# Digital Homes - Part One
# Creating a Home Network Infrastructure

**Dermot Kelly**
**Department of Computer Science**
**National University of Ireland, Maynooth**

## 1 Introduction

Consumer electronics for media acquisition, playback and other forms of entertainment are ubiquitous in the modern home. Many homes have digital cameras, camcorders, personal music players, games consoles, media recorders and players of different kinds, as well as desktop PCs and laptops. Home automation is becoming more main stream – the ability to turn on lights or heating while away from the home, monitor security cameras or perhaps to enable music to follow you from room to room can easily be controlled from mobile Wi-Fi capable devices in a home network, or managed via the Internet, from a mobile phone or remote PC. Home security cameras or webcams are easily integrated into home network environments and viewable through web based interfaces on the Internet. Many people today want to set up home networks in order to achieve better more seamless integration of these devices. This can enhance the functionality of these digital devices, enable better accessibility and sharing of media from many sources by household users and provide some degree of reliability and durability for the household's valuable digital archive. A good home network set-up can lead to better data management policies and enhance access performance, saving people time, avoiding data loss, and offering fuller enjoyment of available media and control throughout the home.

## 2 Home Network Infrastructure

Digital consumer devices may be categorised as primarily fixed or primarily mobile. Some consumer devices such as a television, stereo equipment, desktop PC or media receiver are relatively large, mains powered devices and generally remain installed in one place. Some of these devices require high network bandwidth and require network performance to be constant for delivering multimedia data in time with viewing requirements. An uncompressed HDTV (1920x1080) signal, for example, requires a network speed of over 1.5Gbps while a compressed signal can require about 30Mbps. Due to limitations of current wireless technologies, these devices generally require a wired network infrastructure, to connect media sources and displays to achieve best operation.

Other devices such as laptops, PDAs, iPods and cellular phones generally operate wirelessly, though there are times when wired data connections, over USB for example, can be advantageous for device configuration, syncing at higher speed, better connection reliability or when more security is needed. The main functional advantages of these devices however are their small size, battery operation, handiness and portability. In order to accommodate both fixed and mobile devices with best performance in the home environment, it is best to provide both wired and wireless network infrastructure.

## 2.1 Wired Network

Ethernet over copper wire is the most pervasive, simple and cheap means of creating a wired network. Ethernet is a data communications protocol used for exchanging data across a point to point physical link in a Local Area Network (LAN) situation and is officially defined under the standards known as IEEE 802.3. Ethernet over copper wire typically operates at speeds of either 10Mbps, 100Mbps, 1Gbps or 10Gbps between network devices depending on the capability of the sending and receiving hardware and the quality of the copper cable and connectors joining them.

### 2.1.1 Connecting devices to a Local Area Network

A network interface card (NIC) is required by each device that wants to connect to an Ethernet network. Most modern cheap NICs are capable of auto-negotiated Ethernet operation up to 1Gbps. The network speed can be automatically negotiated by the NIC to the highest speed achievable by the slowest adapter device on the segment. Historically, NICs were separate components available as cards which plugged into the computer system bus, but now in the context of advanced Internet capabilities, digital electronic devices and computers are no longer designed to operate effectively in stand-alone mode with NICs an optional extra, but instead NICs are generally integrated into system motherboards and Internet integration is now essential standard functionality. The term NIC has become a misnomer and *network adapter* is more representative of the current design than the term *network interface card*. A built-in network adapter facilitates, among other things, easy upgrading of embedded device software via the Internet, while it is operating in the field. This is another reason why a home network is essential – it enhances the capability of your devices to perform automatic updates, add new features and saves you time, even while you sleep.

### 2.1.2 Choosing Network Cable

The Ethernet adapter on each device exposes an 8-pin RJ-45 socket for connecting the device to an Ethernet network via an RJ-45 plug attached to an 8-core copper wire cable (shown below).

Copper cable comes in different grades which are designed to permit different signalling speeds in different environmental situations. In order to be able to transmit speeds up to 1Gbps on a wired home network you require Category 5 (CAT 5) cable and connectors as a minimum. CAT5 components have essentially been deprecated in favour of the enhanced CAT 5e standard and use of these is recommended in 1Gbps Ethernet applications. CAT6 or CAT 6a may also be used and although there will be a greater component cost, the higher grade cable may provide better future proofing when 10Gbps Ethernet becomes the norm.

High speed electronic transmissions on copper wire are susceptible to electrical interference, emitted by a variety of electrical devices in the environment of the wire, which can lead to transmission errors. Cable design can help reduce the effect of this interference. As a first means of defence against radio frequency interference (RFI), a cable wraps the signalling wires in a grounded aluminium foil or wire braid or both.

A CAT 5e cable (shown on the left) typically contains eight 0.5mm insulated copper cores organised as four twisted pairs. By twisting signalling pairs, they essentially then occupy the same space, and any induced interference picked up on one wire will also be induced onto the other in the pair. The signalling difference then remains constant between the pair. A differential receiver on the NIC then determines the signal value by the difference between the pair rather than the actual signal voltages received.

Making connections with this cable involves untwisting small lengths of the signalling pairs. It is important when making connections to minimise the length of untwisted sections of the signalling pairs to maximise resistance to RFI.

Cable that is used for fixed (horizontal) installation, i.e. connecting wall outlets within the home to the house network's central patch panel, should use CAT 5e solid wire cores for greater reliability when making connections to patch-panels and RJ-45 keystones using punch tools. Solid core cable is more rigid and care should be taken not to place any sharp bends or kinks in the cable which may affect the signalling performance. Cable runs should not exceed 100M per 1Gbps Ethernet segment (including the length of any patch leads) but this is unlikely to be a problem in a home situation. A typical home installation may require 100M to 200M of cable depending on the number of network points required and distance to the central patch panel.

Cable that is used for connecting equipment to wall socket outlets and other short distance connection applications, known as patch cable, typically uses stranded cores which give the cable greater flexibility and better plug fitting. These cables can be bought cheaply in various lengths (1M to 10M) from any good hardware or computer store. A pack of 10 or more of these can probably be purchased cheaper than you could make them yourself and will probably be more reliable. You may also be able to avoid having to buy an RJ-45 crimp tool as well, necessary for putting RJ-45 plugs on CAT 5e cable.

### 2.1.3 Connecting the Wired Network Infrastructure

There are three additional elements, other than CAT 5e cable, necessary to creating the wired infrastructure. Firstly, each room where an Ethernet capable device is located will require an RJ-45 wall outlet.


It is probably worthwhile to put at least two RJ-45 outlets in each room of your house, especially where home computers, laptops, media centres and television points are located.
To highlight this need, consider games consoles like the Nintendo Wii, Sony Playstation 3 and Microsoft Xbox 360 all of which are Ethernet capable, Media receivers (and some televisions) are Ethernet capable enabling video on demand, internet browsing and so on, and networked audio devices like

the Apple Airport, used for bringing music to your home stereo, can utilise a wired Ethernet port. You may also have some other home automation applications or IP security cameras which will require conveniently located ports.

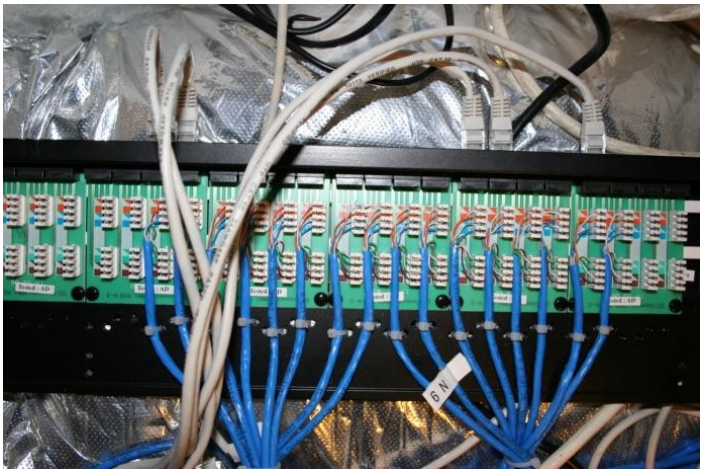
Although placing a small local network switch in a room will allow you to share a 1Gbps link among a number of devices, having two ports will allow 2x1Gbps links to your network to be shared by local devices in a room giving a degree of future proofing and fault tolerance and also giving the capability where two devices can communicate with two other devices on your network without contention on their respective 1Gbps links. There is very little additional trouble running two cables instead of one.

For each outlet point you need a single-gang dual RJ-45 face plate with a suitable back-box to sit inside your wall and two CAT 5e keystone jacks (shown on left). The keystone jack is used to connect the solid core CAT 5e cable and it then clips into the back of the wall plate. The keystone jack terminals are colour coded to match the CAT 5e core colours.

The CAT 5e wires must be untwisted, and aligned with the keystone jack terminals and then punched and cut in a single operation using a Krone 110 Punch down tool (shown below).

A YouTube video demonstrating how to connect the cable to a keystone jack is available here if required.

Secondly, the other end of the cable is terminated at a CAT 5e patch panel as shown below. The blue wires are from RJ-45 wall outlets and the grey wires are patch leads connecting active sockets to ports on the network switch. Be sure to label both ends of all cables when installing, for easy patching and troubleshooting later. A 24-terminal patch panel should be adequate for home use.



As a future proofing measure, when creating a house network, more network Access Points will probably be created than are required by the current number of Ethernet capable devices in the

household. Many of the points remain unused and, while it is good practice to label the installed cables and terminate them in a patch panel, it is not necessary to connect them all by patch leads to the house network when not in use.

Finally, the third component needed for creating the wired network infrastructure is a network switch. This is an electronic device which enables the electrical interconnection of the home network wall outlets so that each active connection can communicate with every other active connection in the home through the network switch. It forms the communication hub of the network.

Each active connection must be connected using a CAT 5e patch lead from the patch panel to a free RJ-45 port on the network switch. The patch panel must have enough terminals for every wall socket in the home, but the network switch, as a minimum, need only have enough ports to handle the number of actual Ethernet devices in the home. It is advisable to get a switch with enough additional spare ports to accommodate some growth in the number of internet capable devices in the home.

The ports on the network switch should be capable of auto negotiation of Ethernet speed up to 1Gbps to allow any type of device to connect to the corresponding RJ-45 wall socket. 10Gbps network switches are also available but are more expensive and require a higher grade CAT 6a cable installation and higher specification 650Mhz RJ-45 outlets. The more expensive installation would obviously provide enough network performance around your home long into the future and, given the trouble associated with installing wired network points, might be worth consideration. At current prices components may cost about three times as much as CAT 5e components.

For a home network, a 16-port gigabit switch is probably more than adequate, offering an interconnecting switching capacity of 32Gbps when simultaneous bi-directional operation of each of its 16x1Gbps ports is in progress. The Dell Powerconnect 2716 (shown on the left) is a reasonably priced 16-port switch for this application and incorporates a web managed interface with a built-in cable tester among other features.

If you intend to use IP cameras conforming to the IEEE 802.3af standard using Power over Ethernet (PoE) on your network, then a PoE network switch will be required, which may cost a little more. This allows the cameras to get their power from the switch through the RJ-45 connection without the need for additional wires. Alternatively you can read a discussion here for details of other solutions.

## 2.2 Wireless Network

Wireless networks are based on the general set of communication standards known as IEEE 802.11 and wireless Access Points using these standards are generally accessible to Wi-Fi enabled portable devices. All radio transmission is regulated for obvious reasons and to enable the general public to set up private wireless networks, without requiring transmission licences, national communication regulators designate certain transmission frequency bands for public use. Therefore all consumer electronics such as wireless broadband modems, telephones, wireless cameras and video

transmitters, baby monitors and other radio controlled domestic equipment operates in these often congested frequency bands.

As a result, wireless signals can experience interference from nearby equipment, such as a microwave oven, emitting in the same frequency band and this might affect the network performance in an unpredictable way. Wireless signals can be intercepted by equipment listening in the same frequency, so security becomes a concern. Your wireless network signal is not confined to the bounds of your home but to the range capability of your transmitter. Walls and solid objects will absorb some of the high frequency signal and it may not travel as far outdoors, but even within your home, a wireless signal may not be equally strong, or available at all, in all parts of your home either despite being within range of your transmitter.

The frequency channel used by the wireless network is the only communication path between wireless devices in the home. Each wireless device must contend or compete with the other devices to share this path for transmission purposes. This contention generates transmission collisions which can affect network performance. Wireless communication needs to be encrypted and various data added by encryption methods detracts, according to some, by up to 20% from signalling bandwidth. A recent study contends the effects of encryption may not be that significant. Wireless networks can use cyclic redundancy checks to detect packet errors and require whole packet retransmission or could use forward error correction where adjustable levels of redundant information are sent with messages to enable reception errors to be fixed at the destination without requiring retransmission. Either way, error detection and correction reduces the effective useful data throughput as does the need for security. Although this is also a factor in wired networks, errors are much more common on wireless networks, as distance increases, than on wired types. Distance and obstructions to the Access Point can significantly reduce performance.

For all these reasons, if at all possible, wired signals are preferable to achieve higher performance. Wired connections to the ports on a network switch are not subject to the same contention problems. However, fitting a wired network point may be difficult in some situations and a wireless network can provide a quick, operable and cost effective solution. Wireless network availability is essential to obtain full functionality from many portable devices operating in the home, but performance can be erratic, private data and passwords can be exposed and compromised.

However, when sitting in your Wi-Fi enabled living room using an iTouch or iPhone to seamlessly browse email, YouTube or your security cameras, or to remotely control your iTunes application playing through an Apple Airport into your Hi-Fi, the magic and application potential of wireless access is uncontested.

### 2.2.1 Wireless Network Standards

There are four main variations of 802.11 wireless networks, known as 802.11a, 802.11b, 802.11g and 802.11n commonly known as Wi-Fi technologies. Client wireless transceivers must be compatible or have backward compatibility with the type of network implemented by an Access Point to utilise it.

By far the most common and cheapest are the 802.11b and 802.11g varieties. Both of these types of network share the 2.4GHz frequency band and are implemented by many domestic internet

router/wireless Access Point devices. The older 802.11b standard supports a maximum data rate of 11Mbps while the more recent 802.11g standard supports a faster maximum data rate of 54Mbps.

The 802.11g standard is backward compatible with 802.11b in that it was designed to allow for the coexistence of slower 802.11b devices operating on the same network. Access Points can typically support wireless access from 802.11b and 802.11g enabled portable devices on the same network, but the presence of a legacy 802.11b device will significantly affect 802.11g performance.


The Netopia 2247, shown on the left, is an example of a relatively cheap 802.11b/g compliant wireless Access Point incorporating a 4-port 10/100 Mbps Ethernet Switch enabling the creation of both wired and wireless private networks with optional ADSL2 Internet connection via a broadband DSL, all in a single device. It is capable of both WEP (not recommended) and stronger WPA encryption.

For the purpose of determining suitability for wireless network applications in the home, the effective maximum throughput of an unhindered 802.11g network is about 19Mbps and that of an 802.11b network is about 6Mbps due to the protocol overheads. These speeds are not really adequate or reliable enough for high quality video streaming but are generally acceptable for audio and data streaming.

802.11a is an alternative parallel standard developed using the 5GHz frequency band and is therefore not compatible with 802.11b or 802.11g equipment. There is less usage of this frequency band space by other types of domestic equipment and 802.11a networks may benefit from higher performance due to encountering less interference. Like the 802.11g standard, a maximum raw data rate of 54Mbps is supported. The range of 802.11a networks is slightly less than 802.11b or 802.11g types however as the higher 5GHz frequency signal is more readily absorbed by walls and solid objects. On the other hand there is a greater number of channels available in the 5GHz band. 802.11a is used in business office environments and in areas which experience higher congestion in the 2.4GHz band and can achieve effective throughputs of 24Mbps.

The 802.11n variety of wireless network is not yet released as a standard but is already becoming widely implemented in domestic products based on the draft versions of the standard emerging from the IEEE task group. The official standard is due for release in late 2009. Draft 802.11n is currently implemented by, among others, the "Apple TV" HD Media Player, Apple's "Airport Express" Wireless Access Point and Audio Streamer and the "D-Link DIR-655 Xtreme" 4-port Gigabit ASDL Router, for example, all shown below.

802.11n takes the raw data rate up to 600Mbps, quicker on initial glance than USB 2 and Firewire, perhaps appearing to approach the speed of a gigabit Ethernet. The maximum effective throughput however is in the region of 100Mbps, still significantly slower than wired connections but potentially five times faster than existing 802.11g networks. 802.11n is designed to be backward compatible in terms of permitting coexistence with 802.11a/b/g devices but the presence of these will significantly affect performance. Bearing in mind that current products only implement draft standards, it is probably still a good idea to purchase a wireless Access Point capable of 802.11n even if your client devices only support the earlier wireless standards, as this will allow you utilise the capabilities of newer 802.11n devices as they come to market while allowing the optional upgrading of your existing client devices in the future. There is always the possibility of future incompatibility until the standard is published.

### 2.2.2 Network Security Overview

Network security is an option that you need to be concerned with, especially when setting up a wireless network, for three reasons:-

1. Without some security for controlling access to your wireless network, anybody nearby with a Wi-Fi device could potentially connect to your wireless network, and if a path to the Internet is present, they can use your bandwidth for free, slowing down your connection, or compromise the Internet usage policy dictated by your Internet Service Provider (ISP). Wireless networks can be accessed typically up to ranges of 100M indoor and 300M unobstructed outdoor.

   Sometimes access to equipment on your network is set-up to be less secure when accessed from within your home than when accessed remotely over the Internet. Anybody who can access your wireless network can communicate with local IP addresses and will most likely have easier access breaking in to other equipment on your network as well, if they are so inclined. There are a number of basic measures that can be taken when configuring a wireless Access Point to make unauthorised network access more difficult.

2. Any data passed around on a wireless network can easily be sniffed by nearby Wi-Fi capable devices using applications like BackTrack, Aircrack-ng, Airsnort and Kesnet all available on the Internet and can reveal information which can be analysed to access your network. If strong measures to encrypt and secure your data transmission are not taken you may unknowingly give up passwords to email, banking and remote access to other private services that compromise your identity to varying degrees. Encryption scrambles data on your network so that only clients with the encryption key can decipher messages. This requires additional configuration of the Access Point and of each client using the network. Note that it is only the wireless traffic that is encrypted by this measure, not any traffic on your wired Ethernet or Internet connection.

3. When your private networks are connected to the wider Internet, you expose machines to intrusion from any part of the world, not just nearby devices, and this magnifies the risk enormously. If left undefended, automated software can repeatedly probe your internet connection from afar until it discovers a password, a weakness in the operating system or any running or forgotten services that may be willing to communicate with it. Such software may find a way to steal or remove personal information from your equipment, interfere with the normal operation of your equipment, or plant unwanted software, spyware or other content on

your equipment. The main defence against inbound threats is the use of a firewall, software which restricts unsolicited incoming connections to your network.

Additional security measures must be taken at the application level to authenticate and encrypt communications on the internet, such as using secure HTTP.

Security is not as much a concern on a local area network if you use wired connections. It is probably true to say that all measures to secure domestic wireless networks can eventually be overcome by experienced individuals who are determined to break in. Your security relies for the most part on people's willingness to remain within the boundaries of the law, people's ignorance or limited understanding of networking technologies, the limited range of your transmitter and the time and effort it takes to break your defences.

If there is something worth having it may be worth the effort. The objective is not to depend on people's morality, tempting them to be nosy by offering an open network, but to reduce your risk of being compromised by making it as difficult as possible in terms of time and effort for those so inclined to gain access. Unfortunately, making a network more secure can lead to a greater awkwardness for legitimate users and administrators of the network. It involves additional time spent on configuration, may hinder some automated functionality and requires regular security key recycling.

### 2.2.3 Securing Access to a Wireless Network

Every wireless network is identified by a name known as the Service Set Identifier (SSID). Every station operating on a particular wireless network must use the same SSID. This can be entered manually in the station's network settings, or, if the name is broadcast publicly by the network Access Point, the station can select and set the SSID automatically. When mobile stations search for nearby network Access Points, the SSID of each network shows up only if its name is broadcast by the Access Point. So the first defence is to turn this off and most people will not know it is there. Legitimate stations won't be able to see it either however, so you will be forced to enter the SSID manually on each one in order to access that network. Like all security measures, this is probably something you might like to postpone until after you get your wireless network operational initially.

At the hardware level, every interface that manages a network connection has a globally unique address assigned to the network interface hardware, known as the Media Access Control Address or MAC address. The MAC address is assigned by the manufacturer of the device. In a Laptop for example, you may have one MAC address assigned to the wired Ethernet adapter and another MAC address assigned to the 802.11 wireless adapter. A wireless Access Point can be configured to recognise and allow access only from a designated list of MAC addresses corresponding to the devices in your home that you permit to access the network. You need to determine all the wireless MAC addresses of such devices and enter them when configuring the Access Point. For devices that have wired and wireless network adapters, be sure to use the MAC address of the wireless one only. New devices cannot join the network until the Access Point is reconfigured to include their MAC addresses. Any attempt to get through the Access Point by an unrecognised MAC address will be refused by the Access Point. Unfortunately it is possible to spoof MAC addresses and a wireless station can be configured to alter its MAC address to one of those in your list. A legitimate MAC

address on your network would have to be discovered for this to work as well as discovering the network's SSID.

SSID and MAC address security on their own can quickly and easily be overcome by using wireless adapters in monitor mode to sniff the network and are really only quick and simple measures to take away temptation from the vast majority of people using wireless equipment in the vicinity of your network. The most important security measure needed to control network access is the setting up of an authentication and encryption scheme. As this is so important, it is generally very simple and user friendly to set up on most devices and need not be feared or postponed. It is advisable to do all infrastructure configurations before you connect your Access Point to the Internet. The only technical issue is what type of scheme to use and the choices are explained next.

### 2.2.4 Authentication and Encryption Schemes for Wireless Networks

For encrypted communication to work both the Access Point and the client stations have to be able to implement the same protocols and with symmetric encryption both must know a shared secret or passphrase which authenticates them to one another. As some older devices and adapters are not capable of some of the newer encryption algorithms like AES, Access Points, particularly in home networks, are often configured to use Wired Equivalent Privacy (WEP) encryption to secure transmissions or are left open completely (unencrypted) as a default common denominator. WEP security has a number of flaws in its design which make it relatively easy to replay or interfere with network transmissions even without the passphrase and fairly simple to crack by listening and analysing enough packets on the network over time to synthesise the network key. The problem with it is not the RC4 stream cipher that is used, but the way it is used, and is worsened by other design flaws in the protocol such as messages not being authenticated by the Access Point subsequent to the initial association; the initial authentication challenge sequence reveals information useful to impersonation; modified packets can go undetected violating integrity requirements; the cipher initialisation vector is too short leading to 'repeating' random sequences from the cipher within a short time frame which can help to reveal the key; and the general practice among WEP users of using a single passphrase used by all stations, for all authentication challenges and all packet encryption. A critical analysis of WEP is available here.

It is important to be aware that encrypted networks are not impenetrable. A "tutorial" on how to go about cracking a WEP enabled network in a very short time can be found here with a companion article here discussing possible attacks on the more secure WPA scheme.

Encryption is used to protect your network from the small percentage of individuals in your vicinity who may monitor network packets and be able to bypass any MAC address security measures. If they have the sophistication to obtain MAC addresses on unencrypted networks then they will have no bother obtaining a WEP encryption key using the same software, so don't bother with either the 40/64-bit or 128-bit WEP schemes and instead use the newer Wi-Fi Protected Access (WPA/WPA2) encryption protocols which are more difficult to crack, assuming private key creation guidelines are followed.

The WPA2 version refers to an implementation of the IEEE 802.11i standard for a Robust Security Network (RSN) required of all new Wi-Fi certified devices since 2006 and is considered to be quite secure against all forms of wireless attack. You should configure your devices to use WPA2 if they all support it. Some IP cameras, media extenders or older adapters without AES encryption hardware,

for example, may not be able to use WPA2. Encryption is done in hardware for performance and no firmware updates can fix this if the hardware is not present.

Like WEP, WPA is a symmetric encryption key system where knowledge of a secret key enables both authentication and correct encryption and decryption of network packets. Also, like WEP, WPA uses the RC4 symmetric stream cipher (in order to utilise encryption engine hardware in existing wireless devices) but unlike WEP, it uses a stronger mutual authentication procedure utilising a third party authentication server to generate a unique *pairwise master key* per station session from which other keys for encryption are then derived; the protocol requires a longer initial private key, a longer cipher initialisation vector and the data encryption key changes automatically and frequently and is unique to each station, all of which combine to thwart statistical means of attack. WPA uses a dynamic method of generating keys known as Temporal Key Integrity Policy (TKIP) whereby a different encryption key is used with each packet transmission. Thankfully, home users do not need to be aware of how the key management policy or the encryption cipher works; they only need to create a private key of at least 20 characters for use in authenticating themselves to the Access Point and the key management and encryption happens by magic.

The WPA2 protocol is the common term used by the Wi-Fi alliance for the official IEEE 802.11i standard for a robust security network (RSN). The first WPA version, which uses TKIP and RC4, emerged from the Wi-Fi alliance as an interim protocol developed to quickly shore up the weaknesses of WEP before the IEEE standard could be ratified. WPA and WPA2 both use the same authentication protocol (EAP) to generate a *pairwise master key*, but differ in the way that the encryption keys are managed and the encryption algorithms used. Where WPA uses TKIP to manage keys and the RC4 stream cipher to encrypt the data, WPA2 uses CCMP (Counter mode/CBC-MAC Protocol) and the Advanced Encryption System (AES) block cipher for encryption and is considered to be more secure in terms of confidentiality and message integrity than WPA. More detail of how these schemes work can be found here. If your hardware doesn't support AES encryption for WPA2, all is not lost, it is still likely to support WPA, as this is based on WEP hardware, and with a firmware upgrade if necessary, WPA should be used instead of WEP.

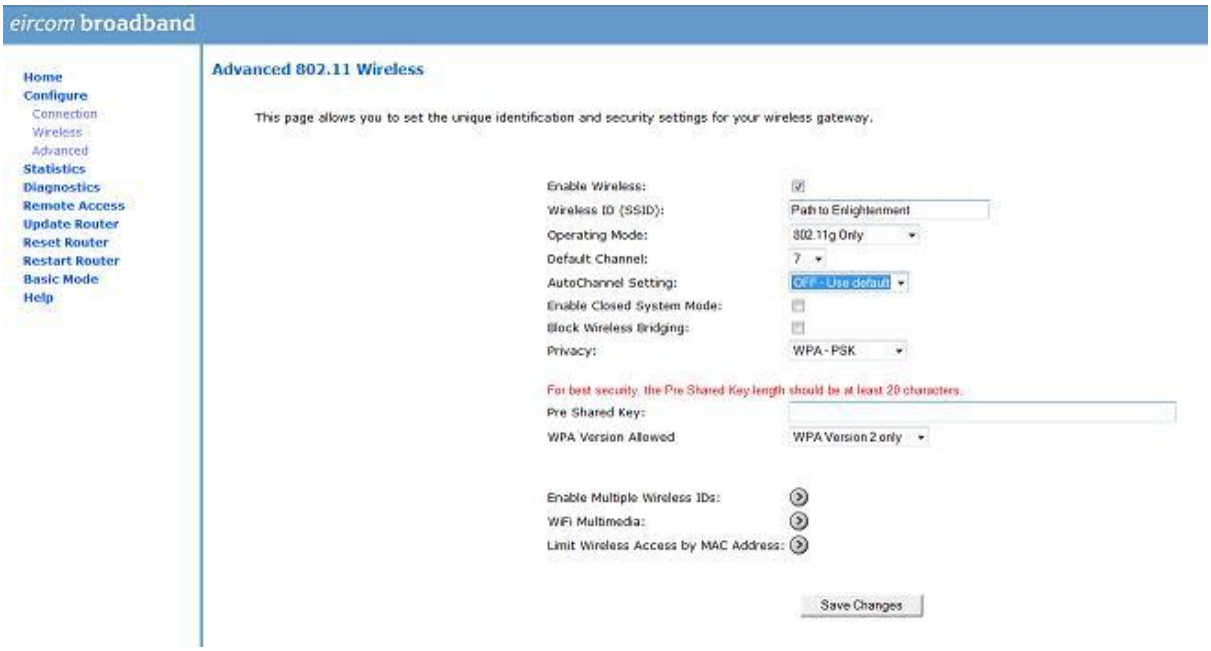
For the end user, there are two ways of securing a wireless network (using either WPA or WPA2) which basically differ in how knowledge of the initial shared secret (private key) is obtained by the stations and the access point.

WPA-PSK is the simplest method and used in most small office/home (SOHO) networks. A private or pre-shared key (PSK) is installed manually on the Access Point and on each of the stations. The same key is used for all stations. For this reason and as the key is long-lived, it is very important to choose a strong key, the strongest of which is in the form of a random 64-digit hexadecimal number. Entering the key in this form, rather than as a simple text passphrase, may take a little longer to administer, but will prevent common dictionary attacks attempting to discover a simpler passphrase. If your equipment only permits the input of a text/ASCII passphrase instead of hexadecimal digits, then you should use a passphrase of at least 20 characters in order to generate a sufficiently secure 64-digit hexadecimal key.

WPA-802.1x (sometimes known as WPA-Enterprise) is the second way of using WPA and is more complex requiring additional infrastructural investment and is used primarily as a way of managing access to larger enterprise networks by greater numbers of user stations and which must control

internal network access policies for different users. Following a login procedure, the WPA *pairwise master key* is distributed automatically and securely per station through the Access Point from a trusted third party, known as an authentication server, using the secure backend RADIUS protocol.

The wireless security configuration screen of the Netopia 2247 is shown below, set up for a WPA-PSK home network:-

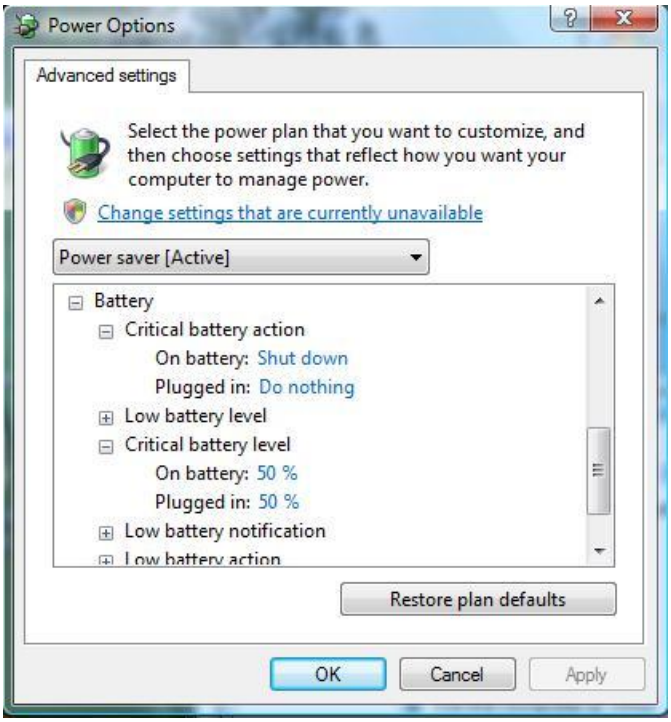



As a final consideration in configuring your local network prior to connecting to the Internet, don't forget to set a strong password for the administrator login account on the wireless Access Point/Gateway Router and if you use a web managed network switch, set one for that as well. If someone is able to login as administrator on your Access Point or network switch through your wireless network, they can interfere with your network setup. If you ever end up being locked out of your Access Point or switch due to forgotten passwords, for example, you can press the recessed factory reset button which restores the default factory settings, and set them up again. As an extra precaution, configure the wireless access point so that the administrator can only log in from your wired network.

## 2.3 Uninterruptable Power Supply

An uninterruptable power supply (UPS) is a device capable of supplying mains voltage to connected equipment for a limited time from an internal battery, as long as the battery has a sufficient charge. UPS units provide backup in the event of power failure to allow systems to remain up during brief outages and to allow graceful shutdown for longer outages. Computer equipment uses a combination of disk and electrical memory to maintain the state of operating system activities, running processes and applications. When a power failure occurs, the electrical memory state is lost leading to possible data loss, file system corruption and so on. A UPS gives the system and the user a window of time to save data that might reside in electrical memory to disk before the system shuts down. UPS systems are essential if operating servers on a network and desirable for protecting most desktop computer equipment. There are many different models to choose from that are affordable to home users. Some models will provide surge protection and/or power cleaning as well.

Normally, a UPS can be connected to a computer using a USB interface to enable the computer to detect a loss of mains power and to monitor other status information. UPS Software (bundled with the UPS) such as APC Powerchute and Belkin Bulldog for Windows XP/Vista or the Gridjunction Add-in for Windows Home Server can be used to configure the behaviour of the computer in response to different power situations. Microsoft XP/Vista and Windows Home Server have built in support for UPS units and additional software may not be required, however sometimes additional software offers extra configuration or monitoring features not available through the basic Power Options settings. Vista standard Power Options settings are shown below.




The power output capability of a UPS must exceed the power requirement of connected equipment or it will be overloaded and simply bypass the battery backup or worse, shutdown the supply. A UPS is very intolerant of overload and may be in danger of bypass at loads of 90% of the rated maximum load. The output power of a UPS is typically specified in VA but this maximum VA rating is specific to an anticipated power factor (PF) rating for the load which is generally considerably less than 1, especially for cheaper UPS systems. On the other hand, modern computer equipment power supplies have power factors very close to 1. The result is that the VA rating of the UPS can easily be underestimated for the load that is to be placed on it. For example, say the PF for a UPS is 0.7, then a UPS rated at 700VA when used with modern computer equipment would likely overload with a load in excess of 400Watts. A discussion of conversion between watts and VA can be found here. A tool for suggesting UPS requirements can be found here.

A 700VA UPS such as the APC back-ups ES/700VA is probably the minimum useful specification needed for a typical desktop computer with 20” monitor or for a small windows home server and should yield up to 15Mins up-time to this load. This device has a single battery, offers surge protection, weighs about 6.8Kgs and connects to a USB port on the computer.

The Belkin universal 1200VA UPS is another reasonably priced tidy unit with similar capabilities and a bit more power. This unit contains 2 batteries, weighs 13.6Kg and will power a maximum load of 670 Watts. You could expect in the region of 25 minutes up time with a typical modest desktop computer load.

Both of these units offer surge protection for power outlets and a phone connection. Voltage regulation though is limited to the UPS cutting in when mains voltage drops below or exceeds specified levels. More expensive models should be selected if power smoothing is a requirement. Batteries typically need replacement after three years.

In addition to providing power backup to your home server or desktop equipment, you may consider allowing enough capacity in the UPS to power your network infrastructure components as well for as long as your computers remain up.

In home server environments shared files are located on the server for access from different machines and for easy backup. These files may be in use on a desktop when power fails. While your computer and server remain up during the power outage on their respective UPS units, they cannot communicate if your Wireless Access Point/DSL Modem and Network Switch are down. Putting these devices on a UPS supply means that you should have 10-15 minutes of fully operational network infrastructure in the event of a power failure. Many households use portable phones. You may consider putting the base station for a portable phone on the UPS as well so that your phone works during a power failure and/or your calls are not rudely interrupted.

So that completes suggestions for the basic infrastructure of digital communication within the home. The next instalment addresses connecting and securing the home network on the Internet, and choices for setting up a personal Internet Domain and some related services.