



WHITE PAPER

The Need To Manage Airspace

A DETAILED LOOK AT THE CHALLENGES FACED IN PROVIDING EFFECTIVE & RELIABLE WIRELESS SERVICES FOR IN-BUILDING, CAMPUS AND METROPOLITAN ENVIRONMENTS



YOU WILL HAVE SOME BASIC FAMILIARITY WITH WIRELESS TECHNOLOGIES AND THE ISSUES INVOLVED IN DEPLOYING THEM, PARTICULARLY IN CHALLENGING ENVIRONMENTS. ALTERNATIVELY YOU MAY HAVE MANAGEMENT RESPONSIBILITY FOR PUBLIC OR COMMERCIAL PREMISES WHERE MULTIPLE OCCUPANTS MAY WISH TO MAKE WIRELESS A PART OF THEIR EVERYDAY BUSINESS. THIS WHITE PAPER GIVES YOU A DEEPER UNDERSTANDING OF THE PROBLEMS AND WAYS OF OVERCOMING THEM, SO YOU WILL BE BETTER EQUIPPED TO MAKE DECISIONS.

THE REASON FOR THIS WHITE PAPER

To show how successful wireless deployments can be leveraged for commercial advantage and how overall cost of ownership can be reduced significantly while, at the same time, enhancing the return on investment through:

- Establishing users' expectations for wireless services
- Describing the challenges facing owners and operators
- Understanding how wireless can be used safely and securely
- Seeing how, with careful planning and engineering, wireless can be used reliably, even for mission critical applications
- Introducing how Red-M can help you manage airspace

EXECUTIVE SUMMARY

Red-M can help deliver successful wireless solutions for in-building, campus and metropolitan areas via its five step life-cycle of best practice:

- **Consulting** - defining exactly how, when and where wireless will be used.
- **Audit** - understanding what is happening and developing a design baseline
- **Design** - optimum wireless performance from a design that works right, first time
- **Implement** - a non-disruptive installation using best-of-breed technologies
- **Manage** - maintaining a healthy network that continues to meet your needs

CONTENTS	PAGE
INTRODUCTION	2
TECHNICAL CHALLENGES	3
The uncertainty of propagation	3
Dealing with interference	5
The indoor solution	7
BUSINESS CHALLENGES	8
Security threats	8
Health & Safety	8
Coverage where & when it's needed	9
Capacity: more is not always better	10
Set the policy, manage the policy	10
MANAGING AIRSPACE	11
CONCLUSION	12

INTRODUCTION

Wireless communication, in its very broadest sense, has been with us almost 100 years, yet its use still continues to grow on an unprecedented scale. It seems that almost every portable electronic device now on sale uses at least one form of wireless. In turn a multitude of wireless applications and services has emerged promising flexibility, connectivity and universal access on the move.

Falling prices and aggressive marketing mean wireless devices are now bought and used in their millions. This massive growth in take-up has brought a shift in expectation. Where once just being able to make a call was enough, today's users - business or otherwise - expect ubiquitous voice and data coverage. From this they expect universal access to an ever-expanding range of applications such as e-mail and web browsing, sharing photos and downloading music: indeed the wireless services on offer, and quality thereof, can influence decisions about how people travel and where they shop, go for coffee or rent office space.

It's tempting to think then that in the presence of such user demand, and with nearly a century of experience behind it, the wireless industry could deliver. And out of doors, in main centres of population and commerce, it mostly can. Where it tends to come undone is indoors, inside public and commercial buildings. This is because building interiors are among the most wireless-hostile environments there are, with many obstructions for radio waves, a high but rapidly changing density of users and a high expectation for the quality of services made available.

The problems are further compounded by the nature of wireless itself. Unlike wired networks, which naturally segregate users and systems, wireless resources are limited and shared amongst all the technologies and applications: 2G & 3G for mobile phones, private radio, Wi-Fi, Bluetooth, RFID and a host of other signals - all of them competing for limited space in the spectrum and all of them potentially interfering with each other.

Where only a few years ago there was little or no wireless inside buildings, today there are a multitude of signals serving an equally varied range of applications, as shown in Table 1.

TABLE 1:
Common wireless applications

GSM/2G	Voice, text and simple data services for mobile phones
3G	As 2G but advanced data services, with higher speeds
Wi-Fi	Internet connectivity for laptop computers Barcode scanners in shops CCTV for security systems Voice as an alternative to 2G/3G
RFID	Inventory tags in shops and warehouses
Bluetooth	Credit card reader in a restaurant Wireless headsets for mobile phones
DECT	Cordless telephones in the back office and in homes
PMR	Security guard communications
TETRA	Radio for the emergency services

It is against this backdrop that building owners, facilities managers, operators and service providers have to match service delivery to user expectation. This document introduces a radical new solution to achieving that goal.

TECHNICAL CHALLENGES

Wireless is a complex technology. It follows immutable laws of physics. It involves radio waves that propagate, invisibly, in diverse ways and that are influenced by a multitude of variables including terrain, environment, weather and the frequency band in use. Out of doors it is a difficult enough medium to master - witness the dead spots that persist in mobile phone coverage - but indoors it is orders of magnitude harder.

It can be tempting to apply to wireless the same rules and best practice that apply to hard-wired networks. But in truth they have little or no relevance to wireless. There are important differences between the two technologies which need to be considered.

There are semantic problems too. For example many people use the terms 'wireless' and 'Wi-Fi' interchangeably, as if they were the same thing. In reality this is not the case. Wi-Fi is but one technology amongst many which can occupy the much broader, more complex wireless spectrum. That said, to consider implementing Wi-Fi without reference to the rest of wireless is probably storing up problems for the future.

Another problem is one of misconception. The easy-to-install-and-use nature of domestic Wi-Fi access points suggests that because the technology works readily at home, then wireless must be easy anywhere. This is not true, as will be highlighted later: business-class, industrial-strength wireless networks (including Wi-Fi, of course) are a world away from the plug-and-play nature of consumer Wi-Fi.

A further issue is that Wi-Fi standards share much in common with wired networking standards, particularly Ethernet. This has led many to suppose that the same thinking and skills which are necessary for wired network design and implementation are appropriate for wireless design. Again, not true: wireless requires a completely different skill set and expertise to wired networking, as will be described later.

The physical reality is that wireless has limited, finite spectrum in which to operate and it is impossible to segregate and segment in the same way cabled or wired systems can. Wireless behaves as a single, amorphous entity and it must be planned, controlled and managed in the same way. Especially indoors.

THE UNCERTAINTY OF PROPAGATION

An obstacle to providing good wireless service in-building is the uncertainty of propagation of radio waves within an enclosed space. In wired networks the signal path between two devices is generally well defined assuming good cabling and termination practices have been followed. In wireless networks, however, signals can follow an almost infinite number of paths as they are reflected, absorbed, scattered, diffracted and refracted by nearby structures and objects, as illustrated in Figure 1.

FIGURE 1:

Some of the mechanisms that affect radio wave propagation, both inside and outdoors

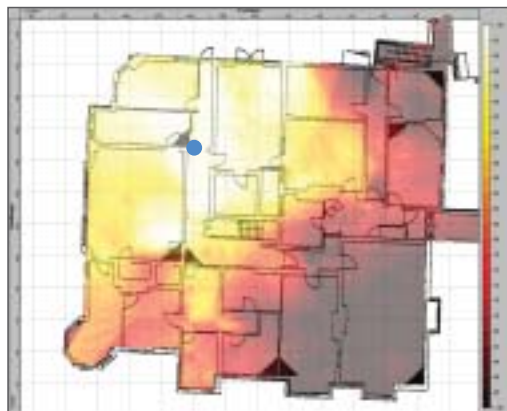


Reflection	From the smooth surfaces of walls and hills
Absorption	By walls, trees and by the atmosphere
Scattering	From rough surfaces such as rough ground, tree branches and the sea
Diffraction	From edges, such as external corners of rooms and building rooftops
Refraction	Due to layered materials like mortared walls, and atmospheric layers

Reproduced by permission of John Wiley & Sons, Ltd. © 1999.
Source: Simon R. Saunders - Antennas and Propagation for Wireless Communication Systems

While all these effects can be predicted in theory, in practice they are hard to forecast accurately. Figure 2 illustrates the complexity in the real-world signal level from a single antenna: far from being a circle, it exhibits great complexity arising from a combination of all of these propagation mechanisms. Ultimately therefore it is difficult to calculate exactly where any required wireless service will be available, and at what quality.

FIGURE 2:
Received Signal Strength within a building from a single antenna transmitting at 21dBm in the 1800 MHz cellular frequency band - the lighter the colour, the higher the signal (scale in dBm)



The reason is that wireless and building interiors do not happily coexist. Brick, concrete, timber, steel, glass, furniture, fittings and even occupants all serve to distort and dissipate the radio signals on which wireless services depend to varying degrees. What's worse, each different material, and even each different batch of the same material, can have drastically different properties.

Source: Red-M, from a typical RF Audit Report

Table 2 illustrates the problem. Based on actual measurements for various building materials, it shows the percentage of radio frequency energy passing through from a standard Wi-Fi access point operating in the 2.4 GHz frequency band. Particularly apparent are the large variations between materials that outwardly appear to be the same.

TABLE 2:
Absorption rates of different materials

Wall Type	Power Transmitted (%)
Block Wall #1	0.251
Block Wall #2	0.126
Brick Wall	0.316
Double Glazed Panel #1	0.063
Double Glazed Panel #2	0.002
Office Floor #1	0.032
Office Floor #2	0.001
Stud Partition Wall #1	0.398
Stud Partition Wall #2	0.126

Source: Red-M, real-world measurements taken in a variety of buildings using high-quality RF data analysis equipment

The variation and degree of attenuation experienced occurs not just with Wi-Fi, it applies to all types of radio waves - 2G, PMR, WiMAX, etc. Underlying the variances are the ways in which building materials are put together. Some plasterboard can contain metal foils or wire mesh; concrete walls, ceilings and floors can hide steel reinforcing; glazing is often itself metallised to enhance appearance or heat reflectivity; curtain walls conceal a steel structure beneath. When all these materials are combined in a contemporary building they present a veritable obstacle course for wireless signals.

One consequence of the variations in materials is that each and every building, while it may look the same as its neighbours, ends up having its own quite unique radio frequency characteristics. Every case, every wireless application, every location is different. And there are no easy, ubiquitous, off-the-shelf solutions that are guaranteed to make wireless work effectively in all buildings. Designing such solutions is therefore a highly skilled task.

The problems are not just restricted to wireless systems that were originally designed to operate indoors (for example, Wi-Fi). Construction methods and materials can also have a profound effect on the ability of signals to penetrate from outside-to-in and vice versa. The general approach to date of mobile phone operators has been to hope the signals from nearby macrocells will penetrate inside a building or around a campus. But the attenuation effects of exterior walls and windows can be so severe that indoor service is generally inadequate.

Technology advances have compounded the problem. 3G networks, launched on a promise of video calls and higher speed data, are pushing the in-building boundaries still further with their higher, more attenuation-prone operating frequencies, and their more signal-path-sensitive spread spectrum technology. Upcoming solutions based on WiMAX technology face similar challenges.

Another issue - because of the way 3G base stations allocate bandwidth and signal power to users - means those accessing macrocells on a campus site or inside a building, where signals may be relatively weak and subject to the vagaries of a poorly performing radio link, can take a disproportionate amount of the available base station resources, so denying service to other users.

DEALING WITH INTERFERENCE

Wireless devices operating in close proximity - inside a building for example - invariably interfere with each other. This happens when they occupy the same or adjacent frequency bands, but it is perhaps less obvious that interference can occur even when different systems are operating on widely separated frequencies.

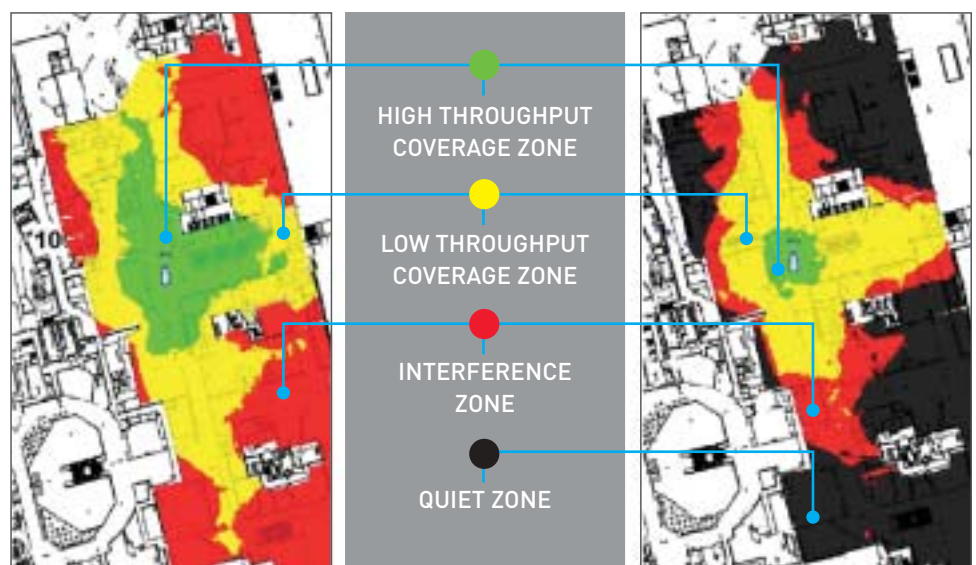
At one time the only wireless signals to be found in a building would have been for the security guards' radios. Now, as already highlighted, there are 2G and 3G mobile phones, Wi-Fi and Bluetooth enabled gadgets, wireless security cameras and a host of other devices. The reality is that when such a mix of devices operates closely together they can both cause and suffer mutual performance degradations, or even stop working altogether. Avoiding interference is therefore a major consideration in any solution, indoors or outside.

The 'same frequency' problem is commonly seen where two Wi-Fi access points within range of each other are installed using the same manufacturer's default channel setting. This not only reduces overall data throughput, but also degrades performance over a large area, as shown in Figure 3.

FIGURE 3:

Left: Interference from a Wi-Fi access point extends over a wide area: although good coverage is only available in the green area, the whole of the red area will experience significant performance degradation - none of the displayed area is 'quiet'.

Right: Even when the transmitted power is substantially reduced (by 100 times in this case) the interference area (red) extends over a much wider area than the coverage area (green).



Source: Red-M, coverage maps from a major UK shopping centre

The 'different frequency' problem has many facets. Limitations in receiver technology render them vulnerable to unwanted signals - particularly from powerful, localised sources. This happens because of inadequate selectivity (the ability to reject all but the wanted signal), blocking by stronger signals (strong signals on different frequencies reducing overall receiver sensitivity, so affecting wanted signals) and spurious responses (low level signals generated by the receiver itself mixing with external signals to create others).

Transmitters contribute to the problem too. Output signals are never pure. They have a tendency to spread either side of the desired frequency. They also create a number of other unwanted signals away from their main frequency of operation. These include harmonics (odd and even multiples of the desired signal) and unwanted mixing products (where signals from earlier stages of the transmitter interact and leak through to the output).

Put several transmitters near to each other and the interference effects can rapidly multiply as signals mix and interact with each other in complex ways to create further, unwanted signals. This problem is aggravated when nearby metallic objects and structures enter the equation. Corrosion, especially where dissimilar metals meet, can create a form of semiconductor junction (effectively a series of diodes). The non-linear nature of diodes makes for a highly effective mixer and harmonic generator. Indeed both of these properties are exploited, by design, in much electronic equipment. The end result is a whole series of unwanted signals and mixing products entering the wireless environment, with the original metal structure acting as its own antenna.

Another fundamental problem is that of frequency allocations. The radio spectrum is a finite resource and already very crowded: consequently it has traditionally been centrally allocated and managed by the regulator, which in the UK today is Ofcom. In recent years, however, market forces have led Ofcom away from the previous majority 'command and control' system for licensed spectrum usage to one based more on market demands.

Historically, spectrum licence holders have been restricted to particular uses (e.g. mobile phones) and often to specified technologies (e.g. GSM). And while licences will still be required to transmit radio frequencies in most cases, many new spectrum awards are 'liberalised', requiring no defined technology in a particular band, with the licence owner free to change technology or application as they see fit. Hence a building owner could find 3G seeping in from a macrocell on one day, but see WiMAX beaming in on the same frequency the next day.

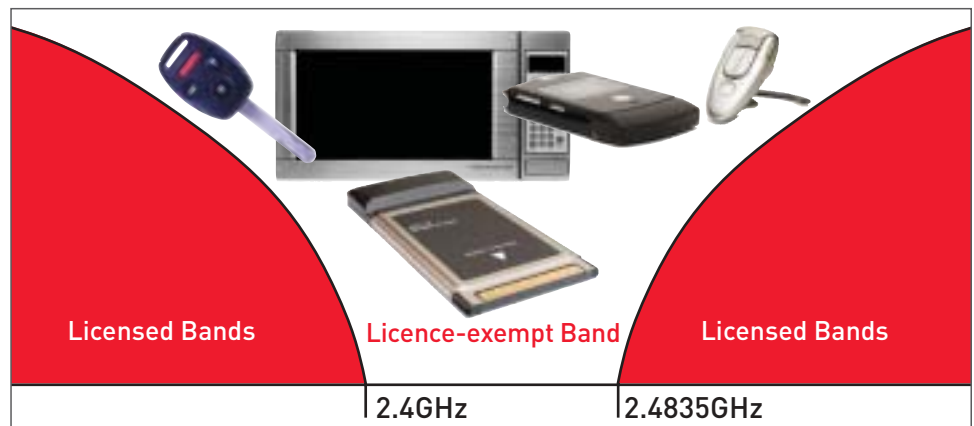
The onus in liberalised spectrum is on licensees to minimise the probability of mutual interference. Note the use here of 'minimise the probability of' rather than 'avoid'. The flip-side of liberalisation has seen responsibility shift to in-building solutions themselves to ensure that multi-technology environments do not suffer intolerable interference.

Another thrust from Ofcom has been to increase the amount of unlicensed – or licence-exempt to use Ofcom parlance – spectrum, to allow businesses to develop and bring to market new technologies and services without the need for a licence. In licence-exempt spectrum no one has control over who uses the spectrum, but power constraints do exist to reduce the probability of interference. Despite this, even Ofcom states that: "users need to be aware that there are no guarantees that the (licence-exempt) spectrum will be free of interference...there (could be) too much interference for (a device) to work in their vicinity."*

*"A Guide to the Spectrum Framework Review"
Ofcom, September 2005

The most widely known licence-exempt band is the industrial, scientific and medical (ISM) band around 2.4GHz. Wi-Fi operates here (both 802.11 b and g variants) and shares this narrow frequency band with other unlicensed devices such as Bluetooth, TV video senders, medical equipment - and even microwave ovens. With all these different technologies vying to use the same band there are necessarily limits on usable bandwidth and greater potential for cross-device interference, as illustrated in Figure 4.

FIGURE 4:
The 2.4GHz ISM band: some of the many different devices competing to use this narrow, licence-exempt wireless environment



Multiple radio signals interact with each other in indiscriminate and unpredictable ways. This fundamental maxim underscores an unbending principle about dealing with interference issues for wireless: the wireless environment in a building, campus or metropolitan environment inherently exists as a single whole and must be designed and managed as a single whole.

THE INDOOR SOLUTION

The answer to the problems surrounding indoor wireless is not to build more outdoor base stations but rather to provide effective and efficient in-building service through a dedicated, discrete in-building system. And only by treating wireless holistically can propagation be optimised, the effects of interference be minimised and effective performance realised.

But designing wireless networks illustrates Metcalfe's Law: they do not scale easily, and they become complicated very quickly. Installing one Wi-Fi access point is easy; installing ten is not. Metcalfe's law tells us there are at least 55 different interference paths between ten access points and a single client device. This principle applies to each technology, but gets multiplied again in multi-technology environments. However, wireless systems designed and installed specifically for use in-building have been seen more and more over recent years, mainly driven by 2G operators as problems arose in particular environments.

But the days of installing separate wireless systems for each operator, or different technology (PMR, TETRA, Wi-Fi...) are now short-lived. With the explosion in the use of wireless, and the multitude of wireless technologies now required inside a building, the only viable solution is a comprehensive, properly designed in-building system which supports all relevant technologies.

Such systems tend to be built around a cable or fibre infrastructure with antennas at strategic locations throughout the interior. The benefits of installing a single, universal infrastructure that supports all wireless technologies - delivering services when and where users need them - are both many and clear, and a future Red-M White Paper will cover the topic of such a Universal Wireless Infrastructure in more detail. But there are other challenges to providing the required wireless service inside or outdoors - and not just technical ones.

BUSINESS CHALLENGES

While the technical challenges of making wireless work effectively can be daunting enough, there are a raft of business challenges that must be considered too, among them security and health & safety concerns, the likely business impact of poor or non-existent wireless services, the negative effects of uncontrolled wireless growth, and the financial risks inherent in not properly taking control of wireless.

SECURITY THREATS

Security is a particular worry. Unlike wired networks, wireless networks have no easily prescribed boundaries. Signals leak outside of buildings where they can be intercepted, and signals penetrate from outside posing an intrusion threat. Both run counter to recent legislation, such as Sarbanes-Oxley & the Freedom of Information Act in the US and the Data Protection Act in the UK, which mandate organisations to adopt responsible attitudes to data protection and storage. Under Sarbanes-Oxley, for example, company directors are personally responsible for the confidentiality, integrity and accuracy of data held.

Wi-Fi networks are arguably most at risk. The Wi-Fi standards do include rudimentary access control and encryption, most usually to the WPA (Wi-Fi Protected Access) and WEP (Wired Equivalent Privacy) standards. But this supposes that these functions have been enabled. The reality is many devices are deployed with their out-of-the-box settings and default administrator passwords. Even if security is enabled it is hardly robust enough to defeat determined attempts at compromising security. There is also a danger that unsecured Wi-Fi enabled devices - laptop computers or access points for example - may be unwittingly attached to corporate networks by well intentioned members of staff, thus creating a way in for intruders.

Security threats are not limited to Wi-Fi, however. Any mobile phone can be used as a listening device and technologies such as Bluetooth create opportunities for hackers to access mobile phones, stealing phonebooks and corporate data, and uploading viruses. The fact is all businesses, whether actively deploying wireless or otherwise, need to manage wireless security risks across the entire range of wireless devices and technologies.

HEALTH & SAFETY

The health & safety issues surrounding wireless are also a source of concern. The high profile media and public interest in new cellular base station plans or in the use of mobile handsets indicates the prevailing attitude to wireless. At work it is an employer's legal responsibility to meet health & safety standards on radio frequency emissions, and see that conditions are safe. In public places the custodians of buildings and open spaces have a duty of care to their visitors. The relevant legislation is EC Directive 2004/40/EC, which the UK's Health & Safety Executive says employers should already be complying with. This states that employers have a legal obligation to:

- Assess and, if necessary, measure the levels of electromagnetic fields (EMF) to which workers are exposed
- Ensure that the Exposure Limit Values, based on ICNIRP** Guidelines, are not exceeded in different frequency bands
- Erect warning signs where EMF levels may cause the Exposure Limit Values to be exceeded
- Provide appropriate information and training

With the effects of radio frequency energy on the human body recognised as cumulative, it is important to ensure legislative compliance, satisfy both employee and public concerns regarding wireless safety and security, and underpin network integrity by taking control of the wireless environment.

**ICNIRP, The International Commission on Non-Ionizing Radiation Protection, is a body of independent scientific experts that provides guidance and advice on the potential human health hazards of non-ionizing radiation exposure. It has published internationally accepted Guidelines that state Reference Levels for limiting exposure to EMF, which are the benchmark for industry compliance. The EC Directive uses these Reference Levels to define Exposure Limit Values.

COVERAGE WHERE AND WHEN IT'S NEEDED

Coverage - ensuring there are no black-spots, holes or dead zones - is an obvious feature of any wireless system. The days of staff being tied to a particular desk, office or even floor are long gone. Hot-desking and flexible working mean people are constantly on the move. They expect telephone service and network access to move with them, extending to outdoor areas too. Effective coverage ensures they are never out of touch. Effective design, by recognised wireless experts, can put that quality of coverage in place.

More and more these days the applications running over wireless are complex and critical to business, with wireless systems required to seamlessly support those applications. To do so properly is again a question of effective system design. The demands of particular applications must be considered when designs are drawn up; indeed the design should revolve around the applications that the system will be required to support. This is especially true in multi-technology wireless environments to ensure cross-frequency interference is avoided.

Wireless users, by their very nature, move around. Networks must be able to cope with the complexities of user mobility as they switch, or get switched, between cells. But if the coverage from the cells overlaps too much, they cause interference. If they don't overlap enough, connections get dropped. There is a trade-off between cell overlap and switching time, and this is very application-dependent. Table 3 shows the different application types.

TABLE 3:
Complex applications require more
sophisticated network design

Standard Applications	Complex Applications
Office-type applications	VPN / Citrix / Remote Desktop
General file server access	Client-Server applications such as centralised databases (e.g. Oracle / SQL Server)
Static internet connectivity	Dynamic internet connectivity (e.g. live video, streaming)
Wi-Fi hot-spots (e-mail and web browsing only)	Wi-Fi hot-spots (voice)
Legacy protocols such as serial communications over IP	Wireless Voice-over-IP / Video Conferencing
Electronic Point of Sale & Chip and Pin	CCTV / Geographical Information Systems / CAD applications
Barcode scanners and general inventory management	Location-based services / Presence applications such as instant messaging

A typical office environment provides a good illustration of these issues: it is clear by now that signal strength varies throughout a building depending on the building's characteristics. For everyday applications such as e-mail and web browsing, different signal levels around the office do not affect system operation - within reason of course, as there must be a minimum level for the network to function - and such signal variations are invisible to the user, whether it's 2G/GPRS on a smart phone or Wi-Fi on a laptop.

Many data applications are built to handle such variances. If signal levels are lower somewhere and delay an e-mail being received from the server for a few seconds, it is not really noticed. However voice, video or other complex applications over wireless have a much higher user sensitivity to delay and drop-outs - a gap in a voice call, or a frozen video screen can be intensely annoying - and thus need a consistently higher signal level across the whole coverage area to ensure call quality is acceptable, or prevent calls being dropped all together.

Many applications today demand an uninterrupted connection: the key element is that the network design is critical, and must take this into account. There are

similar challenges for in-building services in open public spaces such as shopping centres, sports stadia or airport terminals where large numbers of people congregate, many of them expecting to stay in touch with friends and family through talking on a phone or text messaging.

CAPACITY: MORE IS NOT ALWAYS BETTER

As described above, coverage is an obvious feature of any wireless system, but capacity - maximising & guaranteeing performance for the user population and applications in use - is perhaps less so. However, both are key requirements for any wireless implementation. The capacity of wired networks can always be extended by adding more wires, and can be readily partitioned into easily manageable segments. Cables do not interact with each other to any great extent and it is common to include spare capacity when wiring a building by installing multiple cables at the outset.

Wireless networks, by contrast, operate using the radio spectrum, a resource shared by all wireless users and which has limited practical bandwidth. Expanding wireless systems requires a great deal of skill and expertise. And although wireless technologists are continuously finding new ways to pack higher data rates into a given segment of bandwidth, there are physical limitations (dictated by propagation and interference) that cannot be overcome.

Reuse of frequencies (as in cellular networks) does allow system capacity to be increased, but only if systems are properly deployed: it is not simply a case of adding more access points or base stations. Indeed, simply adding more access points or base stations may actually worsen performance and data rates if systems are not properly planned and managed. The truth is that when looking to increase capacity, more is not always better. Good network management is about expansion and growth to meet changing demands. It should be a proactive process with constant monitoring of the wireless environment to show up any likely trouble spots and to allow coordinated expansion to meet demand.

SET THE POLICY, MANAGE THE POLICY

Multi-occupancy commercial premises such as managed offices or shopping centres need to embrace the concept of 'wireless policy': this is the process of setting rules and objectives at the outset for the use of wireless, and ensuring they are adhered to. Where buildings have multiple occupants they may all be eager for effective wireless services in their own part of the shared space. If it is not available any other way they may be tempted to install hardware of their own to get it. But because of the ever present issue of interference, this kind of uncontrolled, uncoordinated expansion creates more problems than it solves. The matter then becomes one of policy, planning and management. If the owners or landlords of such shared facilities, whether a shopping centre or corporate HQ, create wireless policies for their buildings and tenants and/or users, it is possible to avoid the problems of ad-hoc implementation and piecemeal expansion.

Better yet, property owners have the chance to turn a potential headache into a lucrative opportunity by offering wireless services of their own, much in the same way they already provide tenants with other utilities like gas, electricity and water. Wireless is now the 4th utility. Not only can they sidestep the pitfalls of wireless they can also open up brand new revenue streams. Imagine a shopping centre with neighbouring stores all struggling to use wireless EPoS terminals on the same or adjacent Wi-Fi channels. With shops unable to go on line to authorise a card payment the sale is lost, the customer leaves unhappy and the effect on business potentially damaging. So it is not enough to solve all of the wireless problems of today but then leave the resulting system to its own devices. It needs constant, perhaps even daily, policing and supervision if it is to remain effective.

MANAGING AIRSPACE

Airspace is defined as the air in and around buildings in which wireless operates

Wireless remains a complex and hard-to-master technology, especially indoors. It does not respond to the same approaches and solutions as hard-wired networks. It does not follow the same rules. What has been found to work by trial and error today will, in all probability, not work tomorrow.

Yet wireless is growing as an influential force in both the business and consumer market places. Its effectiveness or otherwise can determine the outcome of big business deals and it can be a decisive factor in the success of a new restaurant or shop. It pays to make sure wireless works, and works well.

Independent of equipment vendors and technologies, Red-M enables organisations to fully realise the benefits of wireless systems by delivering high quality solutions through an integrated five step cycle of best practice. This is a comprehensive, all-embracing approach underpinned by a combination of unique technologies.

This five step cycle is offered in full or as individual steps for all wireless systems, wireless devices and radio spectrum as appropriate for each individual customer. Such a far-reaching approach is necessary because the challenges of wireless are numerous, varied and seldom the same from one case to the next. The five step cycle is not just a set of products and services; it is a combination of best-practice strategies and processes aimed at taming the wireless environment.

The five step cycle of best practice comprises a number of different and complementary elements that owners, managers and users of wireless airspace can choose to use at different stages in their wireless deployments.

FIGURE 5:

A Five Step Cycle of Best Practice



CONSULTING

Consulting usually encompasses the development of a wireless strategy that aligns closely with the business needs of the customer. Often delivered by the experienced Red-M consultancy team, this will consider the advantages and disadvantages of various wireless technologies and techniques, or even if wireless is appropriate at all. The end result is a clear technical specification for progressing projects to the next phase whilst ensuring that wireless systems do not conflict with each other, dovetail with the rest of the business, operate within health and safety guidelines and meet other necessary requirements.

AUDIT

Comprehensive radio and/or physical audits of radio systems in an environment provide a clear understanding of the performance of all current wireless activity in the airspace. Red-M's survey capabilities span all wireless technologies including Cellular (2G, 3G & GSM-R), PMR, Wi-Fi and WiMAX as well as electromagnetic exposure levels. Measurements taken across all areas will show the status of current wireless networks, allow existing coverage and performance to be mapped. A benchmark may be created as a baseline for subsequent comparison or as a comparison of the performance of differing networks.

DESIGN

This step takes the site or area-specific plan and translates it into a working, fully-optimised design for a wireless infrastructure to support current and future business needs. Where appropriate in creating a design, Red-M may use its Universal Wireless Infrastructure approach based around a multi-technology, multi-operator infrastructure containing a mix of passive and active components. In these cases, appropriate isolation between network operators and interference minimisation is a key element. The design will also address all health and safety and environmental concerns and comply with necessary legislation and industry best practice.

IMPLEMENT

This step follows sign-off of the design. Systems may involve just a single wireless technology, supported by cabling, or a whole range of multiple wireless technologies including Cellular (2G, 3G & GSM-R), PMR, Wi-Fi and WiMAX. Effective coordination and project management is essential to keep disruption to a minimum. Resilience and scalability are also built in where necessary.

MANAGE

Management of the finished wireless infrastructure is key to its efficient ongoing operation, control and security and also for ensuring adherence to service level agreements. For this reason Red-M offers a maintenance and management step. This includes a unique Airspace Policy Management service in environments where there are a large number of unlicensed spectrum users. In this way it is possible to maintain customer satisfaction levels through the provision of consistent, reliable wireless services.

ONGOING PROCESS

Crucial to the whole five step cycle of best practice is that it is an ongoing process, repeating in response to changing business and user demands, new wireless technologies and changes in airspace itself; constantly assessing needs and risks, then providing solutions. In this way airspace owners, operators and users can stay in control and avoid any security or technical lapses that might impact their commercial advantage.

CONCLUSION

In-building, campus and metropolitan wireless brings with it real challenges. Different wireless technologies and applications interact and interfere with each other in unpredictable ways. The fabric, fixtures and fittings of buildings add further uncertainties. There is the issue of mobility and maintaining service as users move around. And there are the demands of business-critical voice, video and data applications that mandate quality and consistency of connection.

All these factors lead to one conclusion: the need for considered, expert and holistic design and implementation based on methodology devised exclusively for wireless environments.

Red-M can provide such a solution.

**CORPORATE OFFICES**

Graylands, Langhurstwood Road, Horsham, West Sussex, RH12 4QD, UK
t: +44 (0) 1403 211100 f: +44 (0) 1403 248597

For more information visit www.red-m.com or email info@red-m.com

DOC.REF: WPAP-TAM-0110:3

Red-M

when wireless matters™