment in mobile VPNs if enterprises wish to use their existing fixed-line VPN infrastructure.

The use of APNs, which allocate public IP addresses to mobile devices, is a way for mobile operators to solve this problem. A public IP address does not require NAT and therefore can work with all VPN solutions out in the marketplace. However, this may require additional investment in IPv6 technology by the mobile operator. IPv6 allows the possibility of creating trillions of public IP addresses, which is not possible with today's IPv4 technology. IPv4, with its 32-bit address space, can support four billion unique IP addresses, but it's a number not expected to be sufficient in the long term to deal with multiple devices and machines connected to the Internet.

D: Web-based portals

If mobile operators can encourage business customers to access their mobile VPN service via a single, Web-based portal – which is branded in their own name – it will provide a convenient platform to promote the use of mobile data services as and when they arrive in the future: the Cisco Service Selection Gateway (SSG) and Subscriber Edge Services Manager (SESM) are examples of products that allow end-to-end mobile VPN access to be integrated into a Web-based portal.

Cisco's SSG and SESM products also give mobile operators the ability to bill differently for different types of service. For example, rather than offer a flat rate for all mobile data services, mobile operators may be able to differentiate themselves by charging for some services on a usage basis. This option will be particularly attractive for IT managers in relation to services that are only used occasionally. With the arrival of 3G, videoconferencing may fall into that category; quality of service guarantees on certain applications over 2.5G or GPRS networks may be another option.

The principle behind the single portal (provided by the mobile operator for business customers) is that there is a so-called 'walled garden' of services, which, apart from end-to-end mobile VPN connectivity, will include plain Internet access and access to specific applications (such as MS outlook) and content. Access rights to these various service options will either be determined by the end-user submitting the appropriate credentials or done so by default (as part of the user profile information stored in the AAA server).

The single portal model is, of course, not unique to GPRS/UMTS networks. Users on all access networks, including WLAN and DSL, can also make use of portal-based services.

E: Be the best pipe

One of the biggest fears of mobile operators is that they will be competing for mobile data traffic on price, the radio access 'pipe' being nothing more than a commodity item.

With end-to-end mobile VPNs, that fear is heightened since the scope for adding value – while real – will still not be easy to realise. It is BWCS's view that this opens up a great opportunity to be more aggressive in promoting SLAs (service level agreements) on GPRS networks as a way for mobile operators to achieve market differentiation.

The mobile operators' ability to do this will be related to the level of network investment they are prepared to allocate. However, the emergence of mobile traffic solutions – from vendors such as Cellglide – promises to make the provisioning of GPRS-based SLAs far more economically attractive to achieve than simply purchasing more base stations to be deployed throughout the network (see Chapter 3).

2.5 Network-based mobile VPNs

2.5.1 Network architecture

Network-based mobile VPNs are primarily targeted at SMEs that do not have their own dedicated IT resources to install and manage an end-to-end VPN configuration.

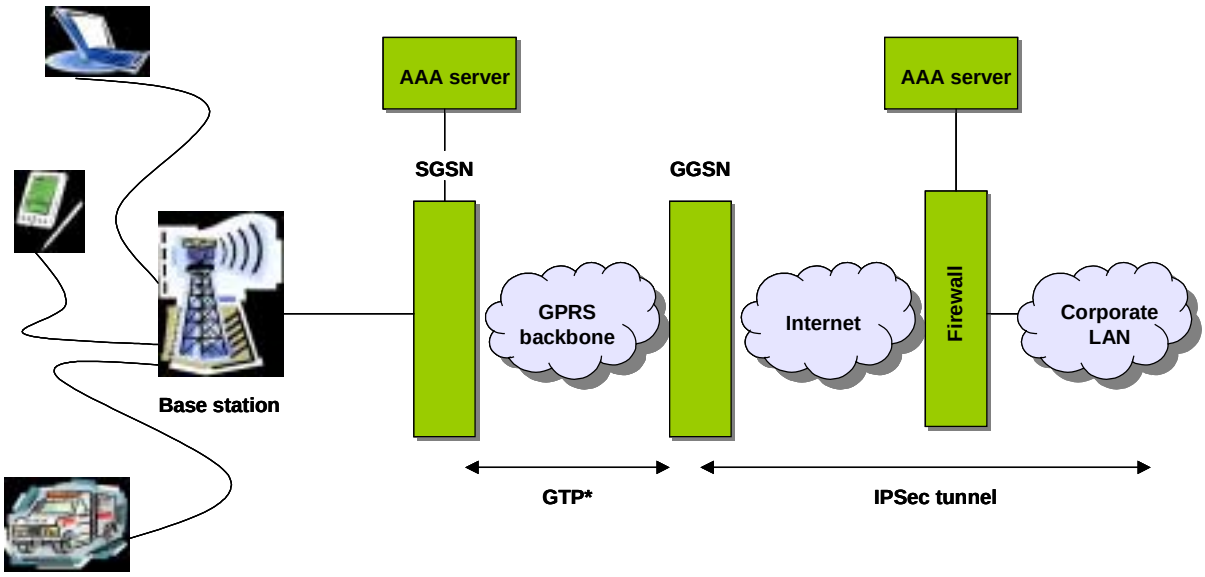
As we have already seen (Section 2.4.3), one variant of a network-based mobile VPN is when the mobile operator hosts the VPN gateway on the enterprise's behalf.

Another variant is when the mobile operator takes on the responsibility of setting up the secure tunnel between the GGSN and the corporate VPN gateway (Figure 2.2) – this is sometimes referred to as 'compulsory' tunnelling. Within this scenario, the enterprise relies entirely on the mobile operator that its corporate data will travel across both the cellular and fixed-line networks securely.

The secure connection between the GGSN and the corporate gateway can be set up in a number of ways by the mobile operator: it can be done through IPSec if the public Internet is used, or MPLS (multiple protocol label switching) in the case of private IP networks. MPLS enables service providers to be more flexible in the way they engineer their networks than they can with ATM or Frame Relay PVCs. With MPLS, VPN links can be dynamically allocated from a network operations centre; ATM or Frame Relay PVCs need to be manually configured to cope with the addition of new sites.

A number of network operators – including Equant, Infonet and AT&T – each have their own MPLS-enabled IP networks, which can offer Class of Service. This opens another door to mobile operators interested in offering end-to-end SLAs on their VPN products, as opposed to the leased line route (expensive) and PVCs (comparatively inflexible). This assumes, of course, that the radio access link carries with it some quality of service guarantee.

Figure 2.2 Compulsory tunnelling architecture



*GTP = GPRS tunnelling protocol

Source: BWCS

Whether it is IP tunnels, ATM/Frame Relay PVCs or an MPLS-based VPN, the GGSN must devote specific routing resources to the APN if the mobile operator is to direct traffic to the correct corporate gateway. Because of this requirement, mobile operators allocate private APNs to their network-based VPN customers rather than public ones. For this reason, a network-based mobile VPN is sometimes referred to as the 'dedicated' or 'private' APN approach.

By using the public Internet, mobile operators will have to partner with ISPs to provide the compulsory tunnelling service. MPLS-based VPN provisioning will also require partnership with fixed-line operators.

If enterprise customers are reluctant to use the public Internet as a medium for their corporate data, mobile operators – again, in partnership with fixed-line network operators – could offer ATM or Frame Relay PVC connections from the GGSN to the corporate gateway. Another option is to offer a dedicated leased line.

BWCS includes all these non-Internet examples as coming under the umbrella of the network-based mobile VPN. Even when the dedicated leased line option is used between the GGSN and the corporate gateway, the mobile user is still sharing resources on the public cellular network with the aim of emulating the security levels of a private network.

2.5.2 Non-payment of the encryption tax

The great advantage for remote workers attached to a network-based mobile VPN is that they can utilise the radio access spectrum far more efficiently than their end-to-end mobile VPN counterparts. By using a PPP (point-to-point protocol) link between the end-user device and the SGSN (serving GPRS service node) rather than IPSec, there is no need to pay the encryption tax. The encryption mechanisms built in to the radio access link – the GPRS encryption algorithm (GEA) in the case of GPRS – provide the security.

If SMEs are to embrace network-based mobile VPNs, they will have to be satisfied that the GEA is inherently secure. They will also have to be convinced that the GPRS tunnelling protocol (GTP), which is designed to separate IP traffic flows between the SGSN and the GGSN, does not pose any security threat either.

If mobile operators can allay these security fears, or, at the very least, demonstrate that the advantages of using a network-based VPN far outweigh any concerns in this area, they will have the chance of significantly boosting their data revenue.

2.5.3 Higher-margin VAS opportunities for mobile operators

In the absence of end-to-end encryption, it becomes possible for mobile operators to 'manipulate' and analyse data traffic. That ability opens up the possibility for mobile operators to offer higher margin network-based VAS services than is possible with voluntary tunnelling.

In a compulsory tunnelling architecture, there are, in effect, two tunnels. The first is between the mobile device and the SGSN, and the second is between the GGSN and the corporate gateway. Whether the second tunnel is a Layer 2 PVC (ATM or Frame Relay) or IPSec-based, it still needs to be de-encrypted before it can be reformatted for wireless transmission (using GEA in the case of GPRS). Unless otherwise stipulated by the IT manager, the radio access link in a network-based VPN will be based on GPRS specifications.

As data can only be compressed once it is de-encrypted, the split-tunnel architecture presents an ideal opportunity for mobile operators to offer network-based software compression and protocol optimisation services. Rather than selling software compression and protocol optimisation as a box to be placed behind the corporate firewall (most likely via its SI and reseller partners) as in the end-to-end mobile VPN model – which is a low-margin business – mobile operators now have the chance to offer a higher-margin network-based service.

According to Flash Networks, an Israel-based vendor, software compression and protocol optimisation can increase the effective data throughput of GPRS by as much as five times for e-mail and web access.

Its own suite of NettGain products can also, so it claims, dramatically improve Microsoft Exchange connectivity performance (Table 2.1).

Table 2.1 MS Exchange connectivity

Activity	Online Outlook	Nettgain Wireless Profile	Acceleration Factor
Log-on	3 min	4 sec	x 45
Receiving a single text message	10 sec	2 sec	x 5
Receiving 10 text messages	4 min	20 sec	x 12
Downloading a 500KB doc attachment	3 min	42 sec	x 4.3
Sending a single text message	23 sec	5 sec	x 4.6
Sending 10 text messages	5 min	26 sec	x 11.5
Sending a message with a 500KB doc attachment	10 min	2 min 20 sec	x 4.3
Moving a 250KB message between folders	2 min	1 sec	x 120
Opening the calendar	22 sec	2 sec	x 11
Checking attendees availability	1 min 15 sec	4 sec	x 19

Basic information:

Device: laptop PC; Win XP OS; GPRS PCMCIA data card
Software: Outlook XP working with Exchange 5.5
Network: A live European GPRS network (3 timeslots downstream, 1 timeslot upstream)

Source: Flash Networks

Other network-based VAS opportunities for mobile operators, courtesy of compulsory tunnelling, include:

- IDS (intrusion detection system)
- application hosting (MS Exchange, for example)
- special tariff arrangements for dedicated APN users
- using the contact established with SMEs to promote other VAS in the future.

2.5.4 Addressing split-tunnelling security fears

The very process that allows mobile operators to offer network-based VAS – the de-encryption of corporate data followed by encryption – will be a source of concern for many IT managers. The perception of 'exposing' data will deter many enterprises from opting for a network-based mobile VPN, unless the mobile operators can assure them that there are no security risks associated with this process.

Tzvi Schechori, vice president of research and technology at Cellcom, an Israel-based mobile operator promoting network-based VPNs to the SME

market, told BWCS: “The perception of a security risk is a big, big problem for us.”

One way that Cellcom attempts to overcome this problem is to call on CheckPoint – who it believes to be a trusted third party – to verify to enterprises that all corporate data is secure within the mobile network. CheckPoint (also from Israel) provides Cellcom with a software-based firewall designed to protect data when it is de-encrypted.

And it is not just the protection of de-encrypted traffic that is required. Mobile operators will have to demonstrate that the different traffic flows going through the optimisation server – say from Bank A and Bank B – do not get mixed up. (Flash Networks claims it has the answer to this very problem with its use of virtual routers – ‘Virtual Nettgain’ – which performs the traffic separation function.)

Mobile operators would like to claim that the security risk of split-tunnelling is more imagined than real, but that’s not the view of everyone. “IT managers are usually scared of split-tunnelling because remote users can be connected to the corporate VPN tunnel and to the Internet simultaneously,” Vincent Bieri, Cisco’s business development manager for EMEA security, told BWCS. “Potentially, that could allow an external user to spread a virus onto the corporate network through the backdoor, as it were, by jumping on the laptop [of the employee] via the Internet.”

Overcoming the security fears associated with split tunnelling will be the biggest hurdle mobile operators will have to jump in taking this ‘business solution’ to market.

2.5.5 Enhanced security with a private APN?

If a network-based mobile VPN configuration avoids the public Internet, and thus removes the need for tunnelling protocols, mobile operators may be able to provide the ‘comfort factor’ that many IT managers are after. T-Mobile Deutschland, for example, argues that its Mobile IP VPN service – based on a private APN – has sufficient in-built security features that will appeal to both small and large enterprises.

Using its own GPRS platform in conjunction with the ATM and Frame Relay networks of Deutsche Telekom, T-Mobile claims it can provide an inherently secure end-to-end service from the terminal to the corporate gateway. Even though the corporate data must undergo the process of de-encryption and encryption for the ATM/Frame Relay PVCs to be formatted for GPRS access – and vice versa – the way the T-Mobile’s Mobile IP VPN service is configured means there is no connection to the Internet (or to other networks) other than the private customer network. (The ATM or Frame Relay PVCs terminate at the point of presence (PoP) closest to the customer; the final leg of the connection is provided by a private, fixed line.)

T-Mobile claims that no entity – other than the 'trusted VPN provider' – can affect the creation or modification of a path within this type of VPN. The perceived security of the Mobile IP VPN service is therefore directly linked to the degree of trust placed in T-Mobile by the business customer.

An additional security feature of the Mobile IP VPN service, as with all the mobile VPN configurations that use a private APN, is that the mobile operator is able to 'screen' who can have access to the corporate gateway. This is because a user can only access the Mobile IP VPN with an authorised T-Mobile SIM card.

Unlike the public APNs – which all mobile users can have access to – the private APN (which maps the Layer 2 PVC to the customer's VPN) is only allocated to users who have provided the relevant identity credentials. Each user, with the same private APN, then forms a closed user group.

For security reasons, access to the private APN is controlled by an HLR (home location register). The checks conducted by the HLR on the SIM card ensure that only approved users get access to the corporate intranet. If the IT manager requires an additional username/password check before corporate LAN access is granted, this can be built into the system. However, a T-Mobile spokesperson told BWCS that these additional security checks were not strictly necessary as the private APN approach – with its closed user group based on SIM-card subscription – provides an inherently high level of security.

2.6 Application-specific VPNs (SSL)

2.6.1 Overview

The technology commonly underpinning an 'application-specific' VPN is SSL (secure sockets layer). Simply put, SSL encrypts data at the so-called 'application layer'. In practical terms, that means that any end-user device with a Web browser can access 'Web-enabled' enterprise resources.

SSL has a strong pedigree in providing secure data transmission as it is widely used for e-commerce and online banking (the 'padlock' icon that appears on the PC screen to indicate a secure connection when buying a book from Amazon.com, for example, is courtesy of SSL).

A main SSL advantage over IPSec is that there is no need for the IT administrator to install, configure and manage VPN clients. Instead, by harnessing the power of the near-ubiquitous Web browser, the 'clientless' approach has clear potential to lower device management costs.

Conversely, a main IPSec advantage over SSL stems from not encrypting at the application layer but at the network layer: IPSec sets up a secure tunnel through which *all* corporate LAN applications can be accessed.

SSL VPNs, on the other hand, can only access server-based applications that have an SSL interface or are Web-based (such as Outlook Web Access).

If corporate LAN applications have to be drastically modified to become 'SSL friendly', or the range of applications that the remote user can access is severely limited when using SSL, then – arguably – it is not a true VPN solution at all.

For the purposes of this report, however, BWCS will characterise SSL as a VPN technology that can be used either as an alternative or complement to IPSec-based VPNs. The reason for doing so is twofold:

- Remote access to Web-based e-mail (and applications) will be sufficient, in many instances, for mobile workers to help carry out their tasks adequately away from the office.
- The range of applications that SSL vendors can offer access to is increasing. Through the so-called 'enhanced clientless mode', where Java or Active X modules are downloaded to the terminal (most likely to the laptop), it is possible for end-users to access corporate-based e-mail (Lotus Notes and MS Outlook) as if they were on the LAN. The enhanced clientless mode can also access other applications, such as SAP and PeopleSoft. Aventail, an SSL-only vendor, has gone as far as developing a full-blown SSL VPN client, known as Aventail Connect, which purports to offer the same level of corporate LAN access as IPSec VPN clients. However, like IPSec VPN clients, Aventail Connect has to be installed and configured on the end-user device.

2.6.2 SSL moves by Cisco and Nortel

In November 2003, two major vendors of IPSec VPN components – Cisco and Nortel – announced they would be launching hybrid SSL/IPSec VPN gateway products in the first and second quarters of 2004 respectively. IT administrators, through one management platform, will now be able to offer SSL and IPSec access through hybrid solutions.

The intention of Nortel and Cisco to move into the SSL space can rightly be interpreted as a validation of this relatively young market and a sign that it is reaching a new stage of maturity. During 2003, the SSL market had already begun to consolidate, with SSL start-ups uRoam, Neoteris and SafeWeb being acquired by F5, NetScreen and Symantec respectively. In February 2004, Juniper Networks then bought NetScreen. There still remain a few independent SSL vendors, the major ones being Aventail, Netilla and Whale Communications.

The initial SSL proposition from Cisco is WebVPN, which is a free software upgrade to existing customers of its VPN 3000 series of IPSec concentrators (or gateways). It supports a narrow range of applications,

including Outlook Web Access, although Cisco has plans to develop its SSL capability to match the access features of the more established SSL players.

Although this is an aggressive pricing move by Cisco into the SSL space, IT managers will take note that SSL consumes far more software processing power than IPSec. For its VPN 3005 concentrator, Cisco reports that one SSL customer absorbs the equivalent processing power of four IPSec clients (see Table 2.2). As such, the VPN IPSec 3005 concentrator, which supports 200 IPSec clients, could be transformed into either 50 SSL connections or a mixture of both – 20 SSL connections and 120 IPSec clients, for example.

Cisco says it is responding to market demand for secure access to basic key applications, such as e-mail, without incurring the costs associated with IPSec.

Table 2.2 SSL capacity on the Cisco VPN 3000 Concentrator series

Model	Number of IPSec 'tunnels' supported	Number of 'clientless' SSL connections supported	Bandwidth capability
VPN 3005	200	50	4Mbps
VPN 3020	750	200	50Mbps
VPN 3030	1,500	500	50Mbps
VPN 3060	5,000	500	100Mbps
VPN 3080	10,000	500	100Mbps

Source: Cisco

Nortel's move into hybrid IPSec/SSL space involves adding SSL capability, via a hardware solution, to its Contivity range of IPSec VPN equipment. That is expected to become commercially available in 2Q 2004. The company also launched its VPN Gateway 3050 in December 2003, which offers SSL access. An upgrade to the VPN Gateway 3050 is expected in 2Q 2004, which will enable it to support IPSec VPN clients.

Prior to announcing its plans for a hybrid SSL/IPSec platform, the Canada-based vendor had been offering SSL support on its Alteon load-balancing switch since July 2002. This piece of hardware performs the function of off-loading SSL processing from servers to increase their productivity. According to Nortel, the number of Web-based transactions a server can typically handle is 20-30 per second, but by off-loading processing onto supporting hardware the number of transactions can increase to 1,000 per second. Nortel claims it has a 50 per cent share of the SSL accelerator market.

2.6.3 SSL and IPSec VPNs: a comparison

The two key issues that will occupy the minds of IT managers when weighing up the pros and cons of each SSL and IPSec VPN solutions for remote access are: total cost of ownership (TCO) and level of functionality.

TCO will revolve around the following areas:

- device management (including help-desk support costs and end-point security solutions)
- VPN gateway investment and maintenance
- formatting server-based applications for mobile terminal access
- end-user training.

Functionality considerations will include the following questions:

- How easy are the mobile devices (including laptops) to use?
- Can remote workers securely access the relevant enterprise resources to carry out tasks effectively away from the office?
- How easy is it to set up extranets with business partners and/or customers?

Getting objective answers to both these areas, particularly on TCO, is no easy task. The SSL-only vendors, for example, generally see their solutions as competing head-on with IPSec VPNs for remote access working. In doing so, there is a danger that they exaggerate the shortcomings of their IPSec 'opponent' as part of their strategy to promote their own products.

Aventail, in one of its white papers – *Comparing Secure Remote Access Options: IPSec VPNS versus SSL VPNs* – talks about there being 'no easy solutions' for NAT traversal (a requirement for IPSec VPN devices using private IP addresses). This is perhaps to overstate the problem since NAT Traversal products – by the likes of Cisco, Nortel and Lucent – are well established in the marketplace and come as part of their VPN 'box'.

It is unlikely that IT managers of large organisations, when weighing up their remote access options, will choose one solution over the other. The most likely scenario is that a mixture of both will be deployed, with 'higher level' staff having access to both a full range of corporate LAN applications (IPSec) and e-mail (IPSec and/or SSL), while other employees (identified by the IT manager) have access to e-mail only (SSL).

2.6.4 SSL advantages over IPSec-based VPNs: summary

- Easier and cheaper to administer than VPN solutions based on IPSec clients. However, if SSL end-point security solutions, such as digital certificates and/or hardware tokens (which generate one-time passwords) are used, the extent of that advantage will be reduced. The use of SSL clients will also undermine the IT administration cost advantage over IPSec clients.
- Easier to set up extranets. Due to lack of interoperability between different vendors' IPSec-based equipment, enterprises may be thwarted in their attempt to build extranets with their customers or partners (different IPSec vendors). SSL-based solutions, through the use of standard Web browsers, would not encounter the obstacle of vendor non-interoperability.
- By operating at the application layer, SSL is immune to the NAT issues that IPSec VPN clients have to deal with. It also makes corporate LAN access easier when making site visits to customers or partners. The visited network may have a firewall policy, for example, which blocks outgoing traffic based on IPSec. SSL would not face that limitation.

2.7 Mobile voice VPNs

Although this report is primarily focused on data connectivity, it is possible to identify a mobile voice VPN. This is where the public cellular network offers PBX functionality. Such a network configuration will allow mobile phone users to call colleagues by using the 'short codes' of their existing fixed-line extension system. The strategic merits of this service for mobile operators are assessed more fully in the profile on Ericsson, a leading proponent of mobile voice VPNs (see Chapter 7).

3 Barriers to Adoption

3.1 Overview

There are numerous reasons why an enterprise might decide not to mobilise large portions of their workforce. First and foremost, IT managers and CIOs may simply see no productivity benefit or meaningful return on investment (ROI) to be gained by adopting a mobile VPN solution. The feedback BWCS has received from both mobile and fixed-line operators (which wholesale mobile network capacity), when they seek to explain the poor mobile VPN take-up rates among their business customers, suggests that this view is a prevalent one among C-level executives.

That being so, there is a strong case for making a more vigorous effort to educate different vertical industry sectors as to the potential productivity and competitive benefits that mobile access to up-to-date corporate LAN information and applications can bring. Mobile operators who best understand the business needs of their customers clearly have the best chance of success in the mobile VPN space.

Concern about security is another obvious barrier to adoption. Although VPN technology, by its very nature, is designed to address these concerns head-on, mobile VPNs are not always assumed to be secure. As we have seen in Chapter 2, mobile operators wishing to promote network-based mobile VPNs that use 'split-tunnelling' – with the potential of introducing higher margin services to their customers – face the problem of convincing IT managers that they can be trusted providers.

Total cost of ownership is also an overriding concern. Not only does the cost of mobile data, terminals and (where required) application reformatting for mobile access need to be considered, but the on-going overheads of device management (installing and updating VPN clients) and help-desk facilities to support mobile workers have to be factored in.

In addition, to keep capita expenditure down to a minimum, enterprises that have already invested in fixed-line VPN equipment want their mobile VPN extensions to be as compatible as possible with existing infrastructure and current versions of laptop operating systems.

It would be unfair to say that mobile operators are unaware of these concerns. Each of the operators profiled in this report – Vodafone, mmO2 and T-Mobile (Chapter 5) – are making strides to address these issues with the help of vendor and system integrator partners.

The fact remains, however, that mobile VPN adoption has yet to gain momentum. This chapter focuses on two key areas why this has been the case:

- **The inadequacy of GPRS as a transmission medium for end-to-end IPSec VPN traffic.** Although mobile operators in Europe are moving forward with commercial 3G network launches, coverage will not, in the short-term, match the ubiquity of GPRS. Maximising GPRS performance is still a priority for mobile operators if they are to gain competitive advantage. Mobile traffic shaping solutions appear to be one way to boost GPRS performance.
- **Prohibitively high (and unpredictable) mobile data charges.** Mobile operators are making headway in pricing mobile data more attractively but there is still room for improvement, particularly on international roaming charges.

Finally, this chapter gives attention to the issues surrounding smartphone support. If mobile data usage among the enterprise workforce is to become widespread, the ability to provide cost-efficient help-desk facilities for smartphone users – both for SSL and IPSec VPN traffic – will be required.

Smartphones, particularly those using Microsoft operating system (OS) software – with its promise of easy synchronisation with desktop applications (where Microsoft is dominant) – are set to become more pervasive in the enterprise space.

3.2 Unreliable GPRS data performance

3.2.1 Overview

"GPRS service performance today is totally uncontrolled and unpredictable. As a result, the quality of GPRS services in some key European markets is already very bad and is rapidly decreasing as GPRS usage increases. This problem significantly threatens the future growth of GPRS services."

These were the words of Haim Zelikovsky, EVP of marketing for Israeli-based Cellglide, speaking at a mobile Internet conference held in Paris in November 2003.

As Cellglide is a provider of 'mobile traffic shaping' solutions (which are specifically designed to address the problem of performance unpredictability), it may be tempting to conclude that Zelikovsky is exaggerating the shortcomings of GPRS to draw attention to his own company. From the research undertaken by BWCS in the compilation of this report, however, there is no reason to believe that Zelikovsky is overplaying his hand. No mobile operator, to BWCS's knowledge, was offering service level guarantees over its GPRS network by the end of 2003. And enterprises themselves – a market segment that has become accustomed to SLAs from their fixed-line service providers – have been

slow to warm to GPRS as a means to remotely access their corporate LAN or web-based applications.

The general lack of enterprise commitment to GPRS can't only be explained by the absence of SLAs: total cost of ownership, security, ease-of-use and the desire for a demonstrable ROI are all key issues as well. However, lack of reliability is still a significant stumbling block.

Some, like Lucent Technologies (Chapter 7), would go so far as to argue that there is insufficient spectrum on the GPRS platform to persuade enterprises that it can be used for anything other than basic e-mail access. Yet Cellglide maintains that, with the appropriate mobile traffic shaping technology, mobile operators can maximise their GPRS investment by offering their consumer and business customers extra services they would be willing to pay for. This can only be done, though, if those services have certain QoS guarantees attached to them.

3.2.2 Why is GPRS unreliable?

A brief look at how GSM/GPRS spectrum is utilised tells us why GPRS data performance becomes more unreliable when usage increases. GPRS, like GSM, uses the TDMA (time division multiple access) technique and that requires discrete parts of the cell spectrum (usually 200KHz) being divided into so-called 'time-slots'. This 200KHz chunk of spectrum (known as a carrier) is typically divided into eight time-slots (which are also known as channels).

For GPRS data usage, mobile operators typically assign four time-slots to each end-user device for downloading data and one time-slot for uploading. If one user has exclusive use of all four time-slots, then he or she will receive throughput in the region of 40Kbps. However, as spectrum is a finite resource, it often happens that time-slots have to be shared among the different GPRS data users who are located within the same 'cell' (a region of the mobile network defined by the radius of one base station). The contention for the same resources leads to performance degradation.

To borrow the analogy used by Cellglide, the GPRS radio access network (without mobile traffic shaping) is equivalent to different vehicles (applications) colliding with each other across different lanes (channels). The end result is chaos and each vehicle is delayed from reaching its destination.

3.2.3 Heterogeneous and bursty data equals chaos

Adding to the 'chaos' in the GPRS cell is the nature of the data traffic itself, which is 'heterogeneous and bursty'. It is heterogeneous because there are multiple applications with different requirements competing for the same finite resources. For example, rich media streaming, which requires a constant bit-rate, could be competing with a file transfer session

for the same capacity resources, which is not as time sensitive. However, with the way GRPS networks are set up today (without traffic shaping) the mobile operator has no way of identifying individual services and can not give one type of application preferential treatment over the other.

Secondly, GPRS data traffic demand is 'bursty' because it makes no constant demand on capacity resources. For example, over a period of time, there will be peaks and troughs of data traffic demand on a single cell as a changing numbers of users – with fluctuating application requests – interact with the GPRS network. By contrast, the available cell capacity remains relatively constant over that same period of time but significantly, in many instances, *below* the 'peak' demands made upon it. When that happens, users experience performance degradation.

One way of solving that problem would be to add more GPRS capacity throughout the network – the 'brute force' approach as Zelikovsky calls it. But that, says Cellglide, would be unnecessarily expensive.

3.2.4 The Cellglide proposition: Mobile Traffic Shaper (MTS)

Extending the vehicle and lane analogy, Cellglide's mobile traffic shaping solution professes to act as a 'traffic policeman'. It makes sure that different types of 'vehicles' (applications) are allocated to dedicated lanes (channels) according to prior agreements made between the mobile operator and the end-user. The result is that mobile operators can offer service level agreements on certain services and applications.

Cellglide officially launched its Mobile Traffic Shaper (MTS) service node product, which fills up a standard seven-foot rack, at the 3GSM Congress event held in Cannes in February 2003. Sitting at the 'edge of the network core', with traffic-monitoring links feeding into the GGSN (Gateway GPRS Support Node), the mobile operator can get a visual real-time view – a screen display – of how individual applications are performing on all cells the GGSN supports.

If the MTS performs as Cellglide says it does, then the mobile operator will be able to 'smooth' the troughs and peaks of the bursty data traffic to match the constant available capacity on the GPRS cell. For example, a large portion of mobile data traffic will be e-mail, but it isn't as time-sensitive as, say, video streaming. As such, video streaming data packets will be given priority over e-mail data packets, thus creating a 'levelling' of the peaks and troughs of traffic demand commonly seen in GPRS cells that don't have some form of mobile traffic shaping. And if the monitoring tools reveal there is still capacity shortage within particular cells, then those can be addressed individually without having to make a blanket investment across the whole network.

In practical terms, the mobile operator can now offer application performance guarantees and, potentially, extra revenue from the enterprise sector. It also provides an important opportunity for mobile operators to

avoid being relegated to the role of mere pipe providers in the mobile VPN space. By owning the mobile network, it is only they who can offer service policies per application and it is only they who can prioritise traffic based on:

- user ID
- the source of the traffic, based on the APN
- device type
- location (based on cell ID)
- time.

Unlike software optimisation and compression platforms, MTS is deployed within the network both for end-to-end and network-based mobile VPNs. There is no difference in the degree performance enhancement for either type of mobile VPN, says Cellglide.

“Our proposition has been validated in a series of meetings [November 2003] with Tier 1 operators in Europe, including Orange UK, Orange Swiss, Vodafone UK, TIM, WIND and Omnitel,” Nir Zamir, director of global marketing for Cellglide, told BWCS. “All operators that have been exposed to the solution have chosen to continue with it and explore further the integration of the system within their networks.”

At the end of 2003, Cellcom – Israel’s largest mobile operator with three million customers – said it was on the verge of launching commercial services based on the MTS product after trialling it throughout the year.

According to Cellglide, a typical installation of the MTS – to serve one GGSN – would cost in the region of US$1 million.

3.2.5 Which applications need SLAs?

Cellglide identifies a number of applications that would require some form of service level guarantee if customers were to pay for them. These include:

- wireless point of sale
- remote control and command
- machine-to-machine
- video streaming
- push-to-talk.

For the corporate space, Cellglide highlights the potential of wireless point of sale as a new and lucrative revenue stream for mobile operators.

"We have one project with a Spanish mobile operator who has a corporate customer with 20,000 mobile sales people selling lottery tickets," says Zamir. "They need to be constantly and securely attached to their corporate network and have a guaranteed quality of service [for wireless credit card transactions] in order to sell tickets right up to the legal deadline. That wasn't possible over GPRS until MTS."

3.2.6 Cellcom: a mobile operator's verdict on MTS

To verify the claims made by Cellglide for mobile traffic shaping, BWCS contacted Cellcom in December 2003, a mobile operator who had been testing MTS within its network for 11 months. "We've finished the trial process [with MTS] and the results are exactly in accordance with the expectations and specifications set by Cellglide," Tzvi Schechori, Cellcom's vice president of research and technology, told BWCS.

In the corporate space, Schechori concurs with Cellglide that wireless point of sale will be a key area for Cellcom to play in; MTS will help it avoid the prospect of competing for business customers purely on the price of the pipe compared with other mobile operators, which is Schechori's biggest fear.

"For wireless point of sale, we're not competing with other mobile operators but with the fixed-line service providers, such as banks," he says. "With MTS we can now go to the enterprise and say we can guarantee that the end-to-end process of taking the credit card from the customer and completing the sale will take no longer than seven seconds [without MTS, the same transaction can take up to 40 seconds]. If you can't offer that guarantee, then corporate users aren't going to use the network. It's the difference between having and not having the customer. And, of course, we can offer the added convenience of mobility, which the fixed-line service providers can't."

Other industry sectors for which Schechori sees MTS having a use include the emergency services. "We can now offer ambulances, hooked into our network, performance guarantees," he says. "We can give their communications priority, even when we have a mass calling event over our network."

It is Schechori's view that while consumers are willing to pay for a best-effort service, this is not acceptable in the corporate space for applications other than e-mail. Business users, he contends, will be willing to pay a premium for QoS guarantees. Although Cellcom has done internal research into how much corporates would be willing to pay over and above its standard GPRS data tariffs, Schechori declined to share those findings with BWCS.

Cellcom is planning to upgrade its GPRS network to EDGE (Enhanced Data Speeds for GSM Evolution) during 2004, which will increase date rates by three to five times compared with GPRS. MTS is also compatible

with EDGE, and Schechori expects the network upgrade will allow it to make an even more aggressive pitch to the business customer.

3.3 Mobile data pricing

3.3.1 Too high

For a mobile data service that seeks only to emulate PSTN dial-up throughput performance, operators have – historically – priced GPRS tariffs at spectacularly high levels, especially when you consider the absence of service level guarantees. When GPRS was first commercially launched Europe in 2001, the typical cost of sending or receiving 1MB of data was €20.

There are encouraging signs in the marketplace, however, that mobile operators are now reducing their data tariffs to more acceptable levels. T-Mobile, for example, openly admitted in April 2003 that it had got its data pricing completely wrong when it slashed its per megabyte charges in each of its European markets by 70 per cent. That took the price per megabyte down to around the €10 mark for subscribers not signed up to any of its data packages.

The promotion of data bundles by mobile operators is also bringing down the cost per megabyte. In March 2004, T-Mobile in Germany launched a series of data packages to stimulate greater usage: 'light' users can now get 2MB for €10 on its Data 2 option, while 'heavy' users, on its Data Flat 500 package, receive 500MB of data for €110.00 a month – that's a cost of €0.22 per MB if the entire budget is used.

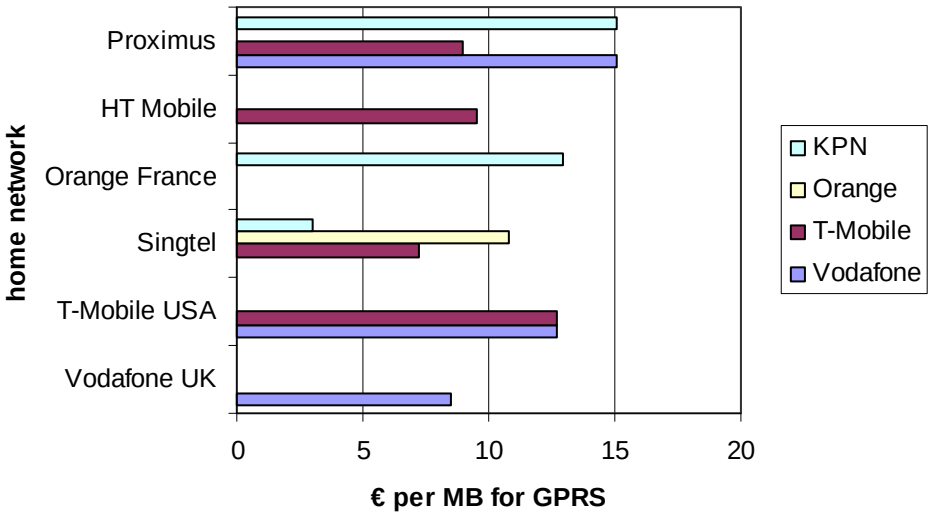
Mobile operators are beginning to recognise that IT managers will actively discourage their mobile workers from using GPRS if information can be updated and synchronised with the corporate LAN at the end of the day – either at home, back in the office or even in a hotel room abroad – if it is cheaper to do so and has no significant bearing on the company's competitiveness. This is particularly true for enterprises that already have toll free numbers in place, which reduce national and international PSTN dial-up charges.

Yes, enterprises will be willing to pay a mobile data premium over PSTN dial-up connections to take into account the 'anytime, anywhere' convenience, but the trick for mobile operators is to pitch the pricing of mobile data at levels that accurately reflect its worth. At the moment, particularly for international roaming, data charging seems over-priced.

According to figures compiled by the INTUG (International Telecommunications Users Group) from operators' websites – see Table 3.1 – users who roam onto the four networks in the Netherlands (which INTUG sees as a typical European market in terms of pricing) can pay in excess of €15 per megabyte. Subscribers to Proximus, a Belgian mobile

operator, will pay €15.13 per megabyte if they roam onto either the networks of KPN and Vodafone. The cheapest rate for data roaming is between Vodafone networks (Vodafone UK on Vodafone NL) at £5.88 per megabyte.

Table 3.1 GPRS roaming in the Netherlands (as of November 2003)



Source: INTUG/mobile operators' websites

"This type of pricing is insane and can be seen in other countries, too," Ewan Sutherland, INTUG's Executive Director, told BWCS. "When I was in Australia [early 2004] and staying at the Intercontinental Hotel, I paid €10 for the use of a broadband connection, installed in the room, for 24 hours. Why should I use GPRS?"

Although you would expect a users group to complain vehemently about pricing, Sutherland nevertheless raises an important issue that mobile operators need to address. There is a perception among end-users that mobile data pricing abroad is in the same exorbitant price league as hotel telecom services and, in some instances, more expensive. This will hold back mobile VPN adoption. Moreover, high per megabyte charging will frighten IT managers even more with the introduction of 3G due to its ability to send and receive larger volumes of data in a shorter space of time.

To remove mobile data pricing as an obstacle to mobile VPN growth, mobile operators need to do two things:

- give IT managers easy-to-understand tariff packages that allow them to predict accurately their monthly mobile data usage costs; and
- demonstrate the value of mobile data usage to justify those predictable costs.

3.3.2 Too unpredictable

Charging by the megabyte brings with it something that IT managers, arguably, dislike more than the high charges themselves – unpredictability of costs. IT managers, in all likelihood, will not be able to forecast accurately how much data their mobile workforce will consume each month. There is no widespread understanding among end-users of what a megabyte means in practical terms and it is extremely hard, if not impossible, to predict the amount of data that a mobile worker may require in the field anyway.

Mobile operators can offer graphical user interfaces in an attempt to make data usage more transparent. Vodafone's 'Dashboard', for example, shows how much data has been consumed as a bar indicator on the laptop. However, to allay IT managers' fears surrounding unpredictability of costs within the per megabyte tariff model, they would need to be able to enforce data usage limits on their mobile workers (not easy) and to have consistent per megabyte charges across different territories (emerging slowly).

The most common strategy employed by mobile operators in Europe to reduce the element of cost unpredictability is to offer data bundles at a flat rate to give the 'all-you-can-eat' feel.

The Vodafone Group, following on from the launch of its 3G/GPRS Mobile Connect Card in February 2004 in seven European territories (UK, France, Germany, Netherlands, Italy, Spain and Portugal) released price plans based on the widely-used principle of the more data subscribed to, the cheaper it is per megabyte. This assumes, of course, that the majority of data allowed in the month is consumed.

Table 3.2 Vodafone UK Mobile Connect 3G/GPRS data card prices (announced February 2004)

User profile	Minimum card price (excluding VAT)*	Standard tariff (excluding VAT) per month	MB bundle included per month	Promotional MB bundles per month (until October 2004)	Out of bundle price per MB (excl. VAT)
Low user	£150 (€225)	£10 (€15)	5	No Promo	£2 (€3)
Medium user	£100 (€150)	£20 (€30)	25	50	£1.50 (€2.25)
High user	£80 (€120)	£45 (€67.5)	150	300	£0.75 (€1.125)
Power user	£50 (€75)	£85 (€127.5)	500	1,000	£0.50 (€0.75)

**17.5 %; Exchange rate used: £1 = €1.50; Source: Vodafone UK*

Vodafone UK says that its data pricing levels, along with its distinction of four types of user, are based on 'extensive research' with trial customers. In particular, these different types of users were found to have the following characteristics:

- **Low-user (average usage of 4MB per month)** – One-man-band business using an Internet-based account and occasional Web browsing. Travels infrequently but wants to be in touch when needed.
- **Medium user (average usage of 20MB per month)** – SoHo business with a need to be mobile around 40% of the time. Uses laptop to show clients the company website; also uses Internet-based e-mail account when on the move.
- **High user (average usage of 150MB per month)** – SME business (up to 250 employees) employing multiple sales people or consultants that are mobile 60% of the time; strong need to connect to company network to receive and send e-mail as well as to access company systems and applications while on the move.
- **Power user (average usage of 430MB per month)** – Suitable for international business travellers that are mobile 85% of the time. Vital need for constant access to company network: downloading and uploading presentations while accessing company systems and applications, plus e-mail access. Also requires access to the Internet in the UK and in other European countries.

T-Mobile UK is the first European mobile operator that BWCS is aware of to offer a genuine 'all-you-can-eat' tariff package – that is, one without any limits on data usage. For £70 (€105) per month, T-Mobile UK is offering unlimited data access over its GPRS, 3G and WiFi networks. This is an aggressive move by T-Mobile UK although, significantly, it has marketed the service as a 'special introductory offer'. It is clearly leaving the door open to withdraw the offer, without loss of face, if the transport costs incurred by T-Mobile UK should become too high to support it.

Although the all-you-can-eat approach is one which should attract IT managers, the T-Mobile UK offer looks expensive when compared to KDDI's Au Win service in Japan. Using KDDI's CDMA2 1X EV-DO network, voice customers can purchase unlimited monthly data usage for 4,200 Yen (€33) with download speeds of up to 2.4Mbps on a best-effort basis. In the US, Verizon offers monthly unlimited data usage over CDMA2000 1X network – 40-60Kbps download speeds, bursting to 144Kbps – for US$79,99 (€68).

Mobile operators are also making progress in removing inconsistency in roaming charges, which, traditionally, have varied markedly from country to country. Vodafone UK, for example, since November 2003, has been offering its data users roaming rates of £5 per MB (excluding VAT) on

other Vodafone networks and £8.75 per MB (excluding VAT) on non-Vodafone networks.

This consistency of roaming charges is not restricted to the Tier One players with large footprints. O2 UK, for example, offers per megabyte charging for its 'Tier A' partners at £6.00 (excluding VAT), which applies to a large number of operators in Europe and Asia. O2 UK subscribers would be well advised, however, to check who the mobile operator's Tier B partners are – roaming onto those networks would cost £18.00 per MB (excluding VAT).

The FreeMove alliance – comprising Orange, Telefónica Móviles, TIM and T-Mobile – has also highlighted the need for 'simple and predictable' roaming price plans between the networks of its members and non-members; it also aims to offer a fixed price for Blackberry roaming anywhere in the world on any network. These intentions were announced at a press conference held in London in March 2004. Hard details, according to FreeMove, will emerge during the course of 2004.

3.3.3 Different approaches to mobile data pricing

Group shared bundles and 'rollovers'

One of the most innovative mobile data pricing packages available in the marketplace today comes from O2 in the UK with its GPRS 'group shared bundles' and the facility of being able to 'roll over' unused data from one month to the next.

The principle behind the scheme is that data bundles can be shared between some or all of the mobile devices in the company rather than simply being used by one individual.

Table 3.3 Tariffs for O2 UK's GPRS group shared bundles

	Group shared bundles (with voice calling plan or as data only)			
	1/4GB	1/2GB	3/4GB	1GB (1024MB)
First user subscription	£180	£330	£460	£560
Additional user subscription	£3.50	£3.50	£3.50	£3.50
Inclusive data	256MB	512MB	768MB	1024MB
Rollover of unused inclusive data	3 months	3 months	3 months	3 months
Rate per MB exceeded	£0.85	£0.85	£0.85	£0.85

**All prices are exclusive of VAT*
Source: O2 UK

Time-based billing for packets

As an alternative to its volume-based data bundles, Vodafone Germany launched a series of time-based billing packages in February 2004 to coincide with the commercial launch of its 3G/GPRS Mobile Connect Card for laptop users (Table 3.4).

Table 3.4 Vodafone Germany: time-based data tariffs

Tariff option	Time allowed	Monthly charge	Overrun charges (for each extra ten-minute block)
Time L	2 hours	€11.60	€2.20
Time XL	10 hours	€34.80	€1.51
Time XXL	30 hours	€69.60	€1.04

Source: Vodafone Germany

T-Mobile Deutschland, effective from 1 May 2004, also offers three time-based packages: 'Time 120' (120 minutes of mobile data transfer for €10); Time 600 (600 minutes for €35); and 'Time 1800' (30 hours for €70). Data can be accessed over T-Mobile Deutschland's 2.5G, 3G or WiFi networks.

The advantages of this billing approach are that IT managers are already used to it and it is far easier to understand than per megabyte charging. The disadvantage is that end-users will be paying for 'thinking time' and not for the amount of data downloaded (as in the volume-based model).

Vodafone and T-Mobile say they have identified a demand for this type of billing, so it would make sense that they provide this option as another tactic to increase mobile data usage over their packet-switched networks. It would also seem to indicate a significant level of dissatisfaction among business customers with volume-based billing.

3.3.4 Mobile e-mail: the need to address IT managers' cost concerns

Aside from the problem of convincing IT managers that granting mobile e-mail access to employees throughout the organisation can give significant productivity gains (Chapter 4), there is also the issue of cost.

IT managers – at least according to those trying to sell mobile e-mail solutions into the workplace – are resisting widespread mobile e-mail access adoption within the enterprise because they fear that data costs will spiral upwards uncontrollably. If 'always-on' GPRS access to corporate e-

mail is given to all mobile employees – not just senior managers – then IT managers believe that the greater amount of data that inevitably would be consumed would exceed wildly the usage caps placed by the mobile operator on existing data packages.

One vendor trying to promote widespread mobile e-mail adoption within the enterprise – and break down the perception that pervasive mobile e-mail access equates to dramatically higher bills – is Mobeon, a Sweden-based company supplying mobile e-mail and IP-based messaging solutions.

Owned 70 per cent by Brainheart Capital (a Swedish venture capital company) and 30 per cent by Ericsson, Mobeon reports that IT managers are the greatest points of resistance to expanding the mobile e-mail access market. Although employees like it and find it useful (Mobeon says that 74 per cent all mobile users who have been provisioned with e-mail access continue to check their mailboxes daily), IT managers are not biting. According to Mobeon's channels to market for its mobile e-mail access product – mobile operators, systems integrators and resellers – perceived high cost and lack of value in the service are the two main stumbling blocks.

Yet, according to Mobeon, concerns over cost are misplaced. Unlike the RIM Blackberry messaging solution, which is proprietary and requires dedicated end-user devices, Mobeon's 'Airlook' product (which can be rebranded under white label OEM agreements) allows e-mail access from workers' standard mobile phones, PDAs or notebooks. (A main Blackberry advantage over Airlook is that it is a 'push' service – incoming e-mails are sent to the device – whereas browser-based solutions like Airlook require the user to 'pull' the e-mail to the device after actively browsing the mailbox.)

Key to driving down costs is the Airlook PIM (personal information manager) server, which is installed within the company's firewall DMZ (a de-militarised zone that separates internal and external zones), which present a 'low overhead interface' to Microsoft Exchange and Lotus Domino over HTTP or WAP (wireless application protocol). By paring the message text and attached files down to the minimum, Mobeon argues that it can offer enterprises a significantly more cost-efficient mobile-email solution than a standard GPRS connection to Outlook Web Access (OWA).

As far back as February 2003, Mobeon published a white paper detailing a cost comparison between OWA and Airlook based on a trial using Vodafone Sweden's network. Technical details of the trial and data costs are shown in Tables 3.5 and 3.6.

Table 3.5 Technical details of trial contrasting OWA access and Airlook

GPRS card	Nokia D211
SW Version	3.25
APN	Internet.vodafone.net
GPRS signal strength	100 percent
Exchange version	Exchange 2003, Beta version
HTML browser	Internet Explorer (version 6.0)
OS on computer	Windows XP

Source: Mobeon

Table 3.6 Cost details of trial contrasting OWA access and Airlook

Fixed cost/month	SEK65 (€7.2) (including 2MB)
Cost of additional KB	SEK0.016 per KB (€0.0018 per KB)
Cost of additional MB	SEK16 (€1.77)
Currency exchange	SEK100 = €9.05

Source: Mobeon

The key findings of the trial were:

- The cost of logging onto the Airlook application is three per cent of the cost of logging onto Microsoft OWA (Mobeon uses 12KB of data, Microsoft OWA uses 421KB). If a user logs onto the application twice a day every workday in the month, the cost difference starts to become noticeable, with €0.84 per month for the Airlook user and €29.7 per month for the OWA user.
- The cost of using Airlook to check and read e-mails is 16 per cent of using OWA (an Airlook user who opens and reads five e-mails twice a day every workday in the month costs €2.80 per month; an OWA user costs €16.79 per month).
- The cost of performing standard procedures using Airlook is 19 per cent of the cost using OWA. Standard procedures include reading and sending e-mails and checking calendars – €8.20 per month for Airlook, €42.7 for OWA. For a company with 2,000 employees, Airlook costs €1,640 per month, while OWA costs €8,540 per month. On a yearly basis the difference is €19,680 compared with €102,480 for OWA.
- From an end-user convenience perspective, the trial also revealed that Airlook had a significant advantage. The time to log onto Airlook took an average of four seconds compared with the average time of three minutes and 33 seconds for OWA using the GPRS card.

If we accept that these findings are accurate and that there is still a heavy resistance to mobile e-mail solutions based on the grounds of cost, then clearly there is an education gap in the marketplace. The challenge is there for mobile operators and interested parties to try and bridge that gap.

3.4 Smartphone support management

3.4.1 A growing problem

The smartphone is a mobile telephony device that allows additional computing functionality with one-handed input. To distinguish it from voice-enabled PDAs (personal digital assistants) we can say that the smartphone is a mobile phone with data applications added onto it. With the PDA, the reverse is true. It's a data-orientated device, with a comparatively large screen, and doesn't lend itself to spontaneous mobile telephony (holding a large, square-like device to the ear is not an attractive prospect for many end-users).

As the retail price of the smartphone comes down and its reliability and functionality improves, its take-up by both consumer and business customers will inevitably increase.

The growth of the smartphone market will place a greater strain on the customer support resources of the mobile operator, device manufacturer and the enterprise IT manager. This is simply because the device is far more complicated to set up and use than a standard handset, which will lead to a greater number of help-desk calls.

"Smartphone users will quickly become frustrated if they can't do what they want to do easily," Andrew Wyatt, vice president of strategic marketing at UK-based Intuwave, told BWCS. "The main reason for that is their service-level expectations are high since they equate the smartphone with the mobile phone. They have become used to 'dialtone' levels of reliability and simplicity."

To illustrate the comparative complexity of the smartphone, Intuwave – a provider of software designed to make smartphone support management easier – holds up the Sony Ericsson P800 as an example. With this smartphone device, there are over 12 parameters to set before the e-mail function can work. "It is almost inevitable that a user is going to input at least one of those parameters incorrectly," says Wyatt.

The large scope for error surrounding e-mail set-up on the smartphone should be a major concern for mobile operators. If users can't access the service on their smartphone, they will more than likely call up the mobile operator – rather than the device manufacturer – to sort out the problem. And if that leads to an unsatisfactory customer service experience, then the likelihood of churn increases and the rate of mobile data take-up slows down.

It also wouldn't auger well for persuading IT managers to mobilise more complex applications in the future, which would generate more mobile data traffic. If mobile operators can't get e-mail support right, or if they can't at least provide enterprises with the tool-set to support their smartphone users, how could they convincingly persuade business

customers that they would be able to provide cost-efficient support for more complex mobile applications – such as sales force automation – in the future?

3.4.2 The cost of smartphone support

As it stands at the moment, Intuwave asserts that smartphone customer support has the potential to cost mobile operators £9 billion a year worldwide by 2007. It arrives at that figure by making the following assumptions:

- 150 million smartphones will be shipped out in 2007
- a smartphone user, on average, will make two 15-minute calls per year to the mobile operator's support staff
- each minute of the call will cost the mobile operator £2 in fully-weighted staff costs.

Intuwave has, of course, a vested interest in describing smartphone management as the 'number one' problem for mobile operators' customer support staff. It did, however, go some way to providing independent information to back up its claims with the publication of commissioned research undertaken by Taylor Nelson Sofres in November 2003. After interviewing 95 smartphone users in the UK, all aged over 16, the survey found the two most common areas of frustration were:

- not knowing what features are available (30 percent); and
- not knowing how to download applications (29 percent).

Additional findings of the survey found that e-mail was the most popular application (44 per cent of the respondents said they used it) while another 19 per cent said they would like to use e-mail but didn't (presumably due to a lack of knowledge of how to do so).

There's no reason to believe that corporate users are inherently more sophisticated than consumers and would not find the same level of difficulty as those interviewed by Taylor Nelson Sofres. In fact, they could be more disadvantaged than consumers since they are more likely to be confronted with more complex tasks, such as the synchronisation of the device with the PC. "Those kind of procedures are generally beyond the grasp of most enterprise employees," says Wyatt.

But couldn't IT departments simply train up their smartphone users to avoid a lot of these usability problems? "It's not as easy as it sounds," argues Wyatt. "How, for example, would you train up, say, 50 workers on how to use a smartphone when it has got such a small screen? Yes, you may use on overhead projector but even then that's not going to be a straightforward exercise. An alternative would be for the IT manager to go

around each employee and explain how the smartphone works and what the correct settings are, but that would take up a lot of time and wouldn't be practical. Another way is to use remote support techniques, which are a lot more cost-efficient."

3.4.3 The Intuwave proposition: m-Support

Intuwave has developed a software-based customer support product, which, it claims, makes it considerably easier and cheaper to diagnose and fix problems on the smartphone compared with the conventional help-desk approach. Called m-Support, the system allows the CSR (customer sales representative) to graphically view and control a smartphone remotely on an Internet-connected PC. The remote smartphone user could either be hooked up to the Internet via a GPRS or Bluetooth connection.

Although Intuwave had not yet announced any commercial contracts for m-Support by the end of 2003, it was trialling the system with mobile operators in the UK. It has also been active in providing live demonstrations of m-Support, one of which was attended by BWCS.

For the purposes of the demonstration to BWCS, Intuwave used a Nokia 3650 smartphone over a GPRS connection; the problem to be fixed was a faulty e-mail connection. To access the support service, the user first of all clicks on the phone's m-Support icon (which can be modified or branded to suit the mobile operator in a commercial implementation). Once the user clicks on the m-Support icon, the CSR immediately sees that in the form of a telephone number on his screen. The CSR then sends a text message requesting a password. Once that is verified, m-Support can be used. Network security for m-Support, which is web-enabled, is provided by SSL encryption.

"One compelling feature of the system," adds Wyatt, "is that the need to ever call the CSR, with the prospect of waiting 15 minutes or so on an IVR [interactive voice response system], can be removed. Once the smartphone user clicks on the support button and is registered on the system, the CSR can analyse the phone on the user's behalf and understand what the problems are before making any interaction with the customer."

m-Support is able to do this because it can access system and application information on the device. The CSR can see, for example, which model the smartphone is, how much memory it has left, as well as its GPRS APN (access point name) settings. It also has access to e-mail settings and, in recognition that this data application is one of the most popular among corporate and consumer customers, the m-Support software has applied a set of rules to those settings. In practical terms, that means that on occasions when e-mail isn't working on the smartphone, the m-Support software can alert the CSR on his PC screen if the current e-mail settings are the potential cause of the problem. The CSR can then alter the setting remotely and inform the smartphone user accordingly (m-Support has a

range of pre-prepared text messages built into the system, which the CSR can 'tab down' to access and send to the user's screen via dialogue boxes).

The reason why there is text-based contact between the CSR and the smartphone is that current GPRS current phones don't allow a simultaneous voice and data session. With 3G, that particular problem goes away. In the meantime, as in the past it is advisable that customers who do ring up their mobile operators regarding smartphone support do so on a device other than the smartphone itself. With the smartphone to the ear of the customer, it will be extremely difficult to check default settings at the same time!

With regard to e-mail problem resolution, Wyatt argues that m-Support goes a lot further than the conventional help desks of mobile operators in making sure that there is a resolution. Instead of just sending back different default settings to the smartphone, without being certain that this will fix the problem, m-Support can test whether e-mail (as well as other applications that the smartphone uses) is working or not and actually 'show' the customer how to operate the application. This is done by the CSR requesting remote control of the handset.

By doing this, the CSR can view the smartphone of the customer on his PC screen and remotely navigate his way around it to make sure that the problem in question is fixed. In doing so, he can also demonstrate to the smartphone user the procedures for accessing and sending e-mail as the customer can see the different scrolling steps that the CSR is going through to activate the service. This can be followed up by the CSR sending a quickly assembled 'tutorial' on how to access and use different applications directly to the smartphone. "Up until this product there has been no way of the CSR actually knowing whether changes made on the handset have had the desired effect," claims Wyatt.

Using Intuwave's assumptions about typical help-desk call times and costs in a traditional CSR environment – two calls per year per customer, 15 minutes each, at a cost of £2 per minute in fully-weighted staff costs – a mobile operator's annual support bill for 500,000 smartphone users would be £30 million. As Intuwave believes that m-Support can reduce the total number of minutes supporting these 'typical' smartphone-generated calls by 50 per cent, the mobile operator with 500,000 smartphone customers would save £15 million per year.

3.4.4 An outsourcing opportunity for mobile operators

Technically, there is no reason why m-Support should be restricted in its deployment to mobile operators. Device manufacturers, ISVs (independent software vendors), and enterprises could all conceivably offer m-Support themselves. This group of players would, however, need access to the operator-specific network settings but there are companies, such as Wireless Data Services (http://www.wdsglobal.com), that offer that type of service.

The reason why Intuwave is initially targeting mobile operators with m-Support is because it believes this route offers the best chance of quickly achieving large-scale adoption. That's not to say that the mobile operator couldn't host m-Support on behalf of the enterprise, which would provide a way for it to increase the 'loyalty' of its mobile VPN customers. If the enterprise customer moves away from the operator they lose the service.

In this outsourcing scenario, the mobile operator hosts all the server software but then provides the enterprise's IT department with access to m-Support (as a browser-based application, this is easily done). The enterprise can then support its own remote workers itself while not having to install, configure and maintain the software.

4 Mobile VPN Benefits

4.1 Overview

To maximise the attraction of a mobile VPN solution to enterprise customers, its benefits to the business must be made crystal clear. It is not sufficient to address only IT managers' concerns surrounding total cost of ownership, business continuity, security and usability of the service. The upside, too, needs to be demonstrated, particularly at a time when IT budgets continue to be constrained. Unless this is done, mobile VPNs will not take traction in the marketplace.

The effort to demonstrate these benefits should not focus exclusively on trying to articulate hard and quantifiable productivity gains, although this is understandably a key area of interest for CIOs and CEOs. 'Soft' benefits, such as increased job satisfaction (better working practices) and an improved company profile in the marketplace (the use of the latest wireless technology to access up-to-date information can impress customers) are also valid selling points.

The problem facing mobile operators (and their vendor and systems integrator partners) is *how* to demonstrate the advantages of adopting a mobile VPN solution. The task is made more difficult when enterprises may already consider mobile networks as unsuitable for data transmission and so might resist trialling a mobile VPN solution, even if it is based on a next-generation 3G network.

An IT manager from Dr Städtler, an IT consultancy and systems house based in Germany, reports that initially the company was reluctant to take part in a pilot trial of a mobile VPN over 3G, which was being run by Lucent. "Because of our experiences with mobile technologies in the past, we were somewhat sceptical about the pilot," he is quoted as saying in Lucent literature. "We expected a mobile technology slightly faster than others but still barely a usable one. Nevertheless we agreed to participate, partly to satisfy our own curiosity and partly because the pilot seemed to have been well organised."

Dr Städtler, along with four other companies in Germany (Rödl & Partner, SanData IT, DATEV and BRZ Deutschland Bauinformationstechnologie) took part in mobile VPN trials over 3G during 2003. Lucent reports that, on average, more than five hours per week per employee were saved during the pilot trials as business processes were able to be streamlined.

It is possible to extrapolate, from calculating how much time is saved, a productivity gain figure. If a Dr Städtler employee was earning US$100,000 per year and the time recovered represented 13 per cent of his or her total working hours, then, arguably, that is the equivalent of an 'extra' US$13,000 gained.

This type of methodology is usually applied to demonstrating the cost-efficiencies of mobile access to e-mail. It is the central pillar, for example, on which a return on investment (ROI) figure is built by RIM for its BlackBerry mobile e-mail solution (see http://www.blackberry.com).

In the absence of quantifiable data that is possible, say, with Field Force Automation (the average number of client visits made per day by the engineer is a quantifiable productivity measurement), such an approach can be a useful guide to illustrate productivity benefits. However, its accuracy will depend on how much of the downtime recovered by having access to e-mail on the move is converted into time spent on other work-related tasks.

While this is one way to demonstrate the benefits of mobile e-mail (and VPN) access to enterprises, it should be only one part of a wider strategy. This will include:

- the design of pilot trials using applications and business processes tailored specifically for the enterprise customer
- an emphasis on 'soft' benefits; greater job satisfaction for employees and increased customer satisfaction
- the internal deployment, wherever possible, of the proposed mobile VPN solution by mobile operators and strategic partners before advocating its use to enterprise customers. Ericsson's Mobile Extension service, for example, has more credibility in the marketplace through the vendor being a customer of its own product (Chapter 7)
- the highlighting, wherever possible, of possible new revenue streams (up-selling and cross-selling, for example). This will catch the attention of the CEO.

The focus of this chapter is on two applications that have the potential to stimulate mobile VPN adoption, provided the business benefits are clearly communicated and made relevant to the intended enterprise customer: Field Force Automation (FFA) and Sales Force Automation (SFA).

4.2 Field Force Automation

4.2.1 Overview

Organisations with large field forces face a number of challenges that threaten to undermine their operational efficiency and market competitiveness. These include:

- field workers having too much 'slack time' between jobs
- customers waiting beyond the appointment time of their service call

- a job being allocated to a field worker who doesn't have the necessary skills to carry out the task effectively
- the field worker having no easy access to up-to-date information on site, which extends the length of time spent on that job
- the dispatch manager allocating a job to a field worker who has to travel a long distance to reach the customer's site; he is unaware that a qualified worker for that job is available and nearer to the customer.

The net result for such an organisation, which suffers from some or all of these problems, is that it isn't getting a good return on its existing field force management investment. More significantly, customer care is likely to be poor as a consequence.

To examine how these issues can be addressed, BWCS looked at the FFA solution developed by Vidus, formerly known as a.p.solve.

4.2.2 Taskforce: the Vidus proposition

The Vidus remedy for field force management shortcomings outlined above is its 'Taskforce' software. Formerly a unit within BT, Vidus (or a.p.solve as it was known then) was spun out from the UK incumbent on 1 April 2003 and is VC-backed by NVP Brightstar, a joint venture created by BT Brightstar (an incubator fund of BTexact Technologies); Coller Capital (a UK-based global private equity secondary investment manager); and New Venture Partners (a US-based VC firm).

However, it was with BT that the Taskforce system was developed and honed. It also enabled Vidus, once it became independent and ready to target other organisations, to make a number of eye-catching claims about what Taskforce had achieved since its deployment by the UK telco in 1994. These include:

- a reduction in the number of BT's manual distribution centres (the location where the dispatch manager allocates tasks) from 100 to three
- a reduction in the number of BT field engineers from 30,000 to 22,000
- an average 30 per cent improvement in productivity
- savings in service costs of £175 million per year
- an expected increase in revenue of an estimated £75 million for BT's 2003/04 fiscal year (ended 31 March 2004).

4.2.3 How does Taskforce work?

The BT deployment of Taskforce is done via a standard GSM connection onto laptops with built-in mobile chips (there is no technical reason why Taskforce cannot work on GPRS and 3G). Although Taskforce can be web-enabled to allow SSL VPN access, BT has opted for an end-to-end VPN implementation. Vidus plays no role in the security aspect of Taskforce, leaving that entirely up to its customers. As well as using end-to-end VPN encryption technology, BT uses RSA SecurID authentication.

The core of Taskforce is Vidus' patented 'dynamic scheduling' system, which uses artificial intelligence to allocate tasks automatically to workers out in the field. In essence, it attempts to simulate how a despatch manager, based in the office, would act in terms of allocating tasks to the mobile workforce. However, as it is not prone to human error, it is a lot more efficient than a dispatch manager and can react immediately to unpredictable events (workers calling in sick or traffic accidents). It can also take into account jobs located in 'high risk' areas and allocate two engineers where necessary. Vidus claims that Taskforce has managed to automate 96 per cent of the tasks confronting the BT engineer out in the field.

The principle underlying the system is to weigh the cost of performing a task against the customer experience. For example, if there was a specific job to do at a customer's site, it could be that the nearest engineer would not have the necessary skills to do that job well. That would mean enlisting another engineer located further away, which would increase the cost of the job (more 'non-productive' travelling time and associated petrol costs). However, according to the parameters fed into it, Taskforce does not necessarily select the best-qualified engineer available regardless of his location in relation to the customer's whereabouts. Instead, it intelligently selects the 'optimum' employee in terms of calculating the costs incurred in doing that job and making sure the customer receives adequate service.

Following on from that, Vidus claims that organisations can then build additional parameters into Taskforce – such as a commitment on fixing problems within a fixed period of time – which then distinguishes level of service for, say, Platinum, Gold and Silver customers. In that way, Taskforce can enable organisations to deliver on more aggressive SLAs (Service Level Agreements).

4.2.4 New revenue streams

Although Taskforce started out as a way for BT to increase its operational efficiencies and improve its customer care, it has also developed into a means whereby the UK telco can tap into new revenue streams. For example, the system can automatically send messages to specially trained mobile workers, when working at a customer's site, of any up-selling opportunities. It can also notify the engineer if the work carried out at the

customer's site is covered by the original contract or not. If it isn't, then the engineer can invoice the customer accordingly. It is in these areas that BT expects to generate an extra £75 million in revenue for its 2003/04 fiscal year; between £25 million and £30 million of extra revenue was generated in this way by BT during its 2002/03 fiscal year, says Vidus.

Weaknesses of the system are by virtue of using wireless spectrum. BT engineers, for example, may have to be disconnected for long periods of time if working near a switch due to signal interference. Hospitals and petrol stations are other locations that may prevent the use of mobile connectivity.

4.2.5 The importance of customised solutions

The operational savings and productivity gains enjoyed by BT illustrate that high bandwidth speeds are not always required to justify the rollout of more 'advanced' mobile workforce applications. What is required – as we shall see from Vidus' marketing strategy to take Taskforce beyond BT – is an understanding of customers' different needs and concerns. Then, crucially, there needs to be an ability to respond appropriately.

Although it's a cliché, the message is nonetheless clear to all players wishing to leverage mobile VPN capabilities within the enterprise space – one size doesn't fit all.

Taskforce itself is initially targeted at telcos, utilities and cable companies but – sometime in the future – Vidus intends to market the system to any type of large-scale organisation that requires the management and synchronisation of a complex network of resources. Examples given by Vidus are the medical world (where the tasks of doctors, nurses and anaesthetists can be automatically synchronised where need be) and the construction industry (where different workers are required for different types of jobs).

While Vidus says the 'core' of Taskforce will remain the same for each industry, it will be modified to accommodate different customer demands. This has already been seen in the two deals Vidus has won since spinning out from BT in April 2003 – one with cable operator NTL in the UK and the other with energy utility, E.ON Hungaria (EHU), a member of the E.ON Group.

4.2.6 NTL: a cable company's FFA requirements

Taskforce went 'live' for NTL in September 2003 with the number of users in the hundreds. By the time the implementation is fully rolled out (mid-2004), Vidus anticipates that Taskforce will be automating tasks for 'several thousands' of NTL field engineers.

The NTL deal is a major milestone for Vidus as it's the first contract for the company outside BT. But in order to win the cable operator's

signature, Vidus had to be flexible in its approach; it couldn't simply replicate what it had done with the UK incumbent. "While BT was primarily interested in making operational cuts when it first deployed Taskforce, NTL's main driver is to improve customer experience," Stuart Potchinsky, Vidus' chief marketing officer, told BWCS. "Of course, NTL is still interested in making operational cuts but we had to demonstrate first and foremost how Taskforce could significantly improve levels of customer care."

A degree of customisation has also been required. A feature of Taskforce – in the BT context – is that field engineers can initiate a line test from their laptop and receive the results directly back almost immediately. For NTL, Taskforce has been modified to enable similar remote testing of STBs (set-top boxes) via the laptop.

To cut costs in the future and make the system easier to use for its field engineers, NTL has asked Vidus to reconfigure Taskforce to work on PDAs. "As its existing range of laptops are becoming obsolete, and because it sub-contracts a lot of its field force work, NTL wants a less expensive implementation and one that's very easy to use and specific to the job," explains Potchinsky. "We're working to meet NTL's requirements but there's always going to be a trade-off between cost [of the PDA] and the amount of information that can be used. Generally speaking, from the [potential] customers we've spoken to, they prefer laptops because of the greater amount of data that can be accessed."

4.2.7 EHU: an energy utility's FFA requirements

To win the contract with EHU – Hungary's gas and electricity utility – Vidus had to demonstrate that Taskforce could meet a range of regulatory requirements imposed on it by the government. From 1 January 2004, EHU has to provide two-hour appointment windows to its customers as well as reduce its prices. Vidus claims that it was the only contract bidder who could meet those stringent targets; EHU itself predicts that it can make 30 per cent productivity gains through Taskforce as well as reducing overall operational costs by five per cent. The utility did not, however, give any timescale as to when it expects to meet those targets.

The value of the EHU deal is worth £4 million to Vidus, the first phase of which covers 1,500 engineers (split into 768 crews). Going into pilot in December 2003, Taskforce is to be made available – 'eventually' – to 30,000 EHU field engineers.

"One of the big concerns of EHU was how to monitor individual engineers within the crew system," says Potchinsky. "Because of the low salaries in Hungary, it's not unheard of for drivers or other crew members to use the van to moonlight on other jobs while their fellow workers remain on site. With Taskforce, the supervisor can keep track of who is doing what and when. The system can also implement 'dynamic crews' –

that is, to change the skill set of the team to match a job's requirements. Each crew member can be given a specific task to do."

According to Potchinsky, 80-90 per cent of the Taskforce product will remain constant across different vertical industries; the remainder will need to be modified to offer bespoke solutions.

4.2.8 SI partnerships and tailored messages

As Taskforce requires change management – business processes are completely different compared to the paper-based approach of field force management – Vidus partners with the likes of IBM, Accenture, Amdocs Clarify and Cap Gemini to help get the business process message across to customers.

Without offering assistance to organisations on how to implement the necessary business process changes, Vidus acknowledges that the full operational and productivity benefits of Taskforce won't be realised.

Cooperation among the different players in the mobile VPN value chain is therefore necessary if a coherent, convincing argument for increased mobilisation of the workforce is to be presented to the enterprise.

The exact roles of each player will have to be defined in order to maximise the impact of the message. "It's rare for a systems integrator to take the lead in marketing Taskforce when we're sitting down with potential customers," reveals Potchinsky. "They [the customers] want to know the ins and outs of how the system works and we're the ones that can tell them."

The nature of that message will also need to change according to the listener. While we can say, generally speaking, that a CIO is primarily concerned about increased operational efficiencies, productivity, security and mobile worker support management, the CEO (while still interested in operational efficiencies) is also keen to know about new revenue streams. Field workers themselves also have to 'buy in' to the FFA system if the full benefits are to be realised. Less time-consuming bureaucracy, more productivity and greater job satisfaction will be the key buttons to press here.

The term 'operational efficiencies' also needs to be used carefully, warns Potchinsky. "If you go to an organisation and say you're going to implement something that requires a 30 per cent reduction in the workforce, that message is going to run into trouble in some countries like France [active trade unions]. And anyway, that's not the main message of Taskforce. The three most important elements are improved operational efficiency in terms of productivity per worker; greater revenue; and improved customer service. The organisation may then conclude they can reduce the size of their field workforce after implementing the system, but that is a decision for them."

Potchinsky notes that the priorities of corporate customers have changed in recent months. No longer is cost reduction the highest item on the agenda; new revenue streams and better customer care are the two main objectives grabbing their attention now. “Cost-reduction is taken as a given [for new FFA implementations],” he says. “The challenge is to come up with a proposition that can help customers grow their business.”

4.3 Sales Force Automation

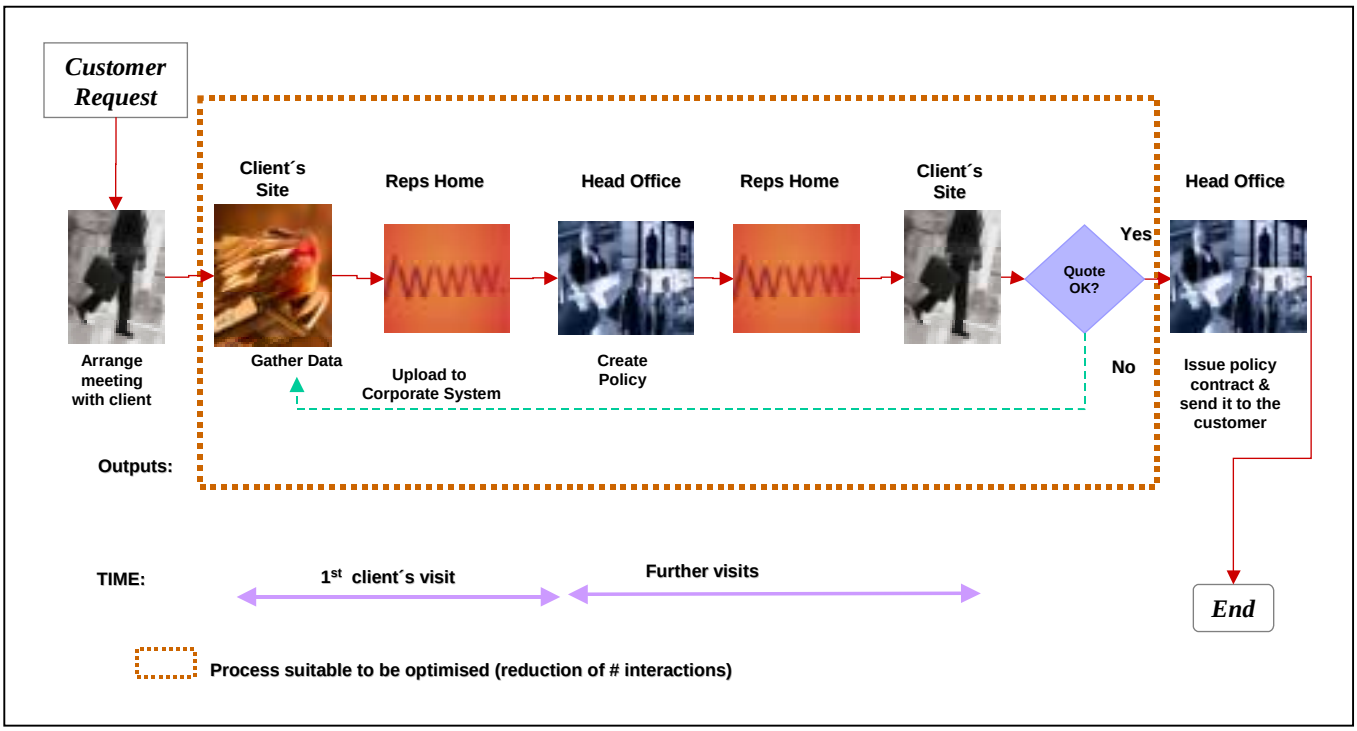
4.3.1 Lucent case study: Spanish insurance company

To illustrate the benefits of a mobile VPN solution in terms of increasing the efficiencies of an enterprise’s sales force, Lucent has conducted numerous pilot trials with potential enterprise customers. One of those trials was with a Spanish insurance company, the name of which Lucent is not allowed to disclose.

Based on 3G, the Lucent mobile VPN pilot revealed a number of benefits that can be had with fast and secure connectivity to the head office (provided that the company’s back-end systems can work in tandem, and automatically, with information requests made by the sales worker).

As can be seen in Figure 4.1, the sales worker, prior to using a mobile VPN based on 3G, could be involved in an elongated sales process with the potential for numerous client visits required. This is because, prior to 3G, the sales worker is unable to download quickly up-to-date information from head office when at the client’s site; nor is he able to initiate an automatic policy creation process. Instead, the sales worker has to return home to upload to the corporate system and then return to the client’s site with, hopefully, an acceptable policy to the customer. This process takes time and resources and can clearly impact on an organisation’s cost-effectiveness and competitiveness.

Figure 4.1 Typical sales process for sales rep (pre 3G)



Source: Lucent Technologies (Offer Management)

The introduction of 3G, combined with the ability to initiate an automatic policy creation, manages to streamline those processes, as can be seen in Figure 4.2.

Figure 4.2 Typical sales process for sales rep (post 3G)

Source: Lucent Technologies (Offer Management)

But it is not only the prospect of one client visit that Lucent highlights as a major benefit of this mobile VPN implementation. Other benefits are:

- Increased potential for up-selling and cross-selling as sales workers are notified, when at the client's site, of other products that could be relevant to the customer based on parameters fed by the sales worker into the system.
- Improved reporting metrics through clearer visibility of quote/policies ratio. In the example of the Spanish insurance company, sales workers, pre 3G, typically made 'offline' quotes that weren't recorded if not accepted. Within the mobile VPN implementation, all quotes are recorded and fed into the system to create the policy (which the customer then accepts or rejects).
- Increased employee job satisfaction through a reduction in working hours and no need to work at home due to real-time access to applications. There is also an increased salary opportunity due to improved conversion rates, says Lucent.
- Improvement of the company image within the market due to being seen as a 'leader' in technology. Arguably, this will also help to attract best sales staff due to the perception of the company having 'best-in-class' systems and processes.

To stimulate mobile VPN adoption, mobile operators and their strategic partners need to emphasise the business process benefits – as Vidus and Lucent are doing – by putting the technology into an application context.

5 Mobile Operator Strategies

5.1 mmO2

5.1.1 Company background

mmO2 has wholly-owned mobile operations in the UK, Germany and Ireland. Formerly known as BT Wireless, it was spun out from the UK's national incumbent in November 2001 and is listed on the FTSE 100.

In June 2003, mmO2 completed the sale of its loss-making mobile operation in the Netherlands (which included a 3G licence) to Greenfield Capital Partners, an independent private equity and corporate finance group. The deal was worth €25 million in cash to mmO2.

As part of its BT heritage, mmO2 has 3G licences in Germany and the UK. In August 2002, mmO2 announced that O2 Ireland had successfully bid for a 3G licence, costing €114.1 million, to be phased over 15 years (€44.4 million paid upfront).

mmO2 expects to launch commercial 3G services by the second half of 2004 in each of its territories. Since December 2001, via Manx Telecom (a wholly-owned subsidiary of mmO2), the company has been trialling 3G services on the Isle of Man. mmO2 has been experimenting with various services and price packages for both the consumer and business market segments on the Isle of Man in preparation for 3G launch in the UK, Germany and Ireland.

During the three months ended 31 December 2003, mmO2 added 855,000 customers to take its total subscriber base to 20.07 million. O2 UK accounts for 65 per cent of that number, followed by O2 Germany (27.8 per cent) and O2 Ireland (6.8 per cent). Manx Telecom had 61,000 subscribers by the end of 2003.

In October 2003, mmO2 signed up to an alliance of other Tier 2 operators in Europe to provide 'seamless, enhanced voice and data solutions for businesses and customers' across Europe. Called 'Starmap', the alliance's founding members, along with mmO2, are: Amena (Spain), One (Austria), Pannon GSM (Hungary), sunrise (Switzerland), Telenor Mobile (Norway) and Wind (Italy). In April 2004, the Starmap mobile alliance announced that Sonofon from Denmark had joined the group.

5.1.2 Financial performance

An increasing customer base, combined with higher ARPU and improved EBITDA margins in each of its territories, has strengthened mmO2 during the first half of it its 2003/04 fiscal year (ended 30 September 2003). This is particularly apparent for its operations in Germany where it achieved an

EBIDTA margin of 16.8 per cent in the first six months of its 2003/04 financial year. For the same period the previous year, O2 Germany generated EBITDA of €2 million on total service revenue of €693 million.

Despite the improvement in Germany, mmO2 still runs far more operationally efficient mobile networks in the UK and Ireland, with EBITDA margins of 29.2 per cent and 39.6 per cent respectively for the first half of 2003/04.

Across the board, mmO2 has benefited from cost cuts, increased net additions of contract customers, and the sale of its operations in the Netherlands. It posted a pre-tax profit of £26 million for the first six months of 2003/04 (compared with a pre-tax loss of £259 million for the same period the year before) on revenues of £2.68 billion (£2.214 billion during first half 2002/03). By the end of September 2003, mmO2 had a total subscriber base of 19.2 million subscribers.

5.1.3 Mobile data performance

In February 2004, mmO2 released key performance indicators for the three-month per period ended 31 December 2003. The figures reveal a continuing an upwards trend in both ARPU and data as a percentage of revenue and confirm mmO2's status as having one of the largest portions of non-voice revenue among Europe's mobile operators.

mmO2 has set itself the target of mobile data revenue accounting for 25 per cent of total sales by the last quarter of its 2004/05 fiscal year.

Table 5.1 Data as a percentage of service revenues

3 months ended	31 Dec 2002 %	31 March 2003 %	30 June 2003 %	30 Sep 2003 %	31 Dec 2003 %
O2 UK	17.4	19.4	18.3	19.4	21.2
O2 Germany	19.7	21.0	18.2	19.1	19.8
O2 Ireland	15.7	17.4	16.1	18.4	21.1
O2 Group	17.8	19.6	18.1	19.2	20.9

Source: mmO2

5.1.4 Threats to voice revenue underline importance of data

The strategic value of growing date revenue has been heightened for mmO2 – and other mobile operators in the UK – by mobile termination cuts and increased voice competition.

Mobile termination rate cuts

In July 2003, a ruling by the UK's Competition Commission came into force whereby all four mobile network operators in the UK (O2 UK, T-Mobile, Orange and Vodafone) had to cut their mobile termination fees by 15 per cent below inflation. (Mobile termination fees are the charges made by mobile operators to other operators – both mobile and fixed – for terminating calls originating on their networks.)

Broadly speaking, the reduction in revenue among the UK's mobile operators terminating each other's traffic will be offset through having to pay each other less. However, each will feel a bottom line impact through 'lost' revenue from the fixed-line operators. mmO2 is particularly exposed as over 65 per cent of its revenue comes from the UK.

According to the original ruling by the Competition Commission, the formula of 'inflation minus 15 per cent' was to be applied each year to the mobile termination rate through to 2006. However, Ofcom, the UK's regulatory body governing telecoms and media, recommended in December 2003 that the second mobile termination price cut should be postponed and rolled into the third price cut (due in mmO2's 2004/05 financial year). mmO2 reckons that the breathing space will enable it to invest in growing the business – 3G rollout and mobile data services – which will offset mobile termination revenue decline, which the company estimates at £50 million per year,

Peter Erskine, CEO, said in a statement in February 2004: "This [the Ofcom recommendation] will increase service revenue in the current financial year, and reduce service revenue in 2004/05, relative to previous expectations. However the overall impact on O2 UK's service revenue over the two-year period is not expected to be material. The additional revenue in the current financial year is expected to be re-invested to enable the business to continue to drive growth."

New entrant: H3G UK

In March 2003, H3G UK became the first commercial 3G operator in the UK. Majority-owned by Hutchison Whampoa (the Hong-Kong based property, ports and telecom conglomerate) '3' – the service brand name of H3G UK – has struggled to make an impact. To try and boost sales, H3G reduced its voice per-minute tariffs in June 2003 to undercut the UK's mobile network operators' charges by as much 25 per cent.

While this seems aggressive, and certainly can't be ignored by O2 UK, the cheaper per minute rates only apply to purchasers of bulk packages, which represents a small portion of the market. Although this minimises the impact on O2's voice revenue, the prospect of H3G UK making further voice per minute price cuts to increase market share can't be ruled out.

5.1.5 Mobile VPN strategy

mmO2's strategy for winning VPN data traffic onto its network can be split into five, broad areas:

1) Demonstrate the compatibility of its mobile network with enterprise customers' existing VPN infrastructure – supplied by the major vendors – to support end-to-end encryption using the following tunnelling protocols: IPSec, L2TP and Microsoft's PPTP.

2) Promote the 'push' e-mail service and other mobile data services enabled by the RIM BlackBerry solution. Since May 2003, as a distributor of BlackBerry 3.6 server version, mmO2 has been able to offer BlackBerry users mobile Internet browsing, access to Interned-based e-mail and Web-based servers, which can provided simplified versions of CRM applications. In May 2004, mmO2 reported that 55,000 BlackBerry devices were in use across its business customer base. The RIM Blackberry solution can support both Microsoft Exchange and Lotus Notes.

3) Promote its customised and voice-enabled PDA, the Xda II, which is based on Microsoft's Pocket PC software. Although the Xda II can be configured to offer full connectivity to corporate LAN applications, mmO2 offers another option to Xda2 customers in the UK and Ireland. Called the Extended Office, this solution – which supports both Microsoft Exchange and Lotus Notes – is targeted at customers requiring access to their inbox, calendar and contact information. O2 UK and O2 Ireland offer Extended Office as a managed 'end-to-end' solution to the enterprise in that they can provide and manage all the elements required, including the server and its associated software. But enterprises, should they wish, have the option to manage the solution for themselves.

One advantage of the Extended Office solution, although it uses end-to-end encryption from the corporate LAN through to the device, is that it can take advantage of software compression. This is because the Extended Office, based on the corporate LAN, compresses information before it is encrypted and, according to O2, can achieve a compression ratio of up to 5:1. This is not insignificant for the IT manager when data is charged on a per megabyte basis. Instead of paying for 5MB, for example, the enterprise would pay for 1MB if a 5:1 compression ratio was achieved.

By May 2004, mmO2 told BWCS that it had sold a combined total of Xda I and Xda II handsets of at least 100,000. The mobile operator does not disclose how many of those Xda users are Extended Office customers.

Laptop and PDA users (other than the Xda II) can also use Extended Office.

4) Offer WiFi connectivity as a complimentary service to its GPRS and, when they become available, 3G networks. In partnership with a software developer, which mmO2 has signed a confidentiality agreement, the mobile operator has developed its Connection Manager software. Working in tandem with VPN clients, Connection Manager gives laptop users a list of all wireless access technologies available. In Ireland and Germany, this includes mmO2's own WiFi hotspot network, located in airports and hotels.

In the UK, where O2 does not have any hotspots, it plans to wholesale WiFi capacity from other providers and launch service in July 2004. O2 UK also has a partnership with Excilan, a Luxembourg-based company, which provides an authentication and payment platform. This will allow O2 to provide one bill for both GPRS/3G and WiFi data traffic. Unified billing is also possible in Ireland, where O2 has its own WiFi network, and in Germany (where O2 has a roaming agreement with T-Mobile's WiFi network).

5) Provide data bundles for individuals and groups in order to simplify data pricing. mmO2 also gives the option of rolling over unused data from one month to the next (see Chapter 3). In its 2004/05 fiscal year, O2 UK says it plans to offer service level agreements on GPRS connections, although the mobile operator declines to give any indication – pre-launch – as to how they will be charged.

mmO2's mobile VPN portfolio revolves around its Mobile Web VPN service (see below), which supports end-to-end encryption from the end-user device through to the corporate gateway. This was developed in response to enterprise customers who wanted to provide user access to the corporate LAN but without access to the Internet.

For customers looking to create their own private data networks, rather than use the public Internet, mmO2 gives enterprises the option of a dedicated leased line between the corporate LAN and its GPRS network. This is supported either by its Datalink service (data-only) or its Link 60 service (voice and data). Link 60 can support 60 voice lines.

To attract mobile VPN customers, mmO2 places great importance on being able to demonstrate to IT departments that Mobile Web is compatible with existing LAN-based VPN infrastructure supplied by the major vendors. Rather than trying to present itself to business customers as a player providing turnkey IT services, mmO2's emphasis is on providing mobile network connectivity.

"We took the view that trying to deliver IT-related infrastructure wasn't the right focus for us," David Keegan, mmO2's business product manager, told BWCS. "It would have meant additional investment in our

channel and service capabilities to compete in an area that is already very competitive. It wouldn't have been a good margin business for us."

As it is, mmO2 works with a number of Tier 2 system integrator partners to target business customers. These include Total Telecom, Lan2Lan and Interchange. "It's more natural for business customers to buy VPN components and management services from systems integrators and vendors rather than mobile operators," adds Keegan.

Even so, mmO2 does have a 'Professional Services' division, which is available to enterprises to assist in the integration of a mobile solution into the workplace should they require it. This team, according to mmO2, typically provides a consulting service to ensure the successful deployment of a mobile solution for specific customer applications.

5.1.6 Mobile VPN portfolio

Mobile Web

Mobile Web was commercially launched by mmO2 across its territories in April 2002. Mobile Web provides fast mobile access to the Internet and Outlook-based email to customers using a Xda II, data card or a wireless-enabled device (such as a PDA or smartphone).

Using a public APN, Mobile Web provides plain Internet access plus corporate VPN connectivity across O2's GPRS network; it is enabled through the installation of the Mobile Web client onto the end-user's device to work in tandem with the existing VPN client. For Xda users, mmO2 recommends that the pre-installed Microsoft PPTP client should be used for Mobile Web access on the grounds of better performance and easier set-up characteristics. As 3G becomes available, mmO2 plans to use the Mobile Web service to offer faster plain Internet access to its customers.

As Mobile Web uses private IP addresses, business customers' existing VPN infrastructure – if using IPSec tunnelling – need to support NAT Traversal. mmO2 says it has tested successfully VPN products from Nortel, Cisco, Checkpoint, Nokia and Sonic to work in conjunction with its Mobile Web service. It does not work with all VPN solutions, though. WatchGuard equipment is not compatible. By May 2004, mmO2 had still to formally test the compatibility of Mobile Web with Lucent's VPN equipment, although Keegan says that it is Mobile Web compatible.

Mobile Web VPN

In July 2003, mmO2 introduced its Mobile Web VPN service in the UK and Germany. The mobile operator says this was in response to the requirement for enterprise customers to offer Internet access through LAN-based Internet-facing gateways.

Unlike Mobile Web, the Mobile Web VPN service connects *all* end-user data requests directly to the corporate LAN. If the end-user has been given clearance by the IT manager to access the Internet, then he or she is able to do so. The IT manager will have visibility on which Web sites have been visited.

Another benefit for IT managers is that because Mobile Web VPN uses public IP addresses, it is compatible with all VPN products out in the marketplace – NAT Traversal is not required.

mmO2 does not disclose how many customers it has for its Mobile Web and Mobile Web VPN services.

5.2 T-Mobile International

5.2.1 Background

T-Mobile International represents the mobile interests of Deutsche Telekom, the fixed-line national incumbent in Germany. It has wholly-owned mobile operations in the US, Germany, the UK, Austria and the Netherlands, plus a majority stake in a Czech Republic mobile operator. Each of these operations is branded T-Mobile.

At the end of 2003, T-Mobile International's customer base – across its wholly-owned and majority-owned subsidiaries – totalled 61 million, a 7.1 million increase compared with the end of 2002. T-Mobile Deutschland contributes the largest portion of that number with 26.3 million subscribers followed by T-Mobile UK (13.6 million, which includes subscribers to Virgin Mobile, a mobile virtual network operator that leases capacity on T-Mobile UK's mobile network), and T-Mobile USA (13.1 million).

T-Mobile International has a presence in 18 countries once its minority shareholdings in Central and Eastern Europe and Asia are included. Its subscriber base across all its mobile operations in which it has an equity holding numbered 66.2 million by the end of 2003.

Like many other mobile operators, T-Mobile is focused on increasing the proportion of contract customers to its network to increase ARPU (average revenue per user), and its marketing efforts over the Christmas period appear to have paid some dividends. In 4Q 2003, T-Mobile Deutschland increased its customer base by 705,000; of these 441,000 were new contract customers. In the UK, T-Mobile added 161,000 contract customers in 4Q 2003. In the US, 89 per cent of T-Mobile USA's customer base were post-paid by the end of 2003.

For its fiscal year ended 31 December 2003, T-Mobile International posted revenue of €22.8 billion with an EBITDA margin of 29.3 percent.

This compared with revenue of €19.7 billion and an EBITDA margin of 25.4 per cent for 2002.

T-Mobile does not give a breakout of its mobile data revenue between consumer and enterprise customers. However, the company highlights 'T-zones' – its consumer-orientated mobile portals from which to download services (such as ringtones and 'caller tunes') – to explain its modest rise in mobile data revenue. Non-voice ARPU (including SMS) in its European markets rose to an average of 16 per cent during 2003 compared to 14 per cent during 2002.

In June 2003, T-Mobile – along with Telefónica Moviles and Telecom Italia Mobile – announced an alliance to provide a 'unified offering' to both their businesses and consumer customers. The alliance was joined by Orange shortly afterwards and, in August 2003, the four members announced their first products: pre-paid roaming and the use of short codes to access voicemail and customer service in each other's territories. The alliance says it is working on developing an 'enhanced service' to its corporate customers, although what this means exactly had yet to emerge at the time of this report's publication.

5.2.2 3G presence

T-Mobile International has 3G licences in six European countries (Germany, the UK, Austria, the Netherlands, Poland and the Czech Republic). It has paid a total of €15 billion for UMTS spectrum.

T-Mobile UK declared that its 3G network had gone 'live' in February 2004 while the 3G networks of T-Mobile Austria and T-Mobile Deutschland were switched on in December 2003 and January 2004 respectively. At the time of writing (February 2004) T-Mobile had yet to announce its 3G rollout timetable for the Netherlands, Poland and Czech Republic.

T-Mobile is cooperating with O2 Germany and O2 UK to share 3G network infrastructure costs.

5.2.3 Mobile data strategy for enterprise

Combining 2.5G/3G with WiFi

Of the 3G licence holders in Europe, T-Mobile International has been the most aggressive in embracing WLANs. It takes the view that to maximise mobile data growth, it needs to offer customers the fastest connection wherever possible. In that way – according to T-Mobile – mobile data users are more likely to access services more frequently than if they were restricted only to cellular access. "3G is important and will be our future bread and butter," declared Rene Obermann, CEO of T-Mobile International, at the 3GSM Congress held in Cannes, February 2004. "But anyone who offers 3G alone is making a big mistake."

The company's push on WLAN hotspot rollout has so far centred on the US, via T-Mobile USA. The strategy there has also been driven by the need to raise the profile of the T-Mobile USA brand name, where it is relatively unknown (T-Mobile USA comprises the GSM networks formerly known as VoiceStream and PowerTel). Beginning hotspot rollout in August 2002, T-Mobile USA had 4,100 hotspots by February 2004, 3,000 of which were split between Starbucks and Borders Bookstores.

To increase traffic over its hotspot network, T-Mobile USA signed a distribution agreement with iPass, a US-based virtual network operator that has 20,000 access points around the world. Customers of iPass, using the iPassConnect client software, can now roam onto the T-Mobile USA hotspot network.

T-Mobile USA does not disclose the number of WLAN subscribers it has, nor their ARPU. It does, however, provide one voice and data bill for its WLAN/GSM customers. T-Mobile USA is aiming to operate 6,000 hotspots in the US by the end of 2004.

In Europe, T-Mobile International was operating 700 hotspots by February 2004; distribution deals include Starbucks and the Starwood Hotel chain. By the end of 2004, T-Mobile International intends to have increased its own European WLAN presence to 4,000 hotspots.

In March 2004, after a period of trials with 'selected customers', T-Mobile International launched 3G services – targeted at laptop users in the SME and corporate markets – in the UK, Germany and Austria. The plug-in data card, branded the Multimedia Net Card, allow seamless roaming between 2.5G and 3G networks. T-Mobile International says that data cards capable of supporting 2.5G, 3G, and WiFi networks will be available before the end of 2004. In the meantime, T-Mobile International's 2.5G/3G subscribers wishing to access T-Mobile hotspots need to have a laptop that is already WiFi-enabled.

Recognising that business users would prefer a WiFi connection to a 2.5G or 3G link given the choice, T-Mobile International is offering its 'HotSpot Locator' software – free of charge – via the T-Mobile website or T-Mobile HotSpot portal. The software is able to match the location of the user with the nearest T-Mobile hotspot and provide directions on how to get there through the use of digital mapping. By the end of 2004, T-Mobile International says it will have software available to allow end-users to 'scan the spectrum' automatically for the optimum connection link.

Promoting the case for mobile data adoption

To stimulate mobile data usage across 2G, 3G and WLAN networks in the future, T-Mobile has partnered with Cisco (WLAN infrastructure) and

Intel (laptops) to pilot a 'seamless' access service on university campus sites across Europe (the service will also be available to students and university staff, at special discounted rates, off-campus).

The thinking behind the scheme is to get university students used to 'broadband mobility' and, once they see its benefits, they will continue to use it (and evangelise it) throughout their working lives. While this project is certainly admirable for its long-term thinking – 100 university campuses are targeted for inclusion in the project, starting with Frankfurt University in April 2004 – it does highlight again how embryonic the mobile/wireless data market is among businesses.

The T-Mobile HotSpot pilot service for universities can also be used by visitors to the campus. T-Mobile, along with its partners, is aiming to demonstrate that it is possible for the same WLAN infrastructure to be used for both private and public use. By doing so, it is actively encouraging mobile data traffic away from the cellular network within the enterprise LAN. But that doesn't matter for T-Mobile so long as it can do two things:

- collect WLAN data revenue; and
- demonstrate increased productivity for businesses who offer on-site high-speed wireless connectivity to either their partners or customers.

T-Mobile also hopes that WLAN users will become sufficiently enthusiastic about the convenience and benefits of wireless connectivity that they will continue to use their laptops when in the vicinity of 2.5G and 3G networks. By the same token, T-Mobile recognises that a major barrier to mobile VPN adoption is that many applications residing on the corporate LAN are not easily accessible by handheld devices.

To demonstrate the business case for 3G adoption within the enterprise, T-Mobile Deutschland conducted a year-long trial throughout 2003 with five companies from the Nuremberg area – Rödl & Partner, SanData IT group, DATEV, BRZ Deutschland Bauinformationstechnologie, and Dr Städtler. According to the results of the trial, which involved laptop users having access to T-Mobile Deutschland's UMTS network via data cards (developed by Lucent in conjunction with Novatel Wireless), an average of five working hours per week per employee were saved. By having high-speed access to corporate networks when 'on the road', field and sales workers were found to benefit in particular as they could carry out tasks that previously required them to return to the office.

Data tariffs

In the UK, T-Mobile has launched a special introductory 'all-you-can-eat' package for corporates and SMEs using its 3G/GPRS data card within the UK (it is not applicable for roaming onto other T-Mobile networks).

For £199 plus a monthly fee of £70, the remote worker gets the following:

- T-Mobile Communications Centre software (a 'simple, 5-step installation')
- Multimedia Net Card for GPRS/3G access (a plug-in card for laptops)
- 'easy-to-follow' user manual
- unlimited data access regardless of the access technology (2.5G, 3G or WiFi).

In March 2004, T-Mobile UK and T-Mobile International also unveiled time-based data tariffs to complement their volume-based packages. This should give IT managers a means by which to predict and control more accurately their monthly mobile/wireless data bill (if they believe end-users will be disciplined enough to restrict time usage). With the 'per megabyte' model, which has been traditionally used by mobile operators, IT managers have needed to rely on employees exercising restraint on the amount of data they download.

T-Mobile Deutschland's 'Time 600' tariff package (effective from 1 May 2004), allows unlimited data access for ten hours at a charge of €35 per month. Like T-Mobile UK, the data can be accessed over 2.5G, 3G or WiFi networks. If users go beyond their ten hour limit, they are charged €1.30 for every extra ten minutes. The graphical user interface on the laptop displays how long the service has been used.

The aim of T-Mobile International is to have consistent mobile data pricing in each of its territories for roaming users, although no time frame has yet been set for achieving that goal. However, these 'consistent' prices will differ depending on which country the international traveller originates from. Users from Poland, for example – to reflect the country's lower GDP – will be charged cheaper data rates for access at home and abroad than, say, those who subscribe to T-Mobile Deutschland.

5.2.4 Mobile VPN strategy

In Germany, T-Mobile Deutschland distinguishes itself in the mobile VPN marketplace by offering a solution that does not utilise the public Internet. By avoiding the Internet and using private APNs, T-Mobile argues that the service – known as Mobile IP VPN – can offer greater levels of security to enterprise customers than is possible with Internet-based solutions.

Moreover, by giving the option of not using dedicated leased lines between the mobile network and the corporate gateway (backhaul is supplied by ATM or frame relay permanent virtual circuits running over Deutsche Telekom's fixed network), T-Mobile further argues that the

appeal of the service is not restricted to large enterprises with large IT budgets.

Mobile IP VPN is a network-based service in the sense that T-Mobile Deutschland, in partnership with T-Systems and T-Com (other members of the Deutsche Telekom Group), is responsible for setting up a secure link between the GGSN and the corporate gateway. Depending on who has the closest contact with the enterprise for supplying its existing services, T-Com, T-Systems or T-Mobile Deutschland will play the lead role in canvassing the Mobile IP VPN product. T-Com's strengths are providing fixed-network infrastructure to small- to medium-sized enterprises, while T-Systems is strong in the provision of managed ICT solutions to large enterprises. T-Mobile Deutschland says that partnerships with other fixed-line VPN providers are planned but it had to make any specific announcements by March 2004.

Since the network architecture of Mobile IP VPN comprises a 'split tunnel' – that is, traffic over the PVCs coming from the corporate gateway has to be de-encrypted before being reformatted for GPRS/UMTS transmission – T-Mobile can offer network-based mobile optimisation services. T-Mobile Deutschland, however, does not offer Web-based portals that integrate mobile VPN access capability and neither does it have immediate plans to do so.

Customers of the Mobile IP VPN product that don't use end-to-end IPSec encryption can experience the full data throughput of GPRS. T-Mobile does report, however, that some of its Mobile IP VPN customers have requested an additional end-to-end IPSec tunnel – running over either the frame or ATM PVCs – which it can provide.

The Mobile IP VPN service is targeted at both large and medium-sized organisations in Germany but not multinational corporations (MNCs); the service is currently only available across Deutsche Telekom's domestic fixed-line data networks. Mobile IP VPN customers include Canon Germany, ADAC, ABX Logistics and LVM.

T-Mobile, through its strategic alliance with Telefonica Mobile, Orange and TIM, may extend the service internationally but, again, it had yet to make any firm announcements on that by May 2004. It is not yet clear whether the international VPN solutions enabled by this strategic alliance will include a non-Internet option for T-Mobile Deutschland's existing Mobile IP VPN customers.

Additional mobile data solutions offered by T-Mobile Deutschland to business customers include:

- Hosted authentication services (DHCP/RADIUS), in partnership with T-Com and T-Systems, for Mobile IP VPN customers.

- Mobile e-mail and data services, based on the RIM Blackberry solution (launched June 2002).
- Mobile Office Optimiser, located behind the corporate firewall, designed to accelerate MS Outlook performance over GPRS (launched August 2002);
- Plain Internet access (tariffs charged at the same rate as corporate LAN access)
- T-Mobile MDA (mobile digital assistant), a customised PDA for T-Mobile International based on Microsoft's Pocket PC software. T-Mobile MD II, launched in August 2003, can deal with attachments in standard formats, such as MS Word and Excel. It also has a tri-band facility making roaming easier between Europe and the US. In March 2004, T-Mobile International announced that it would offer Blackberry support for MDA II, Sony Ericsson P900 and Nokia 6820 to its customers in Europe.
- Business Voice VPN: enables office staff to call colleagues in the field via a single PBX. A numbering plan using short codes, perhaps based on existing extension numbers, can be used.

Outside Germany, where T-Mobile doesn't have recourse to Deutsche Telekom's data network, Internet-based mobile VPN solutions are used. T-Mobile UK, for example, offers its 'Office Link' service, which is an end-to-end IPSec encryption service using the GPRS network plus either the Internet or leased lines to connect back to the corporate network.

5.3 Vodafone

5.3.1 Company background

Vodafone is the largest mobile operator in the world in terms of footprint and subscriber base. It has equity interests in 26 countries and partner networks in a further 13. By the end of 2003, Vodafone's proportionate customer base (in relation to its shareholdings) stood at 130.4 million.

In the key markets of Western Europe, with the notable exception of France, Vodafone has either wholly-owned or majority-owned mobile operations. Vodafone only owns 43.9 % in Cegetel SFR, France's second largest mobile operator behind Orange, with Franco-American media conglomerate, Vivendi, holding the remaining equity.

Extending the Vodafone brand name to the US has also proven elusive. The mobile operator does have a 45 per stake in Verizon Wireless but Vodafone, led by CEO Arun Sarin, gave the impression that this was not enough to match its global ambitions when it entered the auction for AT&T Wireless on 9 February 2004. Nine days later, Vodafone withdrew

from the auction, claiming the price had risen too high and was no longer in the shareholders' interest to pursue.

Beyond Europe and the US, Vodafone has interests in Japan via Vodafone K.K. (formerly known as J-Phone), Egypt, South Africa, Australia and New Zealand and China.

5.3.2 Mobile data strategy

Overview

Due to what it claimed as higher-than-expected voice revenue, Vodafone adjusted its original mobile data target of 25 per cent of total service revenue down to 20 per cent (for 2005) in 2002. For 2003, mobile data revenue accounted for 15.9 per cent of its service revenues (13.9 per cent for 2002).

Consumers

Whether or not Vodafone achieves or comes near its revised 20 per cent target will depend largely on how well its consumer data service fares – Vodafone live!

Vodafone live!, which was launched in October 2002, offers end-users the ability to navigate – via a colour-display portal – a range of services other than SMS. These include e-mail, instant messaging, picture messaging and previously downloaded applications and ringtones. By the end of 2003, the service had attracted 4.5 million subscribers. The mobile operator says that Vodafone live! users, on average, generate 7% greater ARPU than standard GPRS users.

In May 2004, Vodafone announced the commercial availability of 'Vodafone live!' over 3G networks in Germany and Portugal. The service, to be known as 'Vodafone live! with 3G', will initially be available on the Samsung Z105 handset to be followed shortly afterwards by the Sony Ericsson Z1010 handset. Other countries will have access to 'Vodafone live! with 3G' in the 'coming months', said Vodafone at the time of the May 2004 announcement, when a wider range of 3G handsets will be available.

Vodafone's UMTS networks had between 25-30 per cent population coverage across its national 3G licence areas in Europe by March 2004.

Enterprises

To lend weight to its pitch to business customers, Vodafone has teamed up with a variety of high-profile systems integrators and software vendors. Major announcements include:

November 2002: Vodafone announces an agreement with major computer suppliers – Dell, Fujitsu-Siemens, HP, IBM, Psion Teklogic and Toshiba

– to offer business customers an extensive range of 'Connected by Vodafone' mobile computing devices (notebooks, PDAs, Table PCs) with in-built SIM-based connection to Vodafone's GPRS data network.

February 2003: Vodafone teams up with HP and Microsoft to put together the 'Outlook Anywhere' package. Aimed at SMEs, Outlook Anywhere comprises the iPAQ Pocket PC (paired to a Bluetooth-enabled Sony Ericsson T68i mobile phone) and the Microsoft Mobile Information Server (MMIS) software running on an HP Proliant server, which, in turn, allows access to Microsoft's Exchange 2000 server. The solution provides secure synchronisation to e-mail, calendar, contacts and tasks.

March 2003: Vodafone, SAP and HP announce a letter of intent to market a suite of mobile capabilities designed to increase the workforce productivity of large enterprises in the EMEA region. The idea is to pool together Vodafone's business connectivity solutions with mySAP business solutions and HP's servers. The aim is to offer business customers the opportunity to quickly mobilise their field and sales forces.

October 2003: Vodafone and Oracle announce a joint initiative to offer enterprise customers integrated mobility solutions based on Oracle 10g (a database designed for enterprise grid computing) and Vodafone's network services. In essence, the partnership is aimed at delivering mobile access to key business systems. Initial vertical sectors targeted are: health care, government, utilities and media.

October 2003: At ITU Telecom World, held in Geneva, Vodafone announced a Web services partnership with Microsoft to bring mobile network services – such as authentication and billing – to the fixed PC Internet. Web services, based on XML (eXtensible Mark-up Language), are a suite of Web-based protocols designed to form the interface between proprietary telco networks and software. Web services would enable application developers to exploit mobile network characteristics, such as location-based information, authentication, billing and messaging.

In addition, since February 2003, the mobile operator has been offering 'BlackBerry from Vodafone', the 'push' e-mail and mobile data services developed by RIM. In November 2003, Vodafone launched the tri-band Blackberry 7230, a customised icon-driven product (in much the same style as Vodafone live!). This is marketed as part of its Mobile Office portfolio.

5.3.3 Mobile VPN strategy

Vodafone offers a number of mobile VPN solutions within its Mobile Office portfolio in order to broaden its appeal to as many types of enterprise customers as possible.

For those organisations that do not have any Internet-based VPN connections into their LAN, Vodafone, in partnership with Cisco and a

systems integrator, can offer – in effect – an all-you-need starter pack to get the customer up and running with mobile VPN functionality. This starter-pack, which Vodafone (either directly or through its channel partners) installs and (if required) manages, includes:

- a VPN client (supplied by Cisco)
- a GPRS data card or a 3G/GPRS data card
- software that enables 'easy connection' to Vodafone's 3G and/or GPRS network combined with a graphical user interface, known as the Dashboard, which allows end-users access to a number of basic functions. These include the 3G or GPRS connection activation; a monthly volume data usage indicator; and configurable buttons to start-up VPN, IM (Instant Messaging), SMS, e-mail and Internet access clients that have been previously installed on the lap-top
- VPN concentrator and router (supplied by Cisco).

Initially branded as the Vodafone Remote Access service when it was launched in November 2002, this 'single' box solution is now referred to as the Vodafone Mobile Connect Card (MCC). Vodafone claims that MMC can take as little as five hours to integrate with customer's existing IT infrastructure. (It needs to be noted that references to MCC in Vodafone literature can also mean simply the data card and associated software; it does not necessarily imply the 'single' box solution incorporating VPN concentrators and VPN clients).

Other mobile VPN options offered by Vodafone are Mylan and its leased line option. Like Vodafone MCC, Mylan uses private IP addresses, so VPN clients and concentrators need to support NAT Traversal. It is targeted at SME and large organisations that already have existing VPN infrastructure in place. Mylan is also configured in such a way – as is the MCC solution – that all traffic goes directly to the corporate LAN first to prevent direct access to the Internet. IT managers are very reluctant to give employees unrestricted and unmonitored access to the Internet.

The leased line option, as its name implies, does not use the public Internet to link the Vodafone mobile network to the corporate LAN but rather a dedicated line with bandwidth options of up to 2Mbps (the maximum bandwidth that the Mylan service can offer on the fixed-line connection is 320Kbps). This mobile VPN option is designed for companies that place a high premium on security and who perhaps distrust making use of the public Internet. An extra security feature that Vodafone provides for leased line customers is a dedicated APN. Both Vodafone MCC and Mylan use public APNs (see Chapter 2 for a fuller explanation of the differences between public and private APNs).

Vodafone also offers an Internet Access Service. Although not designed for corporate LAN access it does allow connectivity to Web-based

services. If the customer's mail server and firewall were to allow external POP3 or IMAP4 access, for example, the Internet Access Service would be a way to retrieve e-mail on a mobile device. This service is pitched at either one-man-band companies or enterprises with few employees.

Key to Vodafone's strategy to differentiate itself in the mobile VPN space is its 'Dashboard' user interface. It puts the Vodafone brand on the laptop with the mobile operator clearly wanting to position itself as being synonymous with ease-of-use – both for the end-user and the IT manager. All icons are clearly displayed (Connect, Usage, SMS, e-mail, Web, VPN, Support) and designed to creating the 'Vodafone experience' similar to that on Vodafone live! – namely, simplicity.

To placate IT managers' fears that employees will wantonly abuse their data budgets, the Usage icon, once pressed, reveals clearly the amount of data used alongside the limit set by the administrator. It is also possible for IT managers to configure profiles for end-users (access rights, data limits) and install the Dashboard themselves on the laptop.

In March 2004, Vodafone announced an enhanced version of its Dashboard software. This includes, for the first time, an automatic hotspot search function allowing the user – working in tandem with Vodafone's hotspot database – the ability to locate the nearest Vodafone hotspot. Also, through an automatic Internet-based update function, users can benefit directly from future improvements and new functions in the Dashboard software.

5.3.4 Can 3G speed up mobile VPN adoption rates?

Despite its attempts to kick-start the mobile VPN market with 'out-of-the-box' solutions and its intuitive graphical user interface in the shape of Dashboard, sales of the Mobile Connect Card have been disappointing for Vodafone (even though the operator claims they have been in line with expectations). By the end of 2003, only 167,000 units had been sold across Vodafone's controlling territories.

This should not be viewed as a failure peculiar to Vodafone, but rather a reflection on a number of other industry-wide factors that have hindered mobile VPN adoption over GPRS. One key barrier to adoption is that IT managers generally view GPRS as an unattractive medium for delivering high volumes of data, both on the grounds of price and throughput performance (see Chapter 3).

To try and break down these barriers, Vodafone commercially launched a UMTS version of MCC in Germany for business users in February 2004. This was followed, in subsequent weeks, by 3G MCC launches in Italy, the UK, the Netherlands, Spain, Portugal and Sweden. Vodafone expects a faster acceleration of take-up for its 3G cards than GPRS since, in the words of a spokesperson, 'they can now simulate the LAN experience' with downstream speeds of up to 384Kbps.

The data cards themselves are manufactured by Belgium-based Option, which enables laptop users to have seamless roaming between 3G and GPRS networks. In Germany, the card retails for €359 (including VAT), provided that users sign up to a data tariff package from Vodafone. As it is technically possible to configure the data card to work with other 3G networks – if the end-user has the appropriate SIM – Vodafone prices the card at €999 for those who do not sign up to one of its data tariff packages.

Since June 2003, Vodafone in Germany has offered customers a dual WLAN/GPRS data card but, at the time of writing (May 2004), had still to announce plans to offer that product in any other of its major European markets. By the end of 2004, Vodafone says it intends to have bundled in WiFi capability to its GPRS/UMTS cards.

On the pricing front, Vodafone continues to cut its per megabyte charges and, in Germany, launched a time-based data pricing option to its 3G business customers in February 2004 (see Chapter 3). Vodafone, along with T-Mobile Germany, says it is responding to a growing demand for pricing structures that are easier to understand than volume-based charging. Vodafone does not disclose any targets it has set for 3G/GPRS MCC sales.

6 Fixed Line Operator Strategies

6.1 Colt Telecommunications

6.1.1 Background

Colt, headquartered in the UK, is a pan-European provider of managed business communication services targeting Europe-based multinational companies; it also has a range of wholesale capacity products for other carriers.

Its network comprises 20,000km of fibre-optic cable, which includes 32 MANs (metropolitan area networks) spread across 13 European countries. It has direct connections to 9,000 buildings. Colt's service portfolio covers leased lines, Ethernet services (metro, national and international), Layer 2 VPNs (ATM and frame relay circuits) and IP VPNs.

For the nine months ended September 2003, Colt posted a turnover of £860.1 million, up 12.6 per cent from the same period in 2002. However, the improved revenue performance was helped along by a weakening GBP compared to the Euro. If currencies had remained constant, Colt's growth in the first three quarters of 2003 would have been a more modest five per cent compared with the previous year's three quarters.

Due to a mix of cost-cutting and the generation of new business, particularly for its IP VPN products, Colt has managed to reduce its operating losses. For the first nine months of 2002 the company turned in an operating loss of £158,101 million, which was reduced to a negative £68,085 million for the same period the following year. Colt asserts that if it maintains its present rate of progress, it will achieve positive free cash flow throughout 2005.

The company argues that its 'strong cash position' (£934 million as of 30 September 2003) gives it a 'competitive advantage'; it has the means at its disposal, Colt says, to respond quickly to customer requirements for new, advanced services.

6.1.2 Remote mobile/wireless access services

Overview

In terms of developing and promoting remote LAN access solutions for its business customers based on cellular and WiFi connections, it's still very early days for Colt. Although the company struck a deal with 'a major European mobile operator' in May 2003 – which added GPRS to Colt's remote access portfolio – it told BWCS at the end of 2003 that it did not want to make that relationship public. At least, the company said, not until

it had defined its wireless product propositions "more fully" and was in a position to announce "major customers".

"There's a low awareness among our customer base that they can even have remote mobile access," Daryl Szebesta, Colt's director of data services and system outsourcing, told BWCS. "It's only niche, early adopters who are coming to us and asking for these type of services."

Szebesta believes that a "period of education" will have to take place among business customers before the remote LAN access market takes off based on mobile and wireless LAN technologies. Nevertheless, he expects traction in this market to happen in 2004 "when customers latch on to the fact that they can get productivity gains from e-mail access via Blackberry and other handheld devices".

Product portfolio

Colt offers its IP VPN customers a number of remote access options, which are split into two categories: IPCorporate Remote Fixed and IPCorporate Remote User.

IPCorporate Fixed is a remote link to the corporate intranet using the public Internet via third-party ISPs. And, as its name suggests, it is a fixed point of access. Most likely this will be a branch office that is deemed too expensive by the enterprise to hook up directly to Colt's IP VPN network via a leased line or where stringent SLAs are not required.

The IPCorporate Remote User set of products caters for the 'mobile' user. This includes the teleworker connected to the corporate LAN using secure IPSec connections on his or her PC/laptop – again, intranet access is via the public Internet using third-party ISPs, usually over DSL connections. The Remote User product suite also includes dial-in access over the PSTN. In all of these fixed-line instances, Colt gives the option to its customers of handling the billing so as to give its enterprise users a single point of contact.

6.1.3 Mobile/wireless strategy

Colt, like many other service providers, would like to give its customers easy and secure access to their corporate LAN, anywhere and anytime they want it. That means being able to offer mobile/wireless access but, by its own admission, Colt has only started out down this road.

By the end of 2003, Colt's wireless strategy primarily revolved around its Managed Microsoft Exchange product to give application-specific remote access rather than general LAN connectivity. Using its relationship with 'a major European mobile operator', Colt offers its IPCorporate Remote User customers the option of accessing general Microsoft Office applications via GPRS-enabled handheld devices (supplied by the operator in question).

In addition, Colt offers the RIM Blackberry messaging solution, which is made up of the Blackberry device and its associated middleware that sits on the MSExchange server. Colt does not disclose the number of subscribers it has to either its GPRS handheld service or the RIM Blackberry.

For laptop users with GPRS PC cards, Colt offers an IPSec VPN client service to enable general LAN access. Unlike Colt's Managed MSExchange product, corporate LAN connectivity means the ability to access company-specific or 'vertical' applications – perhaps sales force automation software – rather than being restricted to the more 'horizontal' applications such as e-mail and calendar updates. Colt says it can also offer a VPN client service on the handheld devices if the customer requires it. The company also tests and pre-configures each mobile device before being used, as well as giving pre-sales support.

Unlike its fixed-line remote access services, Colt does not give the option of being the exclusive point of contact for the GPRS access service. Instead, the customer signs a contract with the mobile operator, with Colt acting as the agent, for a fixed volume of data – usually 250MB per month – which is paid as a flat rate and can be used by all employees. Any data consumed above the agreed amount is billed by the mobile operator on a usage basis. For its part, Colt bundles in the GPRS access option as part of its IPCorporate Remote User set of products.

No SLAs are offered by Colt on any of its remote access products that rely on third-party providers.

6.1.4 Future directions

Colt says that it is in discussions with various mobile operators across Europe. In particular, it is looking at ways to reduce international roaming charges for its customers who move from one 'Colt country' to another.

Colt is also seeking to "raise the expectations" surrounding WiFi to provide a complete wireless solution for its customers. Instead of WLAN access points being connected to 2Mbps DSL pipes, Colt wants corporate customers to have bandwidth speeds from 10Mbps to 100Mbps to give a true desktop LAN experience. In November 2003 the company said that it had completed a deal with one hotel service provider to provide 100Mbps WiFi and fixed broadband access at a 'top London hotel'.

"We believe the winning remote access proposition is to be able to bundle in WiFi, GPRS and fixed-lines," says Szebesta.

6.2 Infonet

6.2.1 Background

Infonet is a global managed network services provider and has around 3,000 multinational entities as clients. Headquartered in the US, Infonet's network – which it calls The World Network – connects 180 countries with access points in over 3,000 cities. The company offers a range of managed network services, including MPLS-based IP VPNs, IPSec VPNs, SSL VPNs, Frame Relay, ATM, satellite and x.25.

Infonet maintains that The World Network, with its high security levels, extensive reach and reputation for high performance, distinguishes it in the marketplace. Another key differentiator, according to Infonet, is its Application-Defined Networking (ADN) approach. This is where Infonet, through direct consultation with the enterprise customer, analyses the application requirements/priorities and then recommends the most suitable networking profile. Infonet's Network Analysis Programme can also demonstrate how individual applications will perform on its network and conducts an ROI analysis for the customer.

Infonet's first half-year results for its 2004 fiscal year (the six months ended 30 September 2003) revealed revenue of US$300.3 million (US$290.1 million for the same period the year previously). The company made an operating loss of US$37 million and a net loss of also US$37 million during the six months to 30 September 2003.

José Collazo, CEO and President of Infonet, speaking at the time of the first half fiscal year 2004 results announcement in November 2003, said that after 'multiple rounds of personnel reductions' and a 're-alignment' of its cost structure, the company was now in a position to grow revenue and reach profitability. Infonet expects to be free cash flow positive in the next 12 months and to be profitable after taxes in the next 24 months, all while maintaining a cash balance in excess of $350 million USD, according to Collazo.

6.2.2 Remote access portfolio

DialXpress

Until September 2003, when Infonet announced its 'next-generation mobility strategy' (see below), the company grouped all its remote access solutions under the 'DialXpress' brand name. The DialXpress product set is circuit-switched: PSTN and ISDN on the wireline side and GSM, HSCSD (high-speed circuit-switched data) and IS-95 (CDMA) on the wireless side. More than 1,200 multinational enterprise customers use Infonet's DialXpress services.

To be able to offer these circuit-switched remote access services, Infonet leases capacity from third-party operators. Infonet's authentication and

billing infrastructure, based on RADIUS (remote authentication dial-in user service) servers and LDAP (lightweight directory access protocol) facilities, enables it to offer a uniform bill for both fixed and wireless access to the corporate LAN across a globally distributed infrastructure. Infonet can also offer a unified ID to its customers: that is, the same username and password for each access technology used.

Different versions of DialXpress are available for different customer requirements. DialXpress Professional, for example, offers private network access across Infonet's IP/MPLS network.

DialXpress SecureID, using RSA Security's method of 'two-tier' authentication, is also supported by Infonet's RADIUS/LDAP infrastructure. Two-tier authentication is a reference to what the user knows (PIN number and/or password) and what the user has (electronic 'tokens'). The tokens usually come in the shape of key fobs, which, working in tandem with an authentication server in Infonet's network, generate a unique, numeric password at 60-second intervals. The authentication server, working in the same time sequence as the electronic token, can then make a 'match' with the remote user (who has typed the one-time password, on display on the key fob, into the laptop) to give him or her access to the corporate LAN.

In Japan, Infonet has been working in partnership with KCOM – a wholly-owned subsidiary of KDDI – since 2000. Using PHS, the Japanese circuit-switched wireless standard (provided by KCOM), in conjunction with Infonet's IP/MPLS network, the mobile VPN service – offering access speeds of up to 64Kbps – currently has a couple of dozen customers. These are all Japanese companies with no international presence since PHS is not available elsewhere.

In September 2003, Infonet, in partnership with DDI Pocket (another KDDI subsidiary) launched the AirH' (pronounced "Air Edge") service in Japan using packet-switched mobile access speeds of up to 128Kbps. Infonet offers a flat-rate monthly package for AirH'.

MobileXpress

In September 2003, Infonet announced its MobileXpress strategy to complement and expand its DialXpress range of remote access solutions. Emphasising the goal of seamless roaming between different access wireless platforms (including 2.5G/3G mobile networks and public WiFi hotspots), the 'next-generation' mobility roadmap is set out in three phases:

- Switched VPN: wireless/mobile circuit-switched VPN access (already in place through DialXpress)

- Broadband: packet-switched wireless/mobile VPN access, enabled through deals with WiFi hotspot providers and 2.5G/3G mobile operators (first commercial WiFi product launched in March 2004)
- Broadband Roaming: wireless broadband roaming and settlement across both WiFi and 2.5G/3G networks. Marc Patterson, Infonet's Vice President and Managing Director of Mobility Services, told BWCS: "Our direct visibility into the activities of strategic technology providers – such as Intel, Cisco and Microsoft – makes us believe that this phase will be feasible within three years."

To move into the Broadband phase, Infonet initially struck wholesale capacity deals with Boingo Wireless and GRIC Communications – both WiFi network operators – in October 2003 and November 2003 respectively.

Infonet's deal with Boingo goes deeper than wholesaling capacity. First, for an undisclosed sum of money, Infonet has taken a minority equity holding in Boingo. Second, the two companies have worked together to develop end-user software that will eventually allow access to the entire WLAN footprints of Boingo and Infonet's other contracted hotspots, while simultaneously using Infonet's existing billing and authentication infrastructure.

Infonet announced the first fruits of its work with Boingo in March 2004 with the launch of its MobileXpress Professional service for remote access via WiFi hotspots. MobileXpress subscribers can initially access over 2,300 active hotspots, which are spread across the US, Europe and Asia. By the end of 2004, Infonet expects the number of accessible hotspots to increase to over 10,000.

Infonet's 'enhanced' end-user software developed with Boingo allows the same user-ID credentials across all of Infonet's remote access products, whether it is wireline or wireless (Boingo's contribution focused on the broadband wireless component of the software).

MobileXpress also works in tandem with VPN clients and contains a so-called 'Mobiscan' capability. This senses and presents all available wireless access methods to the end-user (Infonet's network infrastructure, as we have already seen, can support circuit-switched wireless access, such as GSM, CDMA and HSCSD, as well as WiFi).

According to Infonet, users of MobileXpress can also set up – quickly and easily – user-profiles to access other public hotspots if none is available from Infonet (although the user would receive a separate bill in those instances). Perhaps more conveniently, workers can use the client software to access enterprise resources via home-based and/or campus-based WiFi networks. High-speed wireless home networking based on WiFi is proving increasingly popular, particularly in the US.

Infonet's strategy, even when diversifying into new wireless and mobile access technologies, is to position itself as the single point of contact for its multinational clients. That, combined with making MobileXpress as easy to use (and monitor) as possible, leads Infonet to conclude that it can convert 30 per cent of its DialXpress customers over to MobileXpress every year, as well as giving it a means to attract new customer accounts.

To achieve those objectives, Infonet believes it must do the following:

Provide a unified bill based on 'easy-to-understand' tariff structures

MobileXpress customers receive one, unified bill for both wireless and wireline access. There are two types of tariff packages for MobileXpress, which, like its circuit-switched DialXpress portfolio, are each based on time. The first is a pay-as-you-go service, charged on an hourly and per-minute basis. Prices vary according to the region from where the user is accessing the service (Infonet has split the world into six regions). The second package is a fixed rate based on a pre-determined number of hours.

Infonet believes that by offering a 'global' WiFi service, it can eliminate the variability of pricing that comes from using multiple suppliers. However, the strength of this argument depends on the availability of the Infonet WiFi network (courtesy of Boingo, GRIC Communications and other hotspot providers). If a MobileXpress Professional customer has to access a hotspot that is not Infonet's, then the IT department still becomes exposed to cost unpredictability.

Offer uniform log-in and authentication procedures

By leveraging its own RADIUS infrastructure for both WiFi and dial-up access, Infonet can offer a common log-in procedure – via the same user interface – for all its remote access service products. The software client that comes with MobileXpress can also be used for 'horizontal roaming' with the same log-in procedure. Horizontal WiFi roaming refers to 'seamless' access across different WiFi networks, which, in this case, belong to Boingo and GRIC; vertical roaming occurs across different types of access networks (such as GSM and WiFi) with one bill. Infonet claims that it is the first Tier 1 operator to execute horizontal WiFi roaming. "From our research and feedback from focus groups, the travelling executive is not going to endure different log-in procedures from one hot spot to another," Greg Hayes, Director of Marketing at Infonet's Mobility Services, told BWCS.

Web-based monitoring tools

Again, due the use of Infonet's 'triple A' infrastructure for each access technology, the company can offer 'visibility' to IT departments about which access technologies its remote workers are using and how the applications are performing. Through a Web-based portal and its

complementary MobileXpress Toolkit, IT departments can also administer usernames and passwords; view usage on a near real-time basis; and manage access policies for its remote workers.

One obstacle that may slow down the realisation of Infonet's single-point-of-contact ambition in the wireless space – and later on in the mobile VPN segment – is convincing customers that it has sufficient helpdesk resources to manage these types of connections. By moving into wireless and cellular, Infonet – like all traditional fixed-line operators – is confronted by a far greater number of variables in the event of a faulty connection than when solely concerned with wireline connections. The question then arises, who is best placed to troubleshoot the network when something goes wrong? The WiFi or mobile network operators themselves, or the fixed-line operator who is leasing wireless/cellular capacity?

For its part, Infonet argues that it has a long track record of being able to coordinate globally its troubleshooting across multiple networks. It also points out that through close helpdesk integration with its wholesale WiFi partners, any fears surrounding service support can be allayed.

However, mobile network operators, in the event of competing with fixed-line network operators for mobile VPN customers, can still forcefully argue that they are better placed to remedy network-related problems since they have direct visibility into the network.

6.2.3 Future directions: smartcard/SIM-based authentication

In much the same way as hotspots are becoming more popular as a remote access medium due to the spread of WiFi-enabled laptops, Infonet envisages that IT managers will increasingly turn to smartcard/SIM-based authentication for remote access as more and more devices become SIM-enabled.

The key benefit of SIM (subscriber identity module) authentication, used already in the world of mobile, is that only a personal PIN number is required to gain authorised access. This is not the case with token-based authentication schemes (the use of key fobs, for example, which produce one-time only passwords), or vouchers, or even a system of usernames and passwords. All of these methods, in comparison with SIM, are time-consuming and potentially very costly if the enterprise needs to invest in extra helpdesk resources to deal with remote workers who have either lost their tokens or have forgotten their passwords.

"You have to look at ID management in terms of how you can truly embed the security, as well as the identity, within a physical asset," says Marc Patterson. "Our major customers are beginning to embrace this idea rather than relying on security [procedures] being adhered to by the end-user."

Infonet believes that two things need to happen before SIM-based authentication can take off:

- PDAs and laptops are embedded with smart card readers (the SIM is a smart card). So far, penetration of such devices is low in the market, but, as an interim measure, SIM card readers are currently available in a USB dongle form (attached to the side of the device). Infonet also identifies a growing trend of 'SIM reuse' where users either place their existing mobile SIM into another device (such as a laptop or PDA) or use a duplicate SIM for the same purpose.
- The EAP (extensible authentication protocol) SIM protocol becomes standardised and established in the marketplace. EAP SIM is key because it allows roaming between GPRS/UMTS and WiFi networks through the use of RADIUS servers interfacing with the HLR (Home Location Register) within the mobile operator's network. This would allow Infonet to use its existing infrastructure to offer a unified bill to remote access users who straddle WLAN, GPRS/UMTS and dial-up networks.

Infonet's work on developing a platform capable of supporting EAP SIM is done through TOGEWAnet, a Swiss company established in 2001 and owned by TOGEWA Holding. In May 2002, Infonet acquired a minority stake in TOGEWAnet.

TOGEWAnet, through its WeRoam service, offers a billing and authentication platform to enable roaming between WLAN and GSM/GPRS networks: its customers are WISPs (Wireless Internet Service Providers) and GSM operators. WeRoam can support SIM, EAP SIM and RADIUS authentication methods.

Another TOGEWA Holding company, Comfone, has been set up to facilitate the management and settlement of roaming agreements between operators who use the WeRoam service. Comfone, aside from its association with WeRoam, acts as a settlement and clearing house for roaming agreements between GSM operators. Infonet owns a minority stake in Comfone.

By the end of 2004, it is Infonet's aim to have in place wholesale capacity deals with GPRS operators. It believes that by exerting its bulk purchasing power, it will be able to offer attractive tariff packages to MobileXpress customers. And, through the use of EAP SIM, combined with the knowledge and experience of TOGAWAnet through its WeRoam service, Infonet will position itself as the one point of contact for billing – with a uniform ID and log-in procedure – for multinational customers using multiple access technologies.

6.3 Equant

6.3.1 Background

Equant, part of the France Telecom Group (which also comprises Orange), is a provider of managed network and IT services. Serving multinational corporations, Equant has 3,700 business accounts. Its network reach spans 220 countries.

Like other international carriers whose traditional revenue streams have been rooted in the provision of managed ATM and Frame Relay services, Equant's financial performance has been adversely affected by customer migration to cheaper IP connections. For 1Q 2004, revenue from Equant's Network Services division declined by 8.7% on a pro forma basis (that is, at constant currency rates), year-on-year, to US$388.5 million.

A large part of the Network Services decline was attributable to Equant's indirect sales channels (which include Radianz, Deutsche Telekom and Sprint). On a pro forma basis, indirect sales declined by 27.1 per cent for 1Q 2004, year-on-year, to US$55 million. Direct sales declined by 4.8 per cent to US$333.5 million over the same period.

Equant's strategy to combat the decline in traditional revenue is to offer multinational customers a wider variety of services. These include IT managed services, such as messaging, hosting and security. It is not Equant's strategy to compete head-on with the major systems integrators – such as IBM, HP, Accenture and EDS – by providing IT integration and management services for business process applications. Instead, its focus is on the management of horizontal applications (such as messaging) which require less IT engineering.

The problem for Equant is that this side of the business is not growing fast and it contributes only a small percentage of overall revenue; that makes the company vulnerable to continued price erosion in legacy service revenue. Turnover from Equant's Total Integration Services (which includes its IT managed service products) accounted for US$108.9 million sales during 1Q 2004 out of a total Equant turnover of US$704.4 million. Revenue from Total Integration Services during 1Q 2004, on a pro forma basis and year-on-year, was up only 0.3 per cent.

6.3.2 Remote wireless access services

As part of its strategy to develop new revenue streams, Equant has also widened its remote access portfolio to include mobile VPNs based on GPRS access.

In May 2003, Equant announced that it had added GPRS access to its remote access portfolio through wholesale agreements with mobile operators in Belgium, France, the UK, Russia and Germany. Equant says it will extend GPRS availability to the US, Australia, Hong Kong and

Singapore in 4Q 2004. There is no exclusivity agreement between Equant and Orange to deliver GPRS access to its customers.

Although the company has its 'Equant Access Companion' software, which, when downloaded onto the laptop or PDA, provides VPN connectivity with log-on procedures identical to Equant customers using fixed remote locations (so making it easier to use), the take-up of the service has been subdued. "We have around 1,000 customer accounts who use dial-up access [PSTN or GSM] but only a few dozen have moved to GPRS since we launched the service," Axel Haentjens, Equant's Head of Stratgey, told BWCS. "We're still in the early adopter mode, but we expect a faster rate of adoption when we make this a fully mobile solution and when customers fully understand the benefits [of using mobile VPNs]."

Haentjens' 'fully mobile' solution means the addition of WiFi access to Equant Access Companion (using France Telecom's WiFi network), which is scheduled for July 2004. Equant, says Haentjens, will also announce a portfolio of fixed-mobile services in partnership with Orange at that time.

For mobile operators to interconnect into Equant's fixed network, a GGSN gateway interfacing with it is required. One benefit for business customers using the Equant network is that, due to its avoidance of the public Internet, a company's existing VPN infrastructure need not support NAT Traversal. Equant, however, will support public Internet access if required. "It's a hybrid solution," says Haentjens.

6.3.3 Strategy

Unlike Infonet or Colt, the other two fixed-line operators profiled in this report, Equant has no strong aspirations to be the single point of contact to business customers that use mobile operators' cellular networks for remote intranet access.

The billing of Equant's GPRS IP VPN extension service, for example, works in a similar fashion to Equant's PSTN or IP dial-up service. The customer pays Equant a flat monthly rate for the access facility but then pays the third-party provider for traffic usage. In this way, Equant can draw a firm line of responsibility between its own network and the network of third-party providers. One benefit of this approach is that if anything goes wrong on the mobile side – perhaps a dropped wireless data session – Equant is not seen as responsible.

That is not to say that Equant will not manage and bill for all of the customer's communications requirements – including fixed and mobile remote access – if asked to do so. In October 2003, Equant won such a contract with Zurich, an insurance company, to manage and bill for all of Zurich Financial Services Group's telecom and network services in seven European countries. As part of the deal, Equant wholesales mobile voice

and mobile data capacity to resell to the customer and, by doing so, offers itself as the “one throat to choke”.

But outsourcing everything over to one service provider is not a route that Haentjens expects most multinational organisations to follow. “We have only a handful of customers that want do that,” he told BWCS.

7 Vendor Strategies

7.1 Lucent Technologies: 3G mobile data evangelist

7.1.1 Background

Lucent Technologies is a supplier of fixed and mobile telecoms equipment. The vendor also offers a range of managed services to operators – including consulting, network design and marketing – via its Lucent Worldwide Services division. Bell Labs is Lucent's well-respected R&D arm.

Patricia Russo, CEO, identifies several 'pockets of opportunity' for growth during 2004 and beyond. These are: voice over IP and softswitches; metro optical; broadband access; and high-speed wireless data and services.

Growth is not something that Lucent has been closely associated with in recent times, but the company is showing signs of turning things around. In its 4Q 2003 fiscal period (ended 30 September 2003), Lucent posted its first net income profit (US$99 million) since 2Q 2002. For 1Q 2004 (ended 31 December 2003), Lucent posted a net income of US$338 million to make it two profitable quarters in a row.

The improved performance in profitability has come about through cost cutting rather than top-line revenue growth. Turnover for fiscal 2003 was US$8.47 billion compared with US$12.312 billion during 2002, but total expenses were slashed by US$5.8 billion over the same period. In the industry boom days of 2001, Lucent's workforce exceeded 100,000. Currently, Lucent has approximately 33,000 employees worldwide.

Revenue for Lucent's Mobility Solutions was US$4 billion during fiscal 2003 (US$5.535 billion the previous year). The company's mobile focus is on supplying CDMA-based 'spread spectrum' technologies for 3G: CDMA2000 and UMTS (which uses W-CDMA radio access technology). Lucent does not give a revenue split between the two 3G platforms but it is far more established in CDMA2000 than UMTS.

7.1.2 Extolling high-speed mobile data for the enterprise

When it comes to promoting mobile data adoption within the enterprise, Lucent is one of the industry's most vocal and active players. It regularly runs roadshows to educate enterprise CIOs and CEOs on the productivity and efficiency gains that can be achieved through high-speed mobile data solutions.

It also firmly believes that mobile operators, systems integrators and vendors should all work together in presenting the business case for

mobile data solutions to enterprise customers. The level of cooperation that Lucent is talking about includes having representatives from each sector – vendor, systems integrator and mobile operator – sitting around a table with the CIO (and, whenever possible, the CEO) in order to address fully the different concerns there may be in mobilising the workforce.

According to Lucent, the early adopters to drive up mobile data growth will come from the business segment. The consumer market, it believes, has little appetite as yet for services based on high-speed mobile networks, such as video telephony.

Within the business segment, Lucent asserts there is both a pent-up demand for mobile data solutions and a willingness to pay – up to US$100 per month per employee on a flat-rate basis according to its own research – but only if the benefits can be clearly identified. The problem for mobile operators wishing to tap into this market is that while their marketing messages are well defined for the consumer, they are not for the business customer. This is because the mobile operator – according to Lucent – has little understanding of the way enterprises operate, not least because the enterprise market is far from homogenous: different industries in different countries have all got different needs. Lucent's strategy is to bridge that gap in understanding and to make it as easy as possible for operators and enterprises to provision mobile VPN services.

Lucent does not believe there is a strong business case for mobile data adoption within the enterprise unless it is based on 3G. "We've conducted primary research across Europe and what we've found is not only a pent-up demand for wireless data solutions among enterprises but a minimum speed requirement of ISDN rates," John Marhino, vice president of marketing, Mobility Solutions, told BWCS. "That means you need an effective throughput of between 140Kbps and 144Kbps at the very least and, from the research we have carried out, the ability to go as high as 300Kbps."

The research that Marhino is referring to was conducted as far back as September 2002 and, more than a year later – despite the availability of software compression, which effectively speeds up data throughput, and growing evidence that businesses can increase productivity at sub-3G data speeds, particularly in the realm of field force automaton – Lucent is sticking to those findings.

Underlining its desire to promote 3G-based mobile data solutions, Lucent is a founding member of the 3G Enterprise Alliance (3gea: http://www.3gea.org). Set up in November 2002, 3gea's mission is to 'identify and promote the benefits of secure, high-speed data services for enterprises'. Other founding members include HP, Sun Microsystems, Atos KPMG Consulting (AKC) and Morgan Stanley.

7.1.3 3G data cards to kick-start the market

Rather than wait for the widespread availability of 3G handsets, Lucent has been canvassing both mobile operators and enterprises that it's possible to move ahead now with high-speed mobile data via laptop PC cards. In 2002, Lucent signed agreements with two companies to supply wireless PC cards with UMTS/GPRS interfaces: the first was with Option (February 2002), a Belgium-based wireless solutions provider; and the second was with Novatel Wireless (August 2002), a US-based software and wireless data modem vendor. Under the terms of both deals, Lucent provides the R&D while its partners manufacture the PC cards.

In Europe, Lucent has worked with Telefónica Moviles España (TME) and T-Mobile Deutschland to conduct trials with enterprise customers connected to UMTS networks via PC cards (developed in conjunction with Novatel Wireless). In February 2004, Lucent announced that it had signed two separate agreements to supply data cards (again, from Novatel Wireless) to TME and Telecom Italia Mobile.

On the CDMA side, Lucent has deployed CDMA2000 1X networks for more than 25 mobile operators worldwide.

In each instance where Lucent works directly with the enterprise, the vendor hopes that the mobile operator will take into account the positive feedback from their business customers and so be encouraged to roll out their 3G networks more widely and more swiftly.

7.1.4 Mobile VPN portfolio

Lucent equipment supports both end-to-end and network-based mobile VPNs. However, it has prioritised end-to-end mobile VPNs as it is they – according to Lucent – which are the clear favourite among the CIO community on the grounds that they are perceived as being more secure.

For enterprises, Lucent's mobile VPN solution comprises the IPSec client and the VPN gateway (responsible for terminating the VPN 'tunnels'). Known as the Lucent Brick family of products, it also supports firewall functionality.

For GPRS and UMTS mobile operators, Lucent's network-based VPN implementation uses virtual routing based on the Cisco 7609 GGSN (Gateway GPRS Support Node). The architecture supports a variety of tunnelling protocols, including IPSec and L2TP.

Cisco 7609 can also support the virtual (or single) APN feature, which allows multiple users to access different physical target networks through a common APN. Lucent outlines the key benefits of the virtual APN for GPRS/UMTS network operators as follows:

- simplified provisioning of APN information at the home location register (HLR), domain name system (DNS) and RADIUS server
- easier deployment of new services
- improved scalability for support of a large number of corporate networks, ISPs and services
- increased flexibility of access point selection.

For a fuller explanation of mobile VPN terminology, see Chapter 2.

Easy Service Setup: Lucent's 'fast provisioning' solution

A significant barrier to mobile VPN adoption is the complexity of provisioning remote workers with access to the corporate LAN or web-based applications – both from a mobile operator's and IT manager's point of view.

From the perspective of the mobile operator, different network elements need to be provisioned so as to recognise each mobile VPN end-user and ensure accurate billing – these network elements include the HLR (home location register) and the billing and mediation systems. If the set-up process is lengthy, then enterprise customers may think twice about using that particular mobile operator. And if the network elements are set up inaccurately – that is, where users either can't access their corporate LAN applications or the enterprise is wrongly billed for services used – that, too, increases the potential for churn.

From the IT manager's perspective – particularly one who is responsible for a large number of remote workers – a major headache is making sure that each employee is provisioned with the correct type of data card for the laptop, the appropriate drivers and the right client software (such as the IPSec VPN client or the 'Mobile IP' client software, which allows roaming between UMTS and WLAN networks).

The problem is made more difficult in large organisations as there is more likely to be a diversity of OS (operating system) software versions in use across the laptop workforce (not all VPN clients, for example, are compatible with every OS). The prospect of having to undergo a series of software installations on each laptop is hardly an appealing one and will dim the attraction of going down the mobile VPN route for many IT managers.

Lucent's answer to this problem is its Easy Service Setup software package, which allows the IT manager and mobile operator to coordinate the provision of wireless access to the corporate intranet.

In development since 2001, Easy Service Setup is the product of examining the workflows and interfaces required on both the client and

network side to facilitate a mobile VPN connection. It can be divided into three main components:

- **Self-installation & registration.** This element is a single install software package that is supplied to users on a CD, together with a data card. With what Lucent describes as 'simple and intuitive instructions', the user is guided through the installation, registration and activation process for accessing high-speed mobile data services.
- **Self-care.** This component offers the ability for end-users to register for the first time and to self-manage their profiles (ie, change password, modify preferences, or add services). It also allows the mobile operator and any other player in the process chain – such as a reseller or IT department – to access user details in order to better provision, control, update and manage their subscribers. All this is done through an 'intuitive' Web-based interface.
- **Integration.** Lucent Worldwide Services ensures systems integration between Easy Service Setup and existing infrastructure.

How it works

The Easy Service Setup provisioning software swings into action once the basic mobile VPN infrastructure has already been established. This could either be a network-based mobile VPN (where the mobile operator has allocated a dedicated APN to the enterprise) or an end-to-end VPN using IPSec clients (where the mobile operator provides only the access over the GPRS or UMTS network).

The value of Easy Service Setup lies in giving the IT manager the flexibility to add (or subtract) remote laptop workers with wireless corporate LAN access – as well as updating access rights – when he or she pleases. It also allows the mobile operator to provision correctly all the required network elements in one fell swoop.

The workflow tasks required to register a wireless VPN connection with Easy Service Setup – whether it is for one user or over a hundred – are as follows:

The IT manager/administrator logs on to the self-care server (via a Web interface) using a password. He then requests the number of users to be activated over the mobile VPN and stipulates what each requires in terms of software.

If the IT administrator has the authority to make that request (ie, there is a sufficient number of SIM cards already allocated by the mobile operator to the enterprise and the air-time/data tariff agreements are in place to cater for more mobile data users) then Easy Service Setup automatically pre-provisions the appropriate elements within the network.

A CD Rom containing all the required client software and drivers – along with a password, user name and data card – is sent to the end-user.

The end-user installs the software onto his or her laptop using the installation 'wizard' guide that comes with the CD Rom. He/she then logs on to the self-care server (using the user name and password provided) whereupon the pre-provisioned elements within the network are activated.

Lucent says it is trialling Easy Service Setup with mobile operators in Europe, the Asia-Pacific and the US. Lucent had not officially announced any commercial implementations of Easy Service Setup by March 2004.

Easy Service Setup: an assessment

It's hard to argue with the convenience of Easy Service Setup. For the mobile operator, it's a great way to attract and 'lock-in' enterprises with mobile data services; for the IT manager, the main attraction is that life becomes considerably easier. There's no longer the need to make several software installations on the laptop to suit the requirements of individual mobile workers. (Some, for example, may need IPSec clients installed on their laptops to access the corporate LAN; others may need their laptops configured to provide restricted – or monitored – access to the Internet.)

Additional software, such as a 'dashboard' client interface to display data usage information, may also need to be bundled onto the laptop, which is another task for the IT manager that Easy Service Setup takes away.

"By working with third parties we're able to customise the solution depending on the requirements of the enterprise," Thomas Evans, UMTS senior manger with Lucent, told BWCS. "Multiple configurations of software, tailored for individual mobile workers, are simply burnt onto a CD [a process undertaken either by the enterprise or the mobile operator], which is then installed easily and quickly onto the laptop by the end-user."

There are, however, some 'issues' with Easy Service Setup that may hinder its take-up:

Where should the self-care server be located? Evans observes that mobile operators will want to host it themselves 'to ensure control'. That being the case, mobile operators will have to prove themselves as trustworthy holders of corporate LAN access information.

The use of passwords as a means of authentication may not convince IT managers as an adequate way to secure the corporate LAN (vulnerable to 'shoulder surfing' and hacker attempts to pose as a mobile worker from another PC). Also, if the password and user name information is sent out by post, that adds two security risks: first, unlawful interception; second, the details sent out can be seen and used by unauthorised personnel. Lucent says it has mitigated these security concerns by enabling the IT

manager to set up specific questions for mobile workers. That, however, adds complexity to the set-up procedure and perhaps places a greater strain on the enterprise's IT resources (more help-desk calls as end-users not only forget their passwords but the answers to the additional questions).

Easy Service Setup works only for laptop CD installations; it will have no relevance for enterprises seeking to mobilise their workforces with smartphones or PDAs.

The waiting time for an 'updated' CD Rom to be sent through the post (as a consequence of a change in access rights, for example) may be too long for some mobile workers, especially sales staff who need access to up-to-date information continuously. IT managers may prefer over-the-air (OTA) device management systems in these circumstances, which offer quicker response times in the event of a change in software requirements.

7.2 Ericsson: voice first, data later

7.2.1 Background

Headquartered in Sweden, Ericsson is a vendor of mobile systems; it claims that 40 per cent of all mobile calls in the world travel across its equipment. The company also manufactures fixed-line infrastructure and, via its joint venture with Sony, is a supplier of handsets.

Like other mobile kit makers, Ericsson has suffered badly during the industry downturn. Scarce capital among mobile operators and the consequent decline in network investment led Ericsson to post an unprecedented series of quarterly losses between 2002 and mid-2003.

In response to the changing marketplace, Ericsson embarked on a stringent cost-cutting programme, which enabled it to return to the black for its 3Q 2003 fiscal period. Between July and September 2003, the company posted an operating income of SEK1 billion on net sales of SEK28 billion (compared with an operating loss of SEK3.6 billion on net sales of SEK33.5 billion for the same quarter during 2002).

To illustrate the scale of the cost cuts, Ericsson's workforce numbered 71,723 at the end of September 2002. Twelve months later, the number of employees was reduced to 53,401.

Ericsson's CEO, Carl-Henric Svanberg, believes that the global mobile systems market (measured in US$) will stabilise in 2004, following a 10 per cent decline in 2003.

7.2.2 Mobile VPN portfolio

Overview

Ericsson's push into the mobile VPN space is two-pronged, and handled by two parts of the organisation:

- **Ericsson Enterprise**: mobility solutions for corporate communications (Mobile Enterprise)
- **Ericsson Systems**: mobile VPN solutions for mobile operators (including specific support for Ericsson Mobile Enterprise).

Ericsson Enterprise: mobile voice VPNs

Ericsson Enterprise promotes a suite of communications products for the enterprise – branded MD110 (for medium-sized and large enterprises) and BusinessPhone (for small and medium-sized enterprises) – that include PBXs (TDM and IP) and a range of business telephones (analogue, digital and IP).

Although the Ericsson Enterprise portfolio covers fixed and mobile access to the corporate communication infrastructure, its marketing emphasis now – to both mobile operators and enterprises – is on its 'Mobile Extension' product. This is where mobile users, via the public mobile network, can enjoy the same PBX voice services as fixed-line extension users. In short, it is promoting mobile voice VPNs.

According to Lars Svensson, president of Ericsson Enterprise, the potential of mobile voice in the enterprise has 'barely been tapped into' by mobile operators. He believes that in the absence of compelling mobile data applications, mobile operators can strategically position themselves closer to enterprise customers through the offering of a Mobile Extension service.

Launched in Sweden in mid-2001, Mobile Extension services are now offered by two Swedish mobile operators, namely TeliaSonera and Vodafone. Customers include ABB, AstraZeneca, Deloitte Touche, Tohmatsu, Saab and Ericsson itself.

What is Mobile Extension?

Mobile Extension is essentially software that sits on the company PBX or server. In combination with support for the feature in the mobile operator's network, Mobile Extension enables the mobile phone to connect to the PBX in the same way as 'normal' fixed extension telephones, with all features and functions of the PBX, including attendant support, made available to the mobile user. Colleagues and customers can reach the Mobile Extension user on his or her usual direct line or

extension number. Conversely, the mobile user can call colleagues using familiar abbreviated dialling.

Another bonus of the Mobile Extension product is that mobile callers can browse the corporate directory without having to store all the contact details on their handsets. They can also use voice-based dialling to call their colleagues (by speaking the person's name).

But the advantages of Mobile Extension, says Ericsson, go beyond the convenience of being able to use the company's extension number system on the handset. They offer economic and strategic benefits to both enterprises and mobile operators.

Proposed benefits for enterprises

- **Reduced end-user device costs**. The IT/communications department, by migrating employees with both mobile and fixed phones to just one handset, can achieve savings on hardware, subscriptions and related support and maintenance costs.
- **Better cost control.** By addressing enterprise needs for mobility, the mobile operator can adapt its tariff structure to enable a transition from fixed to mobile as the primary method for calls both within and outside the office. The air-time packages from the mobile operator can be also be customised. For example, they could be based on a monthly flat fee (with 'free' internal calls), zone-based charging, or a combination of these.
- **Service level agreements.** Agreements between enterprises and mobile operators for Mobile Extension services can include service guarantees. This may require the mobile operator to increase network capacity in the area where the enterprise is located. Indoor coverage might also need special attention.
- **Better management of incoming calls.** Calls to a busy mobile user can be taken by an attendant, rather than simply being forwarded to voicemail.
- **More control.** The IT manager has greater visibility and control of the mobile calling patterns of employees if there is just one company account with one mobile operator. The spread of individual mobile accounts within an enterprise – with no central point of control – can quickly lead to excessive bills, particularly on international calling.
- **Increased productivity.** Greater mobilisation of the workforce with access to a range of PBX services on the mobile handset (conferencing, for example) leads to greater efficiencies within the enterprise, argues Ericsson. Another useful application, according to Ericsson, is mobile access to the company's unified messaging system. It becomes possible, for example, to access e-mails (sent to the PC) as a voice mail on the mobile phone. This level of fixed and

mobile integration is not available within the traditional PBX environment.

Proposed benefits for mobile operators

- **Revenue growth.** More traffic is passed on to the mobile network, which is a revenue growth opportunity.
- **Churn reduction.** By linking PBX functionality with the capability of the mobile network, operators can reduce the possibility of churn since it becomes more difficult, from a logistical point of view, for the enterprise user to 'transfer' its company extension number system to another supplier. The relationship would resemble even more of a 'lock-in' if the enterprise customer selected the mobile operator to host its PBXs. This level of outsourcing is possible through Ericsson's mobile telephony products.
- **Closer ties with the enterprise.** The mobile operator can form a closer relationship with the IT/communications department and, theoretically, be in a stronger position to market and sell value-added data services when they become available or are asked for.
- **Mobile Extension: an assessment.** Enterprises can clearly achieve cost-savings through the use of Mobile Extension. Ericsson itself is in the process of rolling out Mobile Extension throughout its operations in Sweden. It has already mobilised more than 7,000 of its workforce in this way and saw a 22 per cent decrease in its internal telephony costs during the first quarter of using Mobile Extension compared with the previous quarter. The scale of cost savings enjoyed by enterprises will be dependent mainly on the reduction in the number of phones and subscriptions in use (along with a reduction in related maintenance and support costs); it will also depend on the pricing approach of the mobile operator.

Ericsson Enterprise argues that the main benefit mobile extensions can bring to the operator is strategic; that is, strengthening links with the enterprise. It will not, in the short terms at least, be a way for the mobile operator to increase revenue dramatically, even if mobile handset penetration within the enterprise is raised from around the current typical level of 20-25 per cent to between 60 and 70 per cent (a target that Ericsson thinks is achievable and desirable from the enterprise's point of view). This is because of the more attractive (cheaper) airtime packages that are needed in order to persuade IT and communications managers to increase mobilisation of the workforce in this way.

However, it makes sense for mobile operators to differentiate themselves as much as possible from their competitors. In the mobile VPN space, with fixed-line service providers also offering GPRS access solutions via wholesale capacity, the use of Mobile Extension is one way for mobile operators to add value to their enterprise service offerings and reduce

churn. Ericsson says that mobile operators who support Mobile Extension services have typically seen a 75 per cent increase in mobile traffic among users equipped with the service. The fixed-line providers cannot offer this service, so the strategic value of Mobile Extension is significant.

The Mobile Extension product will also become more attractive to large organisations if it can be used on an international basis. Although it will require co-operation among different operators to make this work, Ericsson Enterprise told BWCS that there were no real technical barriers to its adoption. Mobile operators with large international footprints, and so less reliant on co-operation with others (such as Vodafone) would therefore appear to be in the best position to offer this service.

Ericsson Systems: mobile data VPNs

Under the product umbrella of 'Wireless Corporate Access', Ericsson Systems has developed a mobile data VPN architecture suitable for deployment in both GPRS and W-CDMA (3G) networks. Using an APN (Access Point Name) within the GGSN (Gateway GPRS Support Node), the mobile network is able to identify external packet data networks. The 'external networks' can either belong to the enterprise or an ISP (whose subscribers have GPRS access).

There are two types of VPN that this architecture can support: 'voluntary VPN' and 'compulsory VPN'. The voluntary VPN (or CPE-based VPN) is where the mobile subscriber initiates the secure tunnel to the corporate LAN, end-to-end, using the mobile network merely as a bearer (tunnelling protocols can either be IPSec or Microsoft's PPTP). Under this type of set-up, the subscriber gets access to the GPRS network via an APN allocated to an ISP, and can get access to wireless LAN and ADSL. This type of mobile VPN is more likely to appeal to large organisations that have sufficient IT resources to manage this type of VPN themselves.

The compulsory VPN (the network-based VPN) is when the mobile operators itself is responsible for establishing secure links between the end-user and the corporate LAN (or web-based applications). The mobile operator allocates a dedicated APN for the corporate traffic in order to set the compulsory VPN up. This solution is more attractive for SMEs without large IT resources.

A fuller explanation of mobile VPN terminology can be found in Chapter 2.