Wireless Networks

IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies including, but not limited to, 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands.

They are the world's most widely used wireless computer networking standards, used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires.

A **wireless network** enables people to communicate and access applications and information without wires. This provides freedom of movement and the ability to extend applications to different parts of a building, city, or nearly anywhere in the world. Wireless networks allow people to interact with e-mail or browse the Internet from a location that they prefer.

Many types of wireless communication systems exist, but a distinguishing attribute of a wireless network is that communication takes place between computer devices. These devices include personal digital assistants (PDAs), laptops, personal computers (PCs), servers, and printers. Computer devices have processors, memory, and a means of interfacing with a particular type of network. Traditional cell phones don't fall within the definition of a computer device; however, newer phones and even audio headsets are beginning to incorporate computing power and network adapters. Eventually, most electronics will offer wireless network connections.

As with networks based on wire, or optical fiber, wireless networks convey information between computer devices. The information can take the form of e-mail messages, web pages, database records, streaming video or voice. In most cases, wireless networks transfer data, such as e-mail messages and files, but advancements in the performance of wireless networks is enabling support for video and voice communications as well.

Types of Wireless Networks

WLANS: Wireless Local Area Networks

WLANS allow users in a local area, such as a university campus or library, to form a network or gain access to the internet. A temporary network can be formed by a small number of users without the need of an access point; given that they do not need access to network resources.

A WLAN can be built using any of several different wireless network protocols, most commonly Wi-Fi or Bluetooth.

Network security remains an important issue for WLANs. Wireless clients usually have their identity verified (a process called authentication) when joining a wireless LAN. Technologies such as WPA raise the level of security on wireless networks to rival that of traditional wired networks.

WPANS: Wireless Personal Area Networks

The two current technologies for wireless personal area networks are Infra Red (IR) and Bluetooth (IEEE 802.15). These will allow the connectivity of personal devices within an area of about 30 feet. However, IR requires a direct line of site and the range is less.

WMANS: Wireless Metropolitan Area Networks

This technology allows the connection of multiple networks in a metropolitan area such as different buildings in a city, which can be an alternative or backup to laying copper or fiber cabling.

WWANS: Wireless Wide Area Networks

These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an ISP. These types of systems are referred to as 2G (2nd Generation) systems.

WLAN Hardware and Connections

WLAN connections work using radio transmitters and receivers built into client devices. Wireless networks don't require cables, but several special-purpose devices (also possessing their own radios and receiver antennas) are usually used to build them.

Local Wi-Fi networks, for example, can be constructed in either of two modes: ad-hoc or infrastructure.

Wi-Fi ad-hoc mode WLANs consist of peer-to-peer direct connections between clients with no intermediate hardware components involved. Ad-hoc local networks can be used to make temporary connections in some situations, but they don't scale to support more than a few devices and can pose security risks.

A Wi-Fi infrastructure mode WLAN uses a central device called a wireless access point (AP) that all clients connect to. In-home networks, wireless broadband routers perform the functions of an AP plus enable the WLAN for home internet access. Multiple APs can be interfaced to either and connect multiple WLANs into a larger one.

Some wireless LANs extend an existing wired network. This type of WLAN is built by attaching an access point to the edge of the wired network and setting up the AP to work in bridging mode. Clients communicate with the access point through the wireless link and can reach the Ethernet network through the AP bridge connection.

WLAN vs. WWAN

Cell networks support mobile phones that connect over long distances, a type of wireless wide area network (WWAN). What distinguishes a local network from a wide network are the usage models they support along with some rough limits on physical distance and area.

A local area network covers individual buildings or public hotspots, spanning hundreds or thousands of square feet. Wide area networks cover cities or geographic regions, spanning multiple miles.

IEEE 802.11 Network Components and Architectural Models :

IEEE 802.11 has two fundamental architectural components:

Station (STA): A STA is a wireless endpoint device/ client device. Typical examples of STAs are laptop computers, PDAs, mobile telephones, and other consumer electronic devices with IEEE 802.11 capabilities.

AP: An AP logically connects STAs with a distribution system (DS), which is typically an organization's wired infrastructure. APs can also logically connect wireless STAs with each other without accessing a DS. In addition, APs can function in a bridge mode, which allows APs to create point-to-point connections to join two separate networks.

The IEEE 802.11 standard defines two basic network topologies. The first, ad hoc mode, does not use APs—only STAs are involved in the communications. The second, infrastructure mode, has an AP that connects wireless STAs to each other or to a DS, typically a wired network. Infrastructure mode is the most commonly used mode for WLANs.

Common term used in wireless networking

Cellular

A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land areas called " cells ", each served by at least one fixed-location transceiver, but more normally, three cell sites or base transceiver stations.

The network is distributed over land areas called "**cells**", each served by at least one fixed-location transceiver, but more normally, three cell sites or base transceiver stations. These base stations provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. A cell typically uses a different set of frequencies from neighbouring cells, to avoid interference and provide guaranteed service quality within each cell.

When joined together, these cells provide radio coverage over a wide geographic area. This enables numerous portable transceivers (e.g., mobile phones, tablets and laptops equipped with mobile broadband modems, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

SSID (service set identifier)

A name assigned to a WLAN that allows stations to distinguish one WLAN from another.

An SSID (service set identifier) is the primary name associated with an 802.11 wireless local area network (WLAN) including home networks and public hotspots. Client devices use this name to identify and join wireless networks. In simple terms, it's the name of your WiFi network. Clients that wish to join a network scan an area for available networks and join by providing the correct SSID. The SSID, typically a null-terminated ASCII string, has a range from zero to 32 bytes (or characters). The default SSIDs used by many IEEE 802.11 WLAN vendors have been published and are well-known, so the default SSID values of APs should be changed from the factory default to

an unidentifiable value or non-discrete name to help prevent users from accidentally connecting to the wrong WLAN and to make it somewhat more difficult for attackers to identify the organization's WLANs. Organizations should be aware that adversaries can capture the SSID by eavesdropping, so organizations should not rely on changing SSIDs to protect their WLANs.

Access Point(AP)

A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.

Antenna

An antenna is an electrical conductor or a system of conductors that radiates/collects (transmits or receives) electromagnetic energy into/from space. Antennas are an essential part of the design aspect of a wireless network.

APs with internal antennas usually have an omni-directional coverage pattern. This coverage pattern is fixed and only varies depending on the orientation of the mounted AP. Typically the AP will be mounted on the ceiling with most of the radiation propagating downwards. In almost all indoor deployments, such as offices, schools, hotels, etc., ceilings mounted APs with internal antennas provide adequate coverage and satisfy aesthetic requirements.

When deploying external antennas, more control is gained over the energy radiated. Compared to internal antennas, which have fixed coverage patterns, external antennas can tailor the shape based of coverage needed — to meet the most challenging design requirements.

Hotspot

A **hotspot** is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local-area network (WLAN) using a router connected to an Internet service provider.

Public hotspots may be created by a business for use by customers, such as coffee shops or hotels. Public hotspots are typically created from wireless access points configured to provide Internet access, controlled to some degree by the venue. In its simplest form, venues that have broadband Internet access can create public wireless access by configuring an access point (AP), in conjunction with a router to connect the AP to the Internet. A single wireless router combining these functions may suffice.

A private hotspot, often called tethering, may be configured on a smartphone or tablet that has a network data plan, to allow Internet access to other devices via Bluetooth pairing.

Security is a serious concern in connection with public and private hotspots. There are three possible attack scenarios. First, there is the wireless connection between the client and the access point, which needs to be encrypted, so that the connection cannot be eavesdropped or attacked by a man-in-the-middle attack. Second, there is the hotspot itself. The WLAN encryption ends at the interface, then travels its network stack unencrypted and then, third, travels over the wired connection up to the BRAS(**broadband remote access server)** of the ISP.

The BRAS sits at the edge of an ISP's core network, and aggregates user sessions from the access network. It is at the BRAS that an ISP can inject policy management and IP Quality of Service (QoS).

Bluetooth

Bluetooth is an open specification (universal) for short-range wireless voice and data communications. Inventors of Bluetooth are Ericsson, Nokia, IBM, Toshiba and Intel formed a Special Internet Group (SIG) to expand the concept and to develop a standard under **IEEE 802.15 WPAN** (Wireless Personal Area Network).

Bluetooth is the first widespread technology for a short-range ad-hoc network that is designed for combined voice and data application. Compared with Wifi, Bluetooth has a reduced data rate. However, it has an embedded mechanism to assist the application. Bluetooth is inexpensive personal area ad-hoc network operating in unlicensed lands and owned by the user.

Bluetooth topology is referred to as a scattered ad-hoc topology. It defines a small cell called Piconet which is a collection of devices connected in an ad-hoc fashion.
There are four states

1. **M(Master):** It can manage seven concurrent and up to 200 active slaves in the piconet.
2. **S(Slave):** Terminals which can take part in more than one piconet.
3. **SB(Stand by):** Waiting to join the piconet later meanwhile retaining its MAC address in it.
4. **P(Parked/hold):** Waiting to adhere to the piconet later and releases its MAC address.

Bluetooth Architecture

Physical connection

The **FHSS (frequency hopping spread spectrum)** modem is utilized in the physical connection of the Bluetooth with a nominal antenna power of 0 dBm(10 m coverage) and alternately operated at 20 dBm(100 m coverage). Bluetooth hopping rate is 1600 hops/second. Bluetooth allocates a specific frequency- hopping format for each piconet.

Connection management

The connection establishment in Bluetooth has two phases- **Inquiry**, **page** and **connection**. Active devices are allocated a 3 bit **AMA (Active Member Address),** Parked devices are assigned an 8-bit **PMA (Parked Member Address)**, Standby devices do not need an address.

Bluetooth Connection Management

1. **Sniff State:** Slaves listens to the piconet at minimized rates.

2. **Hold state:** Slave stops ACL (Asynchronous Connection Less) transmission but can exchange SCO (Synchronous Connection Oriented) packets.
3. **Park state:** Slave releases its AMA.
4. **Page state:** AMA is assigned (becomes master).
5. **Connected state:** Listen, transmit and receive.
6. **Standby state:** Listen periodically.
7. **Inquiry state:** To discover what other devices are out there.

Security

Bluetooth offers usage security and information confidentiality. It uses a 128 bit long **random number**, 48-bit **MAC address** of the device and two keys – **Authentication** (128 bits) and **Encryption** (8 to 128 bits). Three modes of operation are **non-secure**, **service level** and **link level**.

Wifi

Wi-Fi **(Wireless Fidelity)** is the name given by the Wi-Fi Alliance to the **IEEE 802.11** suite of standards. 802.11 defined the initial standard for wireless local area networks **(WLANs)**, IEEE specifications are wireless standards that define an interface which uses are as the medium for transmitting and receiving signals between a wireless client and a station or access point, as well as among wireless clients.

The aim of the 802.11 standards was to develop a **MAC** and **PHY layer** for wireless connectivity for permanent, portable and mobile stations inside a local area.
IEEE 802.11 standard involves the following special features –

- It provides asynchronous and time-bounded delivery facility.
- It supports continuity of service within extended areas via distribution system.

Requirements of IEEE 802.11

1. Single MAC is supporting multiple PHYs'.
2. Mechanisms to allow multiple overlapping networks in the same area.
3. Provisions to manage the interface from other ISM based radios and microwave oven.
4. Mechanisms to manage "hidden" terminal.
5. Options to support time-bounded services.
6. Provision to handle privacy and access security.

Reference Architecture

There are two operations models or topologies defined in IEEE 802.11-

1. **Infrastructure mod:** In this mode, the wireless network comprises of minimum one access point (AP) which is generally linked to the wired network infrastructure and a collection of the wireless end station. Access controls encryption on the network and may bridge or route the wireless traffic to a wired ethernet network (or internet).
2. **Ad- hoc mode:** In this mode, multiple 802.11 wireless stations interact directly with each other in the absence of an access point or any connection to a wired

network. It is also called independent Basic service set (IBSS) or a peer-to-peer mode.

Security

IEEE 802.11 has provisions for authentication and privacy. Two types of authentication supported by IEEE 802.11 are-

1. **Open system authentication:** Default authentication scheme. The request frame sends the authentication algorithm ID for an open system. The response time sends the results of the request.
2. **Shared Key authentication:** It provides a greater amount of security. The request frame carries the authentication frames ID for the shared key using a 40-bit secret code that is shared between itself and IP. The 2nd station sends a challenge text of 128 bytes. The 1st station sends encrypted text as a response. The 2nd station sends authentication results.

Privacy is maintained in IEEE 802.11 by **WEP(wired equivalent privacy)** specification. A key sequence is constructed by a pseudorandom generator and 40-bit secret key where the key sequence is simply an XOR-ed with the plain-text message.

Basically, Bluetooth considered as short distance wireless communication while Wifi provides more privileges and long range, large number of users and cost effective way to connect to internet.

Comparison Chart

BASIS FOR COMPARISON	BLUETOOTH	WIFI
Bandwidth	Low	High
Hardware requirement	Bluetooth adapter on all the devices connecting with each other.	Wireless adapter on all the devices of the network and a wireless router.
Ease of Use	Fairly simple to use and switching between devices is easier.	It is more complex and requires configuration of hardware and software.

Range	10 meters	100 meters
Security	Less secure comparatively	Security features are better. Still, there are some risks.
Power consumption	Low	High
Frequency range	2.400 GHz and 2.483 GHz	2.4 GHz and 5 GHz
Flexibility	Supports limited number of user	It provides support for a large number of users

Attenuation in networking

Attenuation in computer networking is the loss of communication signal strength through automated monitoring that is measured in decibels (dB). As the rate of attenuation increases, the transmission, such as an email a user is trying to send or a phone call, becomes more distorted.

Wireless signal strength can be attenuated (lessened) due to noise, physical barriers, and long distances. As signal attenuation increases, full signal transmission decreases. Attenuation rates in cabling are affected by external sources of noise at frequencies that penetrate the signal carried by the cable. Fiber optic cables are excellent at transmitting with low attenuation rates because they transmit signals in the form of light waves before changing them back to electronic signals on the receiving end.

Attenuation occurs on computer networks because of:

- Range – over longer distances both wired and wireless transmissions gradually dissipate in strength

- Interference – radio interference or physical obstructions, such as walls, dampen communication signals on wireless networks
- Wire size – thinner wires suffer from more attenuation than thicker wires on wired networks

Jamming

An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable.

To jam a network, you need to broadcast radio signals on the same frequency, overpowering the original signal. Jamming devices that broadcast on a wide range of frequencies at once can disrupt everything from police radar to GPS systems, and are illegal in many countries.

Jamming is a type of Denial of Service (DoS) attack targeted to wireless networks. Jamming happens when RF frequencies interfere with the operation of the wireless network. Normally jamming is not malicious and is caused by the presence of other wireless devices that operate in the same frequency as the wireless network. Hackers can perform Denial of Service (DoS) jamming attacks by analyzing the spectrum used by wireless networks and then transmitting a powerful signal to interfere with communication on the discovered frequencies.

Wireless attacks

Wireless networks face many network attacks. Some wireless network attacks are listed below.

War Driving

War Driving is defined as the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or PDA. The term War Driving is derived from the 1980s phone hacking method known as war dialing. War dialing involves dialing all the phone numbers in a given sequence to search for modems. The War Driving gained popularity in 2001, because that time wireless network scanning tools became widely available.

Some people do War Driving as a hobby and map out different wireless networks. But hackers will look for wireless networks and then break into the networks to steal data or to perform malicious activities.

The initial war driving tools included simple software coupled with the WNIC (Wide-area Network Interface Coprocessor). Many organizations are not worried about their wireless networks because they could spot the war drive attacker inside their parking space and have onsite security pick and throw them out. But recent wireless technology developments enable a network to extend far beyond the parking space of an office building. In some cases, a wireless network has the ability to span several miles. Now an attacker can stay far away from the building and still catch a strong signal from the network. A good war driving software package is NetStumbler.

War-walking

War-walking—War-walking is similar to war-driving, but the hacker is on foot instead of a car. The act of walking around with a laptop computer to find an access point for a wireless network. War walking refers to the same process, commonly in public areas like malls, hotels, or city streets, but using shoe leather instead of the transportation methods listed above. The disadvantages of this method are slower speed of travel (but leading to discovery of more infrequently discovered networks) and the absence of a convenient computing environment. Consequently, handheld devices such as pocket computers, which can perform such tasks while users are walking or standing, have dominated this practice.

War-flying

War-flying—War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

Warflying or **warstorming** is an activity consisting of using an airplane and a Wi-Fi-equipped computer, such as a laptop or a PDA, to detect Wi-Fi wireless networks. Warstorming shares similarities to Wardriving and Warwalking in all aspects except for the method of transport.

Warflying is the act of using an airplane and a wireless **network detector** to find wifi **wireless network** locations. The main benefit of warflying is the speed at which networks can be found across a wide area. Using an airplane, individuals are able to cover far greater distances in a much shorter period of time. The use of an airplane also eliminates many other barriers that are often present and interfere with wireless signals, such as other buildings, trees, and other objects on the ground. Given the lack of interference, warflying can be effective at relative altitudes of 2,500 feet or higher.

One of the major disadvantages of warflying is that it can be difficult to tell exactly where the wireless Internet signal is coming from. This makes the identification of hotspots with any degree of accuracy nearly impossible, especially if there are many different wifi signals in a single geographical area. Once an area has been scouted from the air, pinpointing signals on the ground may be easier through warwalking or wardriving.

The main purpose some companies may have in warflying is simply to monitor how many of their products are out there compared to another company's products. This could help determine what the market share is, at least for a particular city or region. That information may help a company determine its marketing strategy for a certain area and lead to more effective, targeted advertising in that area.

Some individuals may practice warflying for fun, even just as an excuse to get in the air. Those who engage in the activity may be responsible for publishing information concerning hotspots online. In such cases, they may indicate whether the connection is secured or unsecured, or meant for public use.

War Chalking

War Chalking is a method to display information on wireless networks by using chalks on the surrounding walls. War drivers search for networks and then the war driver will mark a network with chalk that gives information about the network to other war drivers.

Warchalking provides information about the type of wireless connection being used, which may be open node, closed node or wired equivalent privacy (WEP) node. This may attract hackers and make them aware of the Wi-Fi hot spot and its security. Hackers may use this information to attack the Wi-Fi network.

Bluejacking

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluejacking is a hacking method that allows an individual to send anonymous messages to Bluetooth-enabled devices within a certain radius. First, the hacker scans his surroundings with a Bluetooth-enabled device, searching for other devices. The hacker then sends an unsolicited message to the detected devices.

Bluejacking is also known as bluehacking.

Bluejacking exploits a basic Bluetooth feature that allows devices to send messages to contacts within range.

Bluejacking does not involve device hijacking, despite what the name implies. The bluejacker may send only unsolicited messages. Hijacking does not actually occur because the attacker never has control of the victim’s device. At worst, bluejacking is an annoyance.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

BlueJackQ is a website dedicated to bluejacking. The website contains a few bluejacking stories taken from the site's forum. The website also includes software that can be used for bluejacking and guides on how to bluejack which are slightly out of date but the basic principle still applies to most makes of phone.

Bluesnarfing and bluebugging, however, are actual attacks that may result in a user losing control of his device. Although bluejacking, bluesnarfing and bluebugging use Bluetooth as the point of entry, bluesnarfing and bluebugging are far more harmful.

Bluejacking can be prevented by setting a device to hidden, invisible or non-discoverable mode.

How to secure wireless networks?

1. Use stronger encryption

Some Wi-Fi access points still offer the older WEP (Wired Equivalent Privacy) standard of protection, but it is fundamentally broken. That means that hackers can break in to a WEP-protected network using a hacking suite like Aircrack-ng in a matter of minutes.

So to keep out intruders, it's essential to use some variant of WPA (Wi-Fi Protected Access) protection, either WPA or the newer WPA2 standard (or WPA3 when it lands).
For smaller companies and households, it may be practical to use WPA with a pre-shared key. That means that all employees or family members use the same password to connect, and network security depends on them not sharing the password with outsiders.

It also means that the password should be changed every time an employee leaves the company.

Some Wi-Fi routers offer a feature called Wireless Protect Setup (WPS) which provided an easy way to connect devices to a WPA protected wireless network. However, this can be exploited by hackers to retrieve your WPA password, so it is important to disable WPS in the router's settings.

2. Use a secure WPA password

Make sure that any password (or passphrase) that protects your Wi-Fi network is long and random so it can't be cracked by a determined hacker.

It is all too easy to set up any equipment with its default settings, especially as the default admin name and password are often printed on the router itself to allow quick access and setup. This means that hackers will try these to access your network. Changing both access name and password will make it more difficult for a criminal to gain access.

You can test the security of your WPA protected network (without revealing your password or passphrase) by using the CloudCracker service. You'll be asked to provide some data (the same data that a hacker could capture or "sniff" out of the air with a laptop from anywhere in range of your network) and the service will attempt to extract your password.

If the service is unsuccessful then a hacker is unlikely to be successful either. But if the service finds your password then you know that you need to choose a longer, more secure one.

3. Check for rogue Wi-Fi access points

Rogue access points present a huge security risk. These aren't your company's "official" Wi-Fi access points, but ones that have been brought in by employees (perhaps because they can't get a good Wi-Fi signal in their office) or conceivably by hackers who have entered your building and surreptitiously connected one to an Ethernet point and hidden it.

In either case, rogue access points present a risk because you have no control over them or how they are configured: for example, one could be set up to broadcast your SSID (the 32 character identifier for a wireless network) and allow anyone to connect without providing a password.

To detect rogue access points you need to scan your offices and the area around it on a regular basis using a laptop of mobile device equipped with suitable software such as Vistumbler (a wireless network scanner) or airodump-ng. These programs allow the laptop to "sniff" the airwaves to detect any wireless traffic travelling to or from a rogue access point, and help you identify where they are located.

4. Provide a separate network for guests

If you want to allows visitors to use your Wi-Fi, it's sensible to offer a guest network. This means that they can connect to the internet without getting access to your company's or

family's internal network. This is important both for security reasons, and also to prevent them inadvertently infecting your network with viruses or other malware.

One way to do this is by using a separate internet connection with its own wireless access point. In fact this is rarely necessary as most business grade (and a lot of newer consumer) wireless routers have the capability of running two Wi-Fi networks at once - your main network, and another for guests (often with the SSID "Guest".)

It makes sense to turn on WPA protection on your guest network - rather than leave it open - for two important reasons. The first is to provide some level of control over who uses it: you can provide the password to guests on request, and as long as you change it frequently you can prevent the number of people who know the password growing too large.

But more importantly, this protects your guests from other people on the guest network who may try to snoop on their traffic. That's because even though they are using the same WPA password to access the network, each user's data is encrypted with a different "session key," which keeps it safe from other guests.

5. Hide your network name

Wi-Fi access points are usually configured by default to broadcast the name of your wireless network - known as the service set identifier, or SSID - to make it easy to find and connect to. But the SSID can be also be set to "hidden" so that you have to know the name of the network before you can connect to it.

Given that employees should know the name of your company Wi-Fi network (and the same goes for family members and friends in a households), it makes no sense to broadcast it so that anyone else who happens to be passing by can easily find it too.

It's important to note that hiding your SSID should never be the only measure you take to secure your Wi-Fi network, because hackers using Wi-Fi scanning tools like airodump-ng can still detect your network and its SSID even when it is set to "hidden."

But security is all about providing multiple layers of protection, and by hiding your SSID you may avoid attracting the attention of opportunistic hackers, so it is a simple measure that is worth taking.

6. Use a firewall

Hardware firewalls provide the first line of defence against attacks coming from outside of the network, and most routers have firewalls built into them, which check data coming into and going out and block any suspicious activity. The devices are usually set with reasonable defaults that ensure they do a decent job.

Most firewalls use packet filtering, which looks at the header of a packet to figure out its source and destination addresses. This information is compared to a set of predefined and/or user-created rules that govern whether the packet is legitimate or not, and thus whether it's to be allowed in or discarded.

Software firewalls usually run on the endpoint desktop or laptop, with the advantage of providing a better idea what network traffic is passing through the device. More than just which ports are being used and where data is going, it will know which applications are being used and can allow or block that program's ability to send and receive data.

If the software firewall isn't sure about a particular program it can ask the user what it should do before it blocks or allows traffic.

7. Enable MAC authentication for your users

You can limit who accesses your wireless network even further by only allowing certain devices to connect to it and barring the rest. Each wireless device will have a unique serial number known as a MAC address, and MAC authentication only allows access to the network from a set of addresses defined by the administrator.

This prevents unauthorised devices from accessing network resources and acts as an additional obstacle for hackers who might want to penetrate your network.

8. Use a VPN

A VPN or virtual private network will help you stay safe and secure online while above all keeping your private stuff private. They keep your data hidden from prying eyes one end to the other by encrypting it. In theory, hackers could penetrate your network and they'd still not be able to do any harm to your system assuming that a VPN is running permanently.