SIEMENS

SIMATIC NET
Industrial Wireless LAN

White Paper • 2001

Objective:

The purpose of this White Paper is to

- provide information on the subject of Wireless LAN technology in automation engineering, and to
- discuss development trends in Wireless LAN technology.

In addition to purely technical aspects and costs, the main factors which contribute to the decision to install a Wireless LAN are

- ease of use (Plug & Play)
- taking advantage of existing synergies
- potential for process improvement
- future developments in wireless technology
- utilization of existing know-how

This symbol identifies references to SIMATIC NET products or special SIMATIC NET solutions

Published by
SIEMENS AG
Automation and Drives Group
SIMATIC NET Industrial Communication
P.O. Box 4848
90327 Nuremberg

Additional support:
Should you have additional questions, please get in touch with the Siemens contact at your local branch office or agency.

You will also find SIMATIC NET on the Internet at

http://www.siemens.com/simatic net

Introduction

Wireless networks are becoming more and more popular. In areas as diverse as offices, warehouses and even industrial production facilities, wireless networks provide a new sense of independence and flexibility. Production data and service data are available company-wide, and can be collected and modified from anywhere in the company. Commissioning engineers can work onsite at the machine and see exactly what they are doing. Different technologies, which are described in detail in the following, are available for implementing this new kind of networking.

Transmission medium

In contrast to LANs which use copper or fiber-optic cables, a wireless local network uses space as its transmission medium. Unlike copper or fiber-optic cables, however, wireless networks do not transmit information through variations in voltage values or light pulses, but rather in the form of electromagnetic waves. As a transmission medium, space responds completely differently than cable with its clearly defined and constant transmission characteristics.
Due to physical circumstances, the usable frequency spectrum for the transmission of electromagnetic waves on earth is limited. Depending on the output power, any given frequency can be used only once within a specific radius around the transmitter (shared medium).

Wave length	Frequency	
10^5-10^4 m	3 – 30 kHz	VLF
10^4 – 10^3 m	30 – 300 kHz	LF/low frequency
10^3 – 10^2 m	0,3 – 3 MHz	MF/medium frequency
10^2 – 10 m	3 – 30 MHz	HF/high frequency
10 – 1 m	30 – 300 MHz	UKW/ultra-high frequency
1 – 0.1 m	0.3 – 3 GHz	**Microwave range**
		D networks 890 – 960 MHz
10 – 1 cm	3 – 30 GHz	E networks 1710 - 1880 MHz
		DECT 1.8 – 1.9 GHz
1 – 0.1 cm	30 – 300 GHz	UMTS 1.97 – 2.2 GHz
		Bluetooth 2.402 – 2480 GHz
1 – 0.1 mm	0.3 – 3 THz	**WirelessLAN (ISM Band) 433 MHz, 860 MHz, 2.4GHz, 5.7GHz**
300 – 0.72 mm	1 – 417 THz	Infrared
0.72 – 0.38 mm	417 – 789 THz	**Visible light**
↓	↓	Ultraviolet /X-rays

Because the frequency spectrum belongs to the public domain, its management and appropriation are under government control. Every country has an administrative body which is responsible for releasing frequencies for specific purposes and coordinating such release approvals internationally. In Germany, the regulatory authority for telecommunication and postal services is responsible for establishing such things as output power, bandwidth and authorized modulation method.
In Europe, the ISM band (Industrial, Scientific, Medical Band) has been approved for cost-free use.

ISM band

The ISM band covers a number of frequency ranges, but only the higher-frequency ranges of 433 MHz, 860 MHz, 2.4 GHz and 5.7 GHz are suitable for data transmission. An even higher frequency range of 24 GHz has not yet been made accessible. While the low-frequency ranges are used for door/gate-control systems, alarm systems, audio systems and measured-value transmission, only the 2.4 GHz and 5.7 GHz frequency ranges are of importance for data transmission at the data signalling rates required by LANs.

- 2.4 GHz provides a bandwidth of 83.5 MHz. This ISM band is the only frequency band which – with few limitations – is available worldwide, and currently enables data rates between 1 Mbit/s and 11 Mbit/s. The objective is to increase data rates by using more complex modulation procedures.
  For historic reasons and due to country-specific interests, differences still exist between countries as regards the use of the frequencies in the various ISM bands. Attempts are being made at both the national and international level at settling these differences in the not-too-distant future.
- 5.725 GHz provides a bandwidth of 150 MHz, permitting implementation of data rates of up to 54 MBit/s.

The prerequisite for cost-free use of the ISM band is that the wireless units do not exceed the prescribed band-specific output power (which is 100 m W in the 2.4 GHz band). All devices which want to use this range must be examined in a testing laboratory and approved for use.

While operation of these wireless devices requires no additional approval, the country-specific conditions for the operation of such a wireless communication system must be taken into account. In Germany, for example, operation beyond property boundaries is subject to registration, allowing the first to register his system to continue to operate that system without modification should two neighboring systems interfere with one another.

Channel distribution in the 2.4 GHz ISM band

As described above, a wireless system uses a shared medium for communication. This means that only one node can actively transmit in any given cell.
If a large area (such as a warehouse) is covered by multiple cells which communicate with their mobile nodes over the same frequency, only one node can actively transmit in that warehouse at any given time.
In order to circumvent this problem, the ISM band's 2.4 GHz frequency was subdivided into 13 5 MHz frequency bands.

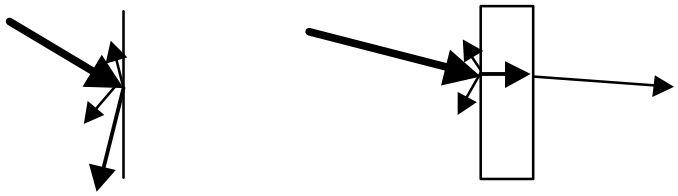
Channel	Frequency
1	2.412 GHz
2	2.417 GHz
3	2.422 GHz
4	2.427 GHz
5	2.432 GHz
6	2.437 GHz
7	2.442 GHz
8	2.447 GHz
9	2.452 GHz
10	2.457 GHz
11	2.462 GHz
12	2.467 GHz
13	2.472 GHz

The transmission of data at a data signalling rate of e.g. 11 Mbit/s requires a bandwidth of more than 20 MHz. In order to make it impossible for adjacent or overlapping cells to interfere with one another, a channel separation of 25 MHz is required. Channels 1, 6 and 11, for example, can be used to operate three cells without reciprocal interference. This means that the mobile nodes in two adjacent cells can communicate in parallel with the relevant access points without intefering with each other. The allocation of the individual channels available in the ISM band must be given careful consideration when planning a wireless LAN. Careful planning can provide for clear separation between adjacent cells, thus increasing the performance capability of the entire wireless network.

Radio waves

The propagation of a radio wave in space is three-dimensional. In order to achieve high-quality data transmission using this medium, careful consideration must be given to the influences which can alter a radio wave's direction and intensity on its way from the transmitter to the receiver.
Low-frequency electromagnetic waves have propagation characteristics which are very different from those of very high-frequency electromagnetic waves. In simple terms, the behaviour of high-frequency electromagnetic waves can be compared to that of light waves.

The way radio waves reflect off objects is of great importance to radio networks such as wireless LANs. Electromagnetic waves are reflected or absorbed by walls, furniture, humans and other obstacles, resulting in signal attentuation. Every material has a frequency-dependent attenuation. Added to this is the fact that every surface, corner or wall reflects, diffracts, refracts or diffuses the incoming wave on the basis of the spacial relationship of wave to obstacle.



Reflection of a radio wave on a metallic / coated surface.

Attentuation of a radio wave due to an obstacle (such as a wall).

Figure 1: Effect of obstacles on radio waves

Because of the different effects on the wave, a number of waves of varying intensity arrive at the receiver over different paths. This method of propagation is referred to as multipath propagation.

The resultant heterodyning of waves at the receiver can lead to amplification, attentuation, or, in the worst-cast situation, to destruction of the signal, depending on the phase angle of the individual wave. From this environment-dependent signal characteristic, the receiver must select the best and strongest signal. Moving sources of interference, such as persons or automobiles, can continually modify this transmission path.
Not only spacial objects present obstacles, however. Adjacent transmitters from other radio systems can also result in a deterioration of the wireless link.

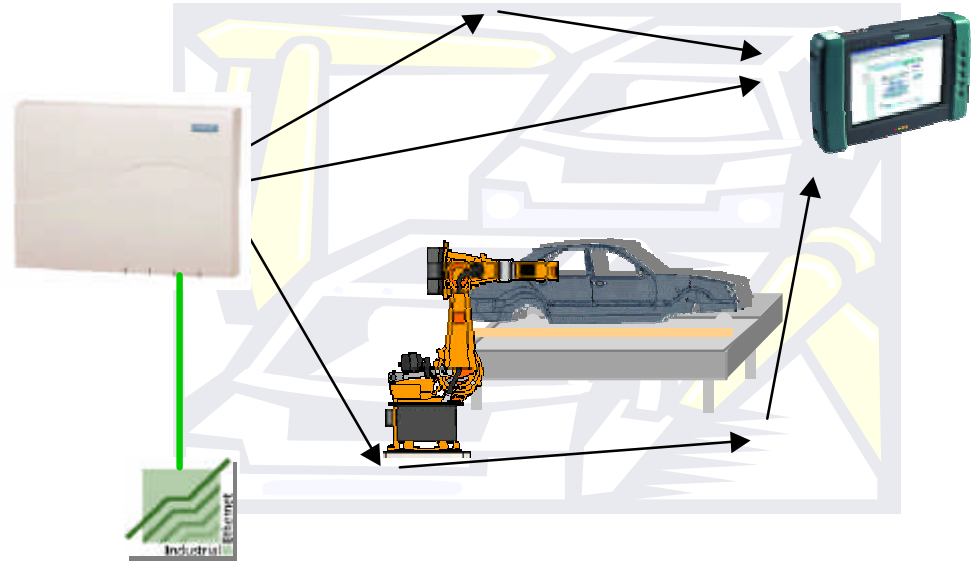


Figure 2: Multipath propagation of radio waves

Wireless LAN standards

Today's wireless LAN components for office applications are normally based on the IEEE 802.11 standard (IEEE stands for Institute of Electrical and Electronics Engineers). Until recently, this wireless LAN standard was subdivided into three groups:

- IEEE 802.11 — Data transmission in the 2.4 GHz band
  Transmission rates of up to 2 Mbit/s
- IEEE 802.11 a — Data transmission in the 5 GHz band with
  transmission rates of up to 54 Mbit/s
- IEEE 802.11 b — Data transmission in the 2.4 GHz band with transmission rates of up to 11 Mbit/s

The standard describes two transmission methods (infrared transmission and radio transmission). Under radio transmission, two different transmission modes were described (DSSS and FHSS) which will be explained in detail in the following.
Because of increasing user acceptance of Wireless LAN systems, the IEEE established additional committees to work on new transmission technologies and techniques such as Bluetooth™ as well as on such things as new security concepts.

- IEEE 802.11 e — Development of new security mechanisms such as WEP2 (Wired Equivalent Privacy, authentification, QoS, video).
- IEEE 802.11 f — Simplification of communications between access points
- IEEE 802.11 g — Data trans. in the 2.4 GHz band with transmission rates of up to 22 MBit/s
- IEEE 802.15 — Data transmission in the 2.4 GHz band using Bluetooth™
- IEEE 802.15.2 — Compatibility between Bluetooth™ and Wireless LAN

Some time ago, an organization called the Wireless Ethernet Compatibility Alliance (WECA) was established in order to ensure the interoperability of IEEE 802.11-based components from different manufacturers. Once they pass compatibility tests, the products are given the Wi-Fi (Wireless Fidelity) seal of approval.

Another European standard is HIPERLAN II (High Performance Radio LAN) in the 5 GHz band. This standard will allow future transmission rates of up to 54 Mbit/s.

Transmission methods used in Wireless LANs

The Spread Spectrum method was developed for military applications, its purpose being to make data transmission as secure against interception as possible. Spreading the data over a much wider frequency range than that of the useful signal reduces the required power density (equivalent to transmission transmitter power as it relates to bandwidth). This technique not only makes locating and tapping the transmitter more difficult, but also minimizes interference from narrow-band and wide-band sources. The standard describes two versions of the Spread Spectrum technique for transmitting Wireless LAN data to IEEE 802.11:

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)

Because they use different technologies, the two are not compatible.

The third transmission method to IEEE 802.11 uses infrared, but is seldom used today because of its physical characteristics.

Current developments in the field of Wireless LAN systems put the progress being made in the development of signal-processing processors to good use, making it possible for the Wireless LANs to use more sophisticated methods of data transmission, such as:

- OFDM (Orthogonal Frequency Division Multiplexing)

to IEEE 802.11g.

Frequency Hopping Spread Spectrum (FHSS)

The FHSS method transmits the useful signal using permanently changing carrier frequencies. The constant frequency changes make signal interception extremely difficult. The frequency change is rhythmic, and the rhythm must be known to the receiver, that is to say, transmitter and receiver must be synchronized prior to data transmission. The frequency band provides the transmitter with 79 different channels for changing the carrier frequency. The FHSS method is not easily susceptible to interference, as carrier frequencies with strong narrow-band interference sources can be left out and the data retransmitted with the aid of other carrier frequencies. The large number of carrier frequencies required reduces the bandwidth for data transmission to transmission rates of between 1 and 2 Mbit/s. The overhead for the sudden frequency changes also complicates the interruption-free forwarding of mobile nodes from one cell to the next (roaming).

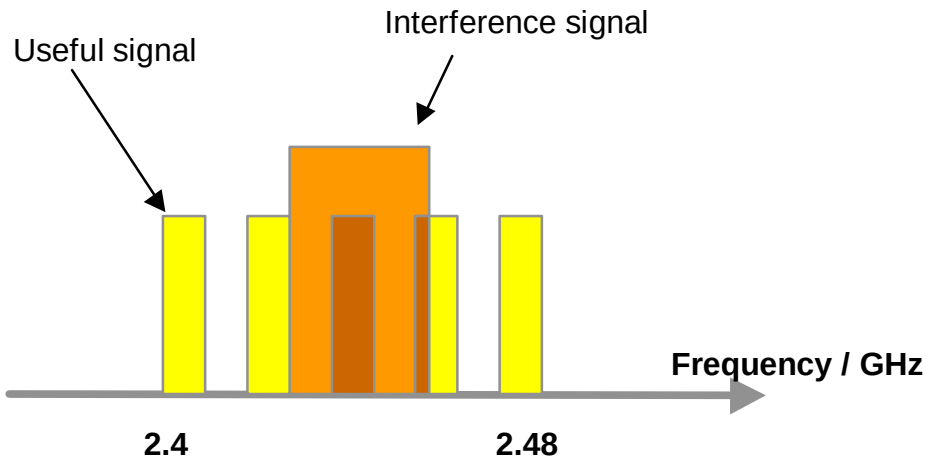


Figure 3: FHSS transmission method

Direct Sequence Spread Spectrum (DSSS)

The DSSS method spreads the useful signal over a channel's available frequency range. In addition, the transmitter encrypts every data bit into a pseudo-random sequence of 11 or 8 characters (signal spreading). Spreading makes the useful signal appear to be noise, thus protecting it against tapping. Only when the spread spectrum has been reversed in the receiver does a signal emerge from what had appeared to be only noise. Narrow-band interference signals can be filtered out of the useful signal by reversing the spread, and thus do not impede data transmission.
By spreading the useful signal over a bandwidth of more than 20 MHz, much higher transmission speeds can be attained with this method than with the FHSS method, in which a bandwidth of only 1 MHz is available. Wideband transmission also has the advantage of eliminating interference caused by multipath reception, as frequency-specific propagation does not have as much of an effect. The DSSS method is thus virtually impervious to narrow-band interference sources, offers better protection against multipath propagation, and enables higher data throughput, albeit using greater bandwidth.

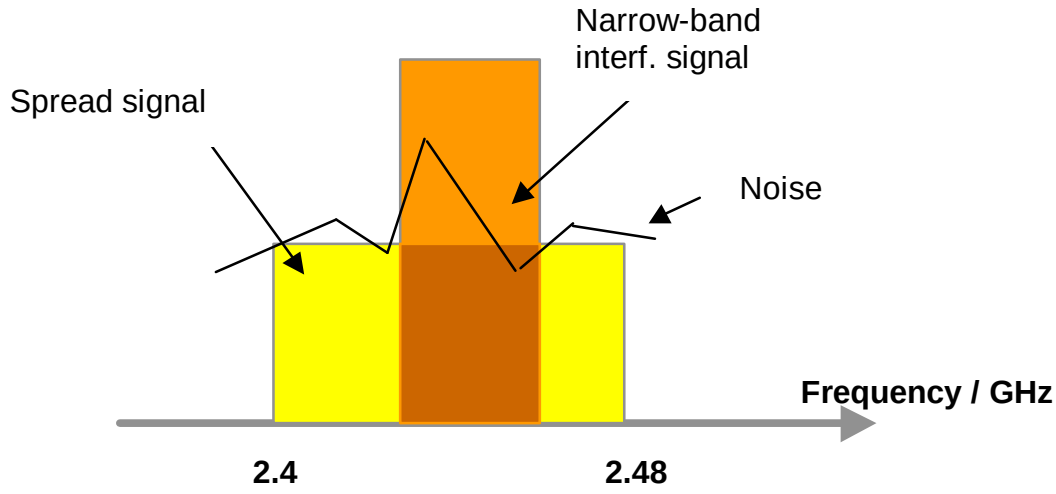
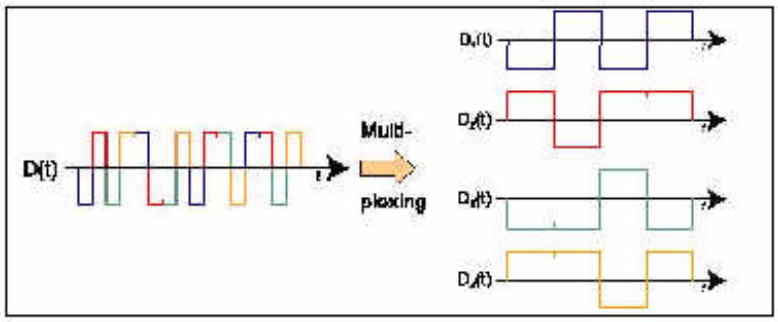


Figure 4: DSSS transmission method

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM (Orthogonal Frequency Division Multiplexing) is a method which is rapidly gaining in popularity thanks to enormous advances in the fields of microelectronics and digital signal processing. The OFDM method divides the data stream into parallel data streams. Each data stream is transmitted with its own carrier frequency. Because the carrier frequencies are orthogonal, they can affect each other little, if at all.
Because OFDM divides a data transmission into frequency channels and uses error-correcting transmission procedures, it is largely impervious to multipath propagation and narrow-band parasitic signals, making this method particularly interesting for industrial applications.



OFDM can also attain transmission ratres of 54 Mbit/s in the 2.4 GHz band, whereby its reach will most probably be greater than that of comparable 5 GHz systems.

Bluetooth™

The name of this Wireless LAN technology, which is frequently discussed and debated in the press, refers to Denmark's King Harald Blåtand. The English translation of Blåtand is "Bluetooth".
The Viking king reigned in the 10th century, and earned his place in the history books for uniting Denmark and Norway.

Bluetooth™ technology stems from developments by Telecom providers Nokia and Ericsson. It was developed for communication between mobile units (establishment of Personal Area Networks, or PANs), and is to become an international standard. The hope is that standardization and ease of use will make this technology suitable for global use and revolutionize most particularly those devices aimed at the commercial consumer market.

Bluetooth™, like IEEE 802.11 b-compatible Wireless LAN systems, uses the 2.4 GHz ISM band, and uses Fast Frequency Hopping as transmission method. Seventy-nine channels, which are changed 1,600 times per second, are available for data transmission.
The system is thus virtually impervious to noise emission, and fast frequency hopping ensures a high level of data security. The system easily dominates other radio systems.

Bluetooth™ systems were originally designed for PANs (transmitter power 1 mW, reach approx. 10 m, data rate 1 Mbit/s, no roaming). In the meantime, however, Bluetooth™ specifies a second device class with transmitter power of up to 100 mW, allowing these systems to compete with IEEE 802.11b systems.

Bluetooth™ devices are identified by a unique, 48-bit serial number, similar to a MAC address on an Ethernet. The Bluetooth™ protocol supports a data channel and three voice channels (64 kbit/s per voice channel, 723.3 kbit/s data channel).
As soon as two Bluetooth™ devices have come within the bridgeable distance of one another, communication can begin without further intervention. The devices exchange profiles, thus determining which services each can make available to the other.

The resulting structure is referred to as a Piconet. As many as right nodes can be integrated in a Piconet. In every Piconet, one Bluetooth™ node assumes the role of master.
Communication between more than eight devices produces multiple, partially overlapping Piconets. Such a network structure is referred to as a Scatternet.

Because radio transmission in general provides a much lower level of data security than cabled systems, Bluetooth's™ data encryption feature plays an important role. With the aid of a random generator, a Piconet master generates a key from the Bluetooth™ address. This key determines the hopping sequence in the pico cell. This sequence must be used by all Piconet nodes. Each time a new connection is established, the random generator generates a new hopping sequence.
In addition to frequency hopping, the transmitted data are encrypted with a 128-bit key.

In order to ensure device compatibility, each new device must be tested and certified by an independent facility (Bluetooth™ Qualification Test Facility, or BQTF).

Bluetooth™ is thus an interesting technology for point-to-point connections in industrial and medical applications (low output power) when reach, roaming and a high data signalling rate do not play major roles.

Universal Mobile Telecommunication System (UMTS)

UMTS (Universal Mobile Telecommunication System) is not a technology used in today's Wireless LAN solutions. The popularity which UMTS has gained thanks to the auctioning off of radio frequencies makes it sufficiently interesting for a brief discussion of its most essential aspects.

UMTS is a mobile radio communication standard of the 3rd generation. The purpose of this new standard, which is supposed to make data rates of up to 2 Mbit/s possible, is to enable

- voice
- audio
- data
- text
- image and
- video transmission

to mobile nodes.
For communication with UMTS systems, the regulatory authority auctioned off frequency bands in the range from 1.9 GHz to 2.2 GHz to network operators.
UMTS is regarded as a chance at the establishment of a global mobile radio communication standard. Initial test installations have confirmed this prognosis.

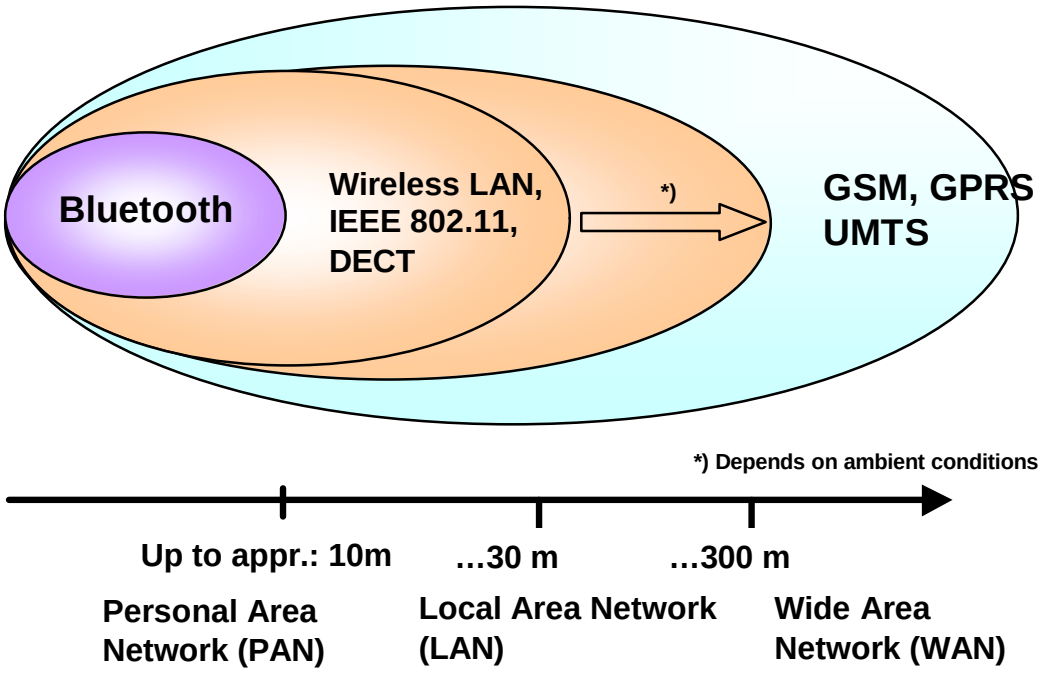


Figure 5: Transmission technologies and bridgeable distances

Coexistence of Bluetooth™ and Wireless LAN systems

Many manufacturers favor the coexistence of the two systems because each is designed for very specific applications.
The Bluetooth™ system was developed for point-to-point linking of mobile nodes. Such nodes might be headsets for handheld units or printer connections for an office laptop. At the same time, devices or plant sections could be integrated in a Wireless LAN network. This second link would be used to exchange visualization data or diagnostic data via Web mechanisms in the network.
In order to implement such a scenario, various tests were carried out in which both systems were operated in close proximity to one another.
The results of these tests were not very encouraging. At present, the two systems compete hotly with one another, that is to say, when operated in parallel, each system interferes strongly with the other.
From the current perspective, parallel operation in close proximity is not recommended.
Driven by the use of different systems for the same applications and by the increasing presence of Bluetooth™ systems on today's market, standardization groups are attempting to define control mechanisms which enable parallel operation of the two systems. Several different approaches are being considered which large manufacturers have heralded as workable.

Comparing the different radio communication systems

Technology	Max. data rate	Reach (m)	Network nodes	Connection charge	Application
IrDA	4 Mbit/s	1 m	2	No	Point-to-point data transmission
DECT	128 kbit/s	50 m	8	Yes	Point-to-point voice transmission
GSM	9.6 kbit/s	9.6 kbit/s		Yes	Point-to-point voice transmission
UMTS	2 Mbit/s	10 km		Yes	Point-to-point voice-, video-, data transmission
Bluetooth	1 Mbit/s	10 m	10	No	Point-to-point data transmission
Home RF	2 Mbit/s	50 m	128	No	Network for voice and data communication in home range
IEEE 802.11	2 Mbit/s	Up to 100 m	Approx. 10 per access point	No	Wireless LAN for data transmission
IEEE 802.11b	11 MBIt/s	Up to 100 m	Approx. 10 per access point	No	Wireless LAN for data transmission
IEEE 802.11g	22 Mbit/s	Up to 100m	Approx. 10 per access point	No	Wireless LAN for data transmission
IEEE 802.11a	54 Mbit/s	Up to 100 m	Approx. 10 per access point	No	Wireless LAN for data transmission
HyperLAN	54 Mbit/s	Up to 150 m	Approx. 10 per access point	No	Wireless LAN for data transmission

Topologies of wireless networks

Depending on the application, there are different topologies for wireless networks.

The simplest form of a wireless network is referred to as an a*d hoc network*. Such a spontaneous network can be established by the radio communication cards of individual devices without user intervention. These networks are used for the temporary exchange of data over short distances.

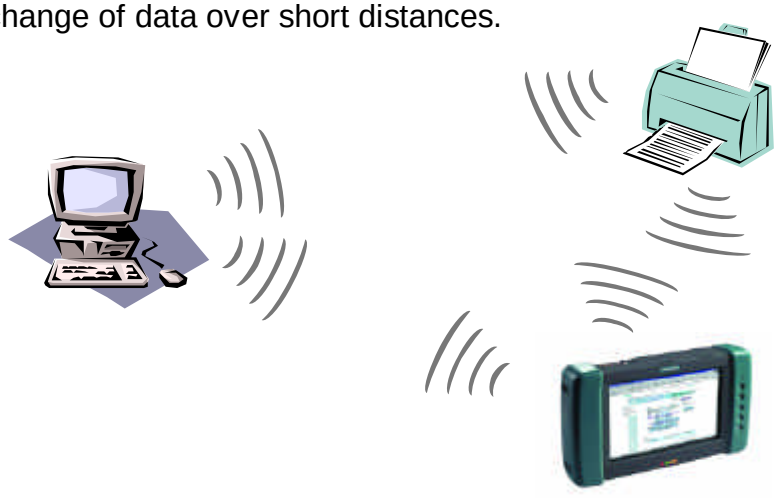


Figure 6: Ad hoc network

The limitations of an ad hoc network as far as distance is concerned can be circumvented by using a radio repeater. A radio repeater is also called an access point because, in addition to its repeater function, it is also capable of serving as a bridge of sorts between Wireless LAN and Wired LAN. This characteristic, in turn, makes it possible to provide all mobile nodes in an ad hoc network with data from the landline network. It is also possible to transfer current production data from the mobile nodes to the landline network for post-processing.

Should the radio range of a repeater prove insufficient to allow a mobile node enough freedom of movement, it is always possible to expand the action radius by installing multiple access points with overlapping transmission/receiving range. The mobile node can move freely within this range. Thanks to a special forwarding procedure used by the access points (roaming), the mobile node can always use the access point to which the connection is best at the time.

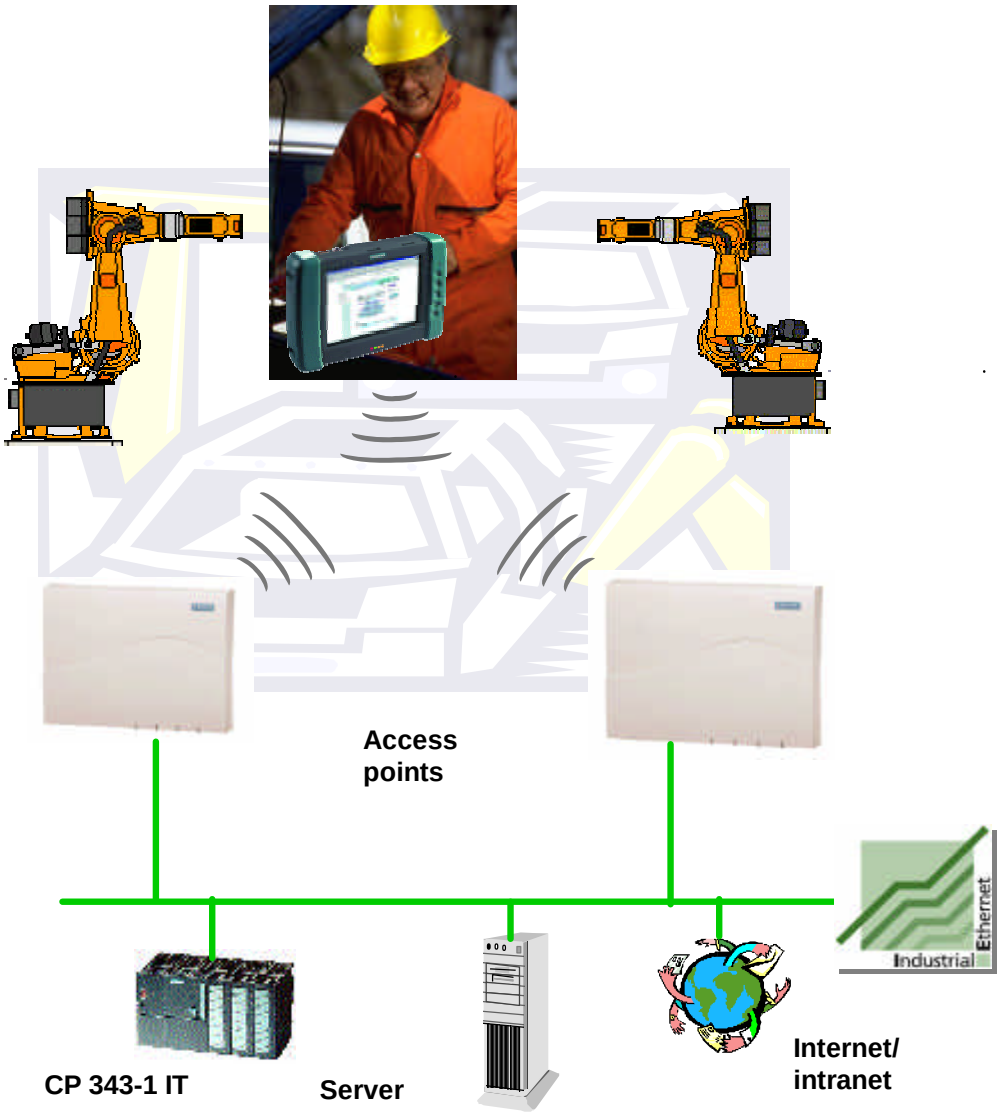


Figure 7: Industrial Wireless LAN with SIMATIC NET components and MOBIC

CSMA/CA communication mechanism

A *wired* Ethernet network uses the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) access method. When the station that wants to transmit has listened in on the line and discovered that it is not busy, the data are transmitted. During transmission, the sending station can recognize a collision on the basis of a level overshoot, and terminates the transmission. When a waiting time of arbitrary length has expired, a new attempt is made to transmit the data to the peer node.
This mechanism can be used only in part in a wireless network. A station can check to see whether the medium is free prior to initiating its own transmissions. During the transmission itself, however, the station can no longer detect a collision. This situation will always occur when stations begin transmission at exactly the same time because the medium appeared to both to have been free when they checked just prior to starting transmission.
A data stream collision can also occur during radio communication due to the so-called hidden node problem. This means that two stations are coincidentally in the same radio cell of an access point but outside their own reach capability. Both stations detect a free medium and begin to transmit.
Another system can also interfere with a radio transmission, for example a Bluetooth™ system that is being operated in parallel.

For these reasons, Wireless LANs do not use CSMA/CD, which detects collisions, but rather CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), in which a "handshake" procedure virtually prevents collisions from occurring.

The handshake procedure specified by IEEE 802.11 uses special message frames which reserve airspace for the station that is ready to transmit.
Once the station that is ready to transmit has recognized the medium as free, it sends an RTS (Request To Send) to the other station. This message reserves the medium (airspace) for one complete data transmission (RTS message frame, CTS message frame, data frame, acknowledgement message and intervals). Within a specified amount of time, the partner station sends back a CTS (Clear To Send) in which the complete remaining time for the now ongoing data transmission is once again given. Every node now knows how long the ongoing data transmission will take. Because of their extreme brevity, loss of the CTS and RTS frames because of a collision is highly unlikely.

If the partner receives the CTS message correctly, the data transmission can begin.

When the data transmission has been completed, an ACK (Acknowledgement) frame tells the sender that the data were transmitted successfully. If no acknowledgement is received, the sending station must assume that a collision or a transmission error has occurred. After a waiting time has elapsed, the sending station makes a new attempt to send.

This handshake procedure, which is also forwarded over the access point, makes it possible to reach stations which do not lie within the reach of the transmitting station (hidden node). These stations also recognize that the transmission medium has been reserved.

Data security in wireless networks

Daily use of the PC in an office environment has made passwords and access codes part of everyday life. Users need these mechanisms to gain access to their or their company's computer system. The data being transmitted over a company's own data lines are not normally encrypted. Not until the data leave the company network are they often subjected to encryption mechanisms to protect against access by a third party or against line-tapping.
When a wireless network is set up on company grounds, it cannot be kept on company grounds like a wired network. Radio waves cannot be stopped by property boundaries or fences.
There are various ways and means of protecting data and data networks against unauthorized access.
First, it has to be determined whether the wireless network is to be operated separately or together with the company's intranet, and what kind of data are to be transmitted, whether the data are worth protecting or simply relate to a warehousing system and direct the forklift to transport a pallet from warehouse location A to warehouse location B.
Once these fundamental questions have been answered, a Wireless LAN system in the 2.4 GHz band offers several security levels:

- **Spread Spectrum technology:**
  Most of today's Wireless LAN systems use the Direct Sequence Spread Spectrum, or DSSS, method, which was originally developed for the military. As already mentioned, the useful signal is spread over the entire available frequency range of a channel, and thus cannot be received with narrow-band receivers. The data signal is therefore perceived as noise. The data signal can be tapped only by

using the same technology as that used in the Wireless LAN system itself.

- **WEP (Wired Equivalent Privacy)**
  WEP is an Layer 2 level encryption method which uses keys of up to 128 bits in length. This function can be activated in the access point and in the mobile nodes. Data are encrypted prior to transmission, and can be decoded and read by the authorized node only with the relevant key. These keys provide a relatively safe but not foolproof protection against tapping, as they not only have a limited length, but are static as well.

- **Reach of a radio communication system**
  The short reach of most radio systems affords a certain degree of natural protection in itself, as long as the systems are placed so that the Wireless LAN remains within the boundaries of a given piece of land or building. This entails the use of directional antennas which help limit radiation of the radio signals to specific company areas. These measures make it even more difficult to tap installed radio systems, as the tapping system must be brought within the range of the cell, subjecting it to the same risks as a wired system.

- **Network name**
  The network name can be used to limit the nodes in a cell. Only nodes that know the right network name can take part in radio communication, thus precluding the use of unauthorized Wireless LAN devices.

- **MAC filtering**
  Filtering of the Wireless LAN cards' MAC addresses enables the access point to identify the mobile node from which the data packets are coming. Unless the access point recognizes the MAC address, it will not forward the data packets. Unknown Wireless LAN cards are thus denied access to the Wireless LAN and to the wired LAN. Because of this security mechanism, care must be taken that the access point manager also be accessible only for specific MAC addresses.

Spurred on by repeated reports in the press regarding the security of Wireless LAN systems, these basic protective mechanisms are constantly being improved and new mechanisms added. These new mechanisms include Layer 3 functions which use secret and automatically generated, constantly changing keys. In newer systems, one of the

functions used for network-wide management of this encryption system is **RADIUS** (Remote Authentification Dial - In User Service).

Biological tolerance of wireless networks

Despite the many advantages which wireless networks (mobile radio networks, wireless data networks, cellular telephone networks) offer users, this technology must also be repeatedly evaluated as regards its possible effects on the human organism. In the last 30 years, approximately 20,000 studies and analyses have been done to examine the effects of artificially generated electromagnetic emissions.
As matters currently stand, adverse health effects can be ruled out, the output power of the communications units being extremely low.

This is certainly due in large part to the authorities responsible for regulation and approval, which determine the environmentally compatible limit values and carefully control all devices and systems for wireless communication which are offered for sale. Care is taken that all limit values which have significance for the frequency range, such as the output power, are carefully and accurately checked. Devices which do not keep to these limit values are not approved for operation. Users can thus be sure that they are always using devices which represent the very latest in research and development.

According to DIN VDE 0848 Part 2 and IEEE, the limit values for 2.4 GHz are as follows:

- Electric field intensity 137 V/m
- Magnetic field intensity 0.36 A/m
- Power density 1 W/m²

Today's Wireless LAN systems are well below these limit values. Wireless LAN systems have a maximum power output of 0.1 W, while the output power of a commercial-grade handheld is approximately 2 W. According to the Federal Agency for Radiation Protection, the radiation from a microwave oven is approximately 5 mW / cm², that is to say, substantially higher overall than the radiated power of a Wireless LAN system.

Use of a Wireless LAN system with output power of less than 0.1 W can thus be considered completely safe.

Industrial use of a Wireless LAN system

The true benefits of Wireless LAN technology lie in the mobility and flexibility of individual components. This mobility makes it possible to reshape work processes and develop innovative solutions.
There are also many applications in the field of automation in which the mobility of individual components is extremely advantageous to the user.

Applications for Wireless LANs in automation

- Mobile data acquisition

  The use of mobile, industrial Web Pads such as the MOBIC (Mobile Industrial Communicator) from SIMATIC NET allows the user to collect data in all production and storage areas and pass these data on to central data processing. The high-overhead, error-prone transfer of data from paper to the central database is no longer necessary.

- Mobile service

  When a problem occurs, service personnel can analyze it on site and view the information needed to quickly remedy the problem via the wireless MOBIC Web Pad. The availability of spare parts in the warehouse can be immediately checked and parts ordered online if necessary.

- Mobile commissioning

  The commissioning phase can be considerably simplified and shortened, in some cases with considerably cost reduction, through the use of mobile communication. Commissioning engineers can monitor machine settings directly via their wireless service units and intervene immediately when problems occur.

- Flexible production

  In today's world, assembly lines must never be rigid, inflexible units which can be modified for other uses only at great expense. Flexible production makes it possible to fulfill customer requirements quickly and with little overhead. Production units can be integrated in the data network quickly and with minimum overhead via a wireless data network.

Wireless LAN components for industrial applications

Wireless LAN technology is often already a part of the office environment. Immense growth is predicted for this technology in the SO/HO (Small Office/ Home Office) sector. In order to be able to use wireless communication technology in industrial applications as well, however, it is recommended that modules be used which have been designed specifically for industrial use.

In industrial environments, there are many influences which can have adverse effects on wireless communication.

These include machine and storage units whose metal-based construction serve as a barrier against radio waves. In addition, the path of the radio waves is constantly being altered by the movement of humans and transport vehicles.
Industrial production facilities are normally located in huge halls in which the effects of multipath propagation are particularly prominent.
It is thus impossible to guarantee the same marginal conditions for all radio communication.

For the use of Wireless LAN technology in industrial environments, SIMATIC NET offers components which ensure reliable data transmission despite difficult ambient conditions.

In order to circumvent the extensive multipath propagation and the resulting attenuation or destruction of radio waves common in assembly halls, the radio modules are equipped with two antennas (antenna diversity), allowing the receiver to choose the stronger of two receive signals.
In order to ensure reliable data transmission, the modules must be capable, despite constant changes in the quality of the transmission path (number of nodes, changes in distance between nodes and access point), to switch from the highest data rate to a lower data rate to ensure reliable data transmission at all times.

The modules themselves must also be designed specifically for a rough industrial environment. This means they must have a high degree of protection, a robust housing, a high-quality connection system, and be easy to install. In addition, the modules must have the user-friendliness of an IT component such as Web Based Management with SNMP or enable the sending of e-mails or SMS messages.

SIMATIC NET offers two components for setting up a wireless industrial network:

- RLM (Radio Link Module), a robust, industrial-quality access point of rugged design for linking Wireless LAN and Wired LAN

- PCMCIA card (CP 1515) for installation in PCs and mobile operator panels with PCMCIA interface, such as the MOBIC or the Field PG

A module is also planned for connecting devices without PCMCIA card interface.

- RCM (Radio Client Module), an industrial-quality client module with Ethernet interface for linking mobile and non-mobile data terminal equipment with Ethernet interface.

With these modules, SIMATIC NET offers a solution which makes it possible to enjoy the advantages of mobile data communication in an industrial setting.

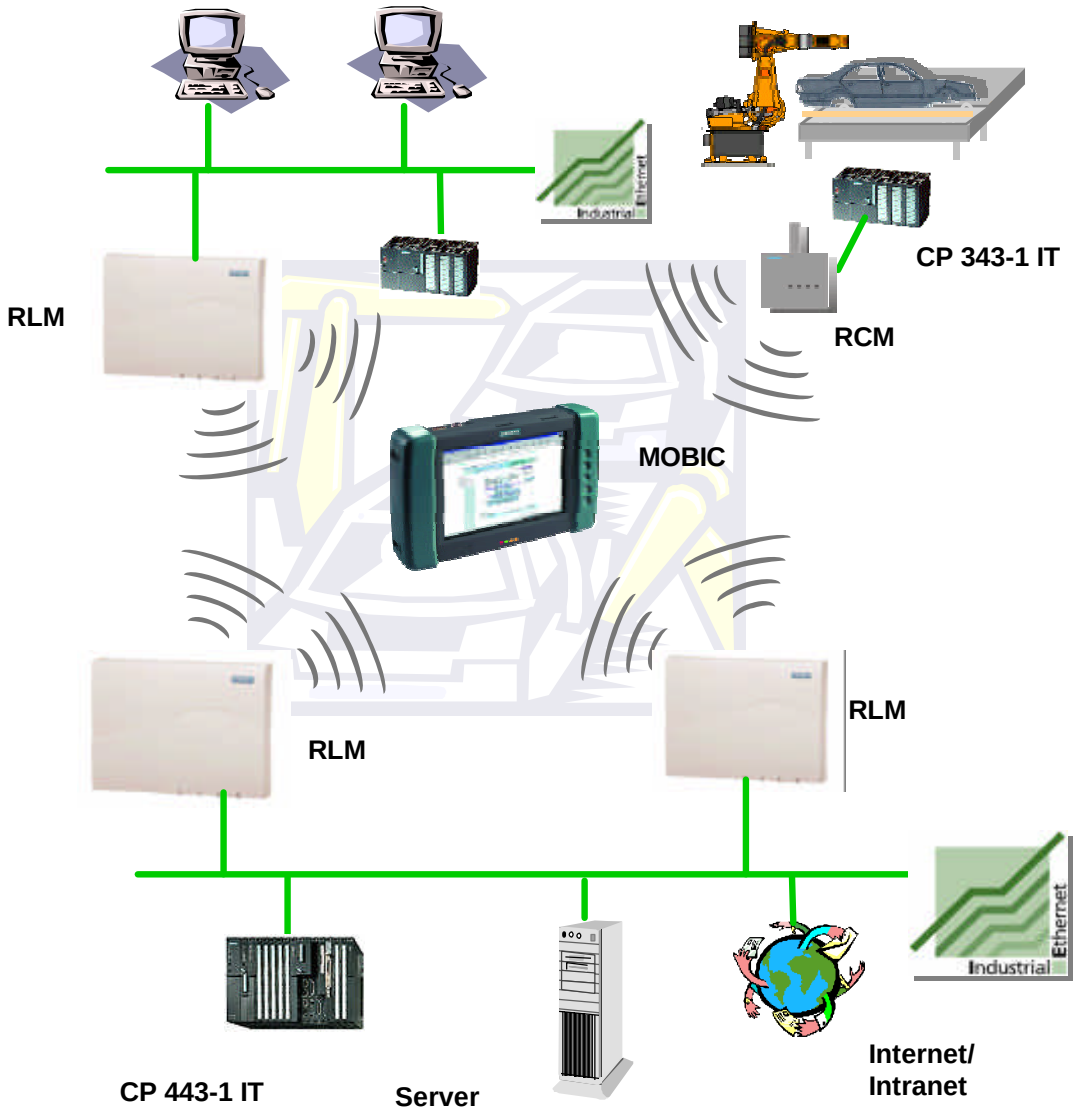


Figure 8: Industrial Wireless LAN

Future developments in the Wireless LAN sector

The wish for totally cable-free, line-free communications networks will certainly not be fulfilled in the near future. Although new standards such as IEEE 802.11a or IEEE 802.11g enable data rates of between 20 and 54 Mbit/s, wired high-speed networks will never become superfluous thanks to their stability and reliability.
It must also be noted that increases in the transmission frequency not only raise the transmission speed, but also the sensitivity of the transmission to attenuation. Higher transmission frequencies thus often entail a demand for line-of-sight connections, and office walls can sometimes represent the boundaries of a radio LAN.
Even the simultaneous use of different radio systems, such as DECT, GSM, Bluetooth™ and IEEE 802.11, requires a certain amount of "topographical" planning within company grounds, that is to say, only technologies which are compatible with one another and do not adversely affect the other systems may be operated simultaneously within a confined space.

Both kinds of networks will find their proper applications:

- Wired networks will find use in applications in which high data rates and reliable transmission are the most important factors.

- Wireless networks will find use in applications in which mobility and flexibility are of prime importance.

A combination of the two will help continue the trend toward more mobility and flexibility in both office and industrial environments.

Glossary

Ad hoc network	Wireless network between individual devices with limited range.
Access point	Access points allow Wireless LANs to be linked to wired Ethernet networks. An access point can also expand the range of individual Wireless LAN components.
Antenna diversity	Radio receivers equipped with two antennas, allowing the receiver to choose between two signals.
BQTF	Bluetooth™ Qualification Test Facility
CSMA/CD	Carrier Sense Multiple Access with Collision Detection, an access method used by wired Ethernet networks.
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance, an access method used by wireless IEEE 802.11 networks.
DECT	Digital Enhanced Cordless Telecommunications, European standard for in-house voice and data communication over distances of up to 100 m at a frequency of 1.9 GHz.
DSSS	Direct Sequence Spread Spectrum, a Spread Spectrum method also used by IEEE 802.11b-compatible devices in which a bit of the useful signal is transmitted as code word, which is the equivalent of multiplying the transmission rate (spreading the transmission rate).
ETSI	European Telecommunication Standard Institute, a European standardization organization.
FHSS	Frequency Hopping Spread Spectrum, a method used in IEEE 802.11b systems, Bluetooth™ and Home RF systems.
GPRS	General Packet Radio Service, a GSM expansion for packet-oriented data communication up to 170 kbit/s.
GSM	GSM (Global System for Mobile Communications) is the standard for digital cell-based telephone services based on frequencies in the 900 MHz, 1800 MHz and 1900 MHz range. GSM permits data rates of up to 9.6 kbit/sec.
Handshake	An acknowledge method used to establish a connection between stations that want to communicate with one another.
HIPERLAN	High Performance Radio LAN, the European standard for the 5 GHz band with a bandwidth of 150 MHz; Version 1 has

	been passed, Version 2 is under development.
Home RF	Standard for wireless communication between PCs and home-oriented consumer devices.
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11	Standard for radio networks in the 2.4 GHz range with transmission rates of up to 2 Mbit/s.
IEEE 802.11a	Standard for radio networks in the 5 GHz range with transmission rates of up to 54 Mbit/s.
IEEE 802.11b	Standard for radio networks in the 2.4 GHz range with transmission rates of up to 11 Mbit/s.
IrDA	Infrared Data Association, standard for data communication with infrared over short distances. Standard interface in many of today's mobile devices (handhelds).
ISM band	ISM band (Industrial, Scientific and Medical Band), band approved for Wireless LAN applications.
FO	Fiber optics, transmission medium for optical networks.
Multipath propagation	Because of the way radio waves reflect off different objects, radio waves of different intensity reach the receiver at different times. This behaviour of radio waves during transmission through airspace is referred to as multipath propagation.
PAN	Personal Area Network, comparable to an ad hoc network, for networking individual small devices over short distances.
RADIUS	RADIUS, Remote Authentification Dial - In User Service
Roaming	A characteristic of Wireless LAN systems which enables free movement of Wireless LAN nodes even beyond the boundaries of an access point's cell. The node can change with no discernable interruption from one cell to the next when the transmission characteristics to that cell are better.
SNMP	Simple Network Management Protocol, standardized protocol for transporting network management information.
UMTS	Universal Mobile Telecommunications System, standard for mobile voice-, audio-, image-, video- and data communication with a transmission rate of up to 2 Mbit/s.
Web Pad	Portable device in DIN A4 format with touchscreen for connecting to the Internet, normally with wireless

	communication capability.
WEP	Wired Equivalent Privacy, encryption method to IEEE 802.11. Developed to ensure the same data security that of a wired network.
WLANA	The Wireless LAN Association, consortium of Wireless LAN providers trying to get more Wireless LAN technology on the network market.
WECA	Wireless Ethernet Compatibility Alliance, an alliance of various Wireless LAN component manufacturers who ensure product compatibility through product testing.
Wi-Fi seal	Wireless Fidelity, seal of approval of the WECA alliance for IEEE 802.11-compatible and tested components.
Wired LAN	Wired network in which communication between nodes based on variation of voltage values on copper cables resp. light pulses on fiber-optics cables.
Wireless LAN	Wireless network in which communication between nodes is based on transmission of electromagnetic waves through airspace.