Understanding Wi-Fi and Wireless Technology

Working for the Benefit of the Broadband Industry

Reference Manual

www.theSCTE.eu

Welcome to the SCTE Manual

This handbook is designed as a stand-alone reference manual for technicians working in the broadband telecommunications industry. It may be used either on its own or as an integral part of a classroom course including practical work to enable the student to progress to examination and certification.

We hope you and your career benefit greatly from this handbook and associated training course. Please consider joining the SCTE and taking advantage of the benefits that come from being part of the industry's foremost technical institution.

About the SCTE

Founded in 1945, the SCTE is a non-profit making organisation, managed by an Executive Committee of elected volunteers, whose aim is to raise the standard of broadband engineering in the telecommunications industry. The Society particularly concerns itself with the training and career advancement of technical professionals in this field.

First introduced in 1994, the SCTE training courses have achieved wide acceptance as the standard for young technicians wishing to enter the field of cable telecommunications and for those wishing to advance their knowledge and career prospects. They are used in-house by a number of operating companies and SCTE engineers can be found working in a variety of international organisations.

As a Learned Society, SCTE is able to provide accreditation and certification for its members, giving them professional standing within the industry. Full Members and Fellows are allowed to use the designations MSCTE and FSCTE after their names whilst Technician Members may use TMSCTE. There are also categories for Student and Associate Members which carry the designations SMSCTE and AMSCTE respectively.

Copyright & Acknowledgements

Published by the SCTE, Communications House, 41a Market Street, Watford, WD18 0PN, UK
Tel:+44 1923 815500 Fax:+44 1923 803203
Email: office@theSCTE.eu Website: www.theSCTE.eu

First published in UK in 2018. ISBN No:

Issue 1 November 2018

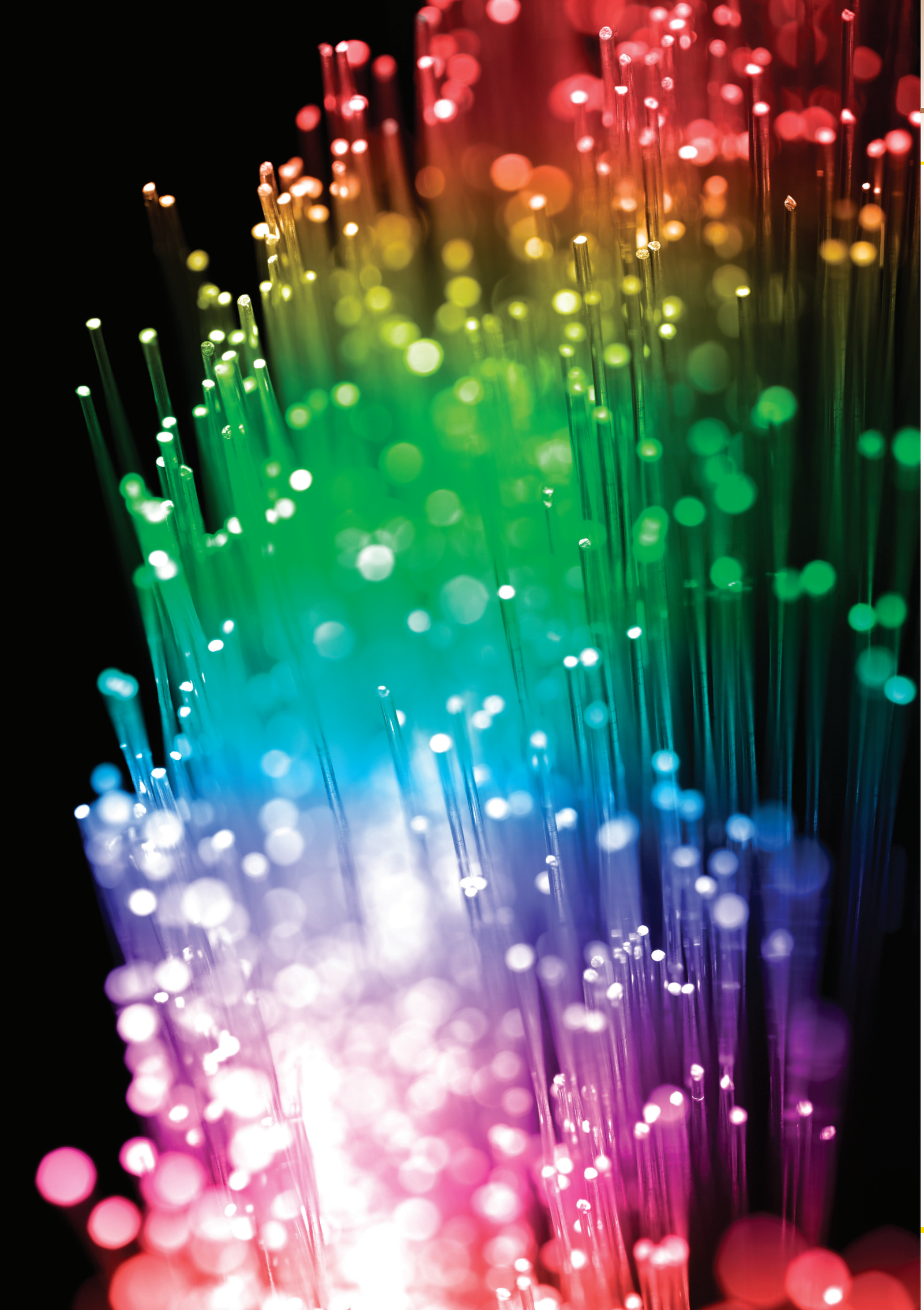
Contents

Contents

Contents

Contents

Appendices



Section One

1.1 Wireless

Wireless communication, or sometimes simply wireless, is the transfer of information or power between two or more points that are not connected by an electrical conductor. The most common wireless technologies use radio waves. With radio waves distances can be short, such as a few meters for Bluetooth or as far as millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking (Wi-Fi). Other examples of applications of radio wireless technology include Global Positioning System (GPS) units, garage door openers, wireless computer mice, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones.

1.2 Wi-Fi

Wi-Fi is the main wireless technology in the home for connectivity of home computers using a Wireless Local Area Network(WLAN) to the internet Wide Area Network (WAN). Most consumers already have this technology in their home, so adding home automation functions via Wi-Fi should be easier and cheaper.

1.3 Internet Of Things

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enable these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities.

1.3.1 Platform Fragmentation

IoT suffers from platform fragmentation and lack of technical standards a situation where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology ecosystems hard. Customers may be hesitant to bet their IoT future on proprietary software or hardware devices that uses proprietary protocols that may fade or become difficult to customize and interconnect.

IoT's amorphous computing nature is also a problem for security, since patches to bugs found in the core operating system often do not reach users of older and lower-price devices. One set of researchers say that the failure of vendors to support older devices with patches and updates leaves more than 87% of active devices vulnerable.

1.3.2 Security

Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary.

Most of the technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IoT devices.

1.4 Home Automation

Home automation is building automation for a home, called a smart home or smart house. It involves the control and automation of lighting, heating (such as smart thermostats), ventilation, air conditioning (HVAC), and security, as well as home appliances such as washer/dryers, ovens or refrigerators/freezers.

Wi-Fi is often used for remote monitoring and control. Home devices, when remotely monitored and controlled via the Internet, are an important constituent of the Internet of Things. Modern systems generally consist of switches and sensors connected to a central hub sometimes called a “gateway” from which the system is controlled with a user interface that is interacted either with a wall-mounted terminal, mobile phone software, tablet computer or a web interface, often but not always via Internet cloud services.

While there are many competing vendors, there are very few worldwide accepted industry standards and the smart home space is heavily fragmented. Manufacturers often prevent independent implementations by withholding documentation and by litigation.

The home automation market was worth £5.0 billion in 2013, predicted to reach a market value of £12.81 billion by the year 2020.

Section Two

2.1 Introduction

Wi-Fi or Wireless Fidelity is an established world-wide networking standard which incorporates the use of radio waves to link computers and other network devices together.

- Allows you to instantly create a home or office network without running cables.
- Allows you to share high-speed Internet wirelessly.
- Listen to streaming audio and view video.
- Synchronize and uplink mobile devices.

2.2 The Name Wi-Fi

The term Wi-Fi, commercially used at least as early as August 1999, was coined by brand-consulting firm Interbrand Corporation. The Wi-Fi Alliance had hired Interbrand to determine a name that was "a little catchier than 'IEEE 802.11b Direct Sequence'". Phil Belanger, a founding member of the Wi-Fi Alliance who presided over the selection of the name "Wi-Fi", also stated that Interbrand invented Wi-Fi as a play on words with hi-fi, and also created the Wi-Fi logo.

Figure 2.1: Wi-Fi Logo

The Wi-Fi Alliance used the "nonsense" advertising slogan "The Standard for Wireless Fidelity" for a short time after the brand name was invented, leading to the misconception that Wi-Fi was an abbreviation of "Wireless Fidelity". The yin-yang Wi-Fi logo indicates the certification of a product for interoperability.

Non-Wi-Fi technologies intended for fixed points, such as Motorola Canopy, are usually described as fixed wireless. Alternative wireless technologies include mobile phone standards, such as 2G, 3G, 4G or LTE.

The name is often written as **WiFi** or **Wifi**, but these are not approved by the Wi-Fi Alliance.

2.3 What Is Wi-Fi And How Does It Work?

Wi-Fi is a way of getting broadband internet to a device without using wires. Wi-Fi uses a wireless transmitter to send information to your computer. A transmitter converts information from the internet into a radio signal. This allows an electronic device to exchange data with the transmitter, sending information to and from the wireless device.

Radio Signals are the keys, which make Wi-Fi networking possible. These radio signals transmitted from Wi-Fi antennas are picked up by Wi-Fi receivers, such as computers and cell phones that are equipped with Wi-Fi cards. Whenever, a computer receives any of the signals within the range of a Wi-Fi network, which is usually 300 — 500 feet for antennas, the Wi-Fi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord.

Access points, consisting of antennas and routers, are the main source that transmit and receive radio waves. Antennas work stronger and have a longer radio transmission with a radius of 300-500 feet, which

are used in public areas while the weaker yet effective router is more suitable for homes with a radio transmission of 100-150 feet.

2.4 Wi-Fi Frequencies

Wi-Fi uses electromagnetic waves that run at a specific frequency. There are two main frequencies used for Wi-Fi, 2.4 Ghz (802.11b) and 5 Ghz (802.11a). Using 2.4 Ghz worked with mainstream devices and was the one that most people used. 802.11b was the Wi-Fi of choice for some years, mainly due to the fact that 11a was more expensive.

Wi-Fi equipment currently operates in license-exempt bands at 2.4 GHz and 5 GHz. Other bands may be used in the future. The frequencies used vary around the world and there are also differences in power levels and other technical aspects. These parameters are set by national regulatory bodies (Ofcom in the UK, FCC in the USA, for example). Wi-Fi equipment will usually allow the user to choose the country where it is to be used so that the regulatory parameters are adhered to.

2.4.1 The 2.4 GHz Band

In the UK, the 2.4 GHz band extends from 2400 MHz to 2483.5 MHz. Devices are limited to a maximum power of 100 mW eirp (effective isotropic radiated power; i.e. the power generated by the device modified by the gain of the antenna). Power levels are usually expressed in dBm (decibels above 1 mW). So 100 mW is equivalent to 20 dBm. If the antenna has a gain of, say, 5 dB then the power delivered to the antenna from the device must not exceed 15 dBm.

Channel numbers are often used instead of frequencies and there is an agreed list. The channels are spaced at 5 MHz intervals but start at 2412 MHz. The list of channel numbers is given in Table 2.1.

The channels start at 2412 MHz to give room for a 20 MHz channel and allow 2 MHz protection from the edge of the band. Similarly, 2472 MHz allows space at the top end of the band.

A consequence of this is that there are not really thirteen channels; in fact there is only room for three 20 MHz ones which don't overlap. In the USA, channels 1, 6 and 11 can be used; in Europe we have a bit more flexibility and can use channels 1, 7 and 13 for better spacing. It is theoretically possible to

Channel Number	Centre Frequency (MHz)	Notes
1	2412	
2	2417	
3	2422	
4	2427	
5	2432	
6	2437	
7	2442	
8	2447	
9	2452	
10	2457	
11	2462	
12	2467	Not available in USA
13	2472	Not available in USA
14	2484	Japan only (not on 5MHz spacing)

Table 2.1: Wi-Fi 2.4 GHz channel numbers

squeeze four 20 MHz channels in using channels 1, 5, 9 and 13 but this is rarely done because it requires very clean transmitters and selective receivers to avoid interference between channels.

Most Wi-Fi devices have the ability to use 40 MHz channels to double the throughput. In the USA, there is only room for one 40 MHz channel but in Europe it is possible to fit in two using the centre frequencies of channels 3 and 11. There is another peculiarity of 40 MHz channels in that the Wi-Fi system normally uses a 20 MHz channel and only transmits in the other half when there is enough data in the buffer. It is usual to specify the 40 MHz channel as, for example, 1 + 5 or, more precisely, “1 + upper” or “5 + lower”. These occupy the same bandwidth but 1 + upper means that channel 1 is normally used and channel 5 is used when necessary; 5 + lower is the other way round. The one that is chosen depends on the presence of other signals in the locality.

Many installers try to avoid using 40 MHz channels in the 2.4 GHz band because of the difficulty of avoiding interference.

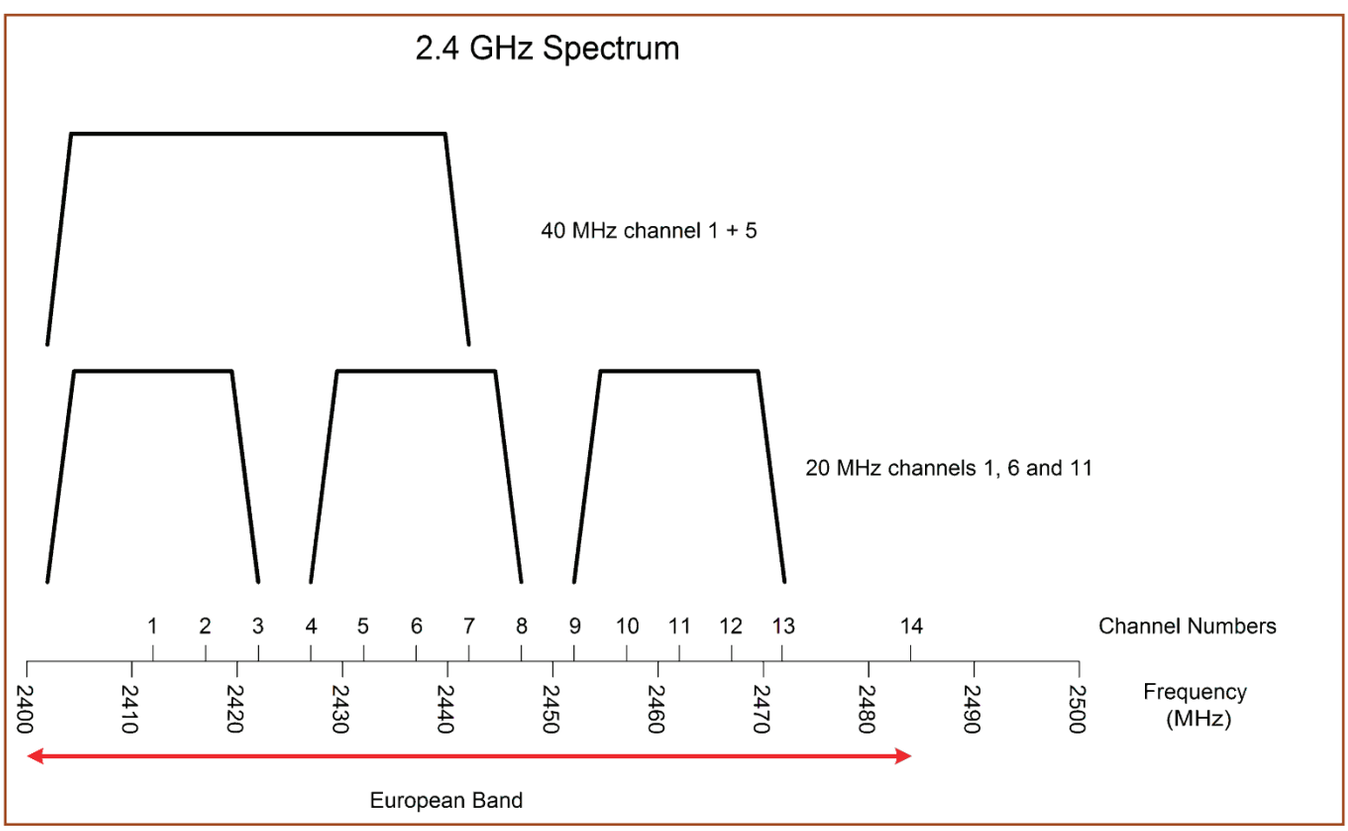


Figure 2.2: Wi-Fi 2.4 GHz Spectrum

2.4.2 The 5 GHz Band

The 5 GHz band is even more complicated than the 2.4 GHz band. However, there is much more spectrum available so it is easier to plan the channel usage. The specifications and the available chips cover the band from 5000 MHz to 6000 MHz. The channel numbers are more logical in that channel 1 is 5005 MHz and channel 199 is 5995 MHz. The available frequencies, power levels and other regulatory parameters vary considerably from country to country.

The following covers the situation in the UK as defined by Ofcom. There are three distinct bands:

Band	Frequencies (MHz)	Usage	Maximum Radiated Power
A	5150 to 5350	Indoor - license exempt	200 mW (23 dBm)
B	5470 to 5725	Indoor or outdoor - license exempt	1 W (30 dBm)
C	5725 to 5850	Lightly licensed for Fixed wireless access (FWA)	4 W (36 dBm)

Table 2.2: 5 GHz frequency bands

Band A is restricted to indoor use in an attempt to avoid interference with certain satellite systems which use the same band. Band C is used for providing wireless Internet connections and not currently permitted for Wi-Fi but may well be added in the future although the Wi-Fi power limit is not likely to be increased.

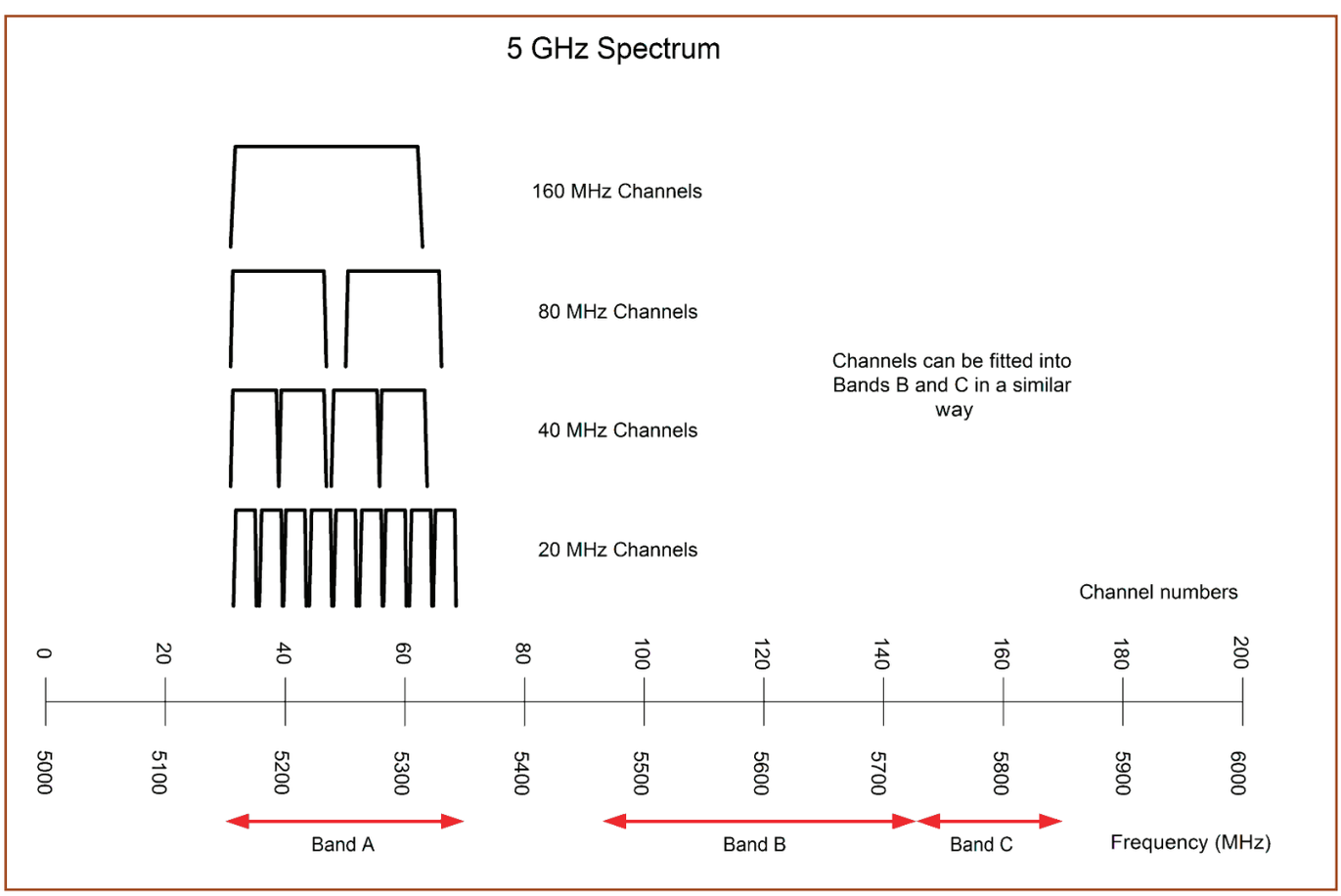


Figure 2.3: Wi-Fi 5 GHz Spectrum

The 5 GHz is band also complicated in that there are several measures to reduce interference between Wi-Fi and other users of the band. Wi-Fi devices have to use Dynamic Frequency Selection (DFS). The idea is that, when switched on, a Wi-Fi device should check whether there are any signals from radar systems on its chosen channel, if there are, it must choose another channel. DFS is not required at the bottom of band A (5150 to 5240) but all other 5 GHz channels must use it. Many 5 GHz routers do not offer DFS channels

so cannot take advantage of the extra spectrum. However, DFS can be a problem to the user; if the router detects a radar signal it will stop transmitting for quite a long period; this could be as long as half an hour.

5 GHz Wi-Fi devices should use the minimum power to achieve the required performance so as to reduce interference; some devices adjust their power automatically.

Note that Wi-Fi devices designed for the USA market will often be illegal if used in the UK because Band C is available for indoor use in the USA.

2.5 Wi-Fi is Half Duplex

All Wi-Fi networks are contention-based Time Division Duplex (TDD) systems, where the access point and the mobile stations all vie for use of the same channel. Because of the shared media operation, all Wi-Fi networks are half duplex.

The coding mechanisms detailed above describe a single direction of transmission. Obviously, real systems need to be able to send data in both directions at the same time. It is theoretically possible to use one channel for one direction of transmission and another for the other direction; however, this would require extremely sharp, high-performance filters. It would also be expensive and use a lot of spectrum.

The method used in the 802.11x series of standards is to occupy one channel and use it either in one direction or the other. Clearly, this can't achieve truly simultaneous transmission but if the delay is kept short, the attached systems will be happy. Note that if the system sends, say, equal amounts of data in each direction the effective throughput in each direction will be halved. Luckily, this situation rarely occurs in practice and the apparent speed is very similar to the maximum.

The problem of sharing a connection that can only support one direction of transmission at a time is very common in communications systems and there are many ways of solving the problem. Perhaps the best known is ethernet where, originally, a single cable was used. Stations transmit when they have data to send but can see whether the data is damaged by other stations sending at the same time; this situation is called a collision. If ethernet devices detect a collision they wait a random time and try again. This mechanism works very well. It is called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

The CSMA/CD scheme is not directly applicable to 802.11 because a transmitter cannot tell whether another device is transmitting at the same time and causing a collision. However, it can tell after the event because it will not receive an acknowledgement from the receiving device. If an 802.11 device finds that its data was damaged it will wait for a period and try again. If the problem occurs again it will wait longer in an attempt to avoid future collisions. This scheme is called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and works well as long as the system is not heavily loaded.

The modulation and coding mechanism is known in 802.11 as the physical layer, or PHY layer. The higher protocols are called the Media Access Control or MAC layer.

The protocols used between an access point and a client are more complicated than described here to handle many different situations but this overview should give a good idea of the basics. More detail can be found in the standards documents which can be downloaded from the IEEE 802 website. Be warned that these documents were written by committee, have to be unambiguous and, therefore, are difficult to understand. Standards are made available for free six months after publication.

2.5.1 Duplex

A duplex communication system is a point-to-point system composed of two connected parties or devices that can communicate with one another in both directions. There are two types of duplex communication systems: full-duplex (FDX) and half-duplex (HDX). Duplex systems are employed in many communications networks, either to allow for a communication "two-way street" between two connected parties or to provide a "reverse path" for the monitoring and remote adjustment of equipment in the field.

2.5.1.1 Simplex

The simplex transmission is the one that travels in only one direction. For example, in TV and radio broadcasting, information flows only from the transmitter site to multiple receivers. This way of transmission can be also called unidirectional or one-way transmission.

2.5.1.2 Half Duplex

In a half-duplex system, each party can communicate with the other but not simultaneously; the communication is one direction at a time. An example of a half-duplex device is a walkie-talkie two-way radio that has a "push-to-talk" button; when the local user wants to speak to the remote person they push this button, which turns on the transmitter but turns off the receiver, so they cannot hear the remote person. To listen to the other person they release the button, which turns on the receiver but turns off the transmitter.

2.5.1.3 Full Duplex

In a full-duplex system, both parties can communicate with each other simultaneously. An example of a full-duplex device is a telephone; the parties at both ends of a call can speak and be heard by the other party simultaneously. The earphone reproduces the speech of the remote party as the microphone transmits the speech of the local party, because there is a two-way communication channel between them, or more strictly speaking, because there are two communication paths/channels between them.

2.6 Wi-Fi Certification

The Wi-Fi Alliance owns and controls the “Wi-Fi Certified” logo, a registered trademark, which is permitted only on equipment which has passed testing. Purchasers relying on that trademark will have greater chances of interoperation than otherwise. Testing involves not only radio and data format interoperability, but security protocols, as well as optional testing for quality of service and power management protocols. A focus on user experience has shaped the overall approach of the Wi-Fi Alliance certification program: Wi-Fi Certified products have to demonstrate that they can perform well in networks with other Wi-Fi Certified products, running common applications, in situations similar to those encountered in everyday use. This pragmatic approach stems from three tenets, around which certification is centered: Interoperability is the primary target of certification. Rigorous test cases are used to ensure that products from different equipment vendors can interoperate in a wide variety of configurations.

Backward compatibility has to be preserved to allow for new equipment to work with existing gear. Backward compatibility protects investments in legacy Wi-Fi products and enables users to gradually upgrade and expand their networks.

Innovation is supported through the introduction of new certification programs as the latest technology and specifications come into the marketplace. These certification programs may be mandatory (e.g. Wi-Fi Protected Access 2 - WPA2) or optional (e.g. Wi-Fi Multi Media - WMM). Equipment vendor differentiation and inventiveness are preserved in areas that are not covered by certification testing.

The Wi-Fi Alliance definition of interoperability goes well beyond the ability to work in a Wi-Fi network. To gain certification under a specific program, products have to show satisfactory performance levels in typical network configurations and have to support both established and emerging applications. A user that purchases a Wi-Fi enabled laptop, for instance, would not be satisfied if the laptop established a connection with the home network, only to get the throughput of a dial-up connection. Similarly, subscribers using a Wi-Fi enabled mobile phone would be disappointed, if a voice call could not go through or was dropped. The Wi-Fi Alliance certification process includes three types of tests to ensure interoperability. Wi-Fi Certified products are tested for:

Compatibility: certified equipment has been tested for connectivity with other certified equipment. Compatibility testing has always been, and still is, the predominant component of interoperability testing, and it is the element that most people associate with “interoperability”. It involves tests with multiple devices from different equipment vendors. Compatibility testing is the program component that helps to ensure devices purchased today will work with Wi-Fi Certified devices already owned or purchased in the future.

Conformance: the equipment conforms to specific critical elements of the IEEE 802.11 standard. Conformance testing usually involves standalone analysis of individual products and establishes whether the equipment responds to inputs as expected and specified. For example, conformance testing is used to ensure that Wi-Fi equipment protects itself and the network when the equipment detects evidence of network attacks.

Performance: the equipment meets the performance levels required to meet end-user expectations in support of key applications. Performance tests are not designed to measure and compare performance among products, but simply to verify that the product meets the minimum performance requirements for a good user experience as established by the Wi-Fi Alliance. Specific performance tests results are not released by the Wi-Fi Alliance.

The Wi-Fi Alliance provides certification testing in two levels:

2.6.1 Wi-Fi Certification - Mandatory

- Core MAC/PHY interoperability over 802.11a, 802.11b, 802.11g, and 802.11n. (at least one).
- Wi-Fi Protected Access 2 (WPA2) security, which aligns with IEEE 802.11i.
- WPA2 is available in two types: WPA2-Personal for consumer use, and WPA2 Enterprise, which adds EAP authentication.

2.6.2 Wi-Fi Certification - Optional

- Tests corresponding to IEEE 802.11h and 802.11d.
- WMM Quality of Service, based upon a subset of IEEE 802.11e.
- WMM Power Save, based upon Automatic Power Save Delivery (APSD) within IEEE 802.11e.
- Wi-Fi Protected Setup, a specification developed by the Alliance to ease the process of setting up and enabling security protections on small office and consumer Wi-Fi networks.
- Application Specific Device (ASD), for wireless devices other than Access Point and Station which has specific application, such as Digital Versatile Disc (DVD) players, projectors, printers, etc.
- Converged Wireless Group–Radio Frequency (CWG-RF, offered in conjunction with Cellular Telecommunications and Internet Association (CTIA)), to provide performance mapping of Wi-Fi and cellular radios in converged devices.
- Passpoint/Hotspot 2.0.

2.7 Wi-Fi Direct

In October 2010, the Alliance began to certify Wi-Fi Direct. Initially called Wi-Fi P2P (Peer to Peer), is a Wi-Fi standard enabling devices to easily connect with each other without requiring a wireless access point. It is useful for everything from internet browsing to file transfer, and to communicate with one or more devices simultaneously at typical Wi-Fi speeds. One advantage of Wi-Fi Direct is the ability to connect devices even if they are from different manufacturers. Only one of the Wi-Fi devices needs to be compliant with Wi-Fi Direct to establish a peer-to-peer connection that transfers data directly between them with greatly reduced setup.

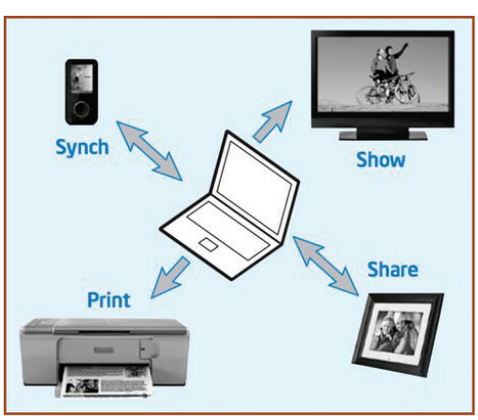


Figure 2.4: Wi-Fi Direct

Wi-Fi Direct negotiates the link with a Wi-Fi Protected Setup system that assigns each device a limited wireless access point. The “pairing” of Wi-Fi Direct devices can be set up to require the proximity of a near field communication, a Bluetooth signal, or a button press on one or all the devices. Since 2009 when it was first announced, some suggested Wi-Fi Direct might replace the need for Bluetooth on applications that do not rely on Bluetooth low energy.

2.8 Wi-Fi Aware

Wi-fi aware is a protocol launched in January 2015, with the aim of users devices when in the range of a particular access point or other compatible device can receive notifications of applications available to them relevant to the location they are in.

Fears were voiced immediately in media that it would be predominately used for proximity marketing.

2.9 Wi-Fi Uses

To connect to a Wi-Fi LAN, a computer has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a station. For all stations that share a single radio frequency communication channel, transmissions on this channel are received by all stations within range. The transmission is not guaranteed to be delivered and is therefore a best-effort delivery mechanism. A carrier wave is used to transmit the data. The data is organised in packets, referred to as “Ethernet frames”.

2.9.1 Internet

Wi-Fi technology may be used to provide Internet access to devices that are within the range of a wireless network that is connected to the Internet. The coverage of one or more interconnected access points (hotspots) can extend from an area as small as a few rooms to as large as many square kilometres. Coverage in the larger area may require a group of access points with overlapping coverage. For example, public outdoor Wi-Fi technology has been used successfully in wireless mesh networks in London, UK.

Wi-Fi provides service in private homes, businesses, as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially, often using a captive portal webpage for access. Organizations and businesses, such as airports, hotels, and restaurants, often provide free-use hotspots to attract customers. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access.

Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other buildings, provide Internet access and internetworking to all devices connected to them, wirelessly or via cable.

Similarly, battery-powered routers may include a cellular Internet radio modem and Wi-Fi access point. When subscribed to a cellular data carrier, they allow nearby Wi-Fi stations to access the Internet over 2G, 3G, or 4G networks using the tethering technique. Many smartphones have a built-in capability of this sort, including those based on Android, BlackBerry, iOS (iPhone), Windows Phone and Symbian, though

carriers often disable the feature, or charge a separate fee to enable it, especially for customers with unlimited data plans. “Internet packs” provide standalone facilities of this type as well, without use of a smartphone; examples include the Mobile Wi-Fi (MiFi) and Wireless Broadband (WiBro) - branded devices. Some laptops that have a cellular modem card can also act as mobile Internet Wi-Fi access points.

Wi-Fi also connects places that normally don’t have network access, such as kitchens and garden sheds.

2.9.2 City-Wide Wi-Fi

In the early 2000s, many cities around the world announced plans to construct city-wide Wi-Fi networks. There are many successful examples; in 2004, Mysore became India’s first Wi-Fi-enabled city. A company called Wi-FiyNet has set up hotspots in Mysore, covering the complete city and a few nearby villages.

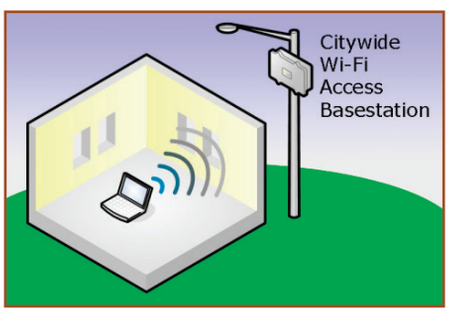


Figure 2.5: City-wide Wi-Fi

In 2005, St. Cloud, Florida and Sunnyvale, California, became the first cities in the United States to offer city-wide free Wi-Fi (from MetroFi). Minneapolis has generated £1 million in profit annually for its provider.

In May 2010, London, UK, Mayor Boris Johnson pledged to have London-wide Wi-Fi by 2012. Several boroughs including Westminster and Islington already had extensive outdoor Wi-Fi coverage at that point.

Officials in South Korea’s capital are moving to provide free Internet access at more than 10,000 locations around the city, including outdoor public spaces, major streets and densely populated residential areas. Seoul will grant leases to KT, LG Telecom and SK Telecom. The companies will invest £30 million in the project.

2.9.3 Campus-Wide Wi-Fi

Many traditional university campuses in the developed world provide at least partial Wi-Fi coverage. Carnegie Mellon University built the first campus-wide wireless Internet network, called Wireless Andrew, at its Pittsburgh campus in 1993 before Wi-Fi branding originated. By February 1997 the CMU Wi-Fi zone was fully operational. Many universities collaborate in providing Wi-Fi access to students and staff through the eduroam international authentication infrastructure.

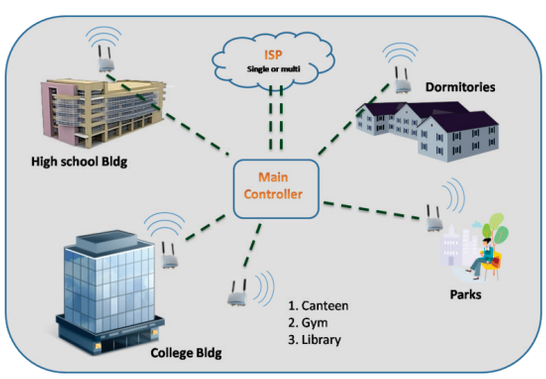


Figure 2.6: Campus-wide Wi-Fi

2.9.4 Computer-To-Computer

Wi-Fi also allows communications directly from one computer to another without an access point intermediary. This is called ad hoc Wi-Fi transmission. This wireless ad hoc network mode has proven popular with multiplayer handheld game consoles, such as the Nintendo DS, PlayStation Portable, digital cameras, and other consumer electronics devices. Some devices can also share their Internet connection using ad hoc, becoming hotspots or “virtual routers”.

Similarly, the Wi-Fi Alliance promotes the specification Wi-Fi Direct for file transfers and media sharing through a new discovery- and security-methodology.

Another mode of direct communication over Wi-Fi is Tunneled Direct Link Setup (TDLS), which enables two devices on the same Wi-Fi network to communicate directly, instead of via the access point.

2.10 Wi-Fi Cards

You can think of Wi-Fi cards as being invisible cords that connect your computer to the antenna for a direct connection to the internet.

Wi-Fi cards can be external or internal. If a Wi-Fi card is not installed in your computer, then you may purchase a USB antenna attachment and have it externally connect to your USB port, or have an antenna-equipped expansion card installed directly to the computer (as shown in the figure given above). For laptops, this card will be a PCMCIA card which you insert to the PCMCIA slot on the laptop.

Figure 2.7: SD Memory Wi-Fi Card

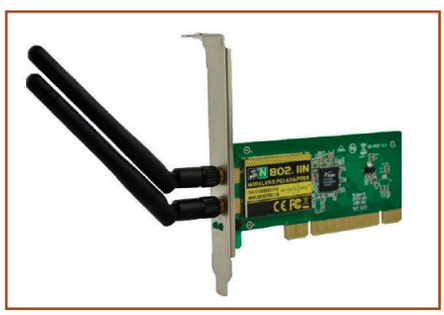


Figure 2.8: Internal Wi-Fi Card

Figure 2.9: Wi-Fi USB plugin card

2.11 Wi-Fi Hotspots

A Wi-Fi hotspot is created by installing an access point to an internet connection. The access point transmits a wireless signal over a short distance. It typically covers around 300 feet. When a Wi-Fi enabled device such as a Tablet PC encounters a hotspot, the device can then connect to that network wirelessly.

Figure 2.10: Wi-Fi Hotspot

Most hotspots are located in places that are readily accessible to the public such as airports, coffee shops, hotels, book stores, and campus environments. 802.11b is the most common specification for hotspots worldwide. The 802.11g standard is backwards compatible with .11b but .11a uses a different frequency range and requires separate hardware such as an a, a/g, or a/b/g adapter. The largest public Wi-Fi networks are provided by private internet service providers (ISPs); they sometimes charge a fee to the users who want to access the internet.

Hotspots are increasingly developing around the world. In fact, T-Mobile USA controls more than 4,100 hotspots located in public locations such as coffee shops, book shops, and the airline lounges. Even select high street restaurants now feature Wi-Fi hotspot access.

Any notebook computer with integrated wireless, a wireless adapter attached to the motherboard by the manufacturer, or a wireless adapter such as a PCMCIA card can access a wireless network. Furthermore, all Pocket PCs or Palm units with Compact Flash, SD I/O support, or built-in Wi-Fi, can access hotspots.

Some Hotspots require Wireless Equivalency Privacy (WEP) key to connect, which is considered as private and secure. As for open connections, anyone with a Wi-Fi card can have access to that hotspot. So in order to have internet access under WEP, the user must input the WEP key code.

If no security is used then anybody on a hotspot in theory could monitor other PC communications on that hotspot.

Understanding Wi-Fi and Wireless Technology

Working for the Benefit of the Broadband Industry

Reference Manual

www.theSCTE.eu