Glossary
Wireless LAN

This document is a collection of explanations of technical terms and abbreviations on the topic of wireless LAN.

802.11
This is the (main) IEEE standard for so-called Wireless Local Area Networks (WLANs).
IEEE 802.11 was approved in 1997 and specified WLANs with (gross) transfer rates of 2 Mbit/s.
Frequency band used: 2,400 to 2,485 GHz

802.11a
Successor of the original 802.11 standard, which was approved in 1999.
- (Gross) data transfer: 54 Mbit/s
- Frequency band: 5 GHz

802.11b
A further successor to the original 802.11 standard of 1999.
- (Gross) data transfer: 11 Mbit/s
- Frequency band: 2,400 to 2,4835 GHz

802.11g
Standard successor from 2003.
- (Gross) data transfer: 54 Mbit/s
- Frequency band: 2,400 to 2,4835 GHz

802.11n
Last approved standard from 2009.
- (Gross) data transfer: 600 Mbit/s
- Frequency band: 2,400 to 2,4835 GHz, optionally also 5 GHz as an additional band

802.11ac
Planned successor of the 802.11n standard.
- (Gross) data transfer: 1 Gbit/s
- Frequency band: < 6 GHz (planned)

Access Point (AP)
An access point is an expansion unit for radio networks that essentially allows the radio network to be connected to a wired (Ethernet) network.
The access point is used as a bridge between the networks and regulates their communication with each other.
Today, access points are (usually) supplied with an integrated firewall, router and DSL modem.

Ad-hoc (network)
An ad-hoc network describes the direct connection of two systems via a (private) WLAN network.
In this case, two systems are usually connected with each other via WLAN so as to enable direct communication between subscribers. This type of connection does not require any additional hardware (e.g. access point) and only has a very limited range.

Bandwidth

Bandwidth describes the frequency range (in MHz) in which radio signals can be sent.
The term ("bandwidth") is often falsely used to specify the transfer rate or "speed".

Data rate

Describes the "speed" of the connection in the number of binary data (bits) that can be transferred per second (unit: bit/s).
The data rate is often also referred to as the (bit) transfer rate.
In radio cells / wireless environments the data rate depends on several factors:

- Number of stations (e.g. linking of several access points, switches, etc.)
- Distance to the access point
- Quality of the connection and disturbing influences (e.g. other WLAN networks or devices; signals through walls/floors)
- Quality of the hardware used (e.g. outdated WLAN cards in the client, antenna(s))

Infrastructure mode

Mode of operation of IEEE 802.11 WLANs, for which an access point (AP) is required. The access point provides the WLAN under a predefined name ("SSID"), to which various clients can be connected.
In this mode of operation a WLAN is then frequently connected to a wired LAN via the access point.

Local Area Network

A network that is limited to a building or a site (reach approx. 2-5 km). Known LAN technologies include e.g. Ethernet, Token Ring, and also WLANs.
LAN and/or Ethernet is among other things the interface for connecting computers or networks with a router or DSL modem.
Modern devices, such as printers or copiers, are also equipped with a LAN interface nowadays, thus enabling direct access to and via the network.

MAC Address

The MAC address is a unique, unmistakable address of all Ethernet adapter cards.
All systems with a network card or devices, which are connected to a network, have such an address.
A MAC address consists of 6 bytes and is written in hexadecimal format. The first 3 bytes indicate a manufacturer and are interpreted as the ID (e.g. 00-01-E3 for Siemens), the second 3 bytes are a unique number assigned by the manufacturer.
The MAC address can e.g. be used to operate the access control of authorized users at an access point, by only granting access to known MAC addresses.

Remote Authentication Dial-In User Service (RADIUS)

The procedure for authenticating users based on user name and password via special servers.
To acquire access it is necessary for the client to have appropriate access with valid certification.
Users without any ID or certification are rejected by the RADIUS server.

Roaming

Roaming is the definition of the procedure, in which a mobile station (e.g. notebook) of a network can switch between several radio cells without interrupting mobile communication.
This is for example the case if there are several access points with the same SSID in one WLAN network.
If you now change between two access points, roaming ensures that the transition takes place without data loss for the user.
Roaming also plays a large role in the GPRS/UMTS network ("mobile telephone network").

Router

A router is a network device / element that connects or couples various networks.
In so doing, the router analyzes the incoming data packets according to their destination address and forwards them specifically, or blocks them where applicable.

Signal Strength

Strength of a signal (expressed in dbm).

Switch
A coupling element in local networks (LAN) that connects several Ethernet devices with each other. A switch independently creates a MAC address table based on the data packets that it should forward and in so doing makes a note of the sender address and the appropriate receiving port.

Service Set Identifier (SSID)
Name of a radio cell or the name of a "WLAN network".
The SSID is normally configured in the access point, and is sent by the latter.
Based on the SSID it is possible to distinguish between and clearly assign several WLAN networks.

Temporal Key Integrity Protocol (TKIP)
TKIP is an encryption protocol and part of the IEEE 802.11 standard for WLANs. TKIP was developed in order to achieve a higher level of encryption security than with the "weak" predecessor WEP (Wired Equivalent Privacy).
TKIP is the encryption method for WPA (Wi-Fi Protected Access), which is seen as the successor/replacement for WEP.

Wi-Fi Protected Access (WPA)
Due to the weaknesses of WEP, WPA was developed as an interim solution for encryption in WLANs. WPA "extended" WEP to include dynamic encryption (TKIP) and port-based user authentication. A second generation of WPA is available in the meantime (WPA2).

Wi-fi (Wireless Fidelity)
The so-called "Wi-Fi Alliance" is an organization of more than 300 companies that certifies the products of various manufacturers on the basis of the IEEE-802.11 standard and thus ensure operation with different wireless devices (mutually compatible). The reason for this was that the 802.11 standard has not been fully implemented or modified/extended in many products. Consequently, there were frequently incompatibilities between products of different manufacturers.
The Wi-Fi Alliance tests appropriate components according to its own guidelines. Products that pass the test receive the Wi-Fi certificate and are allowed to use the Wi-Fi logo. This results, for example, in the fact that a "Wi-Fi"-certified notebook should be able to communicate with every "Wi-Fi"-certified access point. However, exceptions and restrictions must be taken into account in the event of any adapted settings.

Wired Equivalent Privacy (WEP)
WEP is an encryption protocol that was specified together with the approval of the first standard IEEE 802.11 in 1997.
Although WEP provides both encryption and user authentication, a static key is nevertheless entered on both end points (e.g. 2 clients that communicate with each other), which is the weakness of WEP.
Encryption with WEP is regarded today as insecure and outdated, and should therefore be replaced by WPA/WPA2 encryption.

Wireless Local Area Network (WLAN)
A local network means a network that is (locally) limited to a building or a site. In this case, "wireless" means - as the name suggests - that no cable/wire is used in such local networks. Instead of transferring electrical or optical signals via suitable cable, WLANs use radio signals and air as the medium between the sender and the receiver.
However, separate/additional hardware is required for this (WLAN cards, access points, etc.). Using the appropriate hardware WLANs can also be coupled with local Ethernet LANs.

WPA-PSK
Wi-fi Protected Access - Pre-Shared Key. A type of authentication for WPA. The pre-shared key is specified in both the access point and the client in order to enable communication between both points. The key consists of 6 to 63 characters and has to be known beforehand and entered in order to establish a connection - hence the name "Pre-Shared Key".
In private use in particular, WPA-PSK is the most common method of safeguarding a WLAN externally and of preventing any unauthorized access.