**Wifi-intro**

**Introduction to Wi-Fi (802.11)**

The IEEE 802.11 specification (ISO/IEC 8802-11) is an international standard describing the characteristics of a [wireless local area network](http://en.kioskea.net/contents/wireless/wlintro.php3) (WLAN). The name **Wi-Fi** (short for "Wireless Fidelity", sometimes incorrectly shortened to WiFi) corresponds to the name of the certification given by the [Wi-Fi Alliance](http://www.wi-fi.org), formerly WECA (Wireless Ethernet Compatibility Alliance), the group which ensures compatibility between hardware devices that use the 802.11 standard. Today, due to misuse of the terms (and for marketing purposes), the name of the standard is often confused with the name of the certification. A Wi-Fi network, in reality, is a network that complies with the 802.11 standard. Hardware devices certified by the Wi-Fi Alliance are allowed to use this logo:

Wi-Fi Certification Logo

With Wi-Fi, it is possible to create high-speed wireless local area networks, provided that the [computer](http://en.kioskea.net/contents/pc/pc.php3) to be connected is not too far from the access point. In practice, Wi-Fi can be used to provide high-speed connections (11 Mbps or greater) to [laptop computers](http://en.kioskea.net/contents/pc/ordinateur-portable.php3), [desktop computers](http://en.kioskea.net/contents/pc/familles.php3), [personal digital assistants](http://en.kioskea.net/contents/pc/pda.php3)([PDA](http://en.kioskea.net/contents/pc/pda.php3)s) and any other devices located within a radius of several dozen metres indoors (in general 20m-50m away) or within several hundred metres outdoors.

Wi-Fi providers are starting to blanket areas that have a high concentration of users (like train stations, airports, and hotels) with wireless networks. These access areas are called "**hot spots**".

**Introduction to Wi-Fi (802.11)**

The 802.11 standard reserves the low levels of the [OSI model](http://en.kioskea.net/contents/internet/tcpip.php3) for a wireless connection that uses electromagnetic waves, i.e.:

* The [physical layer](http://en.kioskea.net/contents/wifi/wifitech.php3) (sometimes shortened to the "PHY" layer), which offers three types of information encoding.
* The [data link layer](http://en.kioskea.net/contents/wifi/wifimac.php3), comprised of two sub-layers: **Logical Link Control** (or **LLC**) and **Media Access Control** (or **MAC**).

The physical layer defines the radio wave modulation and signalling characteristics for data transmission, while the data link layer defines the interface between the machine's bus and the physical layer, in particular an access method close to the one used in the [Ethernet](http://en.kioskea.net/contents/technologies/ethernet.php3) standard and rules for communication between the stations of the network. The 802.11 standard actually has three physical layers, which define alternative modes of transmission:

|  |  |
| --- | --- |
| **Data Link Layer (MAC)** | 802.2 |
| 802.11 |
| **Physical Layer (PHY)** | |  |  |  | | --- | --- | --- | | DSSS | FHSS | Infrared | |

Any high-level protocol can be used on a Wi-Fi wireless network the same way it can be used on an[Ethernet](http://en.kioskea.net/contents/technologies/ethernet.php3) network.

**The various Wi-Fi standards**

The IEEE 802.11 standard is actually only the earliest standard, allowing 1-2 Mbps of bandwidth. Amendments have be made to the original standard in order to optimise bandwidth (these include the 802.11a, 802.11b and 802.11g standards, which are called 802.11 physical standards) or to better specify components in order to ensure improved security or compatibility. This table shows the various amendments to the 802.11 standard and their significance:

|  |  |  |
| --- | --- | --- |
| **Name of standard** | **Name** | **Description** |
| **802.11a** | Wifi5 | The 802.11a standard (called WiFi 5) allows higher bandwidth (54 Mbps maximum throughput, 30 Mbps in practice). The 802.11a standard provides 8 radio channels in the 5 GHz frequency band. |
| **802.11b** | WiFi | The 802.11b standard is currently the most widely used one. It offers a maximum thoroughput of 11 Mbps (6 Mbps in practice) and a reach of up to 300 metres in an open environment. It uses the 2.4 GHz frequency range, with 3 radio channels available. |
| **802.11c** | Bridging 802.11 and 802.1d | The 802.11c bridging standard is of no interest to the general public. It is only an amended version of the 802.1d standard that lets 802.1d bridge with 802.11-compatible devices (on the data link level). |
| **802.11d** | Internationalisation | The 802.11d standard is a supplement to the 802.11 standard which is meant to allow international use of local 802.11 networks. It lets different devices trade information on frequency ranges depending on what is permitted in the country where the device is from. |
| **802.11e** | Improving service quality | The 802.11e standard is meant to improve the quality of service at the level of the *data link layer*. The standard's goal is to define the requirements of different packets in terms of bandwidth and transmission delay so as to allow better transmission of voice and video. |
| **802.11f** | Roaming | The 802.11f is a recommendation for access point vendors that allows products to be more compatible. It uses the *Inter-Access Point Roaming Protocol*, which lets a roaming user transparently switch from one access point to another while moving around, no matter what brands of access points are used on the network infrastructure. This ability is also simply called *roaming.* |
| **802.11g** |  | The 802.11g standard offers high bandwidth (54 Mbps maximum throughput, 30 Mbps in practice) on the 2.4 GHz frequency range. The 802.11g standard is backwards-compatible with the 802.11b standard, meaning that devices that support the 802.11g standard can also work with 802.11b. |
| **802.11h** |  | The *802.11h* standard is intended to bring together the 802.11 standard and the European standard (HiperLAN 2, hence the *h* in 802.11h) while conforming to European regulations related to frequency use and energy efficiency. |
| **802.11i** |  | The *802.11i* standard is meant to improve the security of data transfers (by managing and distributing keys, and implementing encryption and authentication). This standard is based on the *AES* (Advanced Encryption Standard) and can encrypt transmissions that run on 802.11a, 802.11b and 802.11g technologies. |
| **802.11Ir** |  | The *802.11r* stadard has been elaborated so that it may use infra-red signals. This standard has become technologically obsolete. |
| **802.11j** |  | The *802.11j* standard is to Japanese regulation what the 802.11h is to European regulation. |

It is also useful to note the existence of a standard called "*802.11b+*". This is a proprietary standard with improvements in data flow. However, this standard also suffers from gaps in interoperability due to not being an IEEE standard.

**Range and data flow**

The 802.11a, 802.11b and 802.11g standards, called "physical standards" are amendments to the 802.11 standard and offer different modes of operation, which lets them reach different data transfer speeds depending on their range.

|  |  |  |  |
| --- | --- | --- | --- |
| **Standard** | **Frequency** | **Speed** | **Range** |
| WiFi a (802.11a) | 5 GHz | 54 Mbit/s | 10 m |
| WiFi B (802.11b) | 2.4 GHz | 11 Mbit/s | 100 m |
| WiFi G (802.11b) | 2.4 GHz | 54 Mbit/s | 100 m |

**802.11a**

The 802.11 standard has a maximum theoretical data flow of 54 Mbps, five times that of 802.11b, but at a range of only about thirty metres. The 802.11a standard relies on a technology called OFDM (*Orthogonal Frequency Division Multiplexing*). It broadcasts in the 5 GHz frequency range and uses 8 non-overlapping channels.

Because of this, 802.11a devices are incompatible with 802.11b devices. However, there are devices that incorporate both 802.11a and 802.11b chips, called "**dual band**" devices.

|  |  |
| --- | --- |
| **Hypothetical speed (indoors)** | **Range** |
| 54 Mbits/s | 10 m |
| 48 Mbits/s | 17 m |
| 36 Mbits/s | 25 m |
| 24 Mbits/s | 30 m |
| 12 Mbits/s | 50 m |
| 6 Mbits/s | 70 m |

**802.11b**

The 802.11b standard allows for a maximum data transfer speed of 11 Mbps, at a range of about 100 m indoors and up to 200 metres outdoors (or even beyond that, with directional antennas.)

|  |  |  |
| --- | --- | --- |
| **Hypothetical speed** | **Range (indoors)** | **Range (outdoors)** |
| 11 Mbits/s | 50 m | 200 m |
| 5.5 Mbits/s | 75 m | 300 m |
| 2 Mbits/s | 100 m | 400 m |
| 1 Mbit/s | 150 m | 500 m |

**802.11g**

The 802.11g standard allows for a maximum data transfer speed of 54 Mbps at ranges comparable to those of the 802.11b standard. What's more, as the 802.11g standard uses the 2.4GHz frequency range with OFDM coding, this standard is compatible with 802.11b devices, with the exception of some older devices.

|  |  |  |
| --- | --- | --- |
| **Hypothetical speed** | **Range (indoors)** | **Range (outdoors)** |
| 54 Mbits/s | 27 m | 75 m |
| 48 Mbits/s | 29 m | 100 m |
| 36 Mbits/s | 30 m | 120 m |
| 24 Mbit/s | 42 m | 140 m |
| 18 Mbit/s | 55 m | 180 m |
| 12 Mbit/s | 64 m | 250 m |
| 9 Mbit/s | 75 m | 350 m |
| 6 Mbit/s | 90 m | 400 m |

**Wifi-modes**

There are several kinds of hardware that may be used to implement a WiFi wireless network:

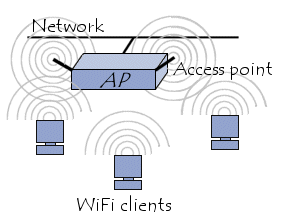
* **Wireless adapters** or **network interface controllers** (NICs for short) are network cards with the 802.11 standard which let a machine connect to a wireless network. WiFi adapters are available in numerous formats, such as [PCI](http://en.kioskea.net/contents/pc/pci.php3) cards, [PCMCIA](http://en.kioskea.net/contents/pc/pcmcia-pc-card.php3) cards, [USB](http://en.kioskea.net/contents/pc/usb.php3) adapters, and [CompactFlash](http://en.kioskea.net/contents/pc/cf-compact-flash.php3) cards. A**station** is any device that has such a card.
* **Access points** (**AP** for short; sometimes called *hotspots*) can let nearby wifi-equipped stations access a wired network to which the access point is directly connected.

The 802.11 standard defines two operating modes:

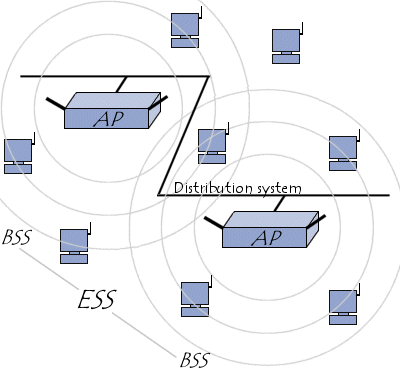
* [Infrastructure mode](http://en.kioskea.net/contents/wifi/wifimodes.php3#infrastructure), in which wireless clients are connected to an access point. This is generally the default mode for 802.11b cards.
* [Ad hoc](http://en.kioskea.net/contents/wifi/wifimodes.php3#adhoc) mode, in which clients are connected to one another without any access point.

**Infrastructure mode**

In **mode infrastructure**, each station computer (**STA** for short) connects to an access point via a wireless link. The set-up formed by the access point and the stations located within its coverage area are called the *basic service set*, or **BSS** for short. They form one cell. Each BSS is identified by a BSSID, a 6-byte (48-bite) identifier. In *infrastructure* mode, the BSSID corresponds to the access point's [MAC address](http://en.kioskea.net/contents/pc/cartres.php3).



It is possible to link several access points together (or more precisely several BSS's) using a connection called a *distribution system* (**DS** for short) in order to form an *extended service set* or *ESS*. The distribution system can also be a wired network, a cable between two access points or even a wireless network.



An ESS is identified with an **ESSID** (Extended Service Set Identifier), a 32-character identifier (in [ASCII](http://en.kioskea.net/contents/base/ascii.php3)format) which acts as its name on the network. The ESSID, often shortened to **SSID**, shows the network's name, and in a way acts a first-level [security](http://en.kioskea.net/contents/wifi/wifisecu.php3) measure, since it is necessary for a station to know the**SSID** in order to connect to the extended network.

When a roaming user goes from one BSS to another while moving within the ESS, his or her machine's wireless network adapter is able to switch access points depending on the quality of the signal it receives from different access points. Access points communicate with one another using a distribution system in order to trade information about the stations and, if necessary, to transmit data from mobile stations. This feature which lets stations move "transparently" from one access point to another is called **roaming**.

**Communicating with the access point**

When a station joins a cell, the cell sends a*probe request* on each channel. This request contains the ESSID that the cell is configured to use, as well as the traffic volume that its wireless adapter can support. If no ESSID is set, the station listens to the network for an SSID.

Each access point broadcasts at regular intervals (about ten times a second) a signal called a **beacon**, which gives information on its BSSID, its characteristics, and, if applicable, its ESSID. The ESSID is automatically broadcast by default, but it is possible (and recommended) to disable this option.

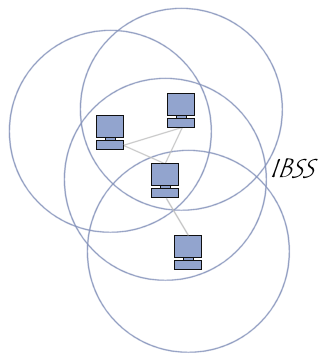
Whenever a probe request is received, the access point checks the ESSID and the traffic volume request found in the beacon. If the given ESSID matches that of the access point, the acces point sends a response containing synchronisation data and information on its traffic load. This way, the station that receives the response can check the quality of the signal being sent by the access point in order to determine how far away it is. Generally speaking, the closer an access point is, the higher its data transfer capacity is.

So a station within range of multiple access points (which have the same SSID) may **choose** the access point offering the best balance of capacity and current traffic load.

|  |  |
| --- | --- |
| Note: | When a station is within range of several access points, the station chooses which one to connect to. |

**Ad hoc mode**

In **ad hoc mode**, wireless client machines connect to one another in order to form a peer-to-peer network, i.e. a network in which every machine acts as both a client and an access point at the same time.



The set-up formed by the stations is called the **independent basic service set**, or IBSS for short.

An IBSS is a wireless network which has at least two stations and uses no access point. The IBSS therefore forms a temporary network which lets people in the same room exchange data. It is identified by an SSID, just like an ESS in infrastructure mode.

In an ad hoc network, the range of the *independent BSS* is determined by each station's range. That means that if two of the stations on the network are outside each other's range, they will not be able to communicate, even if they can "see" other stations. Unlike infrastructure mode, ad hoc mode has no distribution system that can send data frames from one station to another. An IBSS, then, is by definition a restricted wireless network.

**Wifi-risks**

**Lack of security**

Radio waves intrinsically have the power to [propagate](http://en.kioskea.net/contents/wireless/wlpropa.php3) in all directions, with a relatively wide range. Because of this, it is very difficult to keep radio broadcasts confined to a limited area. Radio propagation also occurs three-dimensionally. The waves can therefore travel from one floor of a building to another (albeit with a high degree of [attenuation](http://en.kioskea.net/contents/wireless/wlpropa.php3).)

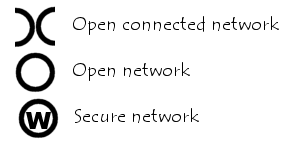
The main consequence of this "wild propagation" of radio waves is that a non-authorised person may be able to [listen to the network](http://en.kioskea.net/contents/attaques/sniffers.php3), possibly beyond the enclosure of the building where the wireless network is set up.

The critical issue is that a wireless network can very easily be installed in a business without the IT department even knowing! An employee only has to plug an access point into a data port for all communication on the network to become "public" throughout the access point's broadcast range.

**War-driving**

Given how easy it is to "listen" to wireless networks, some people have taken to travelling around a city with a wireless-compatible laptop computer (or PDA) looking for wireless networks. This practice is called**war driving** (sometimes written *wardriving* or *war-Xing* for "war crossing"). Specialised war-driving software allows the locations of these open access points to be mapped accurately with the help of a Global Positionning System (GPS).

These maps can show available unsecured wireless networks, sometimes allowing people to access the Internet. Many websites have been started to share this information; in fact, in 2002, students in London invented a sort of "sign language" to indicate the presence of wireless networks in an area by drawing symbols on the sidewalk in chalk. This is called "**warchalking**". Two opposing semicircles mean that the area is covered by an open network that provides Internet access, a circle indicates the presence of an open wireless network without access to a wired network, and a W inside a circle shows that there is a properly secured wireless network.



**Security risks**

There are several risks involved in not properly securing a wireless network:

* [Data interception](http://en.kioskea.net/contents/wifi/wifirisques.php3#interception) is the practice of listening in on the transmissions of various wireless network users.
* [Cracking](http://en.kioskea.net/contents/wifi/wifirisques.php3#detournement) is an attempt to access a local network or the Internet.
* [Transmission jamming](http://en.kioskea.net/contents/wifi/wifirisques.php3#brouillage) means sending out radio signals so as to interfere with traffic.
* [Denial of service](http://en.kioskea.net/contents/wifi/wifirisques.php3#DoS) attacks make the network unusable by sending out false requests.

**Data interception**

By default, a wireless network is unsecured. This means that it is open to everyone, and anyone within the coverage area of an access point may potentially listen to communications being sent on the network. For an individual, there is little threat, as data is rarely confidential, unless the data is of a personal nature. For a business, however, this may pose a serious problem.

**Network intrusion**

When an access point is installed on a local network, it lets any station access the wired network, as well as the Internet, if the local network is connected to it. For this reason, an unsecured wireless network gives hackers the perfect gateway to an business or organisation's internal network.

Besides letting the hacker steal or destroy information on the network and giving him or her free Internet access, the wireless network might also be helping him or her to carry out cyber-attacks. Indeed, since there is no way to identify a hacker on a network, the business which installed the wireless network might be held responsible for the attack.

**Radio jamming**

Radio waves are very sensitive to interference. This is why a signal can easily be jammed by a radio transmission with a frequency close to that used by the wireless network. Even a simple microwave oven can make a wireless network completely inoperable if it is being used within an access point's range.

**Denial of service**

The 802.11 standard's network access method is based on the [CSMA/CA](http://en.kioskea.net/contents/wifi/wifimac.php3) protocol, which involves waiting until the network is free before transmitting data frames. Once the connection is established, a station must be linked to an access point in order to send it packets. Because the methods for accessing a network and associating with it are known, it is easy for a hacker to sent packets requesting for a station to become disassociated from the network. Sending out information intended to disrupt a wireless network is called a denial of service attack.

What's more, connecting to wireless networks uses up power. Even if the wireless peripheral devices have power-saving features, a hacker may be able to send enough encrypted data to a machine for it to overload. Many portable peripherals (like PDAs and laptop computers) have limited battery life. Therefore, a hacker may want to cause excessive power consumption that renders the device temporarily unusable, which is called a *battery exhaustion attack*.

**Wifi-security**

## Introduction to WPA

**WPA** (WiFi protected Access) WiFi network security solution offered by the WiFi Alliance, in order to fill gaps in [WEP](http://en.kioskea.net/contents/wifi/wifi-wep.php3).

## WPA - WiFi Protected Access

WPA is a "light" version of the 802.11i protocol, which relies on authentication protocols and a strong encryption algorithm: **TKIP** (Temporary Key Integrity Protocol). TKIP generates keys randomly and can alter an encryption key several times a second, for greater security.

WPA requires installing an authentication server (most commonly a RADIUS server), which identifies users on a network and sets their access privileges. Nonetheless, small networks can make use of a simpler version of WPA, called WPA-PSK, by deploying the same encryption key on all devices, which eliminates the need for a RADIUS server.

WPA (in its first build) only supports networks in [infrastructure mode](http://en.kioskea.net/contents/wifi/wifimodes.php3), which means it cannot be used to secure wireless peer-to-peer networks ([ad hoc mode](http://en.kioskea.net/contents/wifi/wifimodes.php3)).

**Introduction to 802.11i**

802.11i was ratified on 24 June 2004, in order to address security issues in WiFi networks. Like WPE, it relies on the TKIP [encryption algorithm](http://en.kioskea.net/contents/crypto/crypto.php3), but it also supports the much more secure AES (Advanced Encryption Standard).

The Wi-Fi Alliance created a new certification, called **WPA2**, for devices that support the 802.11i standard (like [laptop computers](http://en.kioskea.net/contents/pc/ordinateur-portable.php3), [PDAs](http://en.kioskea.net/contents/pc/pda.php3), [network cards](http://en.kioskea.net/contents/pc/carte-reseau.php3), etc.)

Unlike WPA, WPA2 can secure wireless networks in [infrastructure mode](http://en.kioskea.net/contents/wifi/wifimodes.php3) as well as networks in [ad hoc mode](http://en.kioskea.net/contents/wifi/wifimodes.php3).

**WPA Architectures**

The IEEE 802.11i standard defines two operating modes:

* **WPA-Personal**: This mode allows for the implementation of a secure infrastructure based on WPA without having to implement an authentication server. WPA-Personal rests on the use of a shared key, called **PSK** for *Pre-shared Key*, which is stored at both the access point and the client devices. Unlike [WEP](http://en.kioskea.net/contents/wifi/wifi-wep.php3), it is not necessary to enter a key of pre-defined length. WPA lets the user enter a passphrase, which a hash algorithm then converts into a PSK.
* **WPA-Enterprise**: Enterprise mode requires 802.1x authentication infrastructure using an authentication server, generally a RADIUS server (which stands for *Remote Authentication Dial-in User Service*), and a network controller (the access point).

**Introduction to 802.1X**

The 802.1x standard is a security solution ratified by the IEEE in June 2001 which can authenticate (identify) a user who wants to access a network (whether wired or wireless). This is done through the use of an authentication server.

802.1x is based on the **EAP protocol** (*Extensible Authentication Protocol*), as defined by the [IETF](http://www.ietf.org). This protocol is used for transporting user identification information.

**EAP**

The EAP protocol is centred around the use of an access controller called an *authenticator*, which either grants or denies a user access to the [network](http://en.kioskea.net/contents/initiation/concept.php3). The user in this system is called a *supplicant*. The access controller is a basic firewall which acts as an intermediary between the user and an *authentication server*, and requires very few resources to function. For a [wireless network](http://en.kioskea.net/contents/wireless/wlintro.php3), the access point acts as the authenticator.

The authentication server (sometimes called the *NAS*, for *Network Authentication Service*or *Network Access Service*) can approve the user's identity as transmitted by the network controller, and then grant the user access depending on his or her credentials. What's more, this type of server can store and keep track of information related to the users. In the case of a service provider, for example, these features allow the server to bill them based on how long they were connected or how much data they transferred.

The authentication server is most commonly a RADIUS server (*Remote Authentication Dial-In User Service*), a standard authentication server defined by RFC 2865 and 2866, but any other authentication service may be used instead.

The following is a summary of how a secure network using the 802.1x standard works:

1. The access controller, having previously received a connection request from the user, sends an identification request;
2. The user sends a response to the access controller, which routes the response to the authentication server;
3. The authentication server sends a "challenge" to the access controller, which transmits it to the user. The challenge is a method of establishing identification. If the client cannot evaluate the challenge, the server tries another one, and so on;
4. The user responds to the challenge. If the user's identity is correct, the authentication server sends approval to the access controller, which allows the user onto the network or part of the network, depending on the rights granted. If the user's identity could not be verified, the authentication server sends a refusal message, and the access controller denies the user access to the network.

**Encryption key exchange**

Besides authenticating users, the 802.1x standard provides users with a secure way to exchange encryption keys, in order to improve overall security.

## Adapted infrastructure

The first thing to do when a [wireless network](http://en.kioskea.net/contents/wireless/wlintro.php3) is installed is to place the access points in reasonable locations depending on the desired area of coverage. However, it is not uncommon to find that the covered area ends up being larger than desired, in which case it is possible to reduce the access terminal's strength so that its broadcast range matches the coverage area

## Avoid using default values

When an access point is first installed, it is configured to certain default values, including the administrator's password. Many novice administrators think that once the network is operational, there is no point in changing the access point's configuration. However, the default settings offer only a minimal level of security. For this reason, it is vital to log in to the administration interface (generally via a web interface or by using a particular [port](http://en.kioskea.net/contents/internet/port.php3) on the access terminal), especially to set an administrative password.

What's more, in order to connect to an access point, it is necessary to know the network identifier (SSID). This is why it is strongly recommended to change the default name of the network and to deactivate broadcasting the name on the network. Changing the default network identifier is all the more important because it can, if left unaltered, give [hackers](http://en.kioskea.net/contents/attaques/typologie-pirates.php3) information on the brand or model of the access point being used.

## Filtering MAC addresses

Every *network adapter* (the generic term for a [network card](http://en.kioskea.net/contents/pc/carte-reseau.php3)) has its own physical address (called a [MAC address](http://en.kioskea.net/contents/pc/carte-reseau.php3)). This address is represented by 12 digits in [hexadecimal](http://en.kioskea.net/contents/base/hexa.php3) format, split up into two-digit groups separated by dashes.

The configuration interfaces of access points generally allow them to keep a list of access permissions (called the ACL, for Access Control List) based on the MAC addresses of the devices authorised to connect to the wireless network.

This somewhat restrictive precaution allows the network to limit access to a certain number of machines. However, this does not solve the problem of securing data transfers.

## WEP - Wired Equivalent Privacy

To solve transfer security issues on wireless networks, the 802.11 standard includes a simple data encryption mechanism called **WEP**(Wired equivalent privacy).

WEP is an 802.11 data frame [encryption](http://en.kioskea.net/contents/crypto/crypto.php3) protocol that uses the symmetrical algorithm RC4 with [64-bit](http://en.kioskea.net/contents/base/binaire.php3) or[128-bit](http://en.kioskea.net/contents/base/binaire.php3) keys. The concept of WEP involves setting a secret 40-bit or 128-bit key ahead of time. This secret key must be declared on both the access point and the client machines. The key is used to create a pseudo-random number of the same length as the data frame. Each data transmission is encrypted this way, by using the pseudo-random number as a "mask"; an "Exclusive OR" operation is used to combine the frame and the pseudo-random number into an enciphered datastream.

The session key shared by all stations is static, which means that to deploy a large number of WiFi stations, they must be configured using the same session key. Therefore, knowing the key is all that is needed to decrypt the signals.

Furthermore, 24 bits of the key are used only for initialisation, which means that only 40 bits of a 64-bit key, or 104 bits of a 128-bit key, are actually used for encryption.

For a 40-bit key, a [brute force attack](http://en.kioskea.net/contents/attaques/passwd.php3) (which tries all possible keys) might not stop a hacker from quickly finding the session key. Also, a flaw detected by Fluhrer, Mantin and Shamir in the generation of the pseudo-random stream makes it possible for the session key to be discovered by storing and analysing 100 MB to 1 GB of traffic.

Therefore, WEP is insufficient for actually ensuring data privacy. Nevertheless, it is strongly recommended to use at least a 128-bit WEP key to ensure a minimum level of [privacy](http://en.kioskea.net/contents/secu/secuintro.php3). This can reduce the risk of[intrusion](http://en.kioskea.net/contents/detection/ids.php3) by 90%.

## Improve authentication

In order to more effectively manage authentication, authorisation, and accounting(**AAA**for short), a RADIUS server (*Remote Authentication Dial-In User Service*) may be used. The *RADIUS* protocol (defined by [RFC](http://en.kioskea.net/contents/internet/rfc.php3)s 2865 and 2866) is a client/server system which lets user accounts and related access permissions be centrally managed.