



Industrial Wireless LAN. Industrial Features and Current Standards

SIMATIC NET White Paper V.1.1 2009 Nov.

Answers for industry.

SIEMENS

Aims

This white paper presents an overview of new technologies involved in Wireless LAN for IEEE 802.11 which will have an effect on the usage in industry applications. Please note that standards that have already been approved and published are not described in this document.

Further information on the topic of Industrial Wireless LAN in SIMATIC NET:

- Basics and setup of a Wireless LAN in the Industrial Environment:
<http://support.automation.siemens.com/WW/view/en/22681042>

The information in this White Paper is as of November 2009

Published by
Siemens AG
Industry Sector
Industry Automation Division
Sensors and Communication
Industrial Communication SIMATIC NET
90475 Nuremberg, Germany

Further Support:

If you have any further questions, please contact your local Siemens representative.

You will also find SIMATIC NET on the Internet at

<http://www.siemens.com/simatic-net>

Introduction	4
New Wireless LAN Standards	5
IEEE 802.11n (high data rates).....	5
IEE 802.11s (meshed Wireless LANs).....	8
Glossary	12

Introduction

Wireless LAN complying with IEEE 802.11 provides a good basis for use in wireless applications for industry and automation whether with driverless transport systems, escalators, storage logistics, transportation of goods, electric monorails, building management or service applications. Such systems can be considered when cabling would be extremely complex or time-consuming or when a high degree of flexibility is called for. Highly contaminated environments are not a problem with a wireless link. This can significantly reduce the effort required for maintenance. Since Wireless LAN is the basis, such applications benefit from the wide range of chipsets, end devices and development tools available. All advantages that are provided by an open standard.

New Wireless LAN Standards

The definition of the following standards is either not yet or was recently completed.

IEEE 802.11n (high data rates)

Initial situation: antenna diversity

WLAN radio networks, working according to IEEE 802.11abg are usually equipped with antenna diversity. This can be quickly recognized at equipment with external antennas because 2 antennas are attached to the device. With this technology the negative consequences of the multipath propagation of the radio wave are reduced considerably. Multipath propagation is typical for radio waves in the GHz frequency band (microwave) where radio waves reach the receiver via different ways, run different distances and change their phase and polarization. The WLAN receiver must be high quality because he has to separate this mixture of different wave fronts to decode the original information. The receiver gets support from a switch which helps to choose one out of those two antennas. If he has decided in favour of one, then he will receive the following data packet (frame) from this antenna and transmits his answer via this antenna. This decision must be drawn again and again. It is important to know that radio chipsets own exactly one sending path and exactly one receive path. Both are connected to the two antennas via a switch. If the system has decided to select one antenna during reception, both the sending path and the other antenna will be switched off. During the consecutive sending both the receive path and one antenna will be deactivated. This mechanism is true for both access points and clients. It is also called "switched antenna diversity".

Diversity becomes MIMO

At IEEE 802.11abg systems at one point of time there is exactly one reception or one transmission path active. There, IEEE 802.11n offers an improvement with MIMO. MIMO means *multiple in multiple out* and is the reception or transmission via several independent sending and reception paths (spatial streams). By means of this separation a higher data rate is achieved but also a more robust signal transmission. This separation of streams is also called spatial multiplexing. Unfortunately, it comes along with more computing effort of the signal processor chip. Furthermore it requires more space (and therefore costs) by several transmission and reception paths on the chip set and in addition increased efforts for the antenna technology. This is compensated by the trend of silicon vendors who integrate more chips of the chipset into one package and reduce costs.

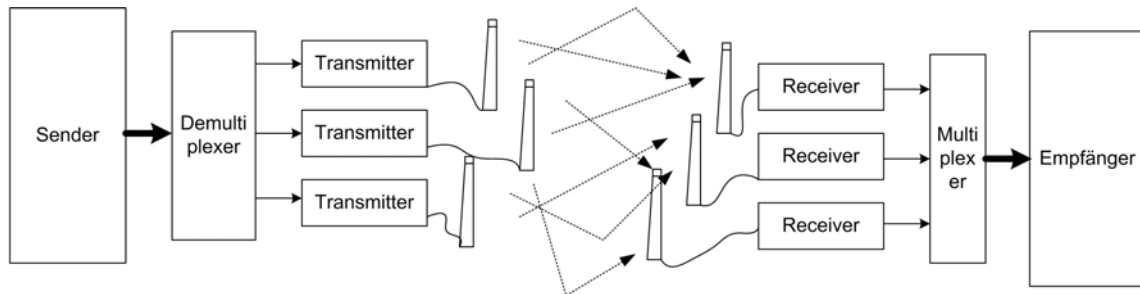


Figure 1: Increased data rate by means of multipath propagation (spatial multiplexing)

Spatial multiplexing is a technology which converts the disadvantage (IEEE 802.11abg) of multipath propagation into an advantage (IEEE 802.11abgn).

By the separation of the data stream into several streams it is possible to distribute the data on several transmitters and afterwards on several (spatially separated) antennas. By this spatial separation the transmitted signals may select different paths, gets reflected at different obstacles and reaches the receiver at different points of time. For an optimized usage of the technology at least the same number of antennas and receivers is necessary. The data rate increases almost linearly with the number of data streams and antennas used.

If a cost reduced client owns only 2 antennas and 2 spatial streams, e.g. an access point with 3 antennas and 3 spatial streams must adjust to this situation. The access point will transmit via his third antenna a redundant signal.

A participant in an IEEE 802.11n radio network is therefore described by the number of antennas for transmission and the number of antennas for reception. In addition, the number of spatial streams should be mentioned. So, a system 3x3 with 2 streams is a WLAN unit with, 3 transmit and 3 receive antennas (in this order) and it is supported by 2 spatial streams in the radio chip set (e.g. because the radio chip set is optimized pricewise).

Modulation with HT-OFDM

In general, Orthogonal Frequency Division Multiplex (OFDM) modulation is well known from IEEE 802.11a and g and it is used in the Physical layer (PHY). But several optimizations are implemented to be used in IEEE 802.11n. For example the frequency spectrum of a 20 MHz channel is divided up in a more optimized way into sub channels. Additional optimizations increase the throughput by approx. 30% compared to OFDM known from IEEE 802.11a and g. However, a real improvement is achieved by channel bonding of two 20 MHz channels to a 40 MHz channel. Only this improvement boosts the gross data up to 150 Mbps for one stream (instead of 54 Mbps of IEEE 802.11a and g). It has to be taken into account, that merely 3 such non overlapping 20 MHz channels are available in the 2.4 GHz frequency band. At 5 GHz there are between 11 and 19 (dependent on the country) available. In general, it can be said that IEEE 802.11n leverages the frequency spectrum in a better way and offers a higher data rate.

For a description of the performance of a WLAN unit according to IEEE 802.11n it is important to check exactly the specification, because lot optimizations are optional. Furthermore it must be measured, which net data rate can be actually achieved, because both chip set and the implementation of the software protocol offer a lot room for optimization.

Improvements in the MAC layer

Known weaknesses in the MAC Layer of IEEE 802.11a and g are also improved and optimize the net throughput. E.g. distances between data packets (interframe space) can be shortened for long data packets. Furthermore single data packets (frames) can be aggregated to increase the density and avoid overhead.

As MIMO offers several transmit and receive streams, energy consumption is an important topic. If a participant is inactive, at IEEE 802.11n it is allowed to switch off all its receive streams except for one. This one listens to the data traffic in the air interface and wakes up the other receivers in case of an incident.

Downward compatibility

Configured for legacy mode an IEEE 802.11n unit acts equal to an IEEE 802.11abg unit. Advantages derive from MIMO, where several transmit and receive streams work together at the same point of time. This results in a higher coverage and more reliable data traffic, for the same data rate.

In mixed mode the first data of a frame, the preamble, is transmitted according to IEEE 802.11ag. Afterwards, the payload is transmitted according the agreed mode, very fast with IEEE 802.11n or as hitherto with IEEE 802.11abg. In this mode, an IEEE 802.11n radio network can integrate IEEE 802.11ag units.

Finally, there is the green field mode, which defines a pure IEEE 802.11n traffic and exploits in the best way the advantages of IEEE 802.11n.

Standardization

Today (2009), IEEE 802.11n is finally approved. Since 2007, there is a version "Draft 2.0" available which is already implemented in lot products. This version was pushed by customers who required higher data rates and it was supported by Wi-Fi. An advantage of Draft 2.0 is the fact that the Wi-Fi has defined the interoperability tests for a mixed installation of units from different vendors and runs already the certification. Therefore, this Draft is wide spread. It can be expected that future products will support both Draft 2.0 and the final version.

Note: Several times IEEE and Wi-Fi have already practiced this process in the past, e.g. at security with IEEE 802.11i / WPA or multimedia with IEEE 802.11e / WMM.

Applications and advantages in home, enterprise and industry

The well known standards IEEE 802.11abg offer (gross) data rates of 54 Mbps which correspond with a net data rate of approx. 27 Mbps. However, a WLAN radio link with this performance represents a bottle neck in today's Fast Ethernet data networks. This kind of network expects data rates up to 100 Mbps (or even 1000 Mbps). Therefore, the higher data rates of IEEE 802.11n are more than appreciated. Video is one of the killer applications in home networks which have big benefit from the improvements of IEEE 802.11n.

Professional installations at enterprise customers expect the connection of as many workers as possible in the smallest area (e.g. conference room). This density requires a high data rate per square meter.

In industry applications a high reliability is the most important feature of a radio network. There, MIMO offers a stable radio link (at the same transmission rate). The usually disturbing multipath propagation favours even the data transmission because the original data stream is separated into several streams and transmitted in parallel. Furthermore, in industrial applications there is also the trend to higher data rates. Not seldom video data can be found, too because e.g. live pictures from the process can be monitored in the control room. To guarantee a continuous data stream, a minimal data rate may not be fallen below. Finally, WLAN is frequently used in point-to-point connections to link to a remote production site. This connection represents the bottle neck of the system and the highest possible net throughput is very important.

IEE 802.11s (meshed Wireless LANs)

The term meshed or mesh network means literally what it says. The basic idea behind mesh networks is based on redundant paths for the transfer of data from one node to the next. If one path is disrupted, the network automatically finds a new one. In many case, the declared aim is also to be able to add additional nodes in a mesh network with little effort. Ideally, the network should manage itself. In conjunction with wireless LAN networks, the idea of a mesh network has become reality in the meantime although previously implemented meshed MANs were always based on proprietary developments.

Systems today

There are many types of mesh networks. Some providers call a Wireless Distribution System (WDS) together with the Rapid Spanning Tree Protocol (RSTP) a mesh network. There are versions with only one or multiple gateways to other cable networks or the Internet. Other providers, on the other hand, consider that a pure mesh network completely does without the use of any backbone infrastructure. In this case, the data is sent over several nodes to a recipient without any routers in between. The clients also function as routers for other clients.

Wireless meshed in automation

In automation, mesh networking allows redundant data paths with which the loss of individual connections (meshes) can be compensated fully automatically. The use of wireless LAN technology in conjunction with meshed networking can allow operation in environments where cable trays would be difficult or uneconomical to install. A further scenario for the use of such networks could be in ad hoc wireless LANs that (equipped with meshed networking technology) could be set up quickly with little administrative effort, for example for trade fairs, festivals or military applications in the field.

Standardisation

An IEEE working group is aiming to establish a heterogeneous standard for wireless mesh networks by spring 2011. This is known as IEEE 802.11s. The aims of this standard are simple extensibility up to and including large distributed wireless LANs, flexibility in production facilities and in similar fast changing environments, the possibility of setting up networks for crisis management, for example in the case of catastrophes, and the formation of highly redundant networks that can be used by the military and in safety-oriented environments.

The future standard currently envisages three basic infrastructure elements for setting up meshed wireless LAN structures. Mesh points establish and expand a wireless backbone; mesh access points have the same function with the additional option of linking clients over a second wireless module. Mesh portals function as backbone providers and acting as a bridge also provide access to different network types. Figure 2 illustrates how the components could be arranged.

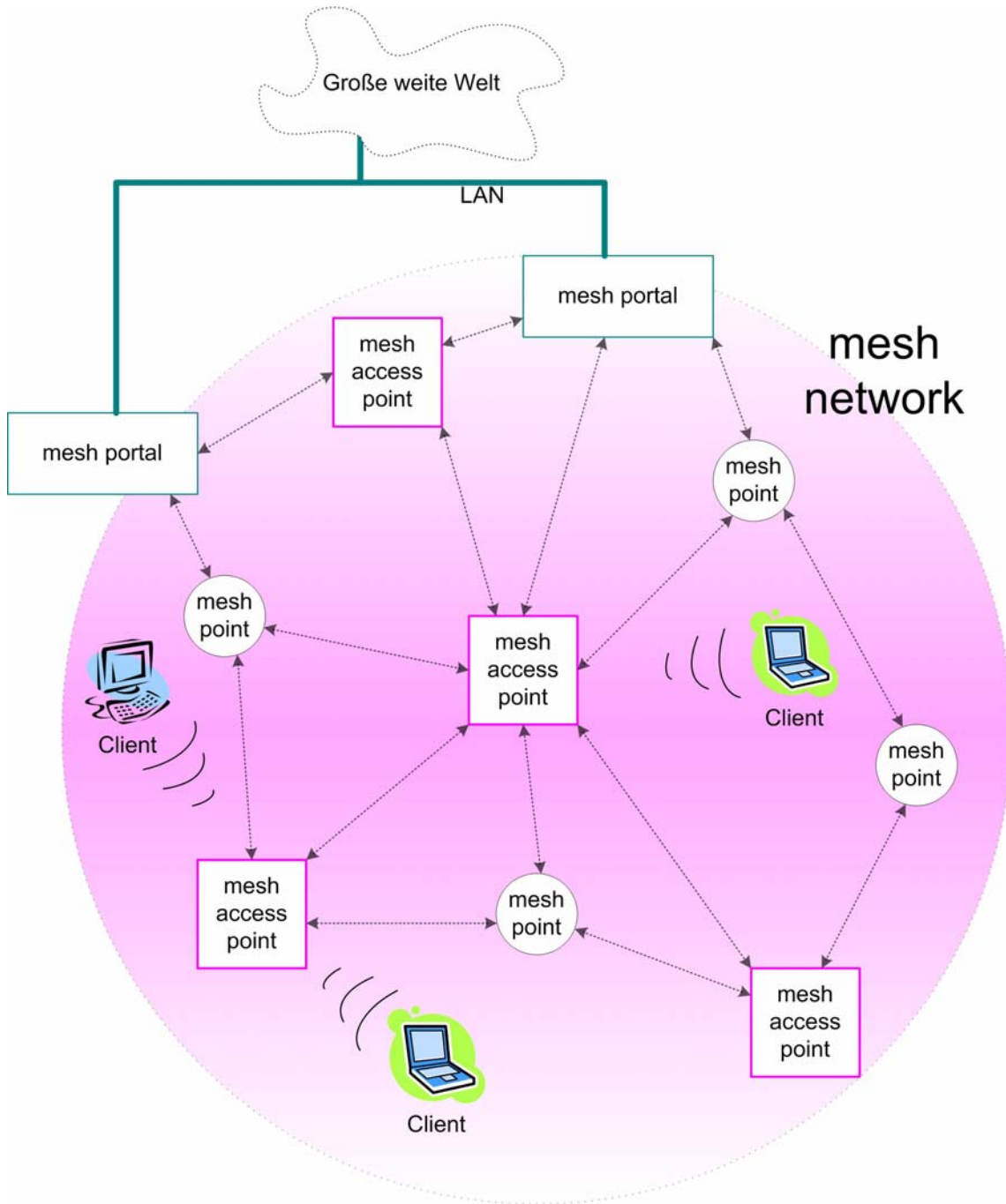


Figure 2: Setup of a Mesh Network

The standard IEEE 802.11s standard describes the capabilities of a mesh point. It should be capable of recognizing its neighbours and of finding the correct route using a path selection protocol. The routing should be very hardware-oriented, in other words, optimized for speed. Data security is based on IEEE 802.11i for which an enhancement is necessary compared with normal wireless LAN environments to implement secure connections with clients over several hops.

The mesh points must, of course, establish secure connections among themselves for which suitable mechanisms must be included for two-way authentication. To allow roaming from one mesh access point to the next, fast reauthentication must also be possible (seamless roaming) to avoid disrupting time-critical applications or sessions relevant for security. A further point is management in mesh networks to avoid overload. An expansion of the IEEE 802.11e standard is planned for management packets (for example flow control). Since the mesh points are located very close to each other, there is inevitably a strong mutual influence due to overlapping of the RF fields and mutual interference. It is therefore important that techniques such as beam forming are used to ensure that the same radio channels are used "at the earliest" in the next but one cell to avoid the channels in immediately neighbouring cells from overlapping. The risk of collisions is also greater.

Glossary

2G	Digital mobile wireless networks of the second generation, for example GSM
3G	Digital mobile wireless networks of the third generation, for example UMTS Occasionally the term 2.5G is used. In this case, the expansions of GSM are meant (EDGE, GPRS)
IEC 61508	Standard relating to functional safety (new)
EN 954-1	Standard relating to functional safety (old)
Access point	WLANs are set up using access points. They also connect the wired data network.
ACK	Acknowledge Signal in handshake protocol for avoiding the hidden node problem
ACL	Access Control List List of MAC addresses with the right to access the wireless network
Ad hoc network	Wireless network between individual devices (point-to-point)
AES	Advanced Encryption Standard New standard for encryption of data in WLANs
Antenna diversity	Technique with which a radio receiver is equipped with two antennas so that it can select the better of two signals
Antenna gain	Improvement of the antenna compared with an isotropic radiator achieved by suitable construction (passive!)
ATM	Asynchronous Transfer Mode Wired network used particularly in the backbone for large distances at high data rates
Authentication	Access control in communication networks (Who am I?) to increase data security
Authorization	Distribution of authorizations in communication networks (What can I do?) to increase data security
BPSK	Binary phase shift keying Modulation technique in WLANs
BQTF	Bluetooth Qualification Test Facility

	Facility for monitoring the interoperability of products of various vendors
BSS	Basic Service Set WLAN network with access to the infrastructure over a single access point
CCK	Complementary code keying modulation mechanism in WLAN
CDMA	Code Division Multiplex Code-controlled medium access control
CF	Compact flash
CFP	Contention free period Period during which access is managed by the access point (to support time-critical services)
CP	Contention period Period in which access is controlled according to CSMA/CA (to support time-critical services)
CP	Communications processor
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance, medium access control on a wireless IEEE 802.11 network
CSMA/CD	Carrier Sense Multiple Access with Collision Detection, medium access control for wired Ethernet network
CTS	Clear to send Signal in handshake protocol for avoiding the hidden node problem
DDE	Dynamic Data Exchange
DCF	Discrete coordinated function Normal medium access control in 802.11 in contrast to PCF
DECT	Digital Enhanced Cordless Telecommunications, European standard for language and data communication
DFS	Dynamic Frequency Selection in the 5 GHz band
Diversity	Wireless receiver with two antennas allowing selection of the best signal
Downstream	Communication from access point to client
DSSS	Direct Sequence Spread Spectrum (IEEE 802.11b)
EDGE	Enhanced Data Rates for Global Systems for Mobile Communications Evolution Further development of GSM with data rates up to 384 Kbps

	for video and wireless applications
EIRP	Equivalent isotropic radiated power The power output that would have to be applied to an isotropic radiator so that it would radiate the same effective power as another antenna in a specific direction. An isotropic radiator is a theoretical antenna that radiates in all directions with equal intensity (isotropic) and is assumed to be infinitesimally small.
ESM	Electrical Switch Module
ESS	Extended Service Set Wireless network consisting of several overlapping basic service sets (BSS)
ETSI	European Telecommunication Standard Institute
Fall back	Gradual reduction of the data rate when receiving conditions are bad to allow the connection to be maintained
FDMA	Frequency Division Multiplex Access
FEC	Forward Error Correction Inclusion of redundant bits in the useful data to make the signal less sensitive to interference
FHSS	Frequency Hopping Spread Spectrum A method used in 802.11b and Bluetooth.
FOC	Fiber-optic cable Transmission medium for optical networks.
FTEG	Law regarding wireless equipment and telecommunications installations in Germany
GFSK	Gaussian Phase Shift Keying Modulation technique in 802.11
GPRS	General Packet Radio Service Expansion of GSM for packet-oriented data communication at up to a maximum 170 Kbps.
GSM	Global System for Mobile Communications Digital telephone services at frequencies in the 900 MHz, 1800 MHz and 1900 MHz ranges
GSM-R	GSM for railroad traffic at high speeds
Handover	Mechanism for transferring a station from one radio cell to the next. The term is often used in conjunction with <i>roaming</i> .

Handshake	Acknowledgment process to establish a connection between stations ready to communicate.
Hidden node problem	Two nodes are arranged in a radio cell so that they are outside their own transmission range. If they both access the medium of the same time, collisions result.
HIPERLAN	High-performance Radio LAN in the 5 GHz band
Home RF	Standard for wireless communication between PCs and home-oriented consumer devices.
HSCSD	High Speed Circuit Switched Data GSM wireless network for higher data rates
HT-OFDM	High throughput OFDM, optimized version of OFDM for increased data rate, is used at IEEE 802.11n
IBSS	Independent Basic Service Set Ad-hoc network for spontaneous and simple establishment of wireless connections without a wireless infrastructure
IE	Industrial Ethernet
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 2 Mbps.
IEEE 802.11a	Standard for wireless networks in the 5 GHz range with transmission rates of up to 54 Mbps.
IEEE 802.11b	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 11 Mbps.
IEEE 802.11e	Standard for wireless networks in the 2.4 and 5 GHz-range, defines realtime requirements for voice and video applications
IEEE 802.11g	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 54 Mbps.
IEEE 802.11h	Standard for wireless networks in the 5 GHz band with transmission rates up to 54 Mbps. Standard for continental Europe; condition DFS/TPC
IEEE 802.11i	Security standard that replaces the obsolete WEP standard; It includes, among other things, the AES encryption technique
IEEE 802.11n	Standard for radio networks in the 2.4 and 5 GHz-range with data rates up to 600 Mbps

IEEE 802.3af	Standard defining power-over-Ethernet (PoE)
IP	Internet Protocol Collection of program routines that the TCP protocol accesses
IP20	Device degree of protection
IP 65	Device degree of protection
IPSec	Internet Protocol Security Open standard for increasing data security in IP networks
IrDA	Infrared Data Association Standard for data communication with infrared over short distances
IS	Intrinsically Safe (protected against explosion)
ISM band	Industrial, Scientific and Medical Band Frequency band for use without license
ISO	International Organization for Standardization
Kerberos	Security system for the encryption of sensitive data
MAC	Media Access Control, protocol level upon PHY, defines access to the the air interface
Multipath propagation	Reflections of an electromagnetic wave from different objects. As a result, the electromagnetic wave arrives at the receiver with different intensities and after different propagation times
MIC	Message Integrity Protocol Technique for increasing the integrity of data in WLANs
MIMO	Multiple In, Multiple Out, reception and transmission with multiple antennas and multiple independent signal paths
Mini PCI	Special design of WLAN adapters for direct integration in products
MSS	Mobile Satellite Service within UMTS
OFDM	Orthogonal Frequency Division Multiplex Method of modulation in 802.11a
OFDM/CCK	Orthogonal Frequency Division Multiplex/complimentary code keying Method of modulation in 802.11a
PAN	Personal Area Network Network for devices at relatively short distances from each

	other.
PC Card	Design and use, see PCMCIA. In contrast to PCMCIA, instead of a 16-bit interface, a 32-bit interface is used so that in the case of WLAN high data rates up to 54 Mbps can also be transmitted
PCF	Point coordinated function Medium access control technique to support time-critical services in WLANs
PCMCIA	Standard for PC cards (credit card size). PCMCIA cards (Personal Computer Memory Card International Association) are used for input/output (for example modem), as additional memory, and also as interfaces for WLAN particularly in laptops
PDA	Personal Digital Assistant Mobile end device
PHY	Physical Layer, lowest level of transmission protocol, describes access to the air interface
Pico network	Network structure in Bluetooth in which up to eight stations are organized
QAM	Quadrature amplitude modulation
QPSK	Quadrature phase shift keying
QoS	Quality of Service
R&TTE	Radio and Telecommunications Terminal Equipment Directive EU directive for telecommunications terminal equipment
RADIUS	Remote Authentication Dial - In User Service for secure communication networks
RCM	Radio Client Module (Ethernet adapter, Ethernet client)
RegTP	Regulatory body for telecommunication in Germany
RLM	Radio Link Module (access point)
Roaming	Free movement of wireless LAN nodes even beyond the boundaries of an access point's cell. The station can change from one radio cell to the next without any noticeable interruption (see also handover)
RSTP	Rapid Spanning Tree Protocol, protocol for autonomous rerouting of the signal path in the infrastructure
RT	Real Time

RTS	Request To Send Signal in handshake protocol for avoiding the hidden node problem
Scatter network	Network structure in Bluetooth in which several Pico networks are organized
SIG	Special Interest Group The user organization for Bluetooth
SNMP	Simple Network Management Protocol Standardized protocol for transporting network management information.
SSID	Service Set Identifier Address Name of the WLAN
TDMA	Time Division Multiplex Access
TKIP	Temporal Key Integrity Protocol Scheme for cyclic changing of the keys in WLANs
TPC	Transmission Power Control Automatic control of transmitter power in the 5 GHz band
UMTS	Universal Mobile Telecommunications System Mobile wireless transmission for voice, audio, image, video, and data communications
UNII	Unlicensed National Information Infrastructure Name of the 5 GHz band in American literature
Upstream	Communication from client to access point
URAN	UMTS Radio Access Network
UTRAN	UMTS Terrestrial Radio Access Network
WCDMA	Wideband CDMA Method of modulation for high data rates
WDS	Wireless Distribution System Radio links for connecting the access points for an extended service set (ESS)
Web pad	Portable device in DIN-A4 size with a touch screen for Internet use
WECA	Wireless Ethernet Compatibility Alliance An alliance of various wireless LAN product manufacturers who ensure product compatibility through product testing.
WEP	Wired Equivalent Privacy Encryption scheme for WLANs (obsolete)

Wi-Fi seal	Wireless Fidelity Seal of approval of the WECA alliance for compatible and tested components.
Wired LAN	Network operated on guided media
Wireless LAN	Network operated using unguided media
WLAN	Wireless LAN (here: IEEE 802.11)
WLANA	The Wireless LAN Association Consortium of wireless LAN providers promoting wireless LAN technology
WMM	Wi-Fi Multimedia, defines interoperability of IEEE 802.11e
WPA	Wireless Protected Access A provisional security mechanism from WECA that closes existing security gaps in WEP. The AES encryption scheme is used. This will be replaced by IEEE 802.11i.