

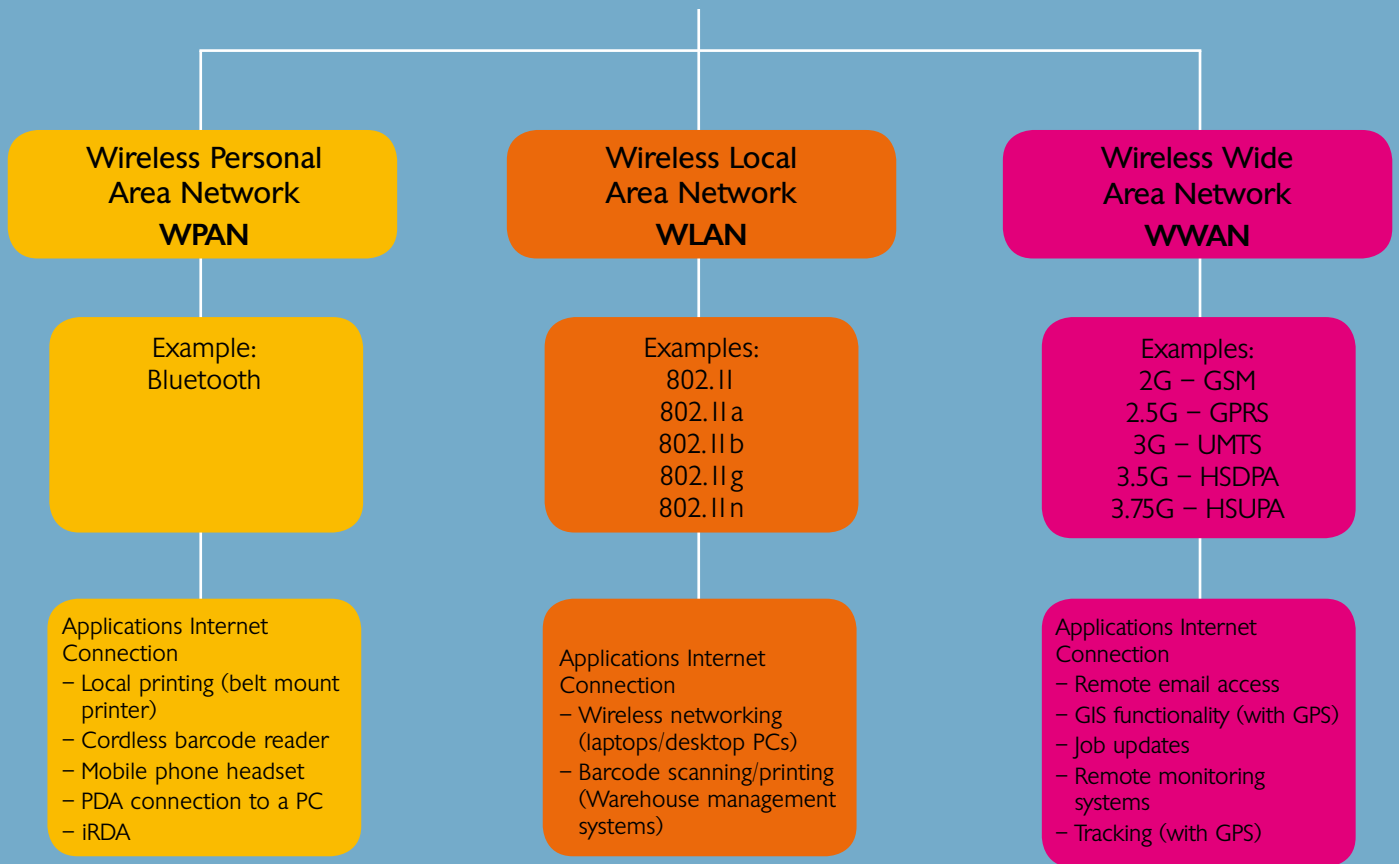


Guide to Wireless Communication

spirit
DATA CAPTURE LTD

Welcome to the Spirit Data Capture Guide to Wireless Data Communication. We hope that you find it useful.

Wireless Communication



Wireless Personal Area Networks (WPANs) operate immediately around a person or device: typically, within a ten metre range. Bluetooth is a common example of the technology used to create a WPAN.

An introduction to Bluetooth

Harald Bluetooth was the king of Denmark in the late 900s. He united Denmark and part of Norway to form a single kingdom. Choosing his name for this standard indicates how important the companies from the Baltic region are to the communications industry.

Bluetooth is a radio frequency standard. It was developed by a group of electronics manufacturers to allow electronic equipment (computers, mobile phones, keyboards, printers, headphones, remote controls etc.) to make connections without the need for wires or cables.

Over 1,000 companies belong to the Bluetooth Special Interest Group (SIG). They use Bluetooth radio instead of wires to connect devices for transferring data.

There are numerous ways in which devices can be connected to one another. For example:

- A personal digital assistant (PDA) can be connected to a PC via a USB cable or a docking cradle.
- A television can be linked to a DVD recorder using SCART or coax cables.
- Hi-fi units can be connected using a wide range of cables (phono, fibre, Neutric).

Few of these various connections use the same types of cables or connectors, because there are so many different standards and sizes available.

However, Bluetooth uses clearly defined standards. This means that a Sony mobile phone will work quite happily with a Plantronics headset. The manufacturer of the phone and the headset is irrelevant as long as they can be connected to each other.

From a user's point of view, these are the key benefits of Bluetooth:

1. It's wireless.
2. When you travel, you don't have to worry about taking any cables with you.
3. You don't have to think about it: Bluetooth doesn't require you to do anything special to make it work. When switched on, the devices find each other and automatically make the connection.
4. It's inexpensive.
5. It's global.

The ways in which we connect things are becoming increasingly complex. It can sometimes seem as if a home or office is being taken over by cabling. This not only looks unsightly but it also harbours dust and can be a safety hazard if it isn't carefully installed.

How Bluetooth works

Bluetooth communicates on a frequency of 2.45 gigahertz. Some existing devices already use this radio frequency (RF) band. For example, the latest generation of cordless phones and some baby monitors and headsets make use of frequencies in the ISM band. Bluetooth's design principles ensure that Bluetooth-enabled devices and other products using the same RF band don't interfere with each other.

To avoid interference with other systems, Bluetooth devices operate at a very low power (1 milliwatt). In comparison, some mobile phones can transmit in hundreds of milliwatts. Bluetooth's low power limits the range of a device to around ten metres. However, even with such low power, the walls of a house or office won't stop the signal completely: they will just reduce its strength.

Although there may be many different Bluetooth devices within the same area, they are unlikely to interfere with each other. This is because Bluetooth uses a technique called spread spectrum frequency hopping (from the early days of wireless data). This enables the device to step across 79 random frequencies. Because the Bluetooth system changes frequencies 1,600 times a second, many more devices can make full use of the available radio frequencies.

Every Bluetooth transmitter frequency-hops automatically, making it extremely unlikely that two will be on the same frequency at the same time. Bluetooth also minimises any disruption to telephones, baby monitors, garage openers etc. because any interference on a particular frequency will only last for a fraction of a second.

When Bluetooth devices come within range of one another, an automatic electronic exchange takes place. This is primarily to establish whether they are compatible; have data to share; or whether one needs to control the other. The user doesn't have to take any action, as the connection should happen within a few seconds.

Once this electronic exchange has occurred, the devices form a small network, called a Personal Area Network (PAN or piconet). This PAN may fill a room (depending on the devices) or be no more than the distance between the mobile phone in your car and your headset. The connected devices randomly hop frequencies in unison, so that they stay in touch with one another and avoid other piconets that may be operating nearby.

To simplify things further, within a normal home environment, there could be a Bluetooth-enabled hi-fi, DVD player, satellite box, TV, cordless telephone and personal computer. When switched on, each of these systems forms its own piconet that communicates with the main unit.

Bluetooth is a radio frequency standard and allows any sort of electronic equipment (computers, mobile phones, keyboards, printers, headphones etc) to make connections without wires or cables.

A cordless telephone has one Bluetooth transmitter in the base and another in the handset. The transmitter is programmed with an address that has been specified for that particular type of device. When the base is first turned on, it sends radio signals asking for a response from any units with an address in that range. The handset responds and a tiny network is formed. From then on, even if one of these devices receives a signal from another system, it will ignore it, as it is not from within the network. All of the other systems perform similar routines, establishing networks among addresses in ranges that have been pre-set by the manufacturers.

Once the networks are established, the systems begin talking amongst themselves, each one hopping randomly through all available frequencies. Because each network is changing the frequency of its operation thousands of times a minute, it's very unlikely that any two or more networks will be on the same frequency at the same time. If they are, the resulting collision will only last for a fraction of a second. Specialist software that is designed to look for these instances will ensure that any corrupted information is ignored.

Bluetooth security

There are some known issues with Bluetooth security. The following are the minimum precautions that you should take:

- Avoid the use of unit keys.
- Use combination keys.
- Perform bonding in an environment that is as secure as possible against eavesdroppers.
- Use long, random Bluetooth passkeys.

Bluetooth specifications

The Bluetooth specification defines a uniform structure that enables a wide range of devices to connect and communicate with each other. There have been a number of enhancements to the Bluetooth specification, with the latest (v4.0) having been released in 2010. In mobile devices, the most commonly used specifications are v1.2, v2.0 and v2.1.

Version 1.2 corrected bugs and issues from the original specification and improved the connection and discovery speed. This version also improved the resistance to radio frequency interference and increased the speed to a theoretical 1Mb/s (although the maximum actual speed is 721 kbits/s).

The major step forward in the specification came with the introduction of v2.0, which is backward-compatible with the previous version (v1.2). The main difference is the introduction of an Enhanced

Data Rate (EDR) for Wireless Personal Area Network (WPAN) faster data transfer. The nominal rate of EDR is about 3Mb/s, although the practical data transfer rate is 2.1Mb/s. The specification is published as 'Bluetooth v2.0 + EDR', which implies that EDR is an optional feature.

Top rugged mobile devices now support v2.1 with EDR and offer improved security by introducing secure simple pairing (SSP). This improves the pairing experience for Bluetooth devices, whilst increasing the use and strength of security. Version 2.1 offers various other improvements, including a reduction in power consumption.

The Bluetooth specification has developed further with versions 3 and 4. These have continued to improve the reliability and speed and have again lowered the power consumption. They are relatively new enhancements to the Bluetooth standard, so they have not yet been widely adopted by the commercial market.

The range of a Bluetooth device is governed by the permitted power output of its transceiver. There are three different classes of device. The table below outlines the range and power required in each case:

Class	Maximum Permitted Power		Range (approximate)
	mW	dBm	
Class 1	100	20	-100 metres
Class 2	2.5	4	-10 metres
Class 3	1	0	-1 metres

A single Bluetooth device can connect with up to seven other active devices in a piconet, which operates with a master to multi-slave connection. The piconet can support up to seven active slaves, but will support other non-active slaves (pairings on your mobile device that aren't currently being used). The Piconet range will vary according to the class of the Bluetooth device. Data transfer rates also vary, depending on whether a synchronous or asynchronous connection is used, and the number of devices in the piconet.

A piconet can have up to three synchronous (SCO) links (using reserved slots set up by the master), with one, two or three slaves. Slots not reserved for SCO links can be used for asynchronous (ACL) links. One master and slave can have a single ACL link. ACL is either point-to-point (master to one slave) or broadcast to all the slaves. ACL slaves can only transmit when requested to do so by the master device.



A WLAN enables a mobile user to connect to a Local Area Network through a wireless radio connection. High speed WLANs are now available and can be implemented quickly and at low cost. A range of standards specify the technology for a WLAN - including 802.11 a, b and g.

What is 802.11?

The origins of 802.11 wireless can be traced back to the early 1940s. In 1942, Hollywood actress, Hedy Lamarr, patented the basic principles of modern spread spectrum technology. The frequency-switching system for torpedo guidance was two decades ahead of its time. Her original concept was based around 88 channels – the same number of keys as on a piano – and formed the basis of the 802.11 wireless systems used today.

During the 1950s, the military began to develop the technology, using (at the time) modern electronics. By the 1960s, spread spectrum radio had become a satellite communications technology. Encrypted data links were used by many national intelligence services. It is only during the last ten to twelve years that spread spectrum radio devices have become part of everyday life – in the form of cordless phones, burglar alarms, wireless local loops (WLL), and wireless local area networks (WLANs).

Standards

Standards are important, as they encourage manufacturers to design products that are 'open standard compliant'. However, this doesn't always mean that all manufacturers will follow the standards. It can still be frustrating when one manufacturer's equipment won't work consistently with another's!

Originally, there was no common standard for spread spectrum radio devices. As recently as the early 1990s, there were many different ways of using this technology. However, none were interoperable. The two well known ones were FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum). FHSS was the slightly more secure method, although only marginally.

Towards the end of the 1990s, the IEEE (Institute of Electrical and Electronic Engineers) developed the 802.11b standard, which has helped to define the modern 802.11 radio system.

The 802.11b committee of the IEEE now develops standards for Local and Wide Area Networks. For example, the 802.3 committee sets standards for Ethernet-based wired networks; the 802.15 group develops standards for personal area networks; and the 802.11 committee produces standards for WLANs.

Variations of 802.11

These are the current main 802.11 standards:

- 802.11a is a different standard for WLANs and operates in the 5 GHz frequency range, with a maximum data rate of 54 Mbps.
- 802.11b, or Wi-Fi, is a WLAN standard that operates in the 2.4 GHz

spectrum, with a bandwidth of 11 Mbps.

- 802.11g is a WLAN standard that operates in the 2.4 GHz frequency, but with a maximum data rate of 54 Mbps. This is now the most common type of network.
- 802.11n is the latest standard to be released and has improved the network throughput. There is a significant increase in the maximum data rate: from 54Mbps to 600Mbps.

The main infrastructure manufacturers are producing 802.11n-ready hardware which still offers support for 802.11a, b and g. However, mobile devices aren't yet readily available with 802.11n-compliant radios, so investment in this standard is still very much at the future proofing stage.

Many systems that deploy the 802.11g standard also include support for 802.11b, as both 11Mb and 54Mb devices run on the same frequency. Some suppliers even incorporate bespoke software that allows transmission at higher data rates. This will only work if all the systems are from the same manufacturer. Generally, it is better to avoid using these special software settings, as the results can be unpredictable.

Other task groups of the IEEE are working on enhanced security (802.11i), spectrum and power control management (802.11h) and quality of service (802.11e).

The implementation of a wireless network broadly involves one of the following two common types of architecture:

Distributed access point architecture

This refers to the original design of 802.11 standard-based access points. These integrate all of the WLAN (Wireless Local Area Network) functionality within a single piece of hardware.

The core wireless functionality is implemented on each of the access points, including access control and encryption, as well as QoS (Quality of Service) functions. All 'enterprise' class access points also provide some higher layer functionality (such as protocol filtering, address filtering, access control lists and configuration tools).

Vendors of these access points also market tools that enable them to be centrally managed. Whilst this capability is probably a requirement of every organisation with a medium or large wireless network, these centralised tools are not essential for the operation of the network. The beauty of this type of architecture is that the access point is the only network component required to provide wireless LAN capabilities.



The 802.11 architecture simplified wireless solutions, so that all that is needed to create a WLAN is to plug an access point into the network and install a client radio in your computer.

The distributed access point architecture is intended to be extremely simple. Wireless becomes an integral part of the overall network. Access points connect directly to the network.

Centralised WLAN switch architecture

This architecture requires two devices to provide a wireless network. The access points are more commonly known as access ports, as they generally hold little or no functionality other than propagating the wireless signal.

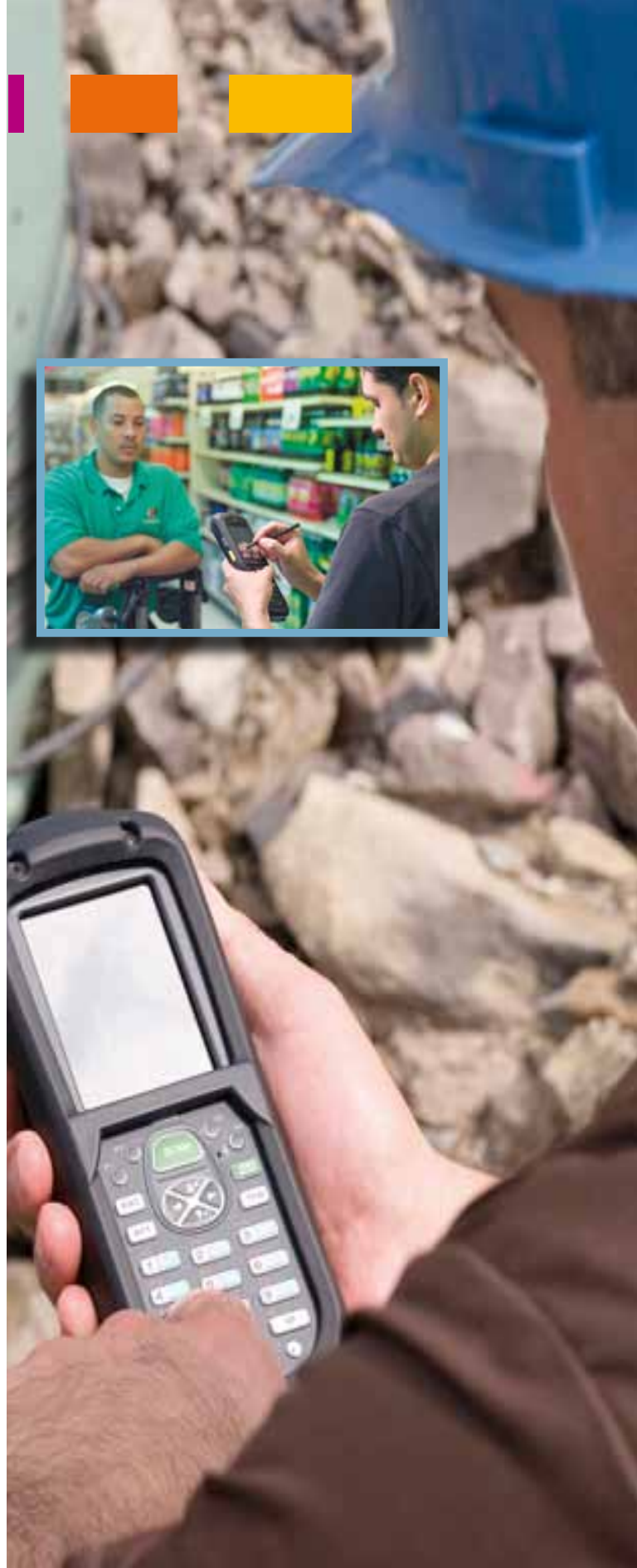
Each WLAN switch vendor makes different choices about how to divide the functionality between the switch and the access ports. Some vendors choose to implement most of the functionality in the WLAN switch. Others decide that some functionality 'belongs' at the network edge and so they put this functionality (e.g. data encryption and access control) in the access ports.

One essential characteristic of all centralised WLAN switch architectures is that all of the

traffic either to or from the wireless network must pass through the switch, which can therefore completely control the flow of wireless traffic.

Each architecture has its own merits, depending upon the size and complexity of the wireless solution requirements. The following factors should be considered when selecting a wireless architecture:

- Resilience
- Security
- Ease of management / support
- Coverage
- Cost
- Scalability



Standards are important, as they generally encourage manufacturers to design products that are 'open standard compliant'. However, this doesn't always mean that all manufacturers will follow the standards.

802.11b/g security

The following are examples of some potential security threats for WLAN networks:

Eavesdropping (disclosure of data)

Eavesdropping on network transmissions can result in the disclosure of confidential data, unprotected user credentials and identity theft. It also allows sophisticated intruders to collect information about your IT environment. This can be used to mount an attack on other systems or data that might not otherwise be vulnerable.

Interception and modification of transmitted data

If an attacker can gain access to the network, they can insert a rogue computer that can intercept and modify network data communicated between two legitimate parties.

Spoofing

Ready access to an internal network allows an intruder to forge apparently legitimate data in ways that wouldn't be possible from outside the network (for example, a spoof email message). People, including system administrators, tend to trust items that originate internally far more than something that originates outside the corporate network.

Denial of service (DoS)

A determined assailant may trigger a DoS attack in various ways. For example, radio level signal disruption can be triggered using something as low tech as a microwave oven. There are more sophisticated attacks that target the low level wireless protocols themselves, as well as less sophisticated attacks that target networks by simply flooding the WLAN with random traffic.

Free-loading (resource theft)

An intruder may want nothing more sinister than to use your network as a free point of access to the Internet. Although not as damaging as some of the other threats, this will, at the very least, lower the available level of service for your legitimate users and may also introduce viruses and other threats. In its simplest terms, free-loading has recently been shown in a Court of Law to constitute theft under the terms of the UK's Theft Act.

Accidental threats

Some features of WLANs make unintentional threats more real. For example, a legitimate visitor may start up a portable computer with no intention of connecting to your network. However, they may then be automatically connected to your WLAN. The visitor's portable computer is now a potential entry point that allows viruses to enter your network. This kind of threat is only a problem in unsecured WLANs.

Rogue WLANs

If your company officially has no WLAN, you may still be at threat from an unmanaged WLAN springing up on your network. Low-priced WLAN hardware bought by enthusiastic employees can open unintended vulnerabilities in your network, especially if no steps are taken by the employee to install basic security measures. Most hardware suppliers have a standard SSID and no other security is enabled. Most hackers will know that almost all new users (and some who should know better) don't bother to change basic 'out of the box' settings.

Protecting your radio network

Nothing is totally secure. However, you can protect your network by making it more difficult for others to gain access to it.

There are a few simple ways to protect yourself against the unauthorised use of a radio network. The most obvious is to change ALL of the standard settings on your chosen equipment to settings that only you know. This is easy to achieve and doesn't take too long, once you understand the basic principles. The absolute minimum steps you should take are:

Change the SSID – this is the first thing that your Access Point uses to allow registration. Most unscrupulous individuals will know all of the standard settings. Even though they may not do any lasting harm on your network, don't give them the opportunity to gain access to it! You won't know they are there but they could cause slow response times and might even gain access to sensitive information.

Use the latest WPA2 security protocol – if your hardware allows it. Most do, as this is a way to stop authentication to your AP. If your hardware doesn't support the latest standard, you could use either WPA-PSK or even WEP authentication. WPA2 works for small offices and home networks with a pre-shared key; for larger networks it operates with an 802.11x authentication server.

Reduce the coverage of your AP by lowering the radio power – so that the coverage is contained within the confines of your property. However, not all devices designed for the SOHO or home user allow this. If you want this feature, you may find that you'll have to spend a little more at the outset. Motorola and Cisco 'enterprise' quality units offer this option, plus some bespoke settings.

There are other ways in which security can be tightened. Wireless Intrusion Protection systems are available, which detect attacks on the wireless network. These systems can be configured to alert staff about an attack and to carry out specific actions. However, these come at a cost which can be prohibitive, unless the data and restricted access on your network warrant it.

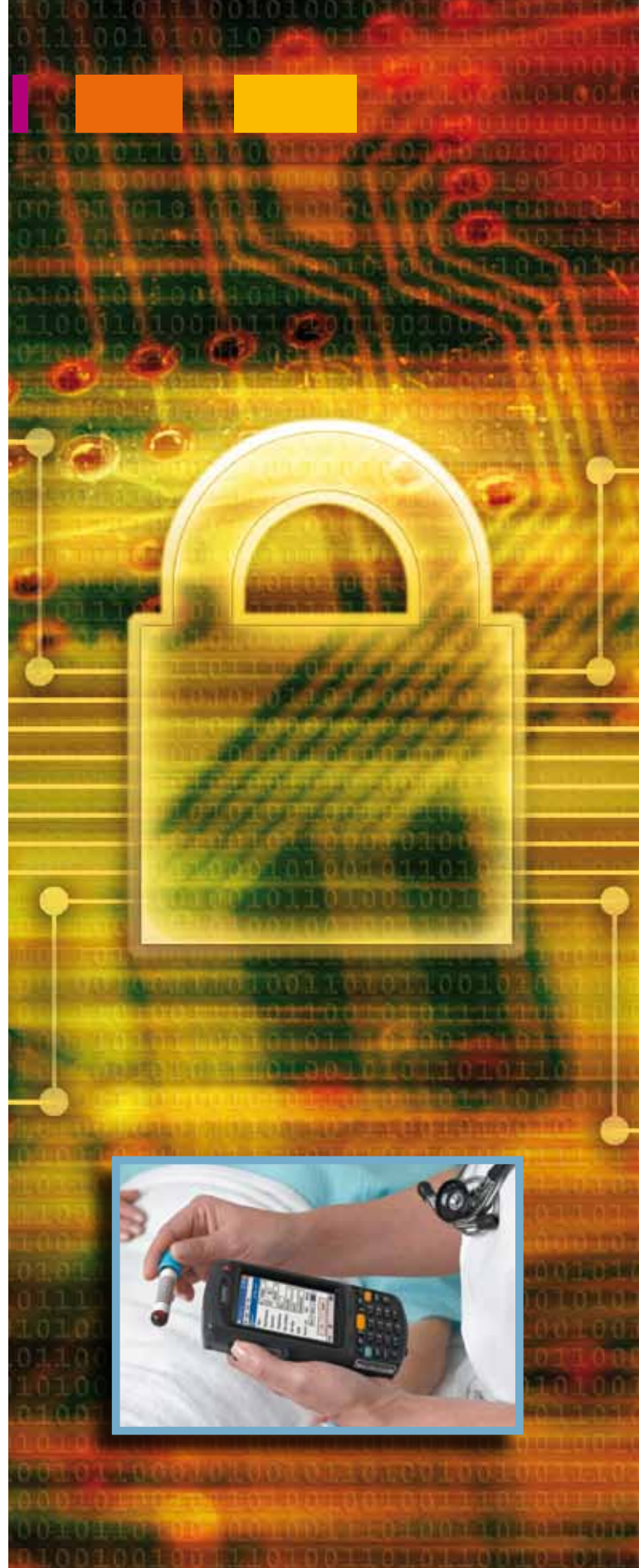
The most important thing to remember is to NOTE DOWN all of the settings you change; the new settings; and the secured storage location. If you forget and you have a problem of some kind or want to add another device, it will be very difficult, if not impossible, to configure it without this information.

Outdoor wireless solutions

The most common use for external wireless solutions is to provide a bridge between two or more buildings over a large geographical area. Many organisations are now opting for wireless bridges to provide high-speed network connectivity. Typical examples include a university campus or any business with multiple buildings in the same area.

Wireless bridges provide fixed links between two or more segments of the network, usually in different buildings. They offer a degree of control of the network that is unavailable with leased lines. Based on the industry-standard IEEE 802.11 specifications, they deliver a performance that is several times faster than E1 or T1 leased lines, at a fraction of the cost.

A more recent application for outdoor wireless is to provide high-speed Internet connection to remote communities that can't access standard broadband networks.



Wireless Wide Area Networks (WWANs) provide access to information anytime and anywhere that there is cellular (data) coverage. This means that you can send and retrieve email and access other corporate information whilst you are away from the office. You can even browse the internet!

Wireless WANs cover a much greater area than wireless LANs. They are generally used to enable the mobility of the entire network or to link all of a company's branch offices.

How does it work?

In WWANs, communication occurs via radio signals over analogue, digital cellular or PCS networks. However, signal transmission through microwaves and other electromagnetic waves is also possible.

Today, most wireless data communication takes place across 2G cellular systems (the term used to describe the GSM second generation digital network technology). The traditional analogue networks were originally designed for voice rather than data transfer and have some inherent problems. However, 2.5G (GPRS) and the new 3.5G digital cellular networks are fully integrated for data / voice transmission. With the advent of 3G+ networks, transfer speeds should also increase greatly.

WWAN connectivity requires wireless modems and a wireless network infrastructure, provided as a chargeable service by a wireless service carrier. Portable devices receive communications as the connected wireless modems and networks interact via radio waves. The modem directly interfaces with radio towers, which carry the signal to a mobile switching centre. From here, the signal is passed to the appropriate public or private network link (i.e. telephone, other high speed line, or even the Internet).

2G – GSM

GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in both Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most popular of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitises and compresses data, then sends it down a radio channel with two other streams of user data, each in its own time slot. It operates on either the 900 MHz or 1800 MHz frequency band.

GSM has become the de facto wireless telephone standard in Europe. According to the GSM MoU Association, it has over 120 million users worldwide and is available in 120 countries. As many GSM network operators have roaming agreements with foreign operators, users can often continue to use their mobile phones when they travel to other countries.

GSM, together with other technologies, is part of an evolution of wireless mobile telecommunication that includes High-Speed Circuit-Switched Data (HSCSD), General Packet Radio System (GPRS), Enhanced Data GSM Environment (EDGE) and Universal Mobile Telecommunications Service (UMTS).

2.5G – GPRS

GPRS is a packet-based wireless communication service. Data rates are typically 56 Kbps, which allows continuous connection to the Internet for mobile phone and computer users. The higher data rate allows users to take part in video conferences and to interact with multi-media websites and similar applications using mobile handheld devices as well as notebook computers. GPRS is based on GSM communication. It complements existing services, such as circuit-switched cellular phone connections and the Short Message Service (SMS).

GPRS packet-based services should cost users less than circuit-switched services, because communication channels are being used on a shared-use, as-packets-are-needed basis rather than being dedicated only to one user at a time. It should also be easier to make applications available to mobile users, because the faster data rate means that middleware (currently needed to adapt applications to the slower speed of wireless systems) will no longer be needed.

As GPRS becomes more widely available, mobile users of a virtual private network (VPN) will be able to access the private network continuously, rather than having to use a dial-up connection.

GPRS also complements Bluetooth. In addition to the Internet Protocol (IP), GPRS supports X.25, a packet-based protocol used mainly in Europe. GPRS is an evolutionary step toward Enhanced Data GSM Environment (EDGE) and Universal Mobile Telephone Service (UMTS).



3G – UMTS

3G is the third-generation wireless technology. It refers to the developments in personal and business wireless technology, especially mobile communications. 3G is now being offered by UK network providers. It includes capabilities and features such as:

- Enhanced multi-media (voice, data, video, and remote control)
- Usability on all popular modes (cellular telephone, email, paging, fax, videoconferencing and web browsing)
- Broad bandwidth and high speeds (upwards of 2 Mbps)
- Routing flexibility (repeater, satellite, LAN)
- Operational at approximately 2 GHz transmitting and receiving frequencies
- Roaming capability throughout Europe, Japan, and North America

3.5G or 3G+ HSPA (HSDPA and HSUPA)

HSPA (High Speed Packet Access) is a family of mobile broadband technologies comprising HSDPA (High Speed Download Packet Access) and HSUPA (High Speed Upload Packet Access). These are enhancements to 3G telephony communications (also called 3.5G, 3G+ or turbo 3G) which allow networks based on UMTS to have higher data transfer speeds and capacity.

Current HSDPA deployments support down-link speeds of 1.8, 3.6, 7.2 and 14.0 Mbit/s. HSUPA supports up-link speeds of up to 5.76 Mbit/s.

Whilst 3G is generally considered to apply mainly to mobile wireless, it is also relevant to fixed and portable wireless solutions.

The ultimate 3G+ system might operate from any location on or over the earth's surface, and is used by homes, businesses, government offices and medical and military establishments. It can be used in personal and commercial land vehicles, private and commercial watercraft and marine craft, and private and commercial aircraft (except where passenger usage restrictions apply). It can also be used by individuals (e.g. when walking) and even by spacecraft!

Proponents of 3G+ technology promise that it will "keep people connected at all times and in all places." Researchers, engineers and marketers are faced by the challenge of predicting how much technology consumers will actually be willing to purchase. Recent trends suggest that people sometimes prefer to be disconnected, especially when on holiday!

Another concern involves privacy and security issues. As technology becomes more sophisticated and bandwidth increases, systems become increasingly vulnerable to attack by malicious people (hackers), unless countermeasures are implemented to protect them against such activity.

Wide area wireless networks can be an enormous benefit to corporations because they can extend the reach of an enterprise application across large geographical areas and even across different countries. However, this expanded range also increases the vulnerability of the company's devices, applications and data. To safeguard their viability, the security of this new infrastructure must be validated.

For a mobile device to communicate over GPRS/3G/HSPA, it must use an APN (Access Point Name), which can be either public or private. Every network provider has a public APN. When the SIM card is enabled for data (e.g. GPRS/3G), the public APN is added by default. This APN is open for everyone to use.

A private APN provides customers with a secure connection for the data, which never goes onto a public network. This reduces the complexity of the communications path and is one less point of failure in the system. As it is secure, it eliminates the chance of any attacks by spammers etc.

Mobile VPN (Virtual Private Network) software can be used in conjunction with either a public or private APN to create a secure connection to a corporate LAN (Local Area Network). This provides the same level of security and network functionality as any PC on the corporate network. The software also provides added security features to completely control the applications and network resources, and ultimately grants access to the mobile devices in the field.



WWAN complementary technologies

GPS overview

The GPS (Global Positioning System) is a constellation of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. These are accurate to within about ten metres for most equipment. Using special military-approved equipment, this accuracy can be improved to within one metre. GPS equipment is widely used in science and has now become sufficiently low cost that almost anyone can own a GPS receiver. The GPS is owned and operated by the US Department of Defense. However, it is available for general use around the world. Here is a brief summary of how it works:

- 24 GPS satellites and three 'working spare' satellites are in orbit 10,600 miles above the Earth. The satellites are spaced so that from any point on Earth, four satellites will always be above the horizon.
- Each satellite contains a computer, an atomic clock and a radio. With an understanding of its own orbit and the clock, it continually broadcasts its changing position and time. (Once a day, each satellite checks its own sense of time and position with a ground station and makes any minor corrections).
- On the ground, a GPS receiver contains a computer that 'triangulates' its own position by getting bearings from three of the four satellites. The result is provided in the form of a geographic position (longitude and latitude).
- If the receiver is also equipped with a display screen, this position can be shown on a map. If a fourth satellite signal can be received, the receiver / computer can calculate the altitude as well as the geographic position.
- If you are moving, your receiver may also be able to calculate your speed and direction of travel and give you estimated times of arrival to specified destinations.

The GPS is being used in science to provide data that have never been available before in such quantity and with such a degree of accuracy. Scientists are using GPS to measure the movement of the arctic ice sheets, the Earth's tectonic plates and volcanic activity.

GPS receivers are now becoming consumer products. In addition to their outdoor use (for hiking, cross-country skiing, ballooning, flying, and sailing), receivers can be used in cars to give the driver's location, along with traffic and weather information. GPS can be combined with GPRS to track the movement of vehicles or people.

The adoption of GPS technology in everyday consumer products has highlighted potential problem areas with the technology. These include tracking difficulties within built up urban areas, where it is hard for devices to obtain and maintain a 'fix' or location. Some devices are therefore now equipped with Assisted GPS – they use GPRS/3G data communications to obtain the latest satellite information from an online database. They also have mobile phone mast triangulation. A mobile device has therefore become a very powerful tracking tool in all environments – and much more than just a GPS receiver.





Have you seen our free technology guides?

- All about barcoding symbologies
- Technology trends forecast – mobile computing and data capture
- Buying a rugged handheld mobile computer and more...

Subscribe to our *free email newsletter* for innovative ideas designed to help you to improve your profitability, accuracy and customer service.

Spirit is a rugged mobile data capture specialist. We offer hardware, software and pre- and post-sales support. We specialise in delivering innovative and cost effective solutions across many industries. If you would like further advice, please contact us at:

t: 01928 718800 f: 0870 762 2824
 email: helen.jones@spiritdatacapture.co.uk
www.spiritdatacapture.co.uk/product_technologies_wirelessmobilecomputing_wirelessnetworkinfrastructure.asp

