

## SIMATIC NET

### **Basics of Industrial Wireless LAN**

System Manual

Preface, Contents

---

**Basics of Wireless LAN** **1**

---

**Wireless Communication  
According to IEEE 802.11** **2**

---

**Data Security in Wireless  
Communication According to  
IEEE 802.11** **3**

---

**Application of Industrial  
Wireless LAN** **4**

---

Glossary, Index

---

## Classification of Safety-Related Notices

This document contains notices which you should observe to ensure your own personal safety, as well as to protect the product and connected equipment. These notices are highlighted in the manual by a warning triangle and are marked as follows according to the level of danger:



---

### **Danger**

indicates that death or severe personal injury **will** result if proper precautions are not taken.

---



---

### **Warning**

indicates that death or severe personal injury **can** result if proper precautions are not taken.

---



---

### **Caution**

with a warning triangle indicates that minor personal injury can result if proper precautions are not taken.

---

---

### **Caution**

without a warning triangle indicates that damage to property can result if proper precautions are not taken.

---

---

### **Notice**

indicates that an undesirable result or status can occur if the relevant notice is ignored.

---

---

### **Note**

highlights important information on the product, using the product, or part of the documentation that is of particular importance and that will be of benefit to the user.

---

#### © Copyright Siemens AG, 1998 to 2004 - All rights reserved

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Siemens AG  
Automation and Drives  
Industrial Communication  
Postfach 4848, D-90327 Nürnberg

#### Disclaimer

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcomed.

C79000-G8976-C168-02  
Technical data subject to change.

## Trademarks

SIMATIC<sup>®</sup>, SIMATIC NET<sup>®</sup>, SINEC<sup>®</sup> and SIMATIC NET Networking for Industry<sup>®</sup> are registered trademarks of Siemens AG.

Third parties using for their own purposes any other names in this document which refer to trademarks might infringe upon the rights of the trademark owners.



# Preface

## Finding Information

To help you to find information quickly, the appendix includes the following sections in addition to the table of contents:

- Glossary
- Index

## Aims

This manual is intended to explain

- the technology of Wireless LANs.
- the use of wireless in automation engineering.

The manual is divided into self-contained chapters each dealing with a specific topic or question. This provides you with a clear overview and allows you to find the answer to a question quickly without having to read the entire document.

## Guide to the Manual

To help you to find specific information quickly, this manual includes the following parts:

- At the beginning of the manual you will find a complete table of contents and lists of the figures and tables in the manual.
- The chapters have headings in the left margin with an overview of the contents of the section.
- Following the appendix, you will find a glossary in which the most important specialist terms used in the manual are defined.
- At the back of the manual, you will find a comprehensive index with which you can find topics quickly.

## References

References to other documentation are indicated by a number enclosed in slashes /.../. Based on these numbers, you can find the title of the documentation in the References section at the end of the manual.

## CD-ROM

You can order the entire SIMATIC NET documentation on CD-ROM.

## Further Support

If you have other questions on SIMATIC NET products, please contact your local Siemens office or representative. You will find the addresses in the catalogs and on the Internet.

## Who to Contact

If you have technical questions about using the described software and your problem is not dealt with in the documentation or in the integrated help system, please contact your Siemens representative or dealer.

You will find the addresses in the following:

- "Readme.rtf" file in the main folder of the SIMATIC NET-CD
- On the Web <http://www.siemens.de/simatic-net>
- Catalog IK PI

## Training for SIMATIC NET

Who to Contact about Training Courses:

Siemens AG  
Trainings-Center für Automatisierungs- und Antriebstechnik  
A&D PT 49 Kursbüro  
Östliche Rheinbrückenstraße 50  
76181 Karlsruhe Germany

Phone: +49 - (0) 721 - 595 - 2917  
Fax: +49 - (0) 721 - 595 - 6087  
Internet: <http://www.sitrain.com>

# Contents

<b>1</b>	<b>Basics of Wireless LAN .....</b>	<b>9</b>
1.1	Introduction .....	10
1.2	Wireless Technology .....	11
1.2.1	Wave Propagation .....	11
1.2.2	Transmission Medium.....	13
1.2.3	Overview of Wireless Technologies .....	14
1.2.4	ISM Band .....	15
1.2.5	Biological Compatibility.....	16
1.2.6	Increasing the Reliability of Wireless LAN Networks.....	17
1.3	Frequencies and Approvals for Specific Countries .....	18
<b>2</b>	<b>Wireless Communication According to IEEE 802.11 .....</b>	<b>21</b>
2.1	Introduction .....	22
2.1.1	Network Architecture .....	24
2.1.2	Channel Access.....	26
2.1.3	Signal Modulation .....	28
2.1.4	Shared Medium .....	33
2.1.5	Station Changes (Number of Stations Changes Dynamically).....	34
2.2	IEEE 802.11b.....	35
2.3	IEEE 802.11g (Further Development of IEEE 802.11b).....	38
2.4	IEEE 802.11a.....	39
2.5	IEEE 802.11h (Further Development 11a) .....	42
2.6	802.11b, 802.11g, 802.11a/h - Overview and Summing Up .....	43
2.7	Further Working Groups of IEEE 802.11.....	45
2.8	Wi-Fi®.....	46
2.9	Effects on WLAN by other Wireless Technologies.....	47
2.9.1	GSM.....	47
2.9.2	Interference between WLAN and Bluetooth .....	47
<b>3</b>	<b>Data Security in Wireless Communication According to IEEE 802.11 .....</b>	<b>49</b>
3.1	Introduction .....	50
3.2	Basics of WLAN Security.....	50
3.3	Basics .....	51
3.3.1	WLAN Adapters in Promiscuous Mode .....	51
3.3.2	WLAN Adapters in Management Mode .....	51
3.3.3	Beacons .....	52
3.3.4	Network Name .....	52
3.4	Traditional Standards for Wireless Security .....	53
3.4.1	Closed Wireless System.....	53
3.4.2	Blocking MAC Addresses (Access Control List).....	54
3.4.3	WEP (Wired Equivalent Privacy) .....	55
3.4.4	WEPplus .....	57

3.5	VPN (Virtual Private Network) .....	58
3.5.1	PPTP (Point-To-Point Tunneling Protocol).....	58
3.5.2	IPSec .....	59
3.5.3	Other VPNs.....	60
3.5.4	Advantages and Disadvantages of VPNs.....	60
3.6	New Standards for Wireless Security .....	62
3.6.1	Authentication Methods .....	62
3.6.2	Generating Certificates .....	67
3.6.3	Encryption Methods .....	68
3.6.4	Standards for Authentication and Encryption .....	70
3.6.5	Advantages and Disadvantages of the New Standard .....	71
<b>4</b>	<b>Application of Industrial Wireless LAN .....</b>	<b>73</b>
4.1	Introduction .....	74
4.2	SIMATIC NET Products for Industrial Wireless LAN.....	77
4.2.1	General Information on Antennas, Lightning Protection, Cables .....	82
<b>5</b>	<b>Glossary .....</b>	<b>83</b>
<b>6</b>	<b>Index .....</b>	<b>93</b>

# Basics of Wireless LAN

# 1

## 1.1 Introduction

### Overview

Wireless networks are becoming more and more popular. Wireless networks allow greater independence and flexibility in the widest variety of areas, such as in offices, warehouses and in industrial production and also mean reduced costs for installation and operation of a system.

All the production and service data connected over a wireless network is available company-wide, and can be collected and modified at the same time. Commissioning engineers can work anywhere on-site and see exactly what is happening throughout the plant.

Different technologies are available for networking using these new methods and these will be described in detail later.

## 1.2 Wireless Technology

### 1.2.1 Wave Propagation

#### Wave Propagation in Space

The propagation of a radio wave in space is three-dimensional. To achieve high-quality data transmission using this medium, careful consideration must be given to the influences that 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 that are very different from those of very high-frequency electromagnetic waves. In simple terms, the behavior of high-frequency electromagnetic waves can be compared to that of light waves.

#### Reflection of 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 obstacles such as walls, furniture, human beings etc., resulting in signal attenuation. 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 incident wave depending on the spatial relationship between the wave and obstacle.

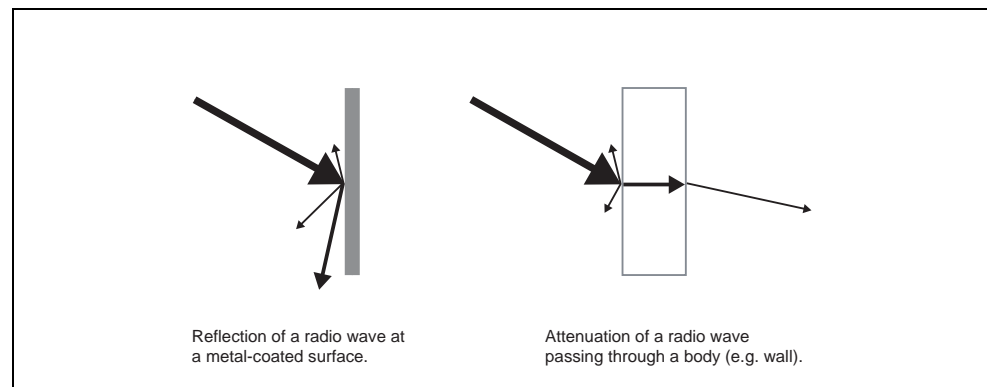


Figure 1-1 Effects of Obstacles on Radio Waves

## Superimposed Waves

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

The resultant superimposing of waves at the receiver can lead to amplification, attenuation, or, in the worst-case situation, total degradation of the signal, depending on the phase angle of the individual wave. From these environment-dependent signals, the receiver must select the best and strongest signal. Moving sources of interference, such as persons or automobiles, can continually modify this transmission path.

However, not only objects cause interference: Neighboring transmitters of other wireless systems can impair the wireless link.

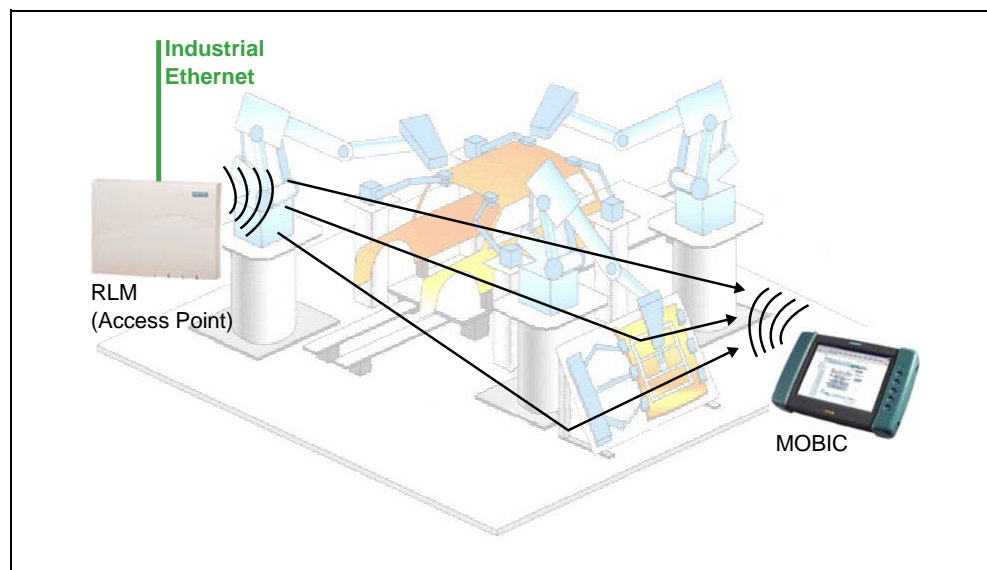


Figure 1-2 Multipath Propagation of Radio Waves

## 1.2.2 Transmission Medium

### Radio Transmission in Free Space

In contrast to LAN cabling with copper or fiber-optic cables, a wireless local area network uses free space as the transmission medium. The transmission of information through space does not use variations in voltage values or light impulses as on copper or fiber-optic cables but takes the form of electromagnetic waves. As a transmission medium, space behaves completely differently compared with a cable with its clearly defined and constant transmission characteristics.

Due to physical conditions, 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).

### Frequency Bands and Wavelengths

Wavelength	Frequency	Explanation								
105-104 m	3 – 30 kHz	VLF								
104 – 103 m	30 – 300 kHz	LF/long wave								
103 – 102 m	0.3 – 3 MHz	MF/medium wave								
102 – 10 m	3 – 30 MHz	HF/short wave								
10 – 1 m	30 – 300 MHz	VHF/ultrashort wave								
1 – 0.1 m	0.3 – 3 GHz	Microwave range								
105-104 m	3 – 30 kHz	VLF								
104 – 103 m	30 – 300 kHz	LF/long wave								
103 – 102 m	0.3 – 3 MHz	MF/medium wave								
102 – 10 m	3 – 30 MHz	HF/short wave								
10 – 1 m	30 – 300 MHz	UKW/ultrashort wave								
1 – 0.1 m	0.3 - 5.825 GHz	Microwave range D networks 890 – 960 MHz E networks 1710 – 1880 MHz DECT 1.8 - 1.9 GHz UMTS 1.97 - 2.2 GHz Bluetooth 2.402 – 2480 GHz								
		<b>Wireless LAN</b>								
		<table border="0"> <tr> <td><b>ISM</b></td> <td><b>2.4 GHz-2.4835,</b></td> </tr> <tr> <td><b>UNII 1</b></td> <td><b>5.15-5.25 GHz,</b></td> </tr> <tr> <td><b>UNII 2</b></td> <td><b>5.25-5.35 GHz,</b></td> </tr> <tr> <td><b>UNII 3</b></td> <td><b>5.47-5.725 GHz,</b></td> </tr> <tr> <td><b>ISM</b></td> <td><b>5.725-5.825 GHz</b></td> </tr> </table>	<b>ISM</b>	<b>2.4 GHz-2.4835,</b>	<b>UNII 1</b>	<b>5.15-5.25 GHz,</b>	<b>UNII 2</b>	<b>5.25-5.35 GHz,</b>	<b>UNII 3</b>	<b>5.47-5.725 GHz,</b>
<b>ISM</b>	<b>2.4 GHz-2.4835,</b>									
<b>UNII 1</b>	<b>5.15-5.25 GHz,</b>									
<b>UNII 2</b>	<b>5.25-5.35 GHz,</b>									
<b>UNII 3</b>	<b>5.47-5.725 GHz,</b>									
<b>ISM</b>	<b>5.725-5.825 GHz</b>									

Wavelength	Frequency	Explanation
10 – 1 cm	3 – 30 GHz	
1 – 0.1 cm	30 – 300 GHz	
1 – 0.1 mm	0.3 – 3 THz	
300 – 0.72µm	1 – 417 THz	Infrared
720 – 320 nm	417 – 789 THz	Visible light
↓	↓	Ultraviolet / X-rays

### 1.2.3 Overview of Wireless Technologies

Technology	Frequency Band	Maximum Data Rate	Maximum Range (m)**	License Fee*
IEEE 802.11	2.4 GHz	2 Mbps	100 m	No
IEEE 802.11b	2.4 GHz	11 Mbps	100 m	No
IEEE 802.11g	2.4 GHz	54 Mbps	100 m	No
IEEE 802.11a	5 GHz	54 Mbps	100 m	No
IEEE 802.11h	5 GHz	54 Mbps	100 m	No
Bluetooth class 2/3	2.4 GHz	1 Mbps	10 m	No
DECT	1,9 GHz	3 Mbps	50 m	Yes
HiperLAN2	5 GHz	54 Mbps	no info	No
Home RF	2.4 GHz	10 Mbps	30 m	No
GSM	900 MHz, 1.8 GHz	14.4 Kbps	5 km	Yes
HSCSD	900 MHz, 1.8 GHz	43.2 Kbps	5 km	Yes
GPRS	900 MHz, 1.8 GHz	171.2 Kbps	5 km	Yes
EDGE	900 MHz, 1.8 GHz	384 Kbps	5 km	Yes
UMTS	1.9 MHz, 2.2 GHz	2 Mbps	3 km	Yes

\* License fees must be paid by the user to the network provider as a basic fee

\*\* The information on transmission ranges depends largely on the products used, the antennas, and the environmental conditions and can only be understood as a rough guideline.

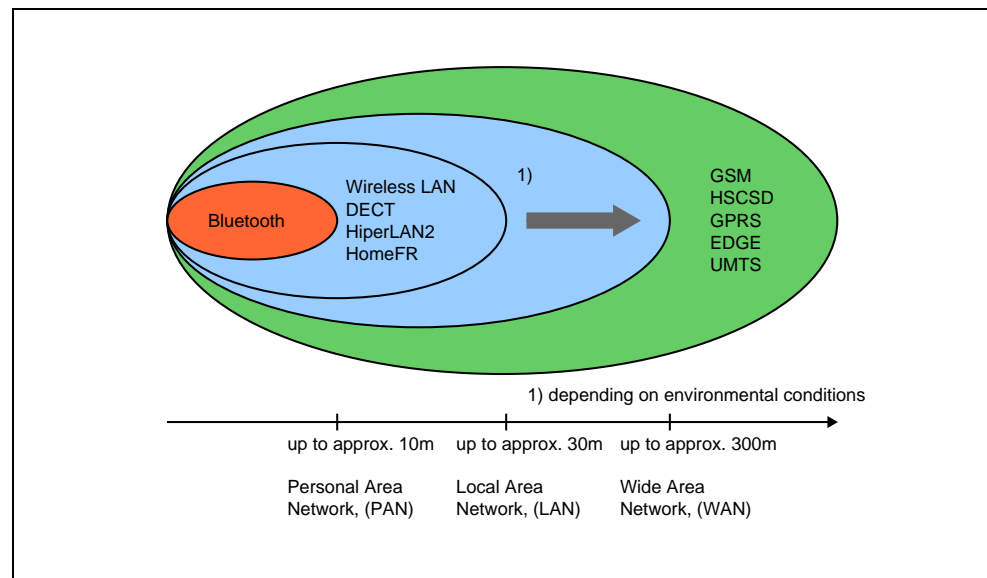


Figure 1-3 Overview of the Technical Specifications of Wireless Technologies

## 1.2.4 ISM Band

### Allocation of Frequency Ranges

Because the frequency spectrum belongs to the public domain, its management and allocation 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 scheme.

### Use of the Frequency Ranges

The ISM band is located in a number of frequency ranges, but only the higher-frequency ranges at 433 MHz, 860 MHz, 2.4 GHz, and 5 GHz are suitable for data transmission. An even higher frequency range at 24 GHz has not currently been developed. 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, 5.15-5.25 GHz, 5.25-5.35 GHz, 5.47-5.725 GHz, and 5.725-5.825 GHz frequency ranges are of importance for data transmission at the data rates required by LANs.

### 1.2.5 Biological Compatibility

With regard to the question of whether electromagnetic fields (for example in association with industrial wireless LANs) can put human health at risk, we refer to a publication of BITKOM (German Association for information Technology, Telecommunication and New Media e. V) dated December 2003:

"The same regulations for the protection of health for all other radio applications also apply to WLAN devices. These regulations are based on the protection concept of ICNIRP<sup>1</sup> or the corresponding recommendation of the European Council.

The independent German radiation protection commission (SSK) was commissioned by the federal German ministry of the environment to investigate the possible dangers - thermal and non-thermal - resulting from electromagnetic fields and came to the following conclusions<sup>2</sup>:

*"The SSK comes to the conclusion that even after evaluation of the latest scientific literature, there is no new scientific evidence regarding proven adverse effects on health that causes any doubt regarding the scientific evaluation on which the protection concept of the ICNIRP or the European Council recommendation is based."*

The SSK also concludes that below the current limit values, there is also no scientific suspicion of health risks.

This evaluation agrees with that of other national and international scientific commissions and with that of the WHO ([www.who.int/emf](http://www.who.int/emf)).

You will find further information on this topic under the following URL:

[www.bitkom.org](http://www.bitkom.org)

---

<sup>1</sup> International Council on Non-Ionizing Radiation Protection

<sup>2</sup> Limit Values and Precautionary Measures to Protect the General Public from Electromagnetic Fields, Issue 29, 2001.

## 1.2.6 Increasing the Reliability of Wireless LAN Networks

### Radio Link Planning

To make access to the "wireless" medium more difficult, apart from the options described for encryption, another approach is also possible. In this approach, the user attempts to restrict the propagation of the radio waves and to achieve a controlled propagation of transmit power. If, during planning of the system, the antennas were chosen according to the principle "more is better than less", the risk of overshooting the target increases and data may be transmitted over unnecessarily long distances.

Although the directional antenna of a snooper no longer finds those narrow-band power peaks of other transmission methods, nevertheless all the coding methods are well-known and standardized. An IEEE 802.11 terminal can therefore prove the existence of all these transmitters. Only the localization of the transmitter and the alignment of the directional antenna is made somewhat more difficult.

### Reflection, Diffraction, and Multipath Propagation

In the 2.4 GHz and 5 GHz ranges, wave propagation is severely affected by reflection, diffraction, and multipath propagation. Added to this, spatial conditions are rarely constant and simply moving a flower tub or changing the arrangement and content of palettes in a storeroom can have strong dynamic effects on the illumination. Dynamic effects do not, however, necessarily mean degradation. If the waves were strongly absorbed by the stored goods the day before, the next day's packing materials or metallic products may significantly improve propagation. This improvement might be so great that the much quoted eavesdropper on the company car park outside the factory might suddenly receive a useful data stream.

### Finding Suitable Installation Sites

Here, careful radio link planning is a must and provides useful support to an approach based on empirical rules. This requires an accurate model of the constructional properties of buildings and their fittings. On top of this, a precise description of machines and equipment is also necessary - often not the easiest of tasks in practice. Using simulations based on this data, potential dangers can be recognized and ideal installation sites found for access points and antennas. During the subsequent verification of the simulated results, the theory is put to the test by measuring the actual transmit power. The result is then available "in black and white" in the form of a protocol and has not simply been estimated based on "gut feeling". A well-performed planning of the radio link also significantly increases the availability of a network. Siemens provides services to undertake the necessary measures.

### 1.3 Frequencies and Approvals for Specific Countries

Country	GHz 2.4-2.4835	GHz 5.15-5.25	GHz 5.25-5.35	GHz 5.47-5.725	GHz 5.725-5.825
Australia		not released	not released	not released	1 W EIRP
Belgium	100 mW EIRP	60 mW EIRP	120 mW EIRP	not released	not released
Chile	100 mW EIRP	not released	not released	not released	50 mW EIRP
China	100 mW EIRP	200 mW EIRP	200 mW EIRP	not released	not released
Denmark	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Germany	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
England	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Finland	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
France	100 mW EIRP	200 mW EIRP	200 mW EIRP	not released	not released
Greece	100 mW EIRP	not released	not released	not released	not released
Hong Kong	100 mW EIRP	200 mW EIRP	not released	not released	1 W TX
Ireland	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Italy	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Canada	1 W TX	200 mW TX	250 mW TX	not released	4 W EIRP
Kuwait	1 W EIRP	not released	not released	not released	not released
Luxembourg	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Netherlands	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Norway	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Austria	100 mW EIRP	60 mW EIRP	not released	not released	not released
Portugal	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Sweden	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Singapore	100 mW EIRP	not released	not released	not released	not released

<b>Country</b>	<b>GHz 2.4-2.4835</b>	<b>GHz 5.15-5.25</b>	<b>GHz 5.25-5.35</b>	<b>GHz 5.47-5.725</b>	<b>GHz 5.725-5.825</b>
Spain	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
South Africa	100 mW EIRP	200 mW EIRP	200 mW EIRP	1 W EIRP	not released
Taiwan	not released	not released	50 mW TX	not released	1 W EIRP
Czech Republic	100 mW EIRP	200 mW EIRP	200 mW EIRP	not released	not released
Turkey	100 mW EIRP	200 mW EIRP	200 mW EIRP	not released	not released
Hungary	1 W EIRP	200 mW EIRP	not released	not released	not released
USA	1 W TX	50 mW TX	250 mW TX	not released	1 W TX

EIRP: Equivalent isotropic radiated power

TX: Transmitter power of the wireless module  
(not including bundling of the radiation by (passive) antenna gain)



# **Wireless Communication According to IEEE 802.11**

# **2**

## 2.1 Introduction

### IEEE 802 Standards in the ISO/OSI Reference Model

The family of IEEE 802 standards describes only the two lowest layers (layer 1 and layer 2) in the ISO/OSI reference model, namely the Physical Layer (PHY) and the Data Link Layer. The data link layer is further divided into the MAC (Medium Access Control) and the LLC (Logical Link Control) layers with the MAC sublayer describing control of access to the medium. IEEE 802.3 MAC governs access in Ethernet and IEEE 802.11 MAC governs access in wireless LANs. The LLC that is uniform for all IEEE 802 members allows higher-level protocol layers such as TCP/IP (layers 4 and 3) to be used in the same way.

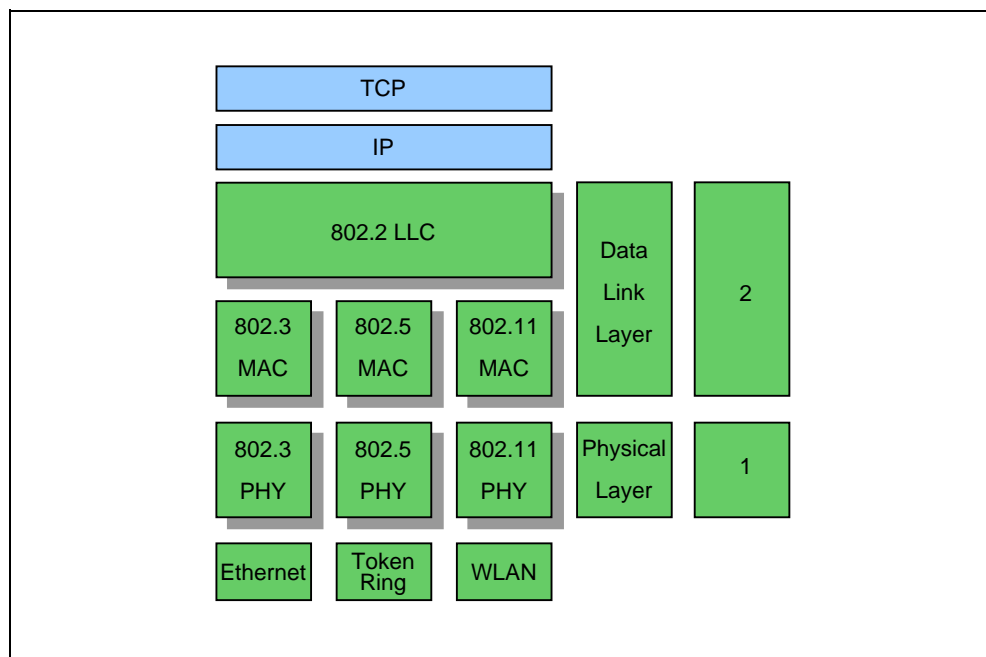


Figure 2-1 Standards from IEEE 802

## History of the Standards for Wireless LANs

For wireless LANs (WLAN), the IEEE completed the first standard in 1997 after a seven year phase by publishing IEEE 802.11 (Note: IEEE 802.11 without an additional letter!). This described a uniform MAC layer and three different PHY layers. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) describe two frequency spreading methods in the 2.4 GHz ISM band that allow data rates of 1 and 2 Mbps. An implementation with infrared technology was also proposed that never found practical application.

In 1999, two further standards IEEE 802.11b and IEEE 802.11a were defined. IEEE 802.11b also operates in the 2.4 GHz ISM band, allows data rates of up to 11 Mbps and goes back to DSSS. This means that IEEE 802.11 systems based on DSSS can be accessed. Systems that use FHSS from IEEE 802.11 cannot, however, be integrated. IEEE 802.11a follows a completely different path with operation in the 5 GHz band and modulation with OFDM for data rates up to 54 Mbps.

The latest member of the IEEE 802.11 family is IEEE 802.11g, a further development of IEEE 802.11b. Here, although the 2.4 GHz band continues to be used, data rates of up to 54 Mbps are possible with OFDM. By using OFDM both in IEEE 802.11g and in IEEE 802.11a, the development of multimode chipsets was made much easier.

The IEEE 802.11h standard represents an expansion of the IEEE 802.11a standard. With the mechanisms of Transmission Power Control (TPC) and Dynamic Frequency Selection (DFS), methods are defined allowing compatible use in the 5 GHz band and therefore allowing higher transmitter power in many countries.

Compatible means: Different products that occupy the 5 GHz band can operate alongside each other without detrimental effects.

## 2.1.1 Network Architecture

Wireless LANs can be divided into two types of network:

- **Ad hoc network**  
Direct connection between stations
- **Infrastructure mode**  
Connection of stations over a common access point

### Ad Hoc Network

The simplest case of a wireless LAN according to IEEE 802.11 is known as an ad hoc network. In a spontaneous network (Independent Basic Service Set, IBSS) of this type, the wireless adapters of the individual devices can set up a network quickly and simply without any major network structure and without any action from the user. These networks are used for the temporary exchange of data over short distances.



Figure 2-2 Ad Hoc Network

## Infrastructure Mode

In infrastructure mode, communication takes place over an access point. In the simplest case, there is a group of IEEE 802.11 stations in the wireless range of this access point. Such a network is known as a Basic Service Set (BSS).

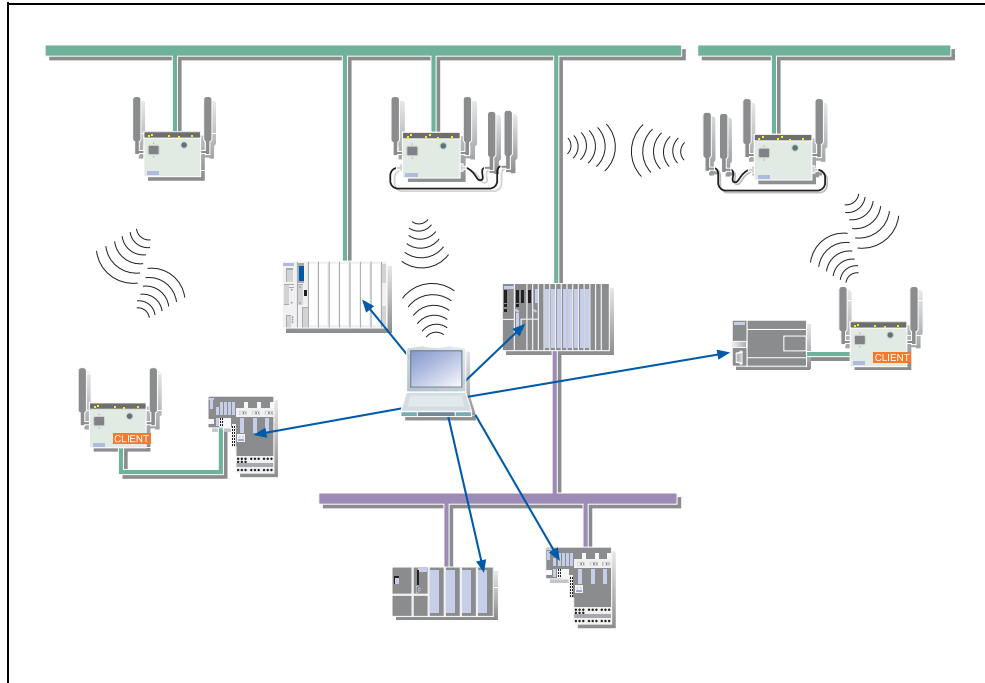


Figure 2-3 Infrastructure Mode

If the cover provided by an access point is not adequate, either because the transmission range is not adequate or because too few stations can be handled, two or more overlapping basic service sets can be operated in a common network (Extended Service Set, ESS). To allow this, the access points must be linked to a background network that can be both wired (for example Ethernet) or implemented with the aid of radio links (Wireless Distribution System, WDS). In this mode, stations outside the direct range of one access point can communicate when they are within the range of another. In ESS mode, the localization of the stations in the BSS and the change of a station from one access point to another (roaming) is managed automatically. In infrastructure mode, stations must log on with the access point and transmit on the channel that it specifies.

Infrastructure mode allows large networks to be set up and, in particular, supports operation within an Ethernet network. Wireless LAN complying with IEEE 802.11 is also known as Wireless Ethernet.

## 2.1.2 Channel Access

### CSMA/CA

A wired Ethernet network uses the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) medium access method. A node wanting to transmit listens in on the cable and if it does not detect any traffic (carrier sense, CS), it transmits its data. The transmitting node can detect a collision (collision detection, CD) with other nodes transmitting at the same time (multiple access, MA) due to the disturbed level and then stops transmitting.

This mechanism is used in just the same way in a wireless network except that collisions are deliberately avoided (collision avoidance, CA) so that the net data throughput is not unnecessarily reduced. Wireless LANs do not, therefore, use the CSMA/CD method in which collisions can occur and are detected but rather the CSMA/CA method (Carrier Sense Multiple Access with Collision Avoidance).

Instead of physically listening in on the channel, a communications protocol is used that reserves the channel for a certain time. Before it transmits, a station checks whether or not the medium is free. During the actual transmission, the station can no longer detect whether or not the data stream is disturbed by collisions (possible remedy: RTS/CTS from the hidden node problem).

## Hidden Node Problem

Collisions occur when stations begin transmission at the same time because they both found the medium free prior to starting transmission. This situation is known as the hidden node problem. This means that two stations are located in the same cell of an access point but outside each other's transmission range.

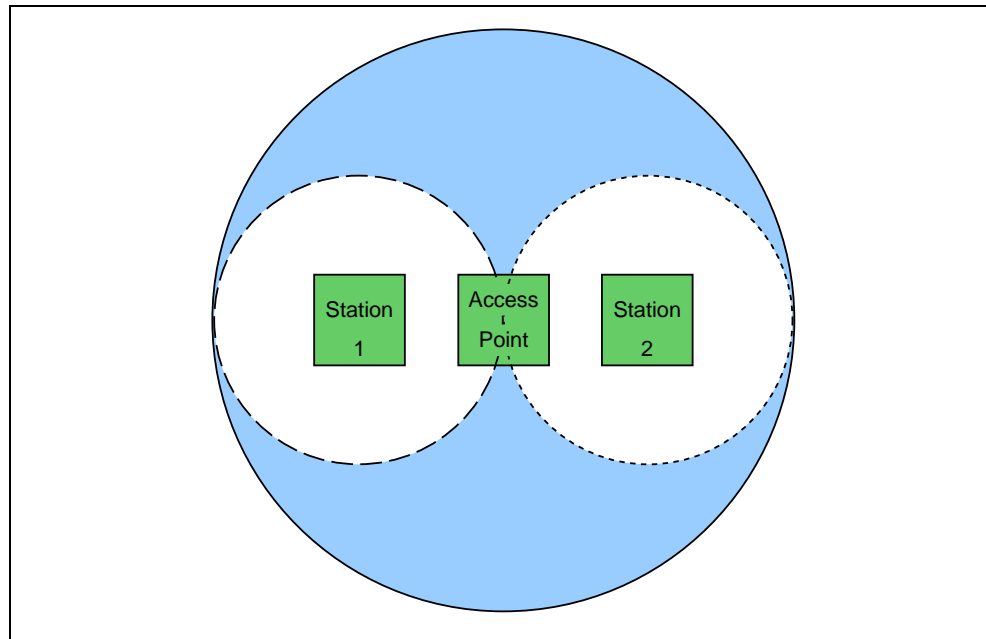


Figure 2-4 Hidden Node Problem

The RTS/CTS (request to send, clear to send) handshake method uses special frames that reserve space for stations wanting to send as specified in IEEE 802.11 and can remedy this problem. It should be noted that RTS/CTS is an optional mode and all devices must be capable of it. The method is used only in constellations in which no acceptable data throughput would otherwise be achieved.

When the station that wants to transmit recognizes that the medium is free, it sends an RTS (Request To Send) to the partner. This message reserves the medium (airspace) for one complete data transmission (RTS frame, CTS frame, data frame, acknowledgment frame and inter-frame spaces). Within a specified time, the partner station returns a CTS (Clear To Send) in which the time required to complete this data transmission is once again announced. Every station now knows how long the ongoing data transmission will take. Loss of the CTS and RTS frames as a result of a collision is very unlikely because the frames are extremely short.

If the partner receives the CTS message correctly, the data transmission can begin. When the data transmission is completed, an ACK frame (acknowledgment) informs the sender that the data was transmitted successfully. If no acknowledgment 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 tries again.

This handshake procedure is also relayed by the access point making it possible to reach stations outside the transmission range of the transmitting station (hidden node). These stations also recognize that the transmission medium has been reserved.

## Fragmentation

If a station has been given access to the channel, it can transfer up to 2312 bytes of user data in one frame. At 11 Mbps, this can take up to 2 ms. To increase the probability of error-free transmission of a frame, IEEE 802.11 provides the mechanism of fragmentation. The user can specify a maximum value of user data that can be transferred within one frame. This does, of course, increase the overheads caused by the protocol and the net data throughput is reduced. Disturbances, however, have nothing like the original severe effects.

Example: SIMATIC NET communication with a maximum of 512 bytes per packet.

## 2.1.3 Signal Modulation

### Frequency Hopping Spread Spectrum

The Frequency Hopping Spread Spectrum method (FHSS) transfers the signal over 1 MHz wide channels with constantly changing frequencies (frequency hopping). The frequency changes following a rhythm that is known to the receiver; in other words, the transmitter and receiver must be synchronized prior to data transmission. For these frequency changes, the transmitter has 79 non-overlapping channels available in the 2.4 GHz ISM band that is divided into three groups each with 26 patterns (USA, Europe). Gaussian Phase Shift Keying (GFSK) is used for modulation.

Data transmission using the FHSS method is not susceptible to disturbances since frequencies affected by narrowband interference can be avoided. The data can be transmitted again using other frequencies. For the FHSS method, however, there are only bandwidths of 1 or 2 Mbps available for data transmission. The FHSS method is therefore only used with IEEE 802.11 and is no longer as important compared with the two modern methods IEEE 802.11b/g and IEEE 802.11a.

## Complementary Code Keying (CCK)

Complementary Code Keying CCK is used as the basic modulation of modern Wi-Fi systems complying with IEEE 802.11b and modulates only one carrier (see Figure 2-5). With complementary code keying, both the preamble/header and the user information are transmitted with CCK modulation. The signal is not narrowband (for example, VHF radio stations) but broadband, spread over an entire spectrum.

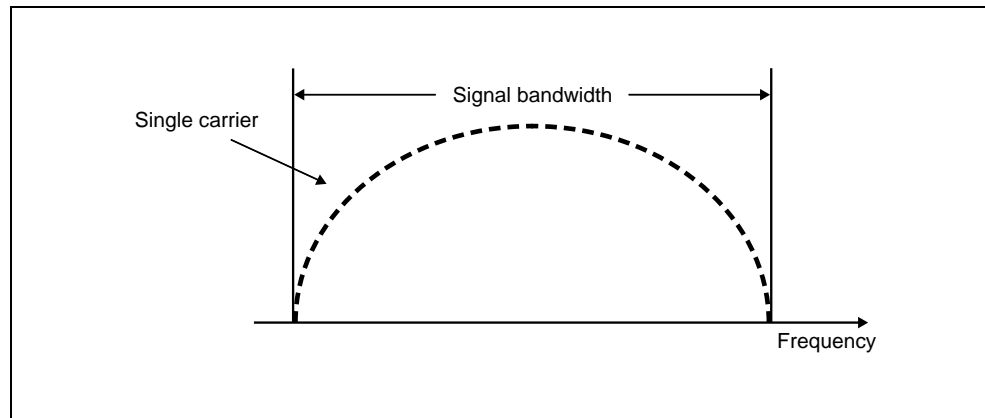


Figure 2-5 Modulation of the Carrier Frequency in CCK

## Direct Sequence Spread Spectrum (DSSS)

The Direct Sequence Spread Spectrum method (DSSS) defines that the information is transmitted over a 22 MHz broad channel. At the transmitter, each data bit to be transmitted is spread over a pseudo-random sequence of eleven (IEEE 802.11) or eight bits (IEEE 802.11b) (signal spreading). In simple terms, one can say that the reliable transmission results not from a particularly strong signal but rather from intensive use of the "frequency" resource. (This becomes obvious when one considers that FHSS transmits information on a 1 MHz wide channel and DSSS uses all of 22 MHz.)

Due to the spreading, it is possible that the signal level is reduced to such an extent that the signal is weaker than the background noise encountered everywhere.

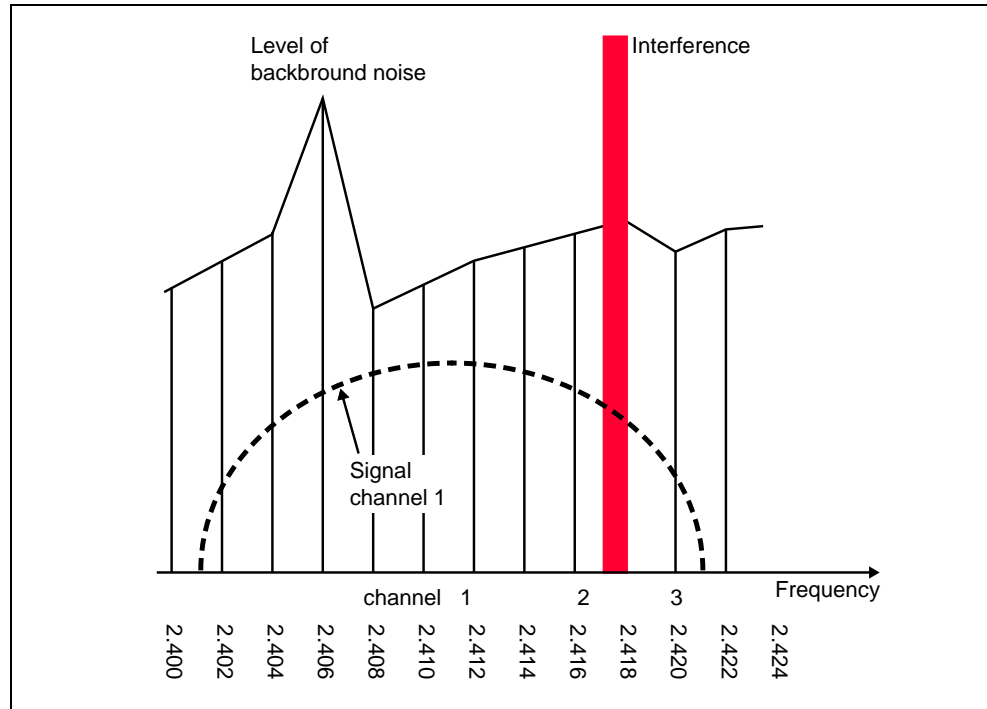


Figure 2-6 Background Noise, Interference, and Signal Level with DSSS

Only when the spread spectrum has been reversed in the receiver does a signal emerge from the noise. Narrow-band interference signals can be filtered out of the useful signal by reversing the spread, and do not deteriorate data transmission.

By spreading the useful signal over a bandwidth of more than 22 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, because frequency-specific propagation effects are reduced. The DSSS method is thus virtually immune to narrow-band interference sources, offers better protection against multipath propagation, and allows higher data throughput. DSSS is used in IEEE 802.11b.

## Orthogonal Frequency Division Multiplexing (OFDM)

With Orthogonal Frequency Division Multiplexing technology (OFDM), several closely adjacent orthogonal subcarriers (frequencies) are combined together to form one channel and transmitted by the transmitter as a composite signal (see Figure 2-7). Orthogonal means that the various subcarriers are selected so that they are at a minimum at the point at which another subcarrier has its information. This is therefore referred to as parallel data transmission with frequency multiplexing. In Wireless LAN IEEE 802.11a, 52 subcarriers are defined in each channel with a spacing of 0.3125 MHz between them. The information to be transmitted is distributed on these subcarriers with redundant bits for strong Forward Error Correction (FEC) and then transmitted. The technology is therefore highly resistant to multipath propagation and narrowband interference and is particularly interesting for industrial applications. OFDM is used in IEEE 802.11a and is also used in IEEE 802.11g to achieve high data rates of up to 54 Mbps.

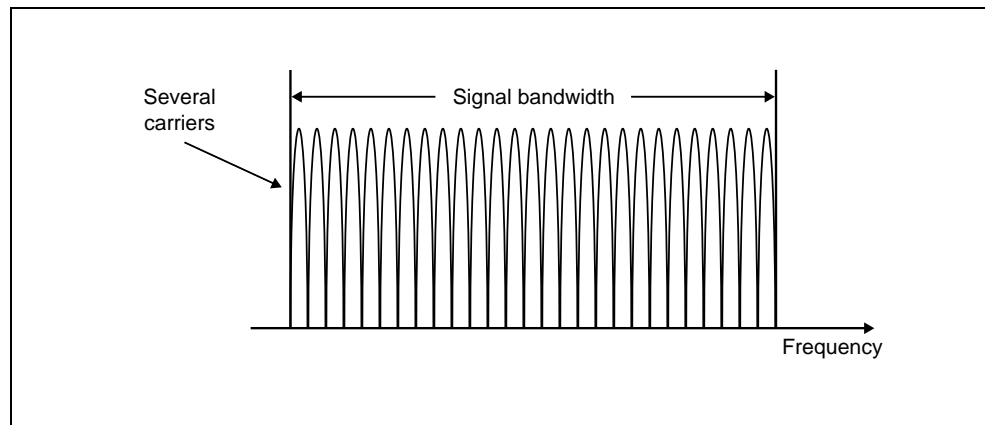


Figure 2-7 Data Transmission in OFDM Systems over Multiple Subcarriers

One advantage of OFDM is the shorter preamble (header): This is only 16 ms compared with 72 ms for CCK (IEEE 802.11b). A shorter preamble is an advantage because it means less overheads for the network. This advantage is particularly noticeable in industrial applications where the packets of useful information are small and the proportion of the packet required for the preamble takes on a greater significance. With a smaller preamble, the overall system has a better net data throughput and therefore better performance.

## **Orthogonal Frequency Division Multiplexing (OFDM) and Complementary Code Keying (CCK)**

Wireless networks complying with IEEE 802.11g use OFDM to modulate their data. This is the only way to achieve data rates of up to 54 Mbps. Since these wireless networks operate in the 2.4 GHz band, compatibility with 802.11b (up to 11 Mbps) must be assured. This was achieved because the option of OFDM/CCK was defined in the 802.11g standard. The preamble (header) is transmitted with CCK, so that 802.11b and 802.11g devices recognize the type of payload data to follow. If OFDM signals are indicated, these are only evaluated by the 802.11g devices. Otherwise, the 802.11b devices activate demodulation.

This mechanism avoids collisions and allows peaceful coexistence between 802.11b (CCK) devices and IEEE 802.11g devices with CCK/OFDM. The preamble for CCK/OFDM is longer than for pure OFDM so that the basic overheads increase. This can generally be ignored because CCK/OFDM allows higher data rates more than making up for the time lost and also allows backward compatibility with existing CCK systems.

Apart from CCK/OFDM, there is a further method of achieving compatibility between 802.11g and 802.11b. The method required for this is known as RTS/CTS. If this method is selected, it should be noted that the preamble for OFDM is shorter than for OFDM/CCK. Nevertheless, a slight loss of performance will be experienced because the handshaking involved in the RTS/CTS mechanism also causes basic overheads in the system. Which method is more suitable must be decided from case to case.

## **Packet Binary Convolutional Coding (PBCC)**

The modulation technique PBCC (Packet Binary Convolutional Coding) is based on one carrier but differs significantly from CCK. It uses a more complex signal constellation (8-PSK for PBCC instead of BPSK/QPSK for CCK) and a convolutional code instead of the block code of CCK. As a result, the decoding mechanism differs greatly from those of the methods mentioned up to now. As with CCK/OFDM, PBCC is also a hybrid method: CCK for preamble/header and PBCC for the useful data. This allows higher data rates and backward compatibility with existing IEEE 802.11b systems in the same way as described for CCK/OFDM.

The maximum data rate for PBCC is stipulated in the draft standard IEEE 802.11g at 33 Mbps. This value is below the peak values for the required OFDM (54 Mbps) and the optional CCK/OFDM. PBCC is of very little significance for IEEE 802.11g.

---

**Note**

PBCC is included as an optional element in the original IEEE 802.11b standard (however, no devices have yet come onto the market that use this method).

---

## 2.1.4 Shared Medium

### Data Security in Wireless Networks

Intrusion into wireless LANs is possible because radio waves are not restricted to a fixed medium such as a wire and because they are subject to effects such as reflection and diffraction. Added to this, wireless LAN means a "shared medium" which means that all the stations require access to the same network infrastructure. This is a different situation in wired "switched Ethernet". In such a system, each node has an exclusive cable as far as the switch and does not need to share this cable with any other node. This difference highlights a central problem: It is never possible to be sure who is currently in the wireless network and accessing the medium because all stations are allowed to do this unless additional measures are taken.

To counter this situation, IEEE and Wi-Fi have described methods in 802.11i and under the name WPA (Wi-Fi protected access). WPA describes mechanisms that ensure automatic and regular exchange of keys. WPA also describes access control using technologies contained in IEEE 802.1x.

There is an additional option of using AES (Advanced Encryption Standard) instead of TKIP. From today's perspective, AES represents a secure encryption technique.

### **2.1.5 Station Changes (Number of Stations Changes Dynamically)**

#### **Antenna Diversity**

To combat the multipath propagation experienced in assembly plants (see Figure 1-2) and the resulting attenuation or obliteration of radio waves, wireless modules are equipped with two antennas (antenna diversity). The receiver can then select the stronger of two received signals.

#### **Automatic Reduction of the Data Rate**

To ensure reliable data transmission, when the quality of the transmission link changes permanently (number of nodes, changing distance from the node to the access point), the modules must be capable of reducing the maximum data rate to a lower data rate to ensure reliable reception of the data.

## 2.2 IEEE 802.11b

### Deadlines

IEEE 802.11b has been adopted by the IEEE and has been approved by the regulating authorities of the countries (in some cases with additional regulations).

### Frequencies, Channels

In the 2.4 GHz band, 13 channels (frequency ranges with a width of 5 MHz) are specified that must be set by the user to operate an access point (USA: 11 channels). This frequency is then valid within the entire area covered by the access point. When using products complying with IEEE 802.11b, a maximum of 3 channels can be used without overlap at one location since the transmission of data requires a signal with a width of 22 MHz.

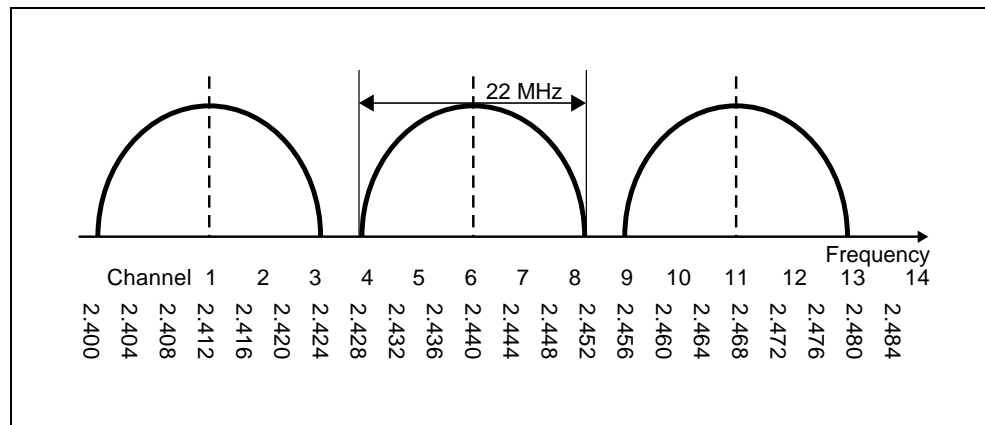


Figure 2-8 Non-Overlapping Channels for DSSS in the 2.4 GHz Band

As can be seen in Figure 2-8, channels 1, 6, and 11 can be operated without overlaps and also provide spacing of 3 MHz between them. This is also the ideal combination in countries where only channels 1 through 11 are approved (for example the USA). In countries in which channels 1 through 13 are approved, other combinations with larger spacing are possible (for example, Europe with channel 1, 7, and 13). At one location, therefore, 3 different channels can be operated without them interfering with each other.

### Available Non-Overlapping Channels

The number of non-overlapping channels is particularly important at the boundaries of a cell when the node automatically switches to the other channel of the neighboring cell. To avoid interference at this boundary, the channels of the cells must not overlap.

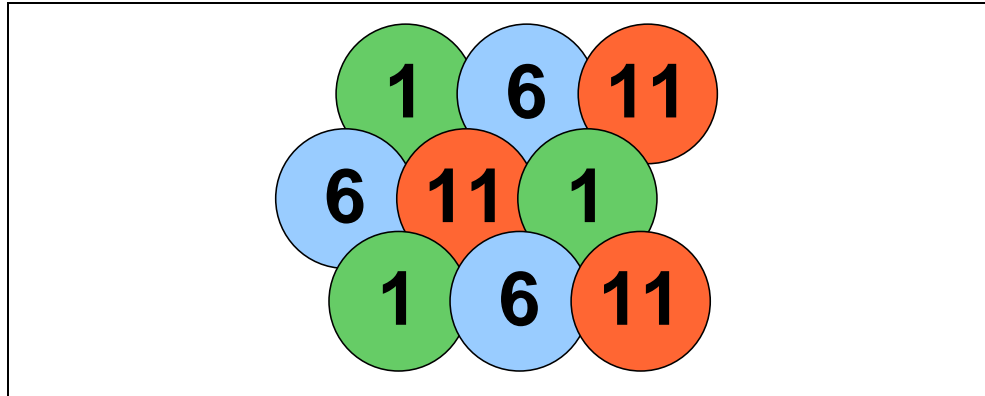


Figure 2-9 Non-Overlapping Channels in a Flat Wireless Network

The significance of this fact becomes clear in Figure 2-9 where at the top channels 1, 6, and 11 provide both full wireless coverage while at the same time causing no interference between the channels used. Flat wireless networks can be implemented easily with 3 channels. To set up spatial radio links (for example throughout floors of a building) the availability of a fourth channel becomes increasingly important to avoid two identical channels being adjacent to each other. Instead of using channels 1, 6, and 11, the option of using channels 1, 4, 8, and 11 (in Europe: 1-5-9-13 if supported by the product) should be considered when operating an IEEE 802.11b network.

Although the spacing between channels is reduced when using 1-4-8-11, this is still better than using a channel from the smaller pool of 1-6-11 when there is a risk that it will border on the same channel at the cell boundaries. It is also important to remember that other effects such as the shadowing caused by floors will be greater in spatial cells. In such situations, thorough deployment planning is absolutely necessary to achieve an optimum wireless network.

### Transmit Power

In the 2.4 GHz ISM band, many countries allow 100 mW (20 dBm) transmit power (EIRP) (see Section 1.3 Frequencies and Approvals for Specific Countries).

## Data Rate

In IEEE 802.11b, data is transmitted at 11 Mbps. It should, however, be remembered that after taking into account packet headers and protocol overheads, the net data rate can hardly exceed 5 Mbps.

If the bit error rate increases in a wireless network, the access point initially falls back to 5.5 Mbps, then to 2 Mbps, and finally to 1 Mbps. This strategy attempts to maintain the connection as long as possible and accepts a compromise in the data rate.

## Transmission Ranges

It is extremely difficult to make generalizations about the transmission range of a wireless LAN. Evaluating the following factors will make it easier to estimate the coverage:

- **Transmit power**  
What is the transmit power of the products used?  
There are vendors with 20 dBm products and others with products providing only 15 dBm where low energy consumption is important.
- **Antenna gain**  
How large is the antenna gain of the antenna used including antenna cable and lightning protection?
- **Environment**  
In what environment is the radio network set up?  
Reflections from metallic objects with multipath propagation, signal attenuation due to walls or doors, interference due to faulty products as well as interference from correctly operated products using the same frequency band have a strong influence.

If a commercially available PC card with 17 dBm (for example the CP 7515) with integrated antennas is used, distances of 30 m indoors and 100 m outdoors can be achieved. With the influences mentioned above, these values can deteriorate by a factor of 2.

## 2.3 IEEE 802.11g (Further Development of IEEE 802.11b)

### Deadlines

IEEE 802.11g was adopted finally by the IEEE in 2003 and approved by the regulatory authorities of the countries (in some cases with additional regulations) (IEEE 802.11g is the compatible further development of IEEE 802.11b in the same frequency band).

### Frequencies, Channels

Since IEEE 802.11g is fully compatible with IEEE 802.11b and represents a further development, exactly the same frequencies and channels are used.

### Transmit Power

The transmit power as with IEEE 802.11b is 100 mW (20 dBm) EIRP.

### Data Rate

In IEEE 802.11g, due to the modulation with OFDM, data rates of up to 54 Mbps are specified. Just as with IEEE 802.11b, this is reduced in deteriorating conditions (fall back to 54, 36, 33, 24, 22, 12, 11, 9, 6, 5, 2, 1 Mbps). The data rates of 11 Mbps and slower are fully compatible with IEEE 802.11b.

### Transmission Ranges

The transmission ranges at the corresponding data rates are very similar to those of IEEE 802.11b but reduce significantly with a need for bandwidth at 54 Mbps.

## 2.4 IEEE 802.11a

### Deadlines

The IEEE adopted the IEEE 802.11a standard for the 5 GHz frequency band as early as 1999 (just as IEEE 802.11b), however the approvals by the regulatory authorities of the countries took varying amounts of time and involved various addenda relating to permitted frequency channels and transmit power. In the USA, IEEE 802.11a products have been available since the end of 2001 that meet the guidelines of the FCC. In the meantime, there are provisions in almost all countries for the use of the 5 GHz band by WLAN.

IEEE 802.11a is approved in many countries in Europe. However, if TPC and DFS are not used, only a low transmit power and limited number of channels can be used.

### Frequencies, Channels

IEEE 802.11a provides a higher number of available wireless channels that can be set for an access point by the user. This frequency is then valid within the entire area covered by the access point. For wireless networks with a high information density (for example enterprise networks or hot spots), this fact is of considerable interest. In the 5 GHz band, there are also fewer competing applications (for example flight navigation or radar equipment) than in the 2.4 GHz band that belongs entirely and worldwide to the ISM (Industrial, Scientific, Medical) bands and that is intensively used by these groups.

Unfortunately IEEE 802.11b and IEEE 802.11a are not compatible since they operate in different frequency ranges.

In the 5 GHz frequency band, it should be remembered that there are very different national regulations that are currently subject to considerable change due to the fast spread of wireless LANs.

Frequency Range/GHz	Bandwidth	Non-Overlapping Channels
5.15 ... 5.25	100 MHz	4
5.25 ... 5.35	100 MHz	4
5.47 ... 5.725	255 MHz	10
5.725 ... 5.825	100 MHz	4

Figure 2-10 Frequency Ranges in the 5 GHz ISM Band

Operation of WLANs in the range from 5.47 GHz through 5.725 GHz is becoming possible in more and more countries. The precise national regulations must be checked. In most cases, the use of dynamic frequency selection (DFS) and automatic transmission power control (TPC) is mandatory in this frequency band.

With the various frequency bands in the 5 GHz range, users should check that the selected products actually support these bands. Many products on the market support the range 5.250 through 5.350 GHz since this can be used in almost all the countries of the world. Currently, most vendors of WLAN chip sets support WLAN the range 5.15 – 5.35 GHz.

In most European countries, the range between 5.150 GHz and 5.350 GHz can be used if certain national rules are adhered to.

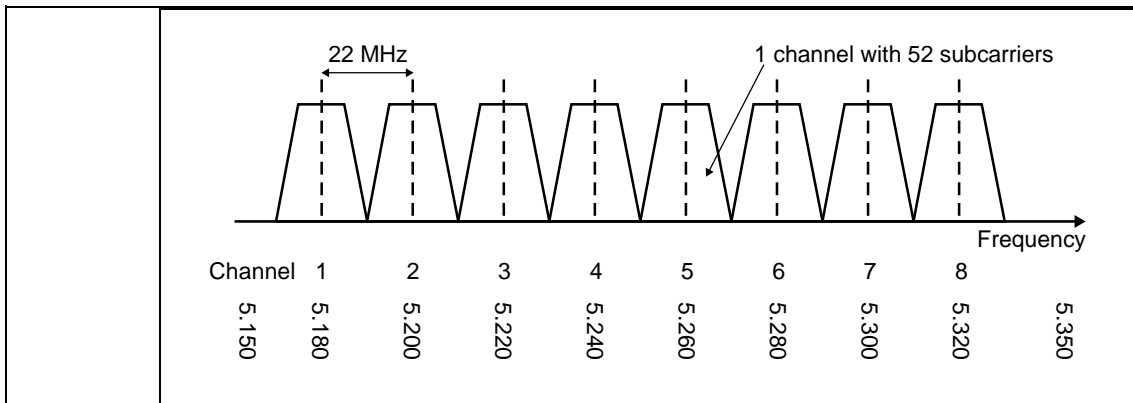


Figure 2-11 Channels in IEEE 802.11a in the 5 GHz Band

### Transmit Power

The maximum permitted transmit power depends on the frequency band and the country in which the WLAN is operated. In particular in the 5 GHz band, it is possible in many countries to use higher transmit power if the device has the technical ability for DFS and TPC. With these expansions, transmit power is possible, for example in Germany, up to a maximum of 200 mW in the band from 5.15 GHz through 5.35 GHz. Without these features, only channels with a maximum of 30 mW are permitted in the 5.15 GHz through 5.25 GHz band.

### Data Rate

Just as IEEE 802.11g, IEEE 802.11a supports data rates up to 54 Mbps and uses the same modulation technology (OFDM) as IEEE 802.11g. The data rates are gradually reduced just as in 802.11g if the transmission conditions deteriorate (fall back to 54, 48, 36, 24, 18, 12, 9, 6 Mbps).

## Transmission Ranges

The transmission range of a wireless system reduces with increasing frequency. With this physical fact, it would be fair to expect that a system complying with IEEE 802.11a has a significantly reduced transmission range at the same power. Measurements made by the IEEE 802.11a vendor Atheros, however, show that an IEEE 802.11a system achieves similar transmission ranges at the same data rates and is even better in some circumstances (see the range 150 through 250 ft in Figure 2-12). This result is noteworthy and reflects the performance of OFDM. It must be pointed out, however, that the measurements were made under laboratory conditions and that the interference to be expected in a real application was ignored. Based on this measurement, it is also impossible to make any statements regarding the penetration of walls and doors. This is one area where significant losses must be expected with IEEE 802.11a. Unfortunately, there has not been enough work done to allow a reliable statement.

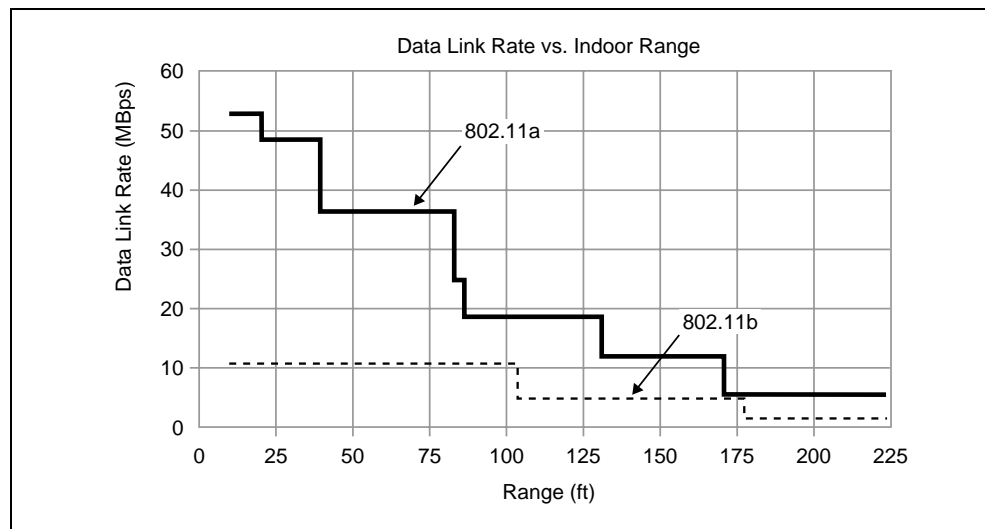


Figure 2-12 Transmission Range Dependent on the Achieved Data Rate for IEEE 802.11b and IEEE 802.11a (Source: Atheros)

Figure 2-12 shows the great advantages of IEEE 802.11a over short distances. In these ranges, high data rates up to 54 Mbps can be achieved. As the distance increases, the achievable data rates are reduced significantly and dropped to those of IEEE 802.11b at a distance of approximately 150 ft (45.72 m).

## 2.5 IEEE 802.11h (Further Development 11a)

To comply with IEEE 802.11h, 11a devices must support dynamic frequency selection (DFS) and transmit power control (TPC). The reason for this is to prevent IEEE 802.11h wireless LANs from interfering with radar transmission for air traffic or amateur radio. Due to these extra regulations, the transmission range of IEEE 802.11h devices still fall short of the distances achieved by 11b/g components. At about 30 to 40 m, however, it is still significantly better than that of 11a devices without DFS and TPC.

### Deadlines

The IEEE 802.11h standard is intended to help wireless LAN components functioning according to IEEE 802.11a to achieve full power in Europe.

### Frequencies, Channels

IEEE 802.11h is based on IEEE 802.11a, but integrates the technical regulations stipulated, for example by the Reg TP for the 5-GHz band in Germany.

Within buildings, IEEE 802.11h devices can transmit within the large frequency range of 5.15 through 5.35 GHz and provide the user with eight non-overlapping wireless channels. The same applies for the frequency ranges 5.47 GHz through 5.725 GHz.

### Transmit Power

IEEE 802.11h allows components a higher transmit power of up to 200 mW and therefore a greater transmission range.

### Transmission Ranges

The transmission range increases due to the higher power. As already mentioned, however, it is always dependent on the environmental conditions.

## 2.6 802.11b, 802.11g, 802.11a/h - Overview and Summing Up

### Overview of the Current IEEE 802.11 Standards

	802.11b	802.11g	802.11a/h	802.11a/h	802.11a/h	802.11a/h
Frequency band	2.4 GHz	2.4 GHz	5.15-5.25 GHz	5.25-5.35 GHz	5.4-5.7 GHz	5.7-5.8 GHz
Data rate	11 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps
Non-overlapping channels	3	3	4	4	10/11	4/5
Transmit power	100 mW EIRP (ETSI), 1 W (FCC)	100 mW EIRP (ETSI), 1 W (FCC)	200 mW EIRP (ETSI) 50 mW (FCC)	200 mW EIRP (ETSI) 250 mW (FCC)	1 W EIRP (ETSI)	1 W (FCC)
Data rate Mbps <sup>2</sup> 1 m 10 m 100 m	11 Mbps 11 Mbps 1 Mbps	54 Mbps <sub>1</sub> <sub>1</sub>	54 Mbps <sub>1</sub> <sub>1</sub>	54 Mbps <sub>1</sub> <sub>1</sub>	54 Mbps <sub>1</sub> <sub>1</sub>	54 Mbps 36 Mbps 6 Mbps
Modulation	DSSS	OFDM	OFDM	OFDM	OFDM	OFDM
Penetration of walls	Medium	Medium	Poor	Poor	Poor	Poor
Reflections, for example from metallic objects	Robust	<sup>1</sup>	Robust	Robust	Robust	Robust
Risk of interference by other radio applications	Medium	Medium	Low	Low	Very low	Very low

<sup>1</sup>: No statement is yet possible

<sup>2</sup>: Outdoors, line of sight between transmitter and receiver, no interference

---

#### Note

FCC regulates approval in America, ETSI in Europe. Special regulations must be adhered to in specific countries.

---

## Summing Up

The significance of IEEE 802.11b will diminish because it will become part of the fully compatible IEEE 802.11g standard. The question of which wireless technology to select will be reduced to IEEE 802.11g and IEEE 802.11a.

IEEE 802.11a has clear advantages when operating at 5 GHz when a frequency band is required in which there are hardly any other wireless systems operating. Due to the great popularity of the 2.4 GHz band, this is unfortunately not the case with IEEE 802.11b and IEEE 802.11g. On the other hand, continued use of the 2.4 GHz band in IEEE 802.11g allows good migration for IEEE 802.11b users. These must otherwise change 11a at 5 GHz in the step towards higher bandwidths.

For applications requiring high information density, IEEE 802.11a is suitable. Here, data rates of 54 Mbps can be achieved and 4 (at times up to 8) channels can be operated at one location. In IEEE 802.11g, 54 Mbps are also possible, however, with "only" 3 channels. By using the 2.4 GHz band, IEEE 802.11g will have advantages over IEEE 802.11a in terms of transmission range since the wave propagation deteriorates as the frequency increases.

The vendors of chipsets are countering this uncertainty by offering multimode chipsets that support both IEEE 802.11g and IEEE 802.11a depending on how they are configured. This is made easier by the use of OFDM in both standards.

## 2.7 Further Working Groups of IEEE 802.11

### Overview of the Working Groups in IEEE 802.11

Due to the increasing acceptance of wireless LAN systems among users, there is a growing demand for more extensive standardization.

The IEEE has reacted to this situation by setting up more working groups.

Standard	Remark	Status
802.11d	Expansion of the PHY definition (for example channel selection, attributes of the management information base MIB) for automatic adaptation of mobile devices to the relevant national settings ("world mode").	In progress
802.11e	Support of quality of service (QoS) and class of service when using HCT and EADF, particularly for roaming and peer-to-peer operation.	In progress
802.11f	Inter Access Point Protocol (IAPP) for roaming, load balancing and communication between the access points.	In progress
802.11h	Expansion of 802.11a by adding transmission power control (TPC) and dynamic frequency selection (DFS) with the agreement of the European committees.	In progress
802.11i	Expansion by adding improved security and authentication mechanisms.	In progress

## 2.8 Wi-Fi®

### Wi-Fi Alliance

The Wi-Fi Alliance is a non-profit-making organization of industrial companies with the aim of promoting the acceptance of wireless technology worldwide according to IEEE 802.11.

- All the leading manufacturers of wireless communications systems and service providers for Wi-Fi technology are members of the Wi-Fi Alliance.
- With strict test programs, the Wi-Fi Alliance makes sure that all components bearing the Wi-Fi Logo can interoperate without problems.
- The Wi-Fi Alliance was founded in 1999, has over 200 members today and has certified well over 1,000 products in the meantime.

### Wi-Fi Certification

Wi-Fi (Wireless Fidelity) is a common name for all products developed on the basis of the IEEE 802.11 standard.

Wi-Fi certified means that a product was tested on the basis of the IEEE 802.11 standard. This covers the test according to IEEE 802.11a or IEEE 802.11b/g or both for products including both technologies (dual band). Such tests also include the interaction with other Wi-Fi certified products.

Wi-Fi products include, for example, PCMCIA cards for notebooks, PCI cards for desktop PCs, USB modules for use in notebooks and desktop PCs, access points, and gateways.

Wi-Fi certified products support a maximum data rate of 11 Mbps (IEEE 802.11b) or 54 Mbps (IEEE 802.11a/g).



## 2.9 Effects on WLAN by other Wireless Technologies

In the discussion of the mutual interference of the technologies mentioned above, the main emphasis will be on the three most successful market technologies (based on numbers sold): GSM, WLAN, and Bluetooth.

### 2.9.1 GSM

GSM is not critical since no interference can be expected thanks to the reserved frequency band (GSM900: 880..915 MHz and 925..960 MHz, GSM1800: 1710..1785 MHz and 1805..1880 MHz).

### 2.9.2 Interference between WLAN and Bluetooth

#### WLAN and Bluetooth

The situation with WLAN and Bluetooth is different since both use the license-free ISM band at 2.4 GHz. However, it must be pointed out that interference is only relevant when the different wireless modules are operated very close together.

The SIG (Special Interest Group) is currently working on a new version of the standard in which Bluetooth avoids the transmission frequencies of a WLAN transmitter when such transmitter is detected. This mechanism will significantly increase the compatibility of the technologies and will mean less problems. In general, we can say that both the frequency hopping of Bluetooth and the DSSS modulation scheme of WLAN are resistant to interference. In frequency hopping, the frequency is changed very quickly and in DSSS there is considerable redundancy due to the spread spectrum. During frequency hopping in Bluetooth, it is perfectly possible that one of the frequencies used is in the range of the WLAN band. Interference occurs, however, only when the power of the Bluetooth transmitter is great enough and the redundancy mechanisms of WLAN can no longer correct the error.

The decisive factor here is the physical distance between the Bluetooth transmitter and the WLAN receiver. It should be noted that the normal Bluetooth class 2/3 transmitter with a power of 1mW only causes real performance problems in the immediate vicinity of the WLAN station. The system operator will think twice about a double investment and will only find a dual system advantageous in very rare cases. This reduces the question of interference to unwanted radiation, for example caused by mobile telephones with an active Bluetooth interface. Here, system operators themselves must take measures to avoid problems occurring. Just as today in factories, there must be clear rules for the layout of the manufacturing area and the routing of cables, it will also be necessary in future to control the active wireless systems used so that certain combinations of systems are not installed alongside each other.

A positive approach can be expected in the next Bluetooth specification. Here, techniques will be implemented to avoid frequencies already in use. It is also worth remembering that the 5 GHz band is now also available for WLANs where such overlaps do not occur.

# **Data Security in Wireless Communication According to IEEE 802.11**

# **3**

## 3.1 Introduction

### How can I made my wireless LAN secure?

The lack of security in wireless LANs has recently been a popular topic in the media. It appears that hackers can break into networks with no problem that all. Well over half of such hacks, however, are simply the result of carelessness on the part of administrators when installing network components.

To stop this happening to you, you should read this chapter to find out about methods that will block potential attacks on your data.

## 3.2 Basics of WLAN Security

Following successful commissioning of your wireless LAN, the next stage is to protect your WLAN against attack and accidental misuse.

Please follow the basic rules outlined below:

- Change all default passwords.  
This prevents unauthorized persons logging on in your network and modifying the settings of your network components.  
You should use at least the integrated WEP encryption mechanism. This, however, only provides security against unauthorized intrusion into your WLAN when the amount of data transmitted with the same key remains below 2 GB.
- Change the key assigned in WEP as often as possible.
- Enter the Ethernet addresses (MAC) of the wireless cards known to you on your access points, and block them for access from other addresses.  
You should, however, remember that MAC addresses are easy to forge.
- If you transfer sensitive data in your network, please make sure you read the sections "VPN (Virtual Private Network)" and "New Standards for Wireless Security" and use one of these mechanisms.

## 3.3 Basics

### 3.3.1 WLAN Adapters in Promiscuous Mode

Practically all LAN Ethernet adapters have a "promiscuous mode". In this mode, they receive not only the packets and broadcasts intended for them but also information transmitted for other nodes in the same LAN. This means that all the packets in a LAN segment can be received and evaluated. Each user in the promiscuous mode can therefore view the packets as they were transmitted.

If you use WEP encryption in the network, the user must have the required key. Otherwise users only see the generally non-encrypted broadcast packets.

The promiscuous mode is activated by "sniffer programs". If you want to try this yourself, one program you could use is "AiroPeek NX™".

<http://www.wildpackets.com>

This is available for all operating systems, very powerful, and free.

### 3.3.2 WLAN Adapters in Management Mode

Using a trick, is possible to move down one layer lower than with the promiscuous mode. This allows you to receive the information of the special IEEE 802.11 management level that precedes Ethernet packets. Hackers would use this mode to see more information. Some attacks are only possible when the adapter is in this mode.

For Windows, there is a program called Airopeek, once again a sniffer program, available at:

<http://www.wildpackets.com/products/airopeek>

### 3.3.3 Beacons

All access points transmit a radio signal on the set channel every 100 ms (default) known as a beacon. This makes the existence of the network and information on the access point known and the client uses this to find the access point.

This means, however, that a hacker knows there is a "target" somewhere. You must therefore take measures to prevent intruders gaining access to discovered access points. If you yourself want to find out just how easy it is to locate an access point, you can do this with the following programs:

- Linux - Kismet (<http://www.kismetwireless.net/>)
- Windows – Netstumbler (<http://www.netstumbler.com/>).

### 3.3.4 Network Name

The network name is transmitted along with the beacon. As a result, you can operate several networks at the same time without them causing mutual interference.

Based on the network name, the client knows which network it should connect to.

If several access points are included in the same infrastructure, the same network name is generally selected for the access points to allow roaming between these access points.

Since the network name is transmitted by the access point every 100 ms with the beacon, you should select a network name that does not indicate the owner of the access point. In other words, not "company A" but, for example, "AP0815". This provides no protection against a hacker finding you but makes identification more difficult.

Do not forget: A hacker does not need any special tools to read network names (standard tool of every WLAN adapter).

## **3.4 Traditional Standards for Wireless Security**

### **3.4.1 Closed Wireless System**

The so-called "closed wireless system" is a function with which the visibility of a WLAN cell can be restricted. With this function, when the beacon is transmitted, the network name (SSID) is simply left empty (or set to zero). If a client wants to use the access point, it queries the name of the network during the logon. (This also happens when the network name is not hidden.) The access point then informs the client whether or not it knows the network with the name "xyz". This means that it is only possible to log on in the system if the network name entered in the access point is known.

Normally, the client is informed of the network name in advance by the administrator. This is not protection but represents a hurdle that costs little to implement. Hackers can get round this easily: They simply need to record the log on packets in the management mode. The network name is transferred in plain language and can then be used again by the hacker. However, the hacker must wait until someone logs into the network and does not automatically receive the network name every 100 ms as with a normal open network name.

### 3.4.2 Blocking MAC Addresses (Access Control List)

Every Ethernet adapter has a six byte long ID that is set in the factory. This ID is unique worldwide and will never be assigned to another adapter. This means that every Ethernet adapter is available individually worldwide.

---

#### Note

In some systems, the MAC address can also be configured and therefore changed.

---

Almost every access point allows you to enter known MAC addresses and to block access by unknown adapters.

There are two methods commonly used:

- Local access lists on the access point (access control list)  
This method is suitable for a small number of access points when there are not many clients to be entered or canceled if changes are required in the network.
- Central access lists using RADIUS  
Here, a central list is managed by the administrator. The service can be provided by a RADIUS server and is generally used to manage access data of all types. Each time a logon is attempted, the access point checks the access rights of the client with the RADIUS server and sends a suitable confirmation. This allows large numbers of clients and access points to be managed.

Unfortunately, this security method is no guarantee for comprehensive security. In the management mode, a hacker can eavesdrop on the communication (between access point and client) even when it is encrypted. Hackers can learn the MAC address of a permitted adapter and then overwrite the MAC address of their own adapters and cheat the system. If they wait until the original client has logged off again before overwriting the MAC address, they do not even cause problems in the network.

### 3.4.3 WEP (Wired Equivalent Privacy)

WEP is a method of encrypting data on a radio link. It is based on the RC4 algorithm and is described in the IEEE 802.11 standard. It can be used with different key lengths.

Typical key lengths are 64 bits or 128 bits. Whatever the length, the first 24 bits are transmitted publicly for the so-called initialization vector. This is used to make packets with the same content appear different. This means that the hurdle to be cleared by an intruder involves 40 or 104 bits.

Internally, the algorithm functions as shown in Figure 3-1 Principle of WEP Encoding.

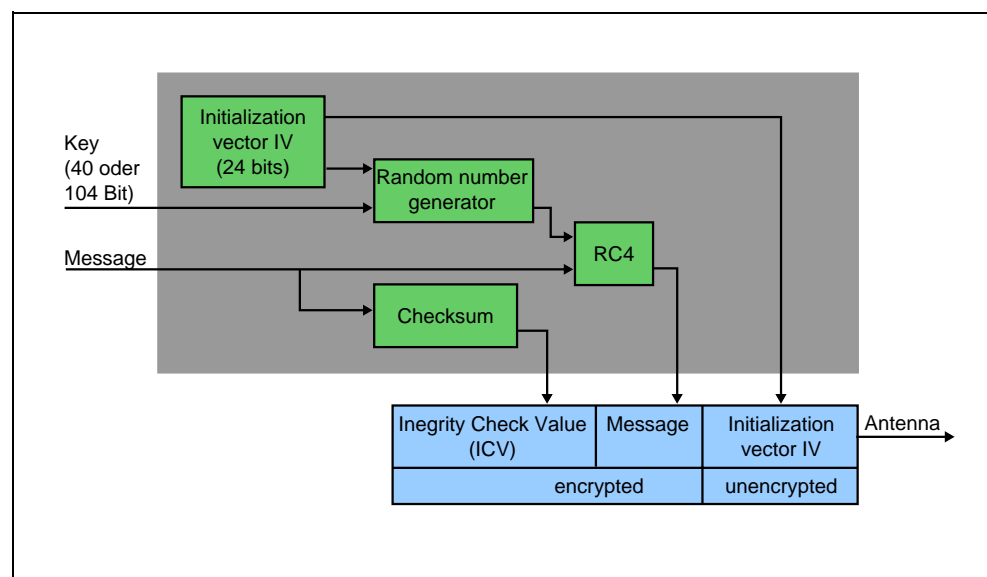


Figure 3-1 Principle of WEP Encoding

For the user/administrator of WEP, management of the encryption is as follows:

1. A secret key is generated.  
Depending on the key depth of the adapters, the length of the key is 5 or 13 characters/bytes.
2. This key is entered on the access point.
3. Users are informed of the key over a secret channel. You must specify this when you configure your wireless adapter otherwise although you can "see" the access point, you have no access to the network.

## Disadvantages

- A secret channel is necessary to exchange the key.
- This is a group key; in other words, anyone who knows the key can decode all the packets including those intended for others that use the same key.
- If the key is known (has been cracked), all clients and access points must be given a new key.
- The algorithm itself does not provide adequate security.

## Why is WEP not secure enough?

A team of researchers from Californian University led by Nikita Borisov published a paper in Berkeley in which some of the weaknesses of the WEP encryption method were pointed out (<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>). Concrete intrusions could not, unfortunately, be recorded. Nevertheless the paper stimulated a deeper cryptanalysis.

In August 2001, Scott Fluhrer, Itsik Mantin, and Adi Shamir published a further paper ([http://www.cryptocom.com/papers/others/rc4\\_ksaproc.pdf](http://www.cryptocom.com/papers/others/rc4_ksaproc.pdf)). This paper describes a concrete attack on WEP encryption. One weakness was the pseudo random number generator (WEP-PRNG) because parts of the key (the 24-bit initialization vector) are transmitted unencrypted permitting the secret part of the key to be reconstructed. Once a hacker has obtained approximately 60 IVs corresponding to this pattern, it is possible to reconstruct the common, secret group key. Of the  $2^{24}=3D16777216$  possible combinations, approximately 0.4% are compromising. It is therefore only a question of time before enough packets have been sent. The volume of data is decisive here: An attacker normally only needs approximately 4,000,000 packets to obtain the key.

Although this paper was purely theoretical, it only took two weeks before a concrete program had been written to perform the attack (<http://sourceforge.net/projects/airsnort>).

A hacker does not therefore need expensive measuring equipment, but simply this program, a WLAN adapter in management mode, a special Linux driver and a degree of patience when building the suitable kernel. It is then simply a matter of waiting until enough packets have been transmitted. In networks with heavy traffic, this might only mean 15 to 20 minutes, the size of the key no longer being of any importance. Once the key has been obtained, the hacker has access to all transmitted data.

There are other methods of attacking WEP that are, however, impractical compared with the method described above and need not be mentioned here.

## Summary

WEP does not represent total security. Nevertheless, WEP is a cost-effective solution that can be used with smaller volumes of data in the home and office environment.

Rules:

- If you do not have a better mechanism, you should certainly use WEP.
- Change the group key as often as possible.
- Use other measures (for example blocking MAC addresses).

### 3.4.4 WEPplus

Some vendors offer an expansion to reduce one weakness of WEP. With this expansion, all weak, compromising initialization vectors are suppressed (skipped) and therefore not transmitted. This makes it more difficult to obtain the key although it does not make it completely impossible.

To use this mechanism, both the access point and the client must support this scheme. The scheme complies with the IEEE 802.11 standard; in other words, communication with WLAN network components that do not support WEPplus is not restricted. During communication with such stations, it is, however, possible that they "give the game away".

The use of WEPplus only provides the specified security when all components involved support the scheme.

There is, however, no guarantee that other methods of attack will not be found or that there are not already unpublished methods of attack. If you transmit very sensitive data over wireless LAN and want to prevent an intruder from using your infrastructure, you can still do more to improve your security.

There are two practical methods of protecting wireless networks:

- VPN and
- new standards for wireless security.

### 3.5 VPN (Virtual Private Network)

In VPN, a gateway is inserted between the access point and LAN. If a client requires access to your network, it must first log on at the VPN gateway. If it is authorized, all the data will be exchanged between the client and the VPN gateway using encryption. If anyone receives these packets, they can only decode them by breaking the coding used up to the VPN gateway. As of the VPN gateway, the packets passed on to the remaining network are not encrypted.

If you use a VPN to secure your wireless network, remember the following:

- The access points in your LAN must be logically (for example using VLAN) or physically (separate hub) separate from the rest of the internal network.
- Install a VPN gateway between the new and old network.
- In addition to the wireless drivers, install VPN client software on the clients.

There are two different widespread standards for VPN:

- PPTP
- IPSec

#### 3.5.1 PPTP (Point-To-Point Tunneling Protocol)

PPTP was developed by Microsoft and is very small and simple to implement. It is therefore found as standard in WinCE devices. While it offers greater security than normal WEP, it is unfortunately not really secure. It is, for example susceptible to cryptographic attacks. The aim here is to obtain passwords that are too simple.

[http://mopo.informatik.uni-freiburg.de/pptp\\_mschapv2/](http://mopo.informatik.uni-freiburg.de/pptp_mschapv2/)

If you use PPTP, remember the following points:

- Passwords should be at least eight characters long.
- Users should not select their own passwords (such freely selected passwords are generally easy to crack).  
Create the passwords with a random generator and distribute them to the users.

### **3.5.2 IPSec**

IPSec is an authentication and encryption method that was originally intended for IPv6, but that can also be used with IPv4 (combined with a firewall). The standard itself is very complex and to date no one has found a point of attack; in other words, of all the methods presented up to now, IPSec is by far the most secure.

Setting up IPSec gateways is, however, no easy matter. The implementation of an IPSec environment should only be undertaken by suitably trained personnel.

The IPSec clients often have vendor-specific features (for example to allow user logon with a user name/password) that do not interoperate with other gateways.

Make sure that the vendor provides client software for all the clients you require (the operating systems must also be taken into consideration).

### 3.5.3 Other VPNs

If you do not want to use IPSec or PPTP, but prefer some other model, make sure that you find out how data encryption works at the transport level. Marketing departments of some firms call transport over a different medium a VPN although the data on the way there is by no means encrypted. If you are told that "our algorithms are our own and better than known algorithms such as DES, AES", you should be very cautious.

Modern cryptanalysis is very time-consuming and requires considerable effort. A classic example is the AES "candidate" Magenta that was cracked during the conference at which it was presented.

<http://www.counterpane.com/magenta-cryptanalysis.html>

### 3.5.4 Advantages and Disadvantages of VPNs

#### Advantages

- VPNs are independent of the manufacturers of the access points since these only transport the data and are not involved in the encryption.
- When using IPSec, VPNs are very secure.
- There may be further options for use, for example for clients wanting to enter the company from the Internet.

## **Disadvantages**

- Access points and "normal" network components must be separated; in other words, the network structure must be changed.
- The gateways must be installed on site between the access points and the remainder of the network making use in a subsidiary network more difficult and causing additional costs.
- VPNs are not easily scalable because encryption resources must be available for each user on the gateway resulting in intensive CPU utilization. You must therefore expect that you will need to upgrade.
- Installation is very complex.
- One VPN client may be very different from another. This means that the system operator is dependent on the vendor of the VPN gateway and its implementation.
- VPNs do not provide protection against rogue access points. This means that potential attackers program their own access point with exactly the same network name as the one being used. As soon as the attacker takes up a position with the AP that is close enough to your AP (or the attacker has a good antenna), the client connects to the rogue due to the better signal strength and not to your actual network. Such an attack can completely disrupt your network operations.

## 3.6 New Standards for Wireless Security

### 3.6.1 Authentication Methods

#### IEEE 802.1x

IEEE 802.1x is an approved and usable standard that defines additional methods. Its purpose is that anyone wanting to log on in a LAN must identify themselves unequivocally. This makes the standard applicable to normal LANs and wireless LANs. This method can, for example, prevent someone from plugging a PC into an unguarded switch port of your LAN and using or undermining your network structure.

Please note the following:

- When clients log on, they must use a special protocol to identify themselves to the nearest network component (the switch/access point).
- The network components over which the users enter your network must not only handle their normal tasks but must also support an authentication protocol.
- The network components send all queries to one (or more) servers that process the authentication queries and can then confirm or deny them. The protocol used for this is RADIUS. The client never comes into direct contact with the authentication server since the network component is always present acting as a go-between.
- Once a client is authenticated, it has unrestricted access to the network. (In wireless LANs, data encryption is also usually negotiated.)

## **Extensible Authentication Protocol (EAP)**

With RFC 2284, the IETF specifies the EAP (Extensible Authentication Protocol). EAP is a method of embedding new techniques of user authentication in existing protocols without having to modify the entire protocol. Originally, this method was intended for PPP (Internet dial in over modem/ISDN). Thanks to IEEE 802.1x, this can also be used for network components.

EAP is simply a generic term for various methods. In individual cases, system operators must check whether a method is supported by the client, the network components, and the authentication server before it can be used. In wireless networks, system operators attempt to combine the user logon using an EAP method with the management of the encryption keys between the client and access point.

- **EAP-MD5**

With EAP-MD5, identification is based on a user name and password. In LANs, this method is very useful to control access to unused network spots. In wireless networks, this method cannot be used because although it is possible to identify someone, static WEP keys are still used. These keys "give themselves away" if they are not replaced regularly.

Further danger points include:

- Dictionary attacks (similar to those with PPTP)
- "Man-in-the-middle" attacks:  
Somebody joins in communication and fools the genuine stations into believing that it is the partner station so that they can read all the data traffic unencrypted. To avoid this danger, a method is necessary in which you can find out which network you are logging on to.

- **LEAP** (Lightweight EAP)  
This method functions in much the same way as EAP-MD5. However in wireless networks, an individual WEP key is negotiated with each client and this remains valid as long as the client is logged in. This method was developed by Cisco and normally only exists in their products, binding users to this manufacturer.

LEAP has two weaknesses:

- The method with which the user name and password are exchanged allows dictionary attacks (see PPTP).
- The user must make itself known to the network but not the other way round. In the worst case, someone can set up their own access point and radius server and wait until clients logon with them. No client would notice that it is not connected to the correct network.  
The attacker then has no problem in attacking the connected clients.

In the meantime, Cisco are making efforts to replace this with a better method (see PEAP)

- **EAP-TLS** (EAP Transport Layer Security)  
EAP-TLS was specified in RFC 2716 and provides a strong cryptographic authentication of the client to the network. This is achieved by both ends, the client and logon server (not the access point/switch which is only a go-between), exchanging cryptographic certificates to verify their identities. To use this method, you require some form of PKI (Public Key Infrastructure). Today, system operators like to combine this with a directory service, for example Active Directory, LDAP, NDS etc. In other words, in companies in which such a service is already implemented, EAP-TLS is relatively simple to use. If you are not already using a directory service/PKI, we would not advise the use of EAP-TLS.  
EAP-TLS works like an SSL connection to a Web browser in which your browser must also identify itself to the server with a certificate. You must first obtain this certificate or it must be assigned to you. As with SSL, an encryption method supported by both sides is selected automatically. If EAP-TLS is used in wireless networks, this involves the client and access point.  
Disadvantage: The certificates are initially transferred in plain language. Encryption is only negotiated afterwards. A hacker can therefore not only see the MAC address of the client but also who logs on to the network since the name of the user is in the certificate in plain language.

- **EAP-TTLS** (EAP Tunneled Transport Layer Security)  
EAP-TTLS was developed by Funk Software and Certicom among others from TLS. It has, however, been implemented by many vendors in their products. The way it works can be compared with an SSL encrypted Web server. In contrast to EAP-TLS, only the logon server requires a unique, digital certificate that is checked by the client during connection establishment. Data encryption is established between the access point and the client generally with an anonymous user name. Once again as with EAP-TLS, different methods can be selected. After the method has been selected, there is a second encrypted logon at the logon server with the correct user name/password. The authentication server can then, for example, relate the user data to an NT domain.  
This method is much simpler to implement than EAP-TLS. The anonymous initial logon also makes it more difficult for the hacker to identify the client.
- **PEAP** (Protected EAP)  
This is a new development with the basic features of EAP-TTLS. Once again, the authentication server requires a certificate and once again encryption is agreed before there is any identification with user name/password. PEAP and EAP-TTLS are two variants of the same method rather than two different methods.  
There are currently two different implementations that are not compatible. One was developed by Cisco, the other comes from Microsoft. These methods differ in their possible options:
  - The Microsoft version supports only authentication by user name/password
  - The Cisco version also supports tokens (for example RSA) in addition to the features of the Microsoft version.

TTLS supports further methods. Before making any decision, you should clarify exactly what you need for your security.

- **EAP-SIM**

This method is currently a draft but has already been implemented in part by some vendors. Here, the SIM card of a GSM phone is used to identify the user to the network. In company networks, this has no practical advantage, however for hotspots the method is extremely interesting. In particular, if you have a smart phone (phone with integrated PC) this can identify itself to the hotspot network without you needing to do anything. Afterwards, individual encryption can be established between the client and access point in much the same way as with most other EAP methods. Normally, no encryption is used in hotspot networks to allow every client simple access.

Unfortunately, only clients for Windows XP are currently available. Since nobody wants to insert and remove their SIM continuously, it will take time before this method becomes established.

### **3.6.2 Generating Certificates**

For EAP-TLS, EAP-TTLS and PEAP, certificates are generally required for authentication.

Creating a certificate generally involves three basic steps.

First a pair of keys, a private and a public key must be created. The public key is then sent to the certificate authority (CA) along with other information (name and parameters of the key owner) as a CSR (certificate signing request). The task of the CA is to verify the correctness of the information using suitable measures and to confirm the CSR with the signature of the CA (acting as a form of witness) and to return the finished certificate to the applicant.

In the meantime, there are companies from which you can obtain a certificate for E-mail traffic and/or an SSL server (fees are charged the service). The advantage of such certificates is that many browsers already know the basic certificates of the CAs and therefore automatically trust them; With self-generated certificates, this is not the case. Here, users must install the CA basic certificate in the browser themselves later.

Creating certificates is described on a number of Web sites.

The free OpenSSL software is often used when creating certificates.

Once the required certificates are prepared, the certificate must be installed on the device. The devices provide special functions for this.

### 3.6.3 Encryption Methods

#### Dynamic (WEP) Keys

As mentioned earlier, normal WEP keys are keys that are sent once and apply to all group members. It is far better if the encryption keys are negotiated individually between the client and access point. An attacker in possession of a key (for example because enough packets have been eavesdropped to calculate the key according to the method explained by Fluhrer, Mantin, and Shamir) can only eavesdrop on this one client and only until the client logs off again.

The individual exchange of encryption keys is already being used in access points that support EAP (with the exception of EAP-MD5). When the client logs on, a dynamic key, for example for normal WEP or TKIP is negotiated under the protection of the relevant EAP method. The authentication server is also included in the negotiation. Since the key is different every time, an attacker who has calculated a key once hardly has a chance to obtain it a second time. The attacker would need to repeat the eavesdropping action every time.

#### Periodic Replacement of the Key

As mentioned above, it is possible to negotiate individual key assignment during the logon. To make life as difficult as possible for the attacker, it is possible to change the key again after a certain time under the protection of the EAP method being used. In this case, the attacker must once again crack the code. Periodic replacement of the key is possible regardless of whether WEP, TKIP, or AES is being used.

#### TKIP

TKIP (Temporal Key Integrity Protocol) along with other measures is intended to eliminate known weaknesses of WEP. TKIP is defined in the IEEE 802.11i standard and is part of the WPA specification (Wireless Protected Access) of Wi-Fi. Although TKIP still uses RC4 as the basis for encryption, other measures have been taken to close the gaps exposed in WEP.

TKIP expansions:

- **Higher initialization vector**  
The initialization vector was increased from 24 to 48 bits to avoid repetitions (due to counter overflow).

- **Temporal keys**

WEP uses the entered group key for each packet that it encrypts (only made possible by the Fluhrer, Mantin, Shamir attack).

In this method, a temporary key is calculated for each packet. This is formed from a hash (a cryptographic checksum method), the IV components (the initialization vector), and the MAC address (the basic key). The temporal key calculated in this way is then used to encrypt an individual packet with WEP.

- **Michael checksum algorithm**

Previously, each packet had a simple checksum at the end that was formed from the entire data content and then appended to the packet. This checksum is used to detect bit errors in transmission. An attacker could, however, use this to insert false packets into the network. If attackers know the checksum algorithm, they can use it to calculate relevant packets. It is also possible to eavesdrop on packets and to send them again after changing a few bits. The checksum usually "confuses" the original application that contains the data. Michael also forms a checksum, however this is "keyed"; in other words, the (temporal) key is also included in the calculation of the checksum. This means it is only possible to calculate the correct checksum if both the data and key are known. This makes it far more difficult for an attacker to falsify packets that would be accepted by the network (due to the correct checksum). A similar mechanism with larger keys is also used in IPsec and is known as HMAC.

- **Additional sequence numbers**

Additional sequence numbers are also included in the data packets and these also count as data for the checksum calculation. The nodes are then programmed so that they only accept packets with the expected sequence number. If an attacker records a packet and then sends it later, it will be discarded since both nodes have moved on to a different sequence number in the meantime.

## AES

AES (Advanced Encryption Standard) is intended to replace the old DES standard (the "Rijndael" algorithm was selected).

With the IEEE 802.11i standard, RC4 will finally be replaced as the encryption for data packets. The security of data packets encrypted with this method is very high. The method does, however, utilize the CPU intensively. Make sure that the WLAN chipsets used perform the AES encryption in the hardware.

### 3.6.4 Standards for Authentication and Encryption

#### WPA

The WPA standard was proposed by the Wi-Fi consortium. Wi-Fi defines numerous compatibility tests for WLAN components to ensure that different components can interoperate with components of other vendors. With WPA, Wi-Fi deals with the compatibility of WLAN components in terms of the security mechanisms. The WPA standard represents a subset of the IEEE 802.11i standard and provides:

- TKIP for improved data encryption (method easy to implement on existing components)
- The use of authentication servers with EAP methods for client identification (for example EAP-TLS, EAP-TTLS, PEAP etc.).
- The use of PSKs (preshared keys) if no authentication server is possible. With PSK, the client and the access point are assigned a common password for identification. To log on at the access point, the client must identify itself as an authorized user by knowing this password (that is not transferred). Only then is encryption established by TKIP. In VPNs, IPsec also uses this method. PSK is suitable as a simple method when the user wants to avoid the expense of an authentication server. WPA-compliant products can be certified by Wi-Fi with the label "Wi-Fi Protected Access".

#### IEEE 802.11i

The standard is still in development (April 2004).  
WPA already integrates the following features of the new standard:

- TKIP for data encryption or
- AES for data encryption
- EAP methods for authentication by a central server
- PSK

### **3.6.5 Advantages and Disadvantages of the New Standard**

#### **Advantages**

- Central authentication of clients
- Used in subsidiary networks possible without extra costs, at least as long as a connection to the authentication server is possible.
- Good scalability (encryption takes place between the client and access point), there are therefore hardly any performance problems to be expected.
- Not only suitable for security of wireless networks but also in a LAN environment.
- Open standards (except for LEAP)
- No change in the network structure necessary.

#### **Disadvantages**

- The access points of the vendors must support the EAP used and the encryption type.
- As long as WEP is still used, the security is not as good as with IPsec. WPA with TKIP eliminates the worst weaknesses of WEP and can be considered as equal to SSL with RC4. The new standard IEEE 802.11i with AES will increase security to better than "normal" IPsec clients (that only use triple DES).
- Clients must exist for the operating system being used. This is, however, also the case with VPNs.

### Comparison of the Methods - An Overview

	<b>EAP-MD5</b>	<b>EAP-TLS</b>	<b>EAP-TTLS</b>	<b>PEAP</b>
<b>Client/Server Authentication</b>	No	Yes	Yes	Yes
<b>Dynamic Key Management</b>	No	Yes	Yes	Yes
<b>Authentication Server</b>	Yes (Radius)	Yes (Radius)	Yes (Radius)	Yes (Radius)
<b>TKIP</b>	No	Yes	Yes	Yes
<b>AES</b>	No	Yes	Yes	Yes
<b>Certificate</b>	No	Client/server	Server only	Server only

# Application of Industrial Wireless LAN

# 4

## 4.1 Introduction

### Areas of Application of an Industrial Wireless LAN (IWLAN) in Automation Engineering

The true benefits of Wireless LAN technology lie in the mobility and flexible application 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 wireless communication between individual stations is an additional advantage for the user. In many cases, however, the performance of the IEEE 802.11 standard is not adequate because there are increased requirements in terms of throughput and reaction times. Furthermore, in an industrial environment, a predictable (deterministic) access to data is necessary to ensure that the process remains fully under control.

The use of a wireless LAN is preferred by customers in particular in cases where there are clearly recognizable advantages compared with the use of cables.

- **Communication with Moving Stations**

Interfacing of moving devices to a data network involves considerable effort. The wireless attachment saves the entire bus installation for data in electric suspension tracks and saves optical systems in unmanned transport systems. In both these applications, routes can also be changed simply achieving considerable flexibility.

The integration of rotating devices in a data network avoids wear and tear on the slippings. The same advantage also applies to the substitution of drag chains. The use of IWLAN provides increased reliability for the application because wireless communication is predictable and fixed throughput times can be defined.

- **Communication with mobile stations, mobile data acquisition**

The user can acquire data from all manufacturing and storage areas with mobile, industrial Internet pads such as the MOBIC (Mobile Industrial Communicator) from SIMATIC NET and pass it on for central data processing. The mobile handhelds used are not assigned to a specific machine or process but to a user. The requirements in terms of numbers of devices are reduced considerably.

Time-consuming transfer of data from paper to the central database and the potential errors involved are eliminated. With a fully integrated concept for data acquisition, significant costs can be saved particularly at interfaces at which data must be transferred from one process step to the next. With IWLAN, it is possible to monitor the wireless connection between stations and the wireless network. If a station unintentionally leaves the area of coverage or wireless contact is suddenly broken, a warning is sent automatically to the control level.

- **Mobile service and diagnostics**

If a fault occurs, service personnel can analyze the problem on site and can obtain information for the fast elimination of the problem over the MOBIC wireless Internet pad. The availability of spare parts in the warehouse can be immediately checked and parts ordered online if necessary.

Diagnostics does not, however, only relate to fault situations. Operational data such as levels or the load on machines can also be assessed quickly and reliably by personnel. The advantage of an IWLAN wireless network is that both "uncritical" data from service and diagnostics as well as process-critical data with higher performance requirements can be transmitted over the same wireless network.

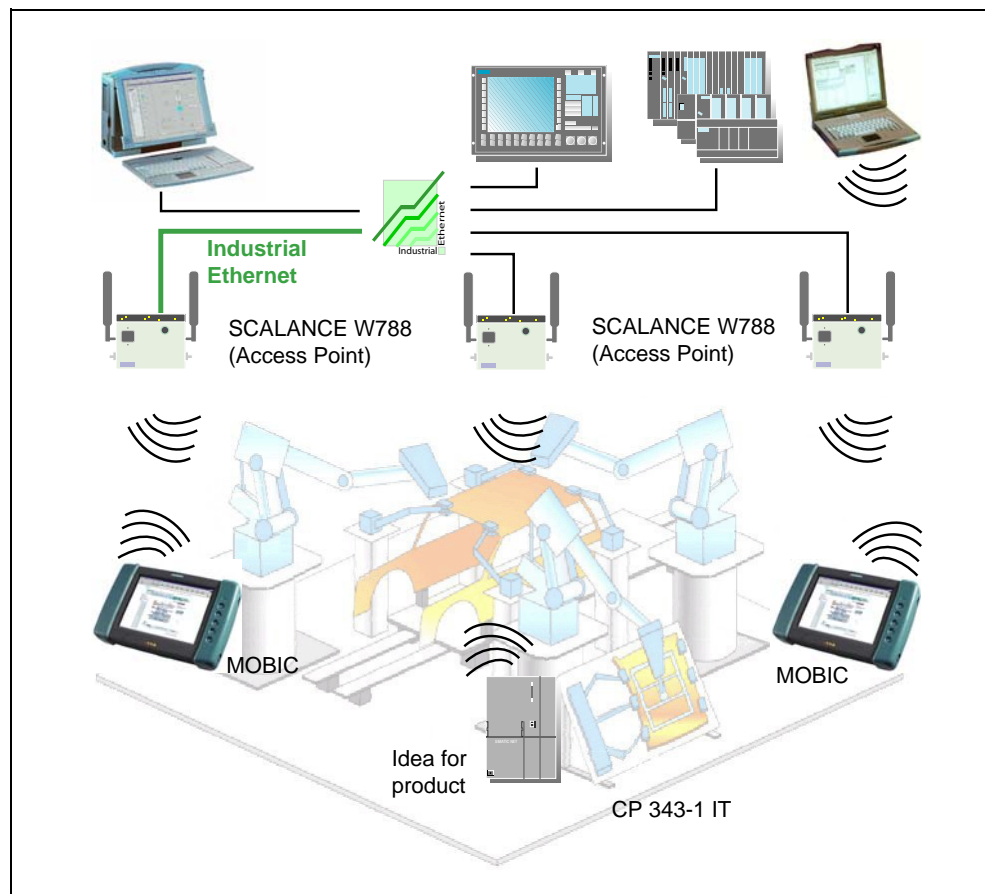


Figure 4-1 Industrial Wireless LAN in Automation Engineering

- **Communication with mobile stations and mobile maintenance**

Maintenance can be greatly simplified and speeded up by the use of mobile communication leading to significant savings in costs. Maintenance engineers can monitor machine settings directly via their wireless service units and intervene immediately when problems occur. Personnel can use devices with which they are familiar such as the field PG because they can be included in the wireless network due to standardized interfaces (PCMCIA wireless adapter).

- **Flexible manufacture in temporary configurations and communication with distant units**

Today, assembly lines must no longer be rigid units that can only be converted with considerable cost and effort for new applications. Particularly in automobile manufacturing plants, the factory layout is liable to fast modification. Flexible production means meeting customer requirements quickly and without long conversion times. By using wireless data networking, production units can be integrated in the data network quickly and with little effort. Test configurations can also be implemented quickly. IWLAN meets the high requirements of reliability and performance in wireless communication because throughput times and data rates can be defined in advance. This property is a function provided only by Industrial WLAN (IWLAN) from SIMATIC NET.

A wireless LAN also allows cost-effective integration of machines and controllers installed in otherwise inaccessible locations. Expensive and time-consuming cabling is avoided.

---

**Note**

Advantages of wireless over cable:

- When an existing cable duct cannot be used (for example data and power cables must not laid together)
  - When a new cable route would otherwise have to be installed
  - When data has to be transferred over paths open to the public.
-

## 4.2 SIMATIC NET Products for Industrial Wireless LAN

Wireless LAN technology is widespread in office environments. A large growth is expected for SOHO (small office/home office) and consumer markets. To be able to use the technology of wireless communication in an industrial area, it is advisable to use products specially designed for such an environment.

In an industrial environment, there are many influences that can have a detrimental effect on a wireless link. These include machines and storage units that shield radio waves due to their metallic construction. The radio link is also changed by the influence of moving people and vehicles. Industrial manufacturing plants are usually in large buildings in which the effects of multipath propagation are particularly noticeable. Constant conditions for wireless transmission cannot therefore be guaranteed. In automation, it is essential that the throughput times are predictable and that part of the data rates available is distributed to devices (for example PLCs) that have more exacting requirements in terms of wireless communication. To increase the value of this IWLAN wireless network, standard 802.11 stations can, of course, also be integrated in the same wireless coverage.

To allow the use of wireless LAN technology in an industrial environment, SIMATIC NET offers products that guarantee reliable data transmission despite the exacting environmental conditions.

To combat the multipath propagation experienced in assembly plants (see Figure 1-2) and the resulting attenuation or obliteration of radio waves, wireless modules are equipped with two antennas (antenna diversity). The receiver can then select the stronger of two received signals.

To ensure reliable data transmission, when the quality of the transmission link changes permanently (number of nodes, changing distance from the node to the access point), the modules must be capable of reducing the maximum data rate to a lower data rate to ensure reliable reception of the data.



The assembly system of the products must also meet the requirements of a rough industrial environment and allow simple installation. The modules must nevertheless provide the convenience of an IT component such as Web Based Management with SNMP or allow the sending of E-mails or SMS messages.


The current SIMATIC NET WLAN products provide additional I-features. The SCALANCE W788-1/2PRO products have the following special characteristics:



- Monitoring of the wireless link (Link Check)
- Monitoring of additional IP links (IP-Alive)
- Redundant wireless links over two different channels to increase availability
- Reservation of a fixed bandwidth and reply time for critical clients


### Available Products

SIMATIC NET offers the following products for setting up an industrial wireless network:

Description	Device
<p><b>RLM (Radio Link Module)</b> An access point suitable for use in industry for setting up a wireless network (infrastructure) and for attaching to the wired data network (Ethernet) (Figure 4-1)</p>	
<p><b>CP 1515 (PCMCIA Card)</b> For installation in PCs and mobile operator control units with a PCMCIA port (for example. MOBIC T8, Field PG)</p>	

Description	Device
<p>Industrial Wireless LAN  <b>SCALANCE W788-1PRO</b> (robust AP)            Access point with a robust design and high degree of protection for the 2.4 GHz and 5 GHz bands</p> <ul style="list-style-type: none"> <li>• Extremely reliable due to reservation of bandwidth and cyclic monitoring of the link</li> <li>• Wireless LAN IEEE 802.11b/g and 802.11a with up to 54 Mbps at 2.4 GHz and 5 GHz</li> <li>• Wireless Distribution System (WDS) for point-to-point links</li> <li>• Degree of protection IP 65, robust metal housing</li> <li>• Operating temperature <math>-20\text{ }^{\circ}\text{C}</math> ... <math>+60\text{ }^{\circ}\text{C}</math> with condensation</li> <li>• Redundant power supply 18 - 57 VDC and Power-over-Ethernet</li> <li>• 10/100 Mbps Ethernet port for connection to the wired network</li> <li>• Modern data security with genuine 128-bit encryption (WPA) and authentication (IEEE 802.1x)</li> <li>• C-plug (configuration plug) for replacement without a programming device</li> <li>• Compatibility with RLM</li> </ul>	

Description	Device
<p>Industrial Wireless LAN  <b>SCALANCE W788-2PRO</b> (robust dual AP)                      Access point with a robust design and high degree of protection for the 2.4 GHz and 5 GHz bands                      Identical to the robust access point plus:</p> <ul style="list-style-type: none"> <li>• Second wireless adapter for wireless LAN 802.11b/g and 802.11a</li> <li>• Redundancy mode for extremely reliable wireless link over two separate wireless adapters</li> </ul>	
<p>Industrial Wireless LAN  <b>SCALANCE W744-1PRO</b> (robust client module)                      Client adapter with a robust design and high degree of protection for linking terminals with an Ethernet interface to the WLAN wireless network for the 2.4 GHz and 5 GHz bands</p> <ul style="list-style-type: none"> <li>• Wireless LAN 802.11b/g and 802.11a with up to 54 Mbps at 2.4 GHz and 5 GHz</li> <li>• Degree of protection IP 65, robust metal housing</li> <li>• Operating temperature <math>-20\text{ }^{\circ}\text{C}</math> ... <math>+60\text{ }^{\circ}\text{C}</math> with condensation</li> <li>• Redundant power supply 18 - 57 VDC and Power-over-Ethernet</li> <li>• 10/100 Mbps Ethernet port for connection to terminals with an Ethernet port</li> <li>• Modern data security with genuine 128-bit encryption (WPA) and authentication (IEEE 802.1x)</li> <li>• C-plug (configuration plug) for replacement without a programming device</li> </ul>	

Description	Device
<p><b>CP 7515</b>                      PCMCIA card (32-bit Cardbus) for installation in PCs and mobile operator control devices (for example Field PG) for the 2.4 GHz and 5 GHz bands</p> <ul style="list-style-type: none"> <li>• Wireless LAN 802.11b/g and 802.11a with up to 54 Mbps at 2.4 GHz and 5 GHz wireless approval in 30 countries and Wi-Fi</li> <li>• PC Card with 32-bit Cardbus interface</li> <li>• Degree of protection IP 20</li> <li>• Operating temperature 0 °C ... +60 °C</li> <li>• Modern data security with genuine 128-bit encryption (WPA) and authentication (IEEE 802.1x)</li> <li>• Installation and maintenance with management tool for Windows 2000, XP, CE.NET</li> <li>• Integration in STEP 7/NCM PC</li> </ul>	 <p>The image shows a Siemens CP 7515 PCMCIA card. It is a rectangular device with a silver-colored metal casing. The front face is white and features the Siemens logo at the top. Below the logo, there is a diagram of a network topology with various nodes and connections. At the bottom of the front face, the text 'SIMATIC NET Networking for Industry' is printed. The card is shown at an angle, revealing its black plastic contacts on the right side.</p>

## **4.2.1 General Information on Antennas, Lightning Protection, Cables**

### **Antennas**

- Omnidirectional antenna for 2.4 GHz and 5 GHz to extend and optimize the wireless link
- Planar antenna (180°) for 2.4 GHz and 5 GHz to extend and optimize the wireless link
- Directional antenna (60°) for 2.4 GHz and 5 GHz to extend and optimize the wireless link
- Vehicle antenna (omnidirectional) for 2.4 GHz and 5 GHz to extend and optimize the wireless link especially in unmanned transport systems

### **Antenna cable (preassembled with plug and socket)**

- Length 5 m

### **Lightning protector**

For attachment to distant antennas installed outdoors.

# Glossary

# 5

<b>2G</b>	Digital mobile wireless networks of the second generation, for example GSM
<b>3G</b>	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)
<b>Access point</b>	Wireless LANs are set up using access points. They also connect the wired data network.
<b>ACK</b>	Acknowledge Signal in handshake protocol for avoiding the hidden node problem
<b>ACL</b>	Access Control List List of MAC addresses with the right to access the wireless network
<b>Ad hoc network</b>	Wireless network between individual devices (point-to-point)
<b>AES</b>	Advanced Encryption Standard New standard for encryption of data in wireless LANs
<b>Antenna diversity</b>	Technique with which a radio receiver is equipped with two antennas so that it can select the better of two signals
<b>Antenna gain</b>	Improvement of the antenna compared with an isotropic radiator achieved by suitable construction (passive!)
<b>ATM</b>	Asynchronous Transfer Mode Wired network used particularly in the backbone for large distances at high data rates

<b>BPSK</b>	Binary phase shift keying Modulation technique in wireless LANs
<b>BQTF</b>	Bluetooth Qualification Test Facility Facility for monitoring the interoperability of products of various vendors
<b>BSS</b>	Basic Service Set Wireless LAN network with access to the infrastructure over a single access point
<b>CCK</b>	Complementary code keying Modulation technique in wireless LANs
<b>CDMA</b>	Code Division Multiplex Code-controlled medium access control
<b>CF</b>	Compact flash
<b>CFP</b>	Contention free period Period during which access is managed by the access point (to support time-critical services)
<b>CP</b>	Contention period Period in which access is controlled according to CSMA/CA (to support time-critical services)
<b>CP</b>	Communications processor
<b>CSMA/CA</b>	Carrier Sense Multiple Access with Collision Avoidance, medium access control on a wireless IEEE 802.11 network
<b>CSMA/CD</b>	Carrier Sense Multiple Access with Collision Detection, medium access control for wired Ethernet network
<b>CTS</b>	Clear to send Signal in handshake protocol for avoiding the hidden node problem
<b>DCF</b>	Discrete coordinated function Normal medium access control in IEEE 802.11 in contrast to PCF

	Normal medium access control in IEEE 802.11 in contrast to PCF
<b>DDE</b>	Dynamic Data Exchange
<b>DECT</b>	Digital Enhanced Cordless Telecommunications, European standard for language and data communication
<b>DFS</b>	Dynamic Frequency Selection
<b>DFS</b>	Dynamic Frequency Selection in the 5 GHz band
<b>Diversity</b>	Wireless receiver with two antennas allowing selection of the best signal
<b>DSSS</b>	Direct Sequence Spread Spectrum (IEEE 802.11b)
<b>EAP</b>	Extensible Authentication Protocol
<b>EDGE</b>	Enhanced Data Rates for Global Systems for Mobile Communications (GSM) Evolution Further development of GSM with data rates up to 384 Kbps
<b>EIRP</b>	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.
<b>EN 954-1</b>	Standard relating to functional safety (old)
<b>ESM</b>	Electrical Switch Module
<b>ESS</b>	Extended Service Set Wireless network consisting of several overlapping basic service sets (BSS)
<b>ETSI</b>	European Telecommunication Standard Institute

<b>Fall back</b>	Gradual reduction of the data rate when receiving conditions are bad to allow the connection to be maintained
<b>FDMA</b>	Frequency Division Multiplex Access
<b>FEC</b>	Forward Error Correction Inclusion of redundant bits in the useful data to make the signal less sensitive to interference
<b>FHSS</b>	Frequency Hopping Spread Spectrum A method used in IEEE 802.11b and Bluetooth.
<b>FTEG</b>	Law regarding wireless equipment and telecommunications installations in Germany
<b>GFSK</b>	Gaussian Phase Shift Keying Modulation technique in 802.11
<b>GPRS</b>	General Packet Radio Service Expansion of GSM for packet-oriented data communication at up to a maximum 170 Kbps.
<b>GSM</b>	Global System for Mobile Communications Digital telephone services at frequencies in the 900 MHz, 1800 MHz and 1900 MHz ranges
<b>GSM-R</b>	GSM for railroad traffic at high speeds
<b>Handshake</b>	Acknowledgment process to establish a connection between stations ready to communicate.
<b>Hidden node problem</b>	Two stations are arranged in a wireless cell so that they are outside their own transmission range. If they both access the medium of the same time, collisions result.
<b>HIPERLAN</b>	High-performance Radio LAN in the 5 GHz band
<b>Home RF</b>	Standard for wireless communication between PCs and home-oriented consumer devices.

<b>HSCSD</b>	High Speed Circuit Switched Data GSM wireless network for higher data rates
<b>IAPP</b>	Inter Access Point Protocol Protocol for communication between the APs
<b>IBSS</b>	Independent Basic Service Set Ad-hoc network for spontaneous and simple establishment of wireless connections without a network infrastructure
<b>IE</b>	Industrial Ethernet
<b>IEC 61508</b>	Standard relating to functional safety (new)
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IEEE 802.11</b>	Standard for wireless networks in the 2.4 GHz band with transmission rates of up to 2 Mbps.
<b>IEEE 802.11a</b>	Standard for wireless networks in the 5 GHz band with transmission rates of up to 54 Mbps.
<b>IEEE 802.11b</b>	Standard for wireless networks in the 2.4 GHz band with transmission rates of up to 11 Mbps.
<b>IP</b>	Internet Protocol Collection of program routines that the TCP protocol accesses
<b>IP 20</b>	Device degree of protection (proof against solid objects up to 12.5 mm)
<b>IP 65</b>	Device degree of protection (fully protected against dust; protected against water jets)
<b>IPsec</b>	Internet Protocol Security Open standard for increasing data security in IP networks

<b>IrDA</b>	Infrared Data Association Standard for data communication with infrared over short distances
<b>IS</b>	Intrinsically Safe (protected against explosion)
<b>ISM band</b>	Industrial, Scientific and Medical Band Frequency band for use without license
<b>ISO</b>	International Organization for Standardization
<b>Kerberos</b>	Security system for the encryption of sensitive data
<b>LLC</b>	Logical Link Control
<b>FOC</b>	Fiber-optic cable Transmission medium for optical networks.
<b>MAC</b>	Medium Access Control
<b>Multipath propagation</b>	Reflections of an electromagnetic wave from different objects. As a result, the electromagnetic wave arrives at the receiver with different intensities and after a different propagation times
<b>MIC</b>	Message Integrity Protocol Technique for increasing the integrity of data in wireless LANs
<b>Mini PCI</b>	Special design of wireless LAN adapters for direct integration in products
<b>MSS</b>	Mobile Satellite Service within UMTS
<b>OFDM</b>	Orthogonal Frequency Division Multiplex Method of modulation in IEEE 802.11a
<b>OFDM/CCK</b>	Orthogonal Frequency Division Multiplex/complimentary code keying Method of modulation in IEEE 802.11a

<b>PAN</b>	Personal Area Network Network for devices at relatively short distances from each other.
<b>PC Card</b>	Special design for wireless LAN adapters (PCMCIA)
<b>PCF</b>	Point coordinated function Medium access control Technique to support time-critical services in wireless LANs
<b>PCMCIA</b>	Special design for wireless LAN adapters
<b>PDA</b>	Personal Digital Assistant Mobile data terminal equipment
<b>Pico network</b>	Network structure in Bluetooth in which up to eight stations are organized
<b>QAM</b>	Quadrature amplitude modulation
<b>QoS</b>	Quality of Service
<b>QPSK</b>	Quadrature phase shift keying
<b>R&amp;TTE</b>	Radio and Telecommunications Terminal Equipment Directive EU directive for telecommunications terminal equipment
<b>RADIUS</b>	Remote Authentication Dial - In User Service for secure communication networks
<b>RCM</b>	Radio Client Module (Ethernet adapter, Ethernet client)
<b>RegTP</b>	Regulatory body for telecommunication in Germany
<b>RLM</b>	Radio Link Module (access point)

<b>Roaming</b>	Free movement of wireless LAN stations even beyond the boundaries of an access point's cell. The stations and can move from one cell to the next without any noticeable interruption.
<b>RTS</b>	Request To Send Signal in handshake protocol for avoiding the hidden node problem
<b>RTS/CTS</b>	Request to send/Clear to send. Scheme for avoidance of collisions
<b>Scatter network</b>	Network structure in Bluetooth in which several Pico networks are organized
<b>SIG</b>	Special Interest Group The user organization for Bluetooth
<b>SNMP</b>	Simple Network Management Protocol Standardized protocol for transporting network management information.
<b>SSID</b>	Service Set Identifier Address Name of the wireless LAN
<b>TDMA</b>	Time Division Multiplex Access
<b>TKIP</b>	Temporal Key Integrity Protocol Scheme for cyclic changing of the key in WLANs
<b>TLS</b>	Transport Layer Security
<b>TPC</b>	Transmission Power Control Automatic control of transmitter power in the 5 GHz band
<b>TX</b>	Transmitter power of the wireless module (not including bundling of the radiation by (passive) antenna gain)
<b>UMTS</b>	Universal Mobile Telecommunications System Mobile wireless transmission for voice, audio, image, video, and data communications

---

<b>UNII</b>	Unlicensed National Information Infrastructure Name of the 5 GHz band in American literature
<b>URAN</b>	UMTS Radio Access Network
<b>UTRAN</b>	UMTS Terrestrial Radio Access Network
<b>WBM</b>	Web Based Management. HTTP-based configuration method in which an HTTP server is used in the access point.
<b>WCDMA</b>	Wideband CDMA Method of modulation for high data rates
<b>WDS</b>	Wireless Distribution System Radio links for connecting the access points for an extended service set (ESS)
<b>Web pad</b>	Portable device in DIN-A4 size with a touchscreen for Internet use
<b>WECA</b>	Wireless Ethernet Compatibility Alliance An alliance of various wireless LAN product manufacturers who ensure product compatibility through product testing.
<b>WEP</b>	Wired Equivalent Privacy Encryption scheme in wireless LANs
<b>Wi-Fi</b>	Wireless Fidelity. Specification for wireless networks.
<b>Wi-Fi seal</b>	Wireless Fidelity Seal of approval of the WECA alliance for compatible and tested components.
<b>Wired LAN</b>	Network operated on guided media
<b>Wireless LAN</b>	Network operated using unguided media
<b>Wireless LAN</b>	Wireless LAN (here: IEEE 802.11)

<b>WLANA</b>	The Wireless LAN Association Consortium of wireless LAN providers promoting wireless LAN technology on the network market.
<b>WPA</b>	Wi-Fi Protected Access. Authentication scheme based on dynamic key exchange.

# Index

# 6

<b>1</b>	
1.2.3 ISM band	
allocation.....	15
<b>A</b>	
Access control lists	
central.....	54
local.....	54
Ad hoc network.....	24
AES.....	69
Antenna cable.....	82
Antenna diversity.....	34
Antennas.....	82
<b>B</b>	
Background noise.....	29
Beacon.....	52
Biological compatibility.....	16
<b>C</b>	
Certificates	
generating.....	67
Closed wireless system.....	53
CP 1515.....	78
CP 7515.....	81
CSMA/CD.....	26
<b>D</b>	
Data security.....	33
Diffraction.....	17
Direct sequence spread spectrum.....	29
DSSS.....	29
<b>E</b>	
EAP.....	63
EAP-MD5.....	63
EAP-SIM.....	66
EAP-TLS.....	64
EAP-TTLS.....	65
<b>F</b>	
FHSS).....	28
Fragmentation.....	28
Frequencies and approvals.....	18
Frequency bands.....	13
Frequency hopping.....	28
<b>H</b>	
Hidden node problem.....	27
<b>I</b>	
IEEE 802 standards	
ISO/OSI reference model.....	22
IEEE 802.11	
Working groups.....	45
IEEE 802.11a	
Data rate.....	40
Frequencies, channels.....	39
Transmission range.....	41
Transmit power.....	40
IEEE 802.11b.....	35
Available non-overlapping channels.....	36
Data rate.....	37
Frequencies, channels.....	35
Transmission range.....	37
Transmit power.....	36
IEEE 802.11g.....	38
Data rate.....	38
Frequencies, channels.....	38
Transmission range.....	38
Transmit power.....	38
IEEE 802.11h	
Frequencies, channels.....	42
Transmission range.....	42
Transmit power.....	42
IEEE 802.11i.....	70
IEEE 802.1x.....	62
Infrastructure mode.....	25
IPSec.....	59
ISM band	
usage.....	15
<b>K</b>	
Key	
dynamic.....	68
renewing after time.....	68
<b>L</b>	
LEAP.....	64
Lightning protector.....	82
<b>M</b>	
MAC address blocking.....	54
Management mode.....	51
<b>N</b>	
Network architecture.....	24

<b>O</b>	
OFDM .....	31
Orthogonal frequency division multiplexing .....	31
Overview of IEEE 802.11 .....	43
<b>P</b>	
PEAP .....	65
PPTP .....	58
Promiscuous mode .....	51
PSK .....	70
<b>R</b>	
Radio link planning .....	17
RAP .....	79
RCM .....	80
RdAP .....	80
Readme.rtf .....	6
Reflection .....	17
RLM .....	78
<b>S</b>	
Safety Notices .....	2
SCALANCE W744-1PRO .....	80
SCALANCE W788-1PRO .....	79
SCALANCE W788-2PRO .....	80
Shared medium .....	33
Signal modulation	
CCK .....	29
CCK/OFDM .....	32
PBCC .....	32
<b>T</b>	
TKIP .....	68, 70
Training .....	6
Transmission medium .....	13
<b>V</b>	
VPN .....	58, 60
<b>W</b>	
Wave propagation	
in space .....	11
reflection .....	11
Superimposed waves .....	12
Wavelengths .....	13
WEP .....	55
WEP/Security .....	56
WEPplus .....	57
Who to Contact .....	6
Wi-Fi Alliance .....	46
Wi-Fi certification .....	46
Wireless LAN	
areas of application .....	74
products (SIMATIC NET) .....	78
security .....	50
Wireless technologies	
interference WLAN - Bluetooth .....	47
mutual interference .....	47
overview of wireless technologies .....	14
WLAN security .....	50
WPA .....	70

