

UnderstandIT

From **MAY DAY CONSULTING LIMITED** in association with **FACILITATORS UK**

A publication designed to inform and enable businesses to understand the implications, costs and advantages of using Information and Communications Technology. Distributed through Chambers of Commerce.

WIRELESS NETWORKS, SECURITY AND INTERNET ACCESS

The whole area of mobile computing and wireless networking has seen major developments in the past year. Many of our clients are enquiring as to how this technology can be applied effectively.

The following notes will hopefully explain how the different components of this technological jigsaw can fit together, and some of the things to remember when configuring your own network, whether it be in the office, or even at home.

In a previous *Understand IT* article, we briefly described the concept behind Wireless Networking (see November 2002 edition). Briefly, a wireless network functions in much the same way as a conventional office network - it connects two or more computers together in either a "peer-to-peer" configuration (this is where a number of computers are inter-connected and share files, folders or printing devices etc between them on an equal footing). Alternatively, it uses a "client/server" model, with a central server providing file and service sharing with its "client" computers.

The principal difference between conventional and wireless networking is perhaps obvious. The former uses copper cabling (Unshielded Twisted Pair or UTP) to interconnect the devices on the network. The latter uses wireless technology and therefore is free from the constraints of physical cabling. This brings obvious major advantages, both in a business and increasingly in a home environment.

Whereas in a conventional network, the key components are Network Interface Cards (NICs) which are located in each computer, providing the connection point for the network cabling. In a wireless network, the key components include the central "Access Point", which is simply a radio "base station" that communicates with the other network devices.



Wireless Access Point/Router

Typically, the Access point will also contain a small number of ports to connect conventionally cabled devices, and usually the connection point to the Internet.

Each network computer then needs to be equipped with a wireless card that provides the same function as the NIC, but communicating via radio frequencies with the Access Point. Most manufacturers provide cards for both desktop and Notebook PCs.



Wireless card (PC)



Wireless card (Notebook)

The advantages of wireless networking are obvious, and the component costs are falling fast in real terms, making it an attractive proposition for many home users too. Many homes now have more than one computer, particularly if the family is large. Now that there is no need for running unsightly cabling around a home, wireless networking allows those in a household to either share information, or more likely share a single broadband internet connection.

Wireless Network Security

For most businesses, and arguably, home users as well, the subject of security is upper-most when implementing a local area network. With a conventionally "wired" network, security is important, since a connection to the Internet can provide an open door to your network. With a wireless network, this security should be of even greater concern, since anyone with a notebook PC and a wireless card, can, in theory gain access to your network simply by entering your office building, or even sitting in a car outside your office. The range of most wireless network Access Points is between 50 and 300 metres, depending on the environment.

Fortunately, the industry standards for wireless networking (conforming to the memorable 802.11b or 802.11g definitions) provide some inbuilt security features.

In a basic wireless network configuration, there are two levels of security that can be implemented:

- The first is to define a discreet name for your network. The manufacturer of the network components will normally have provided a default name, but since this will be the same for all their networks, it is wise to change it to something that only users within your organisation or home will know.

This name is referred to as the SSID (**S**ervice **S**et **I**dentifier) and is configured by entering the setup configuration of your Access Point device (see the manufacturer's operating manual on how to access the setup of your particular device). With in the set up, you will be able to re-define the SSID for your network.

Then each computer that you wish to have access to your network will need to configure their wireless card to search for and connect to your network (NB: a computer can be configured to search for and connect to more than one network – this is useful if for example a notebook user wishes to access the Internet via a public “hotspot”; see below for more information on Hotspots). The SSID is configured by going to CONTROL PANEL and double-clicking on NETWORK CONNECTIONS and then selecting the WIRELESS NETWORK CONNECTION and PROPERTIES. On the WIRELESS NETWORKS tab, you can specify the SSID under the CONFIGURE button.

- The second level is to implement the security protocol built in to the 802.11b/g protocol called WEP (an also memorable Wired Equivalent Privacy). This facility encrypts the information flowing between the devices on a wireless network, to avoid unwanted “eaves-dropping” on that information.

The above steps might be a little too complex for the average person to undertake, but seeking advice from your IT Support organisation, or contacting May Day Consulting (on 01224 697457) may be necessary to ensure that security on your wireless network is set up correctly.

WIRELESS HOTSPOTS

Following on from the article above, with the advent of truly mobile computing, a number of enterprising companies and organisations have installed publicly available Access Points (typically providing access to the Internet via one of the major telecommunications providers). They are usually located in public places – railway stations, airports, coffee bar or restaurant chains etc.. The objective is to permit anyone with a laptop computer or handheld PDA (Personal Digital Assistant) equipped with a wireless network card to access the Internet whilst using their establishment(s).

In order to be validated to that particular vendor's network, you will normally have to be a subscriber to the relevant network or Internet Service Provider.

However, this can be done often by purchasing a card which provides a User ID, password and either a set number of hours of access time, or in some cases unlimited time over a specific time-frame. The areas in which the wireless radio access are available is normally referred to as a “Hotspot”, and extends to the 50-300 metre range defined by the wireless protocol defined in the previous article. You can now wait in the station or airport, or enjoy a coffee, whilst surfing the Internet and checking your email etc.

WIRELESS BROADBAND

On the same theme as all other articles in this edition, the following explains what is meant by Wireless Broadband services. These services are now being discussed widely within the industry and a number of international industry standards are in the process of being ratified.

Basically, the idea is to provide very high-speed Internet access using the radio spectrum. Wireless networking is capable of offering comparably fast transmission speeds and is infinitely more flexible than the conventional cable method of providing access to the Internet, particularly in rural areas, where there is no cable infrastructure to use.

One of the standards currently in the process of being developed will provide for “fixed” radio links running at up to 70Mbps (70 million bits per second) over a range of up to 70Km – clearly good news for rural users when the technology comes to the market place.

Another standard is aimed at providing interconnection between the existing wireless networks and maybe mobile users travelling at speed (on trains, on aircraft, or on the road). The ability to move from a “conventional” hotspot into a fast moving train, or even onto an aircraft and have unbroken Internet access, similar to that experienced by mobile phone users, maybe attractive to some business users in the future.

SMALL BUSINESS - FINANCE

Money is often the topic that creates most anxiety: How much will I need? How much will I make? What if I don't earn enough to pay the bills? Will anyone lend me what I need? Answers to these and other questions can be found at:

http://www.bgateway.com/factsheet_intro.asp

Here there are fact sheets to tackle your money questions, from what you need to know about investment, to practical advice on financial forecasting.

We wish to acknowledge with thanks that some of the material contained within this publication has been sourced from Computer Weekly.

May Day Consulting Limited and your Chamber of Commerce have endeavoured to ensure the accuracy of the information contained in this publication, but do not accept liability for any inaccuracy or omission contained within it.

Information on other Business and IT services can be found on our web site at: <http://www.maydayconsulting.co.uk> or by calling Alan Finch on 07968 262079.

May Day Consulting Ltd
.....stress free IT

9 Benbecula Road
ABERDEEN AB16 1FT
Tel: (01224) 697457

E-mail: info@maydayconsulting.co.uk
Internet: <http://www.maydayconsulting.co.uk>