Computer network options - wired and wireless solutions for home and business

www.rdcs.com/network-options.htm

Computer Networks - options

Networks are collections of computers, software, and hardware that are all connected to help their users work together. A network connects computers by means of cabling systems or wireless connectivity, specialized software, and devices that manage data traffic. A network enables users to share files and resources, such as printers, as well as send messages electronically (e-mail) to each other.

Computer networks fall into two main types: *client/server* networks and *peer-to-peer* networks. A client/server network uses one or more dedicated machines (the server) to share the files, printers, and applications. A peer-to-peer network allows any user to share files with any other user and doesn't require a central, dedicated server.

The most common networks are *Local Area Networks* or *LANs* for short. A LAN connects computers within a single geographical location, such as one office building, office suite, or home. By contrast, *Wide Area Networks* (WANs) span different cities or even countries, using phone lines or satellite links.

If you need help with your network then give us a call to find out more.

Typical home network (basic)

Typically you will have a router to connect you to broadband. This will share the internet connection with multiple devices using a combination of wired and wireless. Some routers don't have wireless built in so you may need an additional piece of equipment or upgrade your router to a wireless ADSL (broadband) router such as the Netgear DGN2000. Most ADSL routers have only 4 network ports. If you have more than this (including network printers) you will need an additional network switch to extend the number of ports.

With a combined network/wireless router in place connected to an ADSL connection all you need to do is connect your device to the router using a wire or wirelessly.

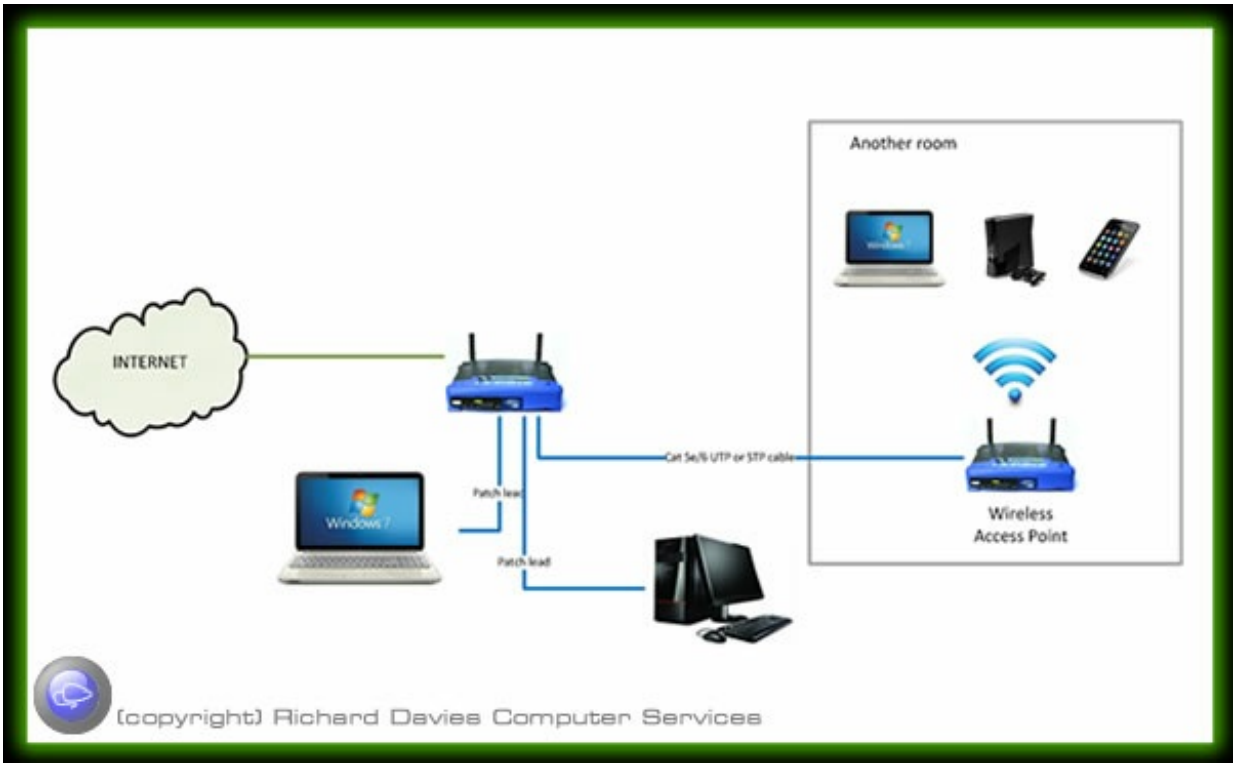
Depending on the size of your home, the thickness of walls and interference from other devices you may need to extend your network further so that you can have wireless or wired connections in all rooms.

Wireless Access Point

Wireless access points (APs or WAPs) are specially configured nodes on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of WLAN radio signals.

Access points used in home or small business networks are generally small, dedicated hardware devices featuring a built-in network adapter, antenna, and radio transmitter. Access points support Wi-Fi wireless communication standards.

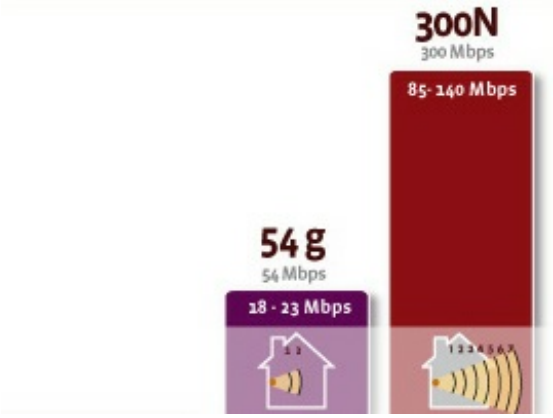
Although very small WLANs can function without access points in so-called "ad hoc" or peer-to-peer mode, access points support "infrastructure" mode. This mode bridges WLANs with a wired Ethernet LAN and also scales the network to support more clients.



Why wireless 300n is best.

What is the difference between “g” and “n”?

There are a number of standards for wireless networks (802.11b, a, g and n). The “n” standard is the latest and fastest of these. The “n” standard distinguishes itself from its predecessor “g” by offering a wireless speed which is up to 12 times faster and a range which is up to 4 times greater.



What is the advantage of n?

Nowadays, wireless networks are not only used to surf the Internet or to send e-mails. With the 802.11n draft 2.0 solutions, users can enjoy unprecedented performance in terms of speed and range for demanding applications, such as streaming HD audio and video, Voice over IP, multiplayer gaming and transferring large quantities of data. “N” meets the demand for faster wireless speeds and delivers impressive performance when, for example, downloading files, viewing videos on YouTube or playing your favourite online games with speeds of up to 300 Mbps.

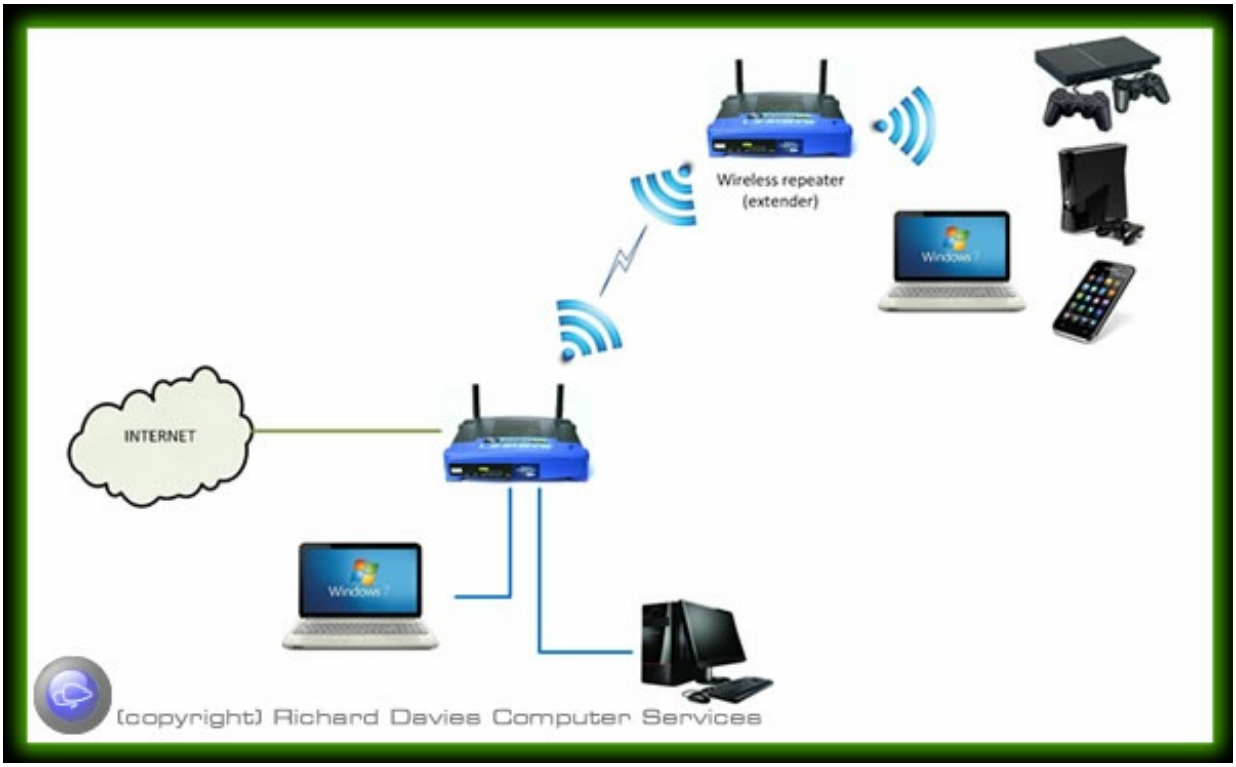
Why is it so easy?

With “n”, you enjoy unprecedented performance in environments with multiple users and demanding applications.

The 300N solutions are backwards compatible and can be used in combination with 802.11b/g devices.

Wireless Repeater (extender)

For this you need a **wireless repeater** or extender. A **wireless range extender** increases the distance over which a WLAN signal can spread, overcoming obstacles and enhancing overall network signal quality.



Several different forms of wireless range extenders are available. These products are sometimes called "range expanders" or "signal boosters." A wireless range extender works as a relay or network repeater, picking up and reflecting WiFi signals from a network's base router or access point.

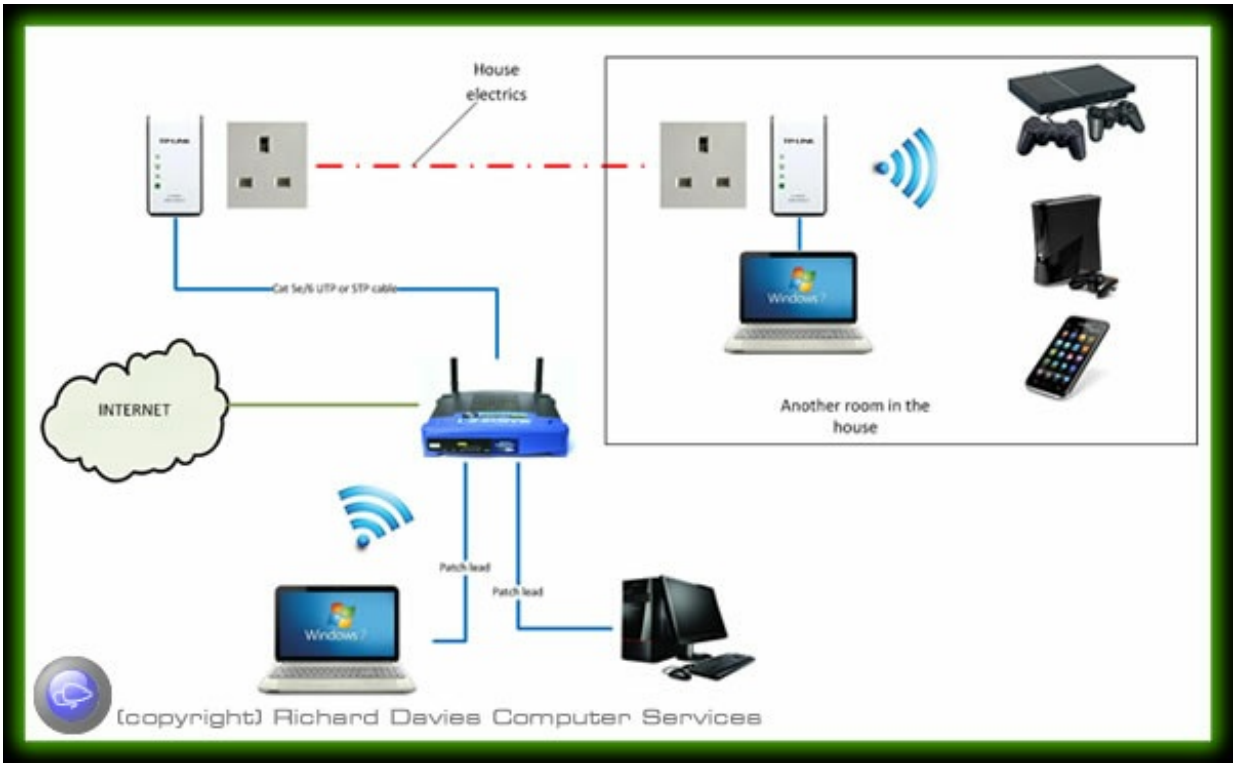
The network performance of devices connected through a range extender will generally be lower than if they

were connected directly to the primary base station.

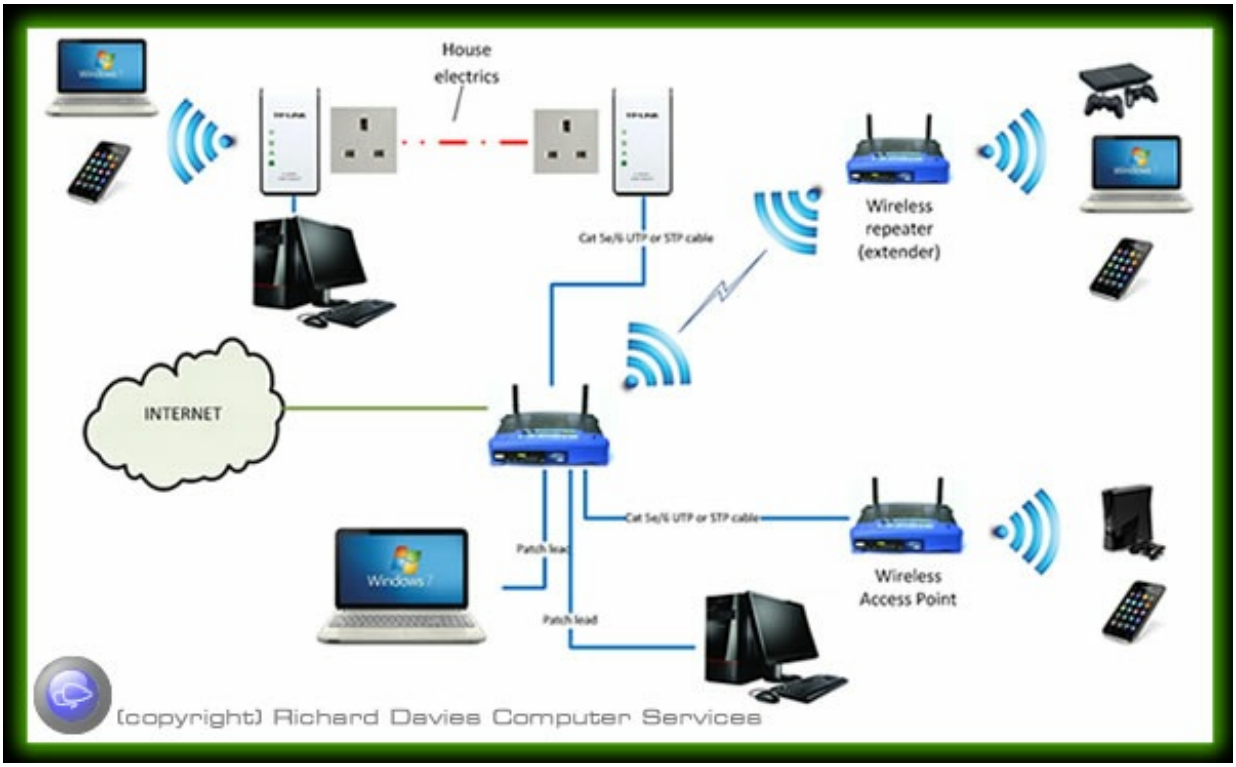
A wireless range extender connects via Wi-Fi to a router or access point. However, due to the nature of this technology, most wireless range extenders work only with a limited set of other equipment.

Network Powerline adaptors

Alternatively you can use powerline adaptors which use your electric mains to communicate through without the need of additional network wiring.

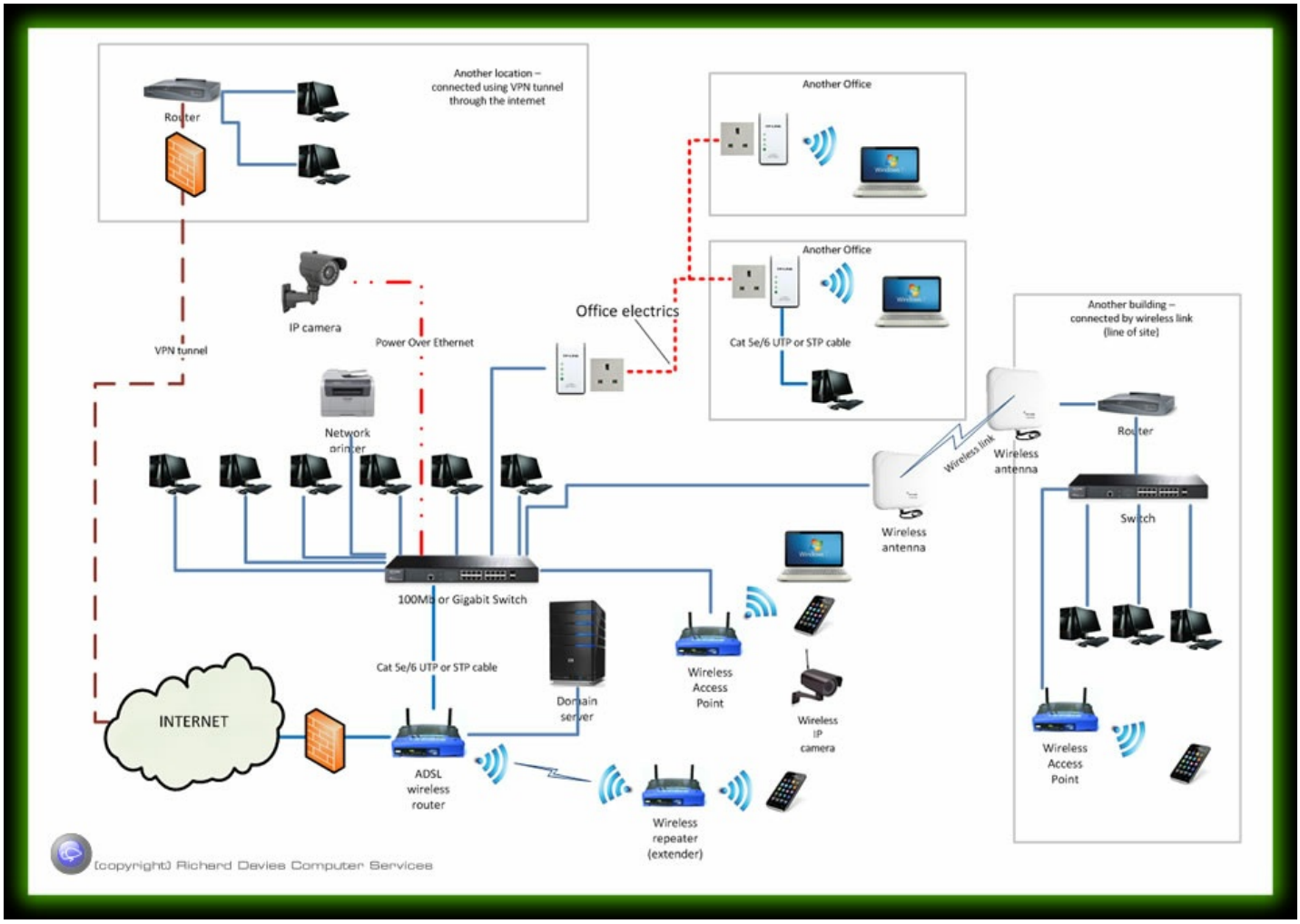


You don’t need to stick to just one type of network extension type, you can adopt a combination of different methods to achieve full network coverage.



Business network topography

Depending on number of machines you need to connect you need to decide whether you are going to configure as a peer to peer network or a domain driven network using a server/s. Have a look at our server page for information about the difference between them. The rule of thumb is; if you require security, require your own email exchange, have remote workers any have more than about 6 Pc's you may require a server driven (domain) network.



If you need help with your network then give us a call to find out more.

Multiple offices

Same rules apply as for a small office; choose between peer to peer and domain. Depending on the number of network connections needed you may need a data cabinet to house the cables from all the network wall ports, the router and switches.

Offices can be connected together using Cat5e/6 cabling back to the data cabinet/switch. It the offices are in different buildings but in line of sight it is possible to link the buildings together using wireless, alternatively you can configure a VPN (Virtual Private Network) using the internet as a conduit.

> *Note: Cat 6 (UTP = Unshielded Twisted Pair) (STP = Shielded Twisted Pair). Cat 5e UTP is fairly cheap to buy and is adequate for most network wiring, however if you require Gigabit (1000Mbit network speed) to work effectively then Cat6 will be required. STP protects the cable from cross talk (interference from other cabling) and therefore better for longer cable runs and where the cable passes electrical cables etc.*

Networking that require high speed (Gigabit etc), components must be consistent throughout the network e.g. Gigabit switch, Gigabit wiring and Gigabit network interfaces on PC's / Laptops etc.

Public WiFi

Your Responsibilities as a WiFi hotspot owner

> *Whether you run a small bed and breakfast or a large 5 star hotel, if you're operating a WiFi hotspot, you need to be aware of, and compliant with, all relevant laws and legislation regarding their operation.*
>
> *There are various laws and pieces of legislation that apply to the operation of public WiFi hotspots in the UK. These laws cover things like copyright infringement, accessing of illegal content, email spam, hacking and all sorts of other questionable activity. If you're running a public WiFi hotspot, you need to be able to make sure you are compliant with these laws.*

Tracking Usage

The first thing you need to be able to do is identify who is using your network, so that you can track activity and keep a record in case the authorities ask you to provide them with information regarding any incident traced back to your network. This is very difficult to do unless you have the proper infrastructure, as a basic, unsecured, public WiFi hotspot will not cater for this, and each user will effectively be anonymous. RDCS' Hotel WiFi service can provide you with everything you need to track usage.

Content Filtering

If you're offering a Hotel WiFi Hotspot and want to fully compliant with the law, it's a lot easier to do if you filter the content users are looking at. RDCS can offer a content filtering service that prevents users from accessing illegal or questionable content.

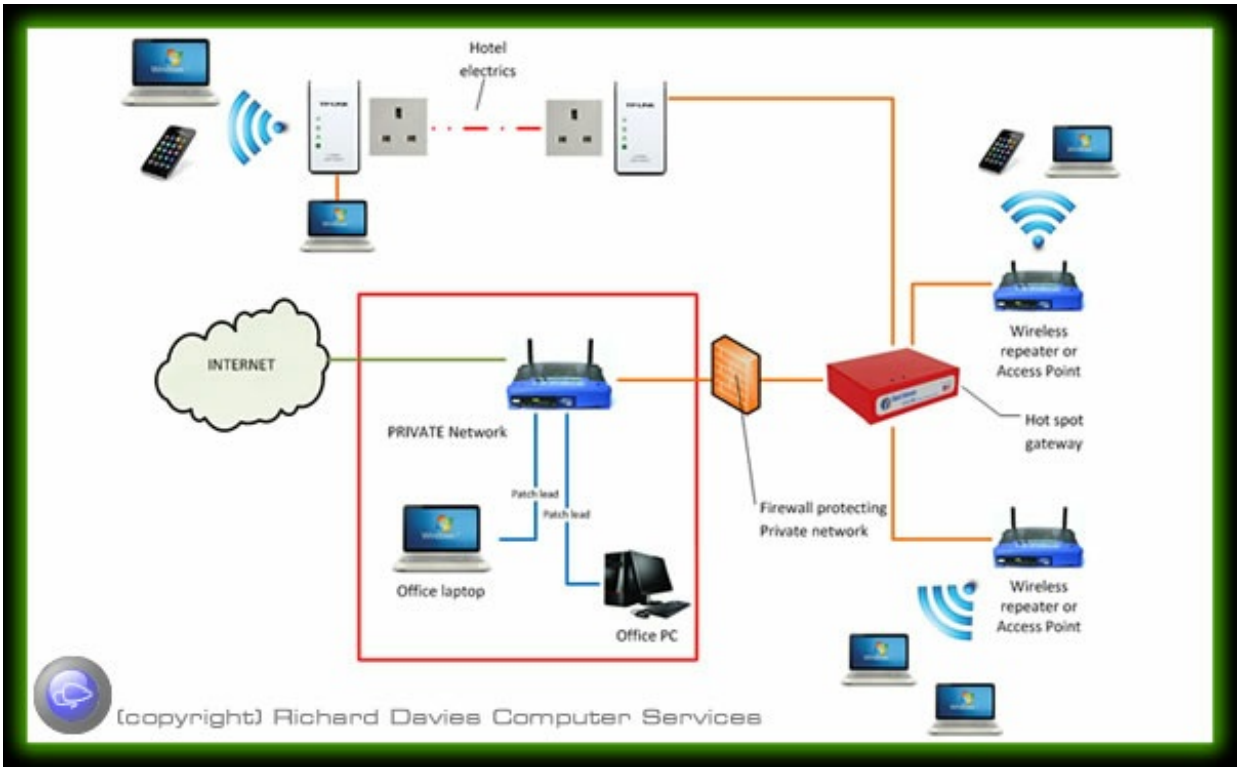
Digital Economy Bill

The recently introduced Digital Economy Bill (DEB) has made data retention and usage tracking even more important. This bill, along with a few other things, covers copyright infringement and the unlawful downloading of copyrighted content online. If your public WiFi hotspot users are carrying out this activity on your network and you aren't at least tracking usage, you could end up getting hit with a hefty fine even though you weren't directly responsible. Our system can record all activity on your hotspot and trace it back to the individual device and account that was used to access the content.

RDCS Public WiFi system

Typical layout for the Hot Spot system (shown in red on the figure below). Multiple Wireless Access Points and network connections can be connected to the hot spot system and separated from your private network whilst sharing the same ADSL connection.

Depending on the configuration guests can log on without providing any details after accepting the terms and conditions, alternatively you could specify any number of details you require from the guest or even charge for access. In either case details are logged of the session against the mac address and IP of the connected devices. Bandwidth throttling and website filtering can also be configured.



Contact us on 01822 810799 if you would like to know more.

Terminology - the short list

ADSL
ADSL (Asymmetric Digital Subscriber Line) is a technology for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. Unlike regular dialup phone service, ADSL provides continuously-available, "always on" connection. ADSL is asymmetric in that it uses most of the channel to transmit downstream to the user and only a small part to receive information from the user. ADSL simultaneously accommodates analogue (voice) information on the same line. ADSL is generally offered at downstream data rates from 512 Kbps to about 6 Mbps.

Power Over Ethernet (POE)
Power over Ethernet (PoE) is a technology for wired Ethernet LAN's(local area networks) that allows the electrical current necessary for the operation of each device to be carried by the data cables rather than by power cords. Doing so minimizes the number of wires that must be strung in order to install the network. The result is lower cost, less downtime, easier maintenance, and greater installation flexibility than with traditional wiring.

For PoE to work, the electrical current must go into the data cable at the power-supply end, and come out at the device end, in such a way that the current is kept separate from the data signal so that neither interferes with the other. The current enters the cable by means of a component called an injector. If the device at the other end of the cable is PoE compatible, then that device will function properly without modification. If the device is not PoE compatible, then a component called a picker or tap must be installed to remove the current from the cable. This "picked-off" current is routed to the power jack.

To minimize the possibility of damage to equipment in the event of a malfunction, the more sophisticated PoE systems employ fault protection. This feature shuts off the power supply if excessive current or a short circuit is detected.

Network Switch

A network switch is a small hardware device that joins multiple computers together within one local area network (LAN). Technically, network switches operate at layer two (Data Link Layer) of the OSI model.

Network switches appear nearly identical to network hubs, but a switch generally contains more intelligence (and a slightly higher price tag) than a hub. Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately. By delivering messages only to the connected device intended, a network switch conserves network bandwidth and offers generally better performance than a hub.

As with hubs, Ethernet implementations of network switches are the most common. Mainstream Ethernet network switches support either 10/100 Mbps Fast Ethernet or Gigabit Ethernet (10/100/1000) standards.

Different models of network switches support differing numbers of connected devices. Most consumer-grade network switches provide either four or eight connections for Ethernet devices. Switches can be connected to each other, a so-called daisy chaining method to add progressively larger number of devices to a LAN.

LAN (Local Area Network)
A local area network (LAN) supplies networking capability to a group of computers in close proximity to each other such as in an office building, a school, or a home. A LAN is useful for sharing resources like files, printers, games or other applications. A LAN in turn often connects to other LANs, and to the Internet or other WAN.

Most local area networks are built with relatively inexpensive hardware such as Ethernet cables, network adapters, and hubs. Wireless LAN and other more advanced LAN hardware options also exist.

Specialized operating system software may be used to configure a local area network. For example, most flavors of Microsoft Windows provide a software package called Internet Connection Sharing (ICS) that supports controlled access to LAN resources.

The term LAN party refers to a multiplayer gaming event where participants bring their own computers and build a temporary LAN.

WAN
A wide area network (WAN) is a telecommunications network, usually used for connecting computers, that spans a wide geographical area. WANs can by used to connect cities, states, or even countries. WANs are often used by larger corporations or organizations to facilitate the exchange of data, and in a wide variety of industries, corporations with facilities at multiple locations have embraced WANs. Increasingly, however, even small businesses are utilizing WANs as a way of increasing their communications capabilities.

Although WANs serve a purpose similar to that of local area networks (LANs), WANs are structured and operated quite differently. The user of a WAN usually does not own the communications lines that connect the remote computer systems; instead, the user subscribes to a service through a telecommunications provider. Unlike LANs, WANs typically do not link individual computers, but rather are used to link LANs. WANs also transmit data at slower speeds than LANs. WANs are also structurally similar to metropolitan area networks (MANs), but provide communications links for distances greater than 50km.

Router
Network router is a device or a piece of software in a computer that forwards and routes data packets along networks. A network router connects at least two networks, commonly two LANs or WANs or a LAN and its ISP network. A router is often included as part of a network switch. A router is located at where one network meets another, including each point-of-presence on the Internet. A router has two key jobs:

- The router ensures that information doesn't go where it's not needed. This is crucial for keeping large volumes of data from clogging the network.
- The router makes sure that information does make it to the intended destination.

In performing these two jobs, a router joins the two networks, passing information from one to the other and, in

some cases, performing translations of various protocols between the two networks. It also protects the networks from one another, preventing the traffic on one from unnecessarily spilling over to the other. This process is known as routing.

Routing is a function associated with the Network layer (layer 3) in the Open Systems Interconnection (OSI) model. Routers use network layer protocol headers, such as IP header where the source and destination addresses are included and routing tables to determine the best path to forward the packets. For the communication among routers and decide the best route between any two hosts, routing protocols such as ICMP are used.

Actually, routers are specialized computers that send messages speeding to their destinations along thousands of possible pathways. One of the tools a router uses to decide which path a packet should go is a routing table. A routing table contains a collection of information, including:

- Information on which connections lead to particular groups of addresses
- Priorities for connections to be used
- Rules for handling both routine and special cases of traffic

Information in the routing tables can be static (with routes manually entered by the network administrator) or dynamic (where routers communicate to exchange connection and route information using various routing protocols). A routing table can be as simple as a few lines in the smallest routers, but can grow to massive size and complexity in the very large routers that handle the bulk of Internet messages. As the number of networks attached to one another grows, the routing table for handling traffic among them grows, and the processing power of the router is increased.

DNS
DNS stands for Domain Name System. It purpose is to allow mapping between Internet names (eg : www.netvigilance.com) and IP addresses (eg : 97.11.12.13). It is based on a distributed network of name servers that allow the resolution of names in a hierarchical namespace, sharing the same "root". Therefore, The Domain Name System is a critical part of the Internet, because domain names are much 'more friendly' than raw IP addresses, a bit like Yellow Pages indexing Telephone numbers against business names.

DHCP
Short for Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

The DHCP is usually managed by the ADSL router on the network, or in the case of a larger network a domain server acting as DCHP for the network.

IPV4
IPv4 is the most widely used version of the Internet Protocol. It defines IP addresses in a 32-bit format, which looks like 123.123.123.123. Each three-digit section can include a number from 0 to 255, which means the total number of IPv4 addresses available is 4,294,967,296 (256 x 256 x 256 x 256 or 2^32).

Each computer or device connected to the Internet must have a unique IP address in order to communicate with other systems on the Internet. Because the number of systems connected to the Internet is quickly approaching the number of available IP addresses, IPv4 addresses are predicted to run out soon. When you consider that there are over 6 billion people in the world and many people have more than one system connected to the

Internet (for example, at home, school, work, etc.), it is not surprising that roughly 4.3 billion addresses is not enough.

To solve this problem, a new 128-bit IP system, called IPv6, has been developed and is in the process of replacing the current IPv4 system. During this transitional process from IPv4 to IPv6, systems connected to the Internet may be assigned both an IPv4 and IPv6 address.

IPV6
This led to the development of a new version of IP called IPv6 (IP version 6), also known as IPng (IP new generation). You will ask what happened to version 5. Well, it was developed, but remained in the domain of research. IPv6 is the version that is ready to be deployed over the whole Internet and be adopted by all human beings (and any creature) using the Internet and networks. IPv6 brings many improvements, mainly in the number of machines that can be accommodated on the Internet.

> *IPv6 Described*
> *An IPv6 address consists of 128 bits, therefore allowing an astronomical number of machines. This is equivalent to the value of 2 raised to the power of 128, a number with nearly 40 trailing zeros.*
>
> *You must now be thinking of the inconvenience of lengthy addresses. This is addressed too - IPv6 address have rules to compress them. First, the numbers are represented in hexadecimal instead of decimal numbers. Decimal numbers are numbers from 0 to 9. Hexadecimal numbers result from the grouping of bits in 4, giving the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. An IPv6 address is made up of these characters. Since the bits are grouped in 4, and IPv6 address will consist of 32 characters. Long, heh? Well, that's not so serious, especially since there are conventions that help reduce the length of IPv6 address by compressing characters of repetition, for example.*
>
> *An example of an IPv6 address is* ***fe80::240:d0ff:fe48:4672****. This one has only 19 characters - there has been compression, something that goes beyond the scope of this article. Note that the separator has changed from the dot to the colon.*
>
> *IPv6 not only solves the problem of address limitation, but also brings other improvements to the IP protocol, like auto-configuration on routers and improved security, among others.*
>
> *Transition From IPv4 to IPv6*
> *The day when IPv4 will no longer be viable is coming, and now that IPv6 is around, the biggest challenge is to make the transition from IPv4 to IPv6. Imagine renewing the bitumen of a road under heavy traffic. There are many discussions, publications and research work going on and we hope that when the time comes, the transition will work out smoothly. This led to the development of a new version of IP called IPv6 (IP version 6), also known as IPng (IP new generation). You will ask what happened to version 5. Well, it was developed, but remained in the domain of research. IPv6 is the version that is ready to be deployed over the whole Internet and be adopted by all human beings (and any creature) using the Internet and networks. IPv6 brings many improvements, mainly in the number of machines that can be accommodated on the Internet.*