Warranty, Liability and Support

Note

The Application Examples are not binding and do not claim to be complete regarding the configuration, equipping and any eventuality. The application examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of the responsibility of safely and professionally using, installing, operating and servicing equipment. When using these application examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these application examples at any time without prior notice. If there are any deviations between the recommendations provided in these application examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document. Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). However, claims arising from a breach of a condition which goes to the root of the contract shall be limited to the foreseeable damage which is intrinsic to the contract, unless caused by intent or gross negligence or based on mandatory liability for injury of life, body or health. The above provisions do not imply a change of the burden of proof to your detriment. It is not permissible to transfer or copy these application examples or excerpts of them without having prior authorization from Siemens Industry Sector in writing. For questions about this document please use the following e-mail address:

online-support.automation@siemens.com
Preface

Purpose of the document

This document provides you with an overview of the specific requirements for the setup of an Industrial Wireless LAN and familiarizes you with the properties of the appropriate SIEMENS products.

First, you will be introduced to the topic of wireless local networks (“WLANs”) in the industrial environment and you will be informed on the essential technical principles. Subsequently, we will show you different SIEMENS products, examine their applications and provide you with decision guidance, enabling you to select the optimum solution to your problem.

Main contents of this document

This document deals with the following key elements:

- Properties of WLANs in general,
- SIEMENS products for setting up wireless networks particularly in industrial environments.

Topics not covered by this application

- This document does not include a detailed description of the software installation and the commissioning of the individual components.

Current and detailed information on this topic is available in the manuals and operating instructions of the corresponding products.

Reference to Automation and Drives Service & Support

This document is an article from the Internet Application Portal of Siemens Industry Automation and Drive Technologies Service & Support. The following link takes you directly to the download page of this document.

Table of Contents

Warranty, Liability and Support........................................................................................................... 2
Preface ...................................................................................................................................................... 3
Table of Contents .................................................................................................................................... 4
1 Biological Compatibility ....................................................................................................................... 7
2 Radio Waves as Basis of a Shared Medium Network ........................................................................ 10
   2.1 Differentiating WLANs from other radio networks ................................................................. 10
   2.2 General properties of radio networks ...................................................................................... 10
   2.3 Preferred fields of application ................................................................................................. 11
   2.4 The physics of radio waves ...................................................................................................... 11
       2.4.1 Propagation .................................................................................................................... 11
       2.4.2 Interferences ................................................................................................................ 13
       2.4.3 Transmission range and data rate .................................................................................. 13
       2.4.4 Frequencies, frequency spacing and channels ............................................................... 14
   2.5 Antennas ..................................................................................................................................... 15
       2.5.1 Characteristics of an antenna .......................................................................................... 15
       2.5.2 Non-directional and directional antennas ....................................................................... 16
   2.6 Requirements for radio communication in the industrial environment .................................. 19
3 IEEE 802.11 as a WLAN Standard .................................................................................................... 21
   3.1 The network standards of the IEEE 802 series ........................................................................ 21
   3.2 Basics of IEEE 802.11 and Wi-Fi ............................................................................................ 22
       3.2.1 The 802.11 standard ....................................................................................................... 22
       3.2.2 Further standards ........................................................................................................... 23
       3.2.3 “Wi-Fi” .......................................................................................................................... 23
   3.3 Modulation and multiplex method ............................................................................................. 23
   3.4 Comparison 2.4 GHz and 5 GHz band ..................................................................................... 26
       3.4.1 The 2.4 GHz band ........................................................................................................... 26
       3.4.2 The 5 GHz band ............................................................................................................ 27
       3.4.3 Comparison of the properties of the 2.4 GHz and 5 GHz band .................................. 27
   3.5 IEEE 802.11e and WMM: “Quality of Service” ....................................................................... 28
   3.6 IEEE 802.11h and the 5 GHz band ............................................................................................. 28
   3.7 Other radio technologies .......................................................................................................... 29
       3.7.1 Bluetooth ....................................................................................................................... 29
       3.7.2 Wireless HART ............................................................................................................ 29
       3.7.3 Zigbee ............................................................................................................................ 30
       3.7.4 AeroScout ...................................................................................................................... 30
4 Topology, Configuration and Organization of IWLANs .................................................................... 32
   4.1 Radio Cells and the Transition between Cells: “Roaming” Method ......................................... 32
       4.1.1 Connection of individual radio cells: “Access points” and “clients” ............................... 33
       4.1.2 Motion of clients between the radio cells: “Roaming” .................................................... 34
       4.1.3 “Hidden node” problem ................................................................................................. 35
   4.2 Infrastructure networks .............................................................................................................. 35
       4.2.1 Stand-alone networks ..................................................................................................... 35
       4.2.2 Mixed Networks ............................................................................................................ 36
       4.2.3 Multi-channel configuration ......................................................................................... 37
4.2.4 Wireless Distribution System ("WDS") ............................................... 38
4.2.5 Redundant wireless LANs ................................................................. 39
4.3 Ad hoc networks .................................................................................. 40
4.4 Advanced management functions ......................................................... 41
4.4.1 VLANs ("Virtual LANs") ....................................................................... 41
4.4.2 VPNs ("Virtual Private Networks") ......................................................... 42
4.4.3 RSTP ("Rapid Spanning Tree Protocol") ..................................................... 44
4.4.4 IWLAN management functions DCF and PCF ........................................ 45
5 Data Security and Data Encryption according to IEEE 802.11i and 802.1X46
5.1 Basics on security in radio networks .................................................... 46
5.2 IEEE 802.11i and IEEE802.1X ................................................................. 46
5.2.1 WEP ("Wired Equivalent Privacy") ....................................................... 47
5.2.2 WPA and WPA2 .................................................................................... 47
5.2.3 RADIUS protocol ............................................................................... 49
5.2.4 Security functions and data rate ......................................................... 49
5.3 Attack scenarios .................................................................................... 50
6 Proprietary Expansions of the IEEE 802.11 Standard ............................... 52
6.1 “iPCF” ("Industrial Point Coordination Function") and Rapid Roaming52
6.2 “iHOP” ("industrial Hopping") ............................................................... 53
6.3 “iQoS” ("industrial Quality of Service") .................................................... 54
6.4 “iPCF-Channel” ("Industrial Point Coordination Function – Management Channel") ..................................................... 57
6.5 “Dual client” technology ....................................................................... 57
7 Coexistence of IWLANs with other Radio Networks .................................. 60
8 Country Approvals .................................................................................. 62
8.1 General information ............................................................................... 62
8.2 Approval methods and responsibility .................................................... 62
8.3 Country approvals in the SCALANCE W devices ..................................... 62
9 SCALANCE Access Points and Clients ....................................................... 66
9.1 SCALANCE W: General information ..................................................... 66
9.1.1 Installation and configuration .............................................................. 68
9.1.2 Power supply ..................................................................................... 69
9.1.3 Security aspects .................................................................................. 71
9.2 Access Points of the SCALANCE W product line .................................. 72
9.2.1 Access Points SCALANCE W788-xPRO/RR ....................................... 72
9.2.2 Access Points SCALANCE W786 ....................................................... 73
9.2.3 Access Points SCALANCE W784-1xx ............................................... 75
9.3 WLAN client modules of the SCALANCE W740 series ......................... 77
9.4 Application Examples ............................................................................ 79
9.5 Deterministic data communication and rapid roaming: iPCF .................. 81
9.6 PROFIsafe with SCALANCE W .............................................................. 81
9.7 Increase in performance by HiPath Wireless ........................................ 82
# Basics on IWLAN Setup

## 10 Further SIMATIC IWLAN products

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>SIMATIC Mobile Panels</td>
</tr>
<tr>
<td>10.2</td>
<td>SIMATIC ET 200pro IWLAN interface module IM 154-6 PN HF</td>
</tr>
<tr>
<td>10.3</td>
<td>IWLAN/PB Link PN IO</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Network transition as a PROFINET IO proxy</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Network transition in standard mode</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Network transition in mobile applications</td>
</tr>
</tbody>
</table>

## 11 SINEMA Software for WLANs

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>The SINEMA E configuration software</td>
</tr>
<tr>
<td>11.1.1</td>
<td>Functional scope of SINEMA E</td>
</tr>
<tr>
<td>11.1.2</td>
<td>Extended functionality for SINEMA E Standard</td>
</tr>
</tbody>
</table>

## 12 HiPath Wireless Products by SIEMENS

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>Basic information</td>
</tr>
<tr>
<td>12.2</td>
<td>HiPath Wireless Portfolio as part of HiPath</td>
</tr>
<tr>
<td>12.3</td>
<td>Properties and customer benefits of HiPath Wireless WLANs</td>
</tr>
<tr>
<td>12.4</td>
<td>SCALANCE W786-2HPW access point for HiPath</td>
</tr>
</tbody>
</table>

## 13 Accessories for Wireless Networks (WLANs)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1</td>
<td>RCoax leaky wave cables</td>
</tr>
<tr>
<td>13.1.1</td>
<td>Data rate and segment length</td>
</tr>
<tr>
<td>13.1.2</td>
<td>Principle of operation</td>
</tr>
<tr>
<td>13.2</td>
<td>“C-PLUG” and PRESET-PLUG</td>
</tr>
<tr>
<td>13.2.1</td>
<td>C-PLUG</td>
</tr>
<tr>
<td>13.2.2</td>
<td>PRESET-PLUG</td>
</tr>
<tr>
<td>13.3</td>
<td>Antennas</td>
</tr>
<tr>
<td>13.4</td>
<td>Connections and cabling</td>
</tr>
<tr>
<td>13.5</td>
<td>Additional accessories</td>
</tr>
</tbody>
</table>

## 14 Glossary

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>

## 15 Internet Links

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>

## 16 Index

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>

## 17 History

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
1 Biological Compatibility

With regard to the question whether electromagnetic fields (for instance, in connection with Industrial Wireless LAN) can endanger human health, we refer to a publication of BITKOM (German Association for Information Technology, Telecommunications and New Media e. V.), as of December 2003:

The same standards for the protection against health impairments as for all other radio applications apply to WLAN devices. These regulations are based on the protection concepts of ICNIRP\(^1\) or the respective EU Council Recommendation.

The independent German Radiation Protection Commission (Strahlenschutzkommission (SSK)) has, commissioned by the Federal Ministry for the Environment (Bundesministerium für Umwelt (BMU)), determined the state of scientific knowledge regarding possible dangers – thermal and non-thermal – through electro-magnetic fields and gives the following statement:\(^2\)

"The SSK comes to the conclusion that, even after the assessment of the recent scientific literature, there is no evidence of current scientific knowledge in view of proven impairments to health to challenge the scientific assessment underlying the protective concepts of ICNIRP or the EC Council Recommendation."

In addition, the SSK states that there is also no scientific suspicion of health risks below the existing limit values. This assessment is in accordance with the assessments of other national and international scientific commissions and of the WHO (www.who.int/emf).

To obtain further information on this topic, please use the following URL:

www.bitkom.org

---

\(^1\) International commission for protection from non-ionising radiation

“Industrial Wireless Local Area Networks” (IWLANs)

Content

This part acquaints you with basic properties of radio networks. You are informed on the characteristic features of WLANs and we explain the most important terms and technologies.

Figure 1-1: Integration of IWLANs in the industrial environment
Structure

Table 1-1

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>This chapter provides information on the general properties of radio waves and radio networks.</td>
</tr>
<tr>
<td>3</td>
<td>This chapter provides you with an overview of the “802.11” standard, which has developed into the de facto standard for wireless networks. The technology and the security-related questions are explained.</td>
</tr>
<tr>
<td>4</td>
<td>This chapter finally describes the aspects related to the organization and administration of radio networks.</td>
</tr>
<tr>
<td>5</td>
<td>Chapter 5 discusses the safety-relevant aspects of 802.11 radio networks, such as encoding and authentication methods.</td>
</tr>
<tr>
<td>6</td>
<td>This chapter explains proprietary expansions of the 802.11 standard by which it is adjusted to the requirements of the industrial environment.</td>
</tr>
<tr>
<td>7</td>
<td>This chapter describes the problem if 802.11 radio networks are operated in the same area as other radio systems (e.g. Bluetooth).</td>
</tr>
<tr>
<td>8</td>
<td>Chapter 8 finally describes the problem of approving individual devices or operating modes in radio operation of different countries.</td>
</tr>
</tbody>
</table>
2 Radio Waves as Basis of a Shared Medium Network

Here you can learn...

... about the consequences of using radio to set up a local network, the properties of the used radio waves and the specific measures required to ensure trouble-free setup and operation of such a network.

2.1 Differentiating WLANs from other radio networks

At present there are a number of different technologies available for setting up radio networks, such as Bluetooth for office communication, GPRS and UMTS for mobile telephone networks, RFID tags for identification and goods tracking, etc. (see also 3.6)

Within the framework of this document we focus on WLANs in the strict sense, i.e. radio networks which follow the IEEE 802.11 standard (see chapter 3). "IWLANs" ("Industrial WLANs") refers to WLANs, which are "hardened" by special measures, i.e. made ready for requirements and utilization in industrial environments.

2.2 General properties of radio networks

Cables compared to radio waves

The use of cables and lines for communication has certain advantages since an exclusive medium is available: the transmission characteristics of this medium are well defined and constant (provided that cables, routers or similar components are not replaced) and it is distinctly recognizable at any time which nodes are connected to a "local area network" (abbreviation: "LAN") and which are not.

However, in return the complexity of the cabling (and the possibility of cable breaks and other hardware faults) increases with the number of nodes. The use of wire-bound methods for the communication with freely moving nodes is only feasible in exceptional cases. Radio links additionally enable to bridge zones for which cabling would otherwise be difficult (streets, waters).

In these applications, radio-based networks can show their advantages (which, in summary, consist in the fact that they are less tied to a specific location). In these cases, the possibly higher investment costs are compensated by increased customer benefits.

Complexity of the radio field

Radio waves propagate through space, are diffracted at obstacles or attenuated when passing through and thus generate a complex radio field which changes when the obstacles move. It is obvious that the range illuminated by one or several transmitter(s) is not sharply defined. There is no clear delimitation of the radio field which causes a fluctuation of the transmission characteristics for the individual nodes of the radio network depending on their position. In addition, it is practically impossible to discover a "silent listener" in a radio network.

These properties have considerable consequences on questions regarding connection reliability and bug proof or interference immunity of a network. Assuming responsible administration, careful planning and the use of trained employees who are sensitized to the specific concerns of a radio network, radio networks are as reliable, secure and robust as wire-bound networks.
2.3 Preferred fields of application

Due to their special properties, radio networks are the preferred, if not the only advisable medium in numerous environments.

The fields of application for which radio networks are predestined include:

- Connection of freely movable nodes to one another and to stationary nodes,
- Connection of mobile nodes with cable-based networks (Ethernet, etc.),
- Contact to rotating nodes (cranes, carousels, ...),
- Connection of nodes with limited mobility (monorail conveyors, high-bay racking systems, ...), for the replacement of sliding contacts or trailing cables,
- Setup of wireless bridges between physically separated (different buildings, streets, waters) cable-based subnets,
- Communication with nodes in areas which are difficult to access.

2.4 The physics of radio waves

2.4.1 Propagation

Unlike signals in a line, radio signals propagate three-dimensionally in space as electromagnetic waves. When the waves hit an object, they are reflected virtually completely if the object is electroconductive. If the object is non-conducting, a part of the waves is reflected, another part is absorbed in the object, and a rest is finally let through the object. When hitting edges, radio waves are scattered into virtually all directions.
Interference and diffraction

Two additional properties are important for the development of the radio field:

- On the one hand, radio waves (unlike incoherent light) can amplify or even extinguish one another ("interference"). If a receiver is located in both, the direct beam and the reflection of a transmitter, it does not necessarily detect the double signal strength, but it will possibly not detect any signal at all.

- On the other hand, the propagation properties of the waves depend on their wavelength, i.e. high-frequency radio waves behave differently than low-frequency radio waves. In particular, radio waves of long wavelength (i.e. low-frequency) can be "diffracted" around objects. Similar to sound or water waves, it is then possible to receive signals even in the “shadow” of a radio source.

Interference and diffraction phenomena are basically in magnitudes that correspond to the wavelength of the used radiation. For WLANs following the IEEE 802.11 standard it is between 12 cm and 6 cm, which means that shifts by one module width may already cause a changed transmission and reception behavior.

Frequency sensitivity of the properties of radio waves

As a rule of thumb, it can be said that the higher the frequency and the shorter the wavelength of the oscillations, the closer the properties of radio waves come to the properties of light: high-frequency transmitters propagate in a straight line and no longer reach receivers behind objects. On surfaces, they are almost completely absorbed or reflected.

Signals of longer wavelength, however, also go “around objects” and penetrate deeper into non-conducting objects or can pass through them.
2.4.2 Interferences

Each object that is spatially located within a radio network can disturb this network if it sends signals on the frequency used by the transmitters. In contrast to lines, which can be shielded relatively easily and reliably, radio networks are susceptible to interferences by any device in their environment which, intermittently or continuously, can radiate on strictly limited channels or emit broadband radiation. These devices include devices designed as transmitters such as and Bluetooth devices, but also microwave ovens, welding equipment etc. However, such interferences can already be counteracted before they occur by carefully planning the radio network.

2.4.3 Transmission range and data rate

The transmission range and the achievable data rate of a radio transmitter depend, among other things, on the used frequency.

Range

Basically, the transmission range of transmitters of short wavelength (higher-frequency) is shorter than the range of transmitters of long wavelength: the short-wave signals behave similarly to light, can only propagate in a straight line and are completely absorbed or reflected on objects. This results in a considerable decrease of the signal quality and the free line of sight between transmitter and receiver is impaired. However, the transmission range can be significantly increased by using directional antennas.

Data rate

The maximum data rate that can be transmitted on a carrier wave is proportional to its frequency, i.e. higher-frequency transmitters achieve higher data rates.\textsuperscript{3} Transmitters on a frequency of 2.4 GHz (as used by the IEEE 802.11 method) can typically achieve ranges between approx. 30 m or 100 m (in the interior or exterior) with omni-directional antennas. (See also Table 3-1) The data rates which can be transmitted on this band amount to up to 54 Mbps. This value is in the range of standard Ethernet connections and exceeds other cable-based systems such as MPI by far.

Relevance of the data rate

Which data rate is actually necessary or sufficient for a specific application depends – even if the connection is optimal – not only on the quantity of the user data. Depending on the protocol, a more or less large overhead results for the handling of the radio communication and interconnected devices such as access points, routers, etc. also cause delays which develop when the signals are relayed. The achievable net data rate is thus influenced in multiple ways by the design and the parameterization of the actually existing radio network.

\textsuperscript{3} The theoretically achievable net data rate (in bit/s) is equal to half of the sender frequency (in Hz). This is mainly the so-called Nyquist-Shannon-Sampling-Theorem. This theoretical value exceeds the rates achievable in practice by the factor 10.
2.4.4 Frequencies, frequency spacing and channels

Only one node can transmit on each radio frequency at any time. (“Half duplex”) When several nodes transmit simultaneously on the same frequency, none of the two can be received; this case is referred to as a “collision”.

One of the most important tasks of a LAN protocol – i.e., the rules according to which the nodes of the network communicate – is to avoid the occurrence of collisions since collisions always require a time-consuming repetition of the individual messages.

Frequencies and required spectrum

Strictly speaking, the definition that a transmitter emits on exactly one frequency is not correct: this would only be the case for a pure sinusoidal signal. However, modulating a signal sequence to a carrier frequency (see section 3.3) broadens the spectrum of the transmitter and the transmitter also takes a range of the frequencies above and below the carrier frequency. For this reason, it is not possible to position different transmitters on a frequency band as close as desired; rather the transmitters must keep a distance from one another that is proportional to the used data rate: This is referred to as “bandwidth” of the transmitter.4

![Figure 2-2: Schematic diagram of the spectrum of a frequency-modulation station](image)

The example shown in the above figure illustrates the behavior of a frequency-modulation station. Aside from the actual carrier frequency (approx. 98.4 MHz), a frequency band is used on both sides (blue). In this case, the width of the band is exaggerated; in reality 40 kHz are sufficient for an FM signal.

Bands and channels

To keep the clarity, the radio spectrum, i.e. the entire frequency range of the radio communication, is divided into individual “bands”. The different bands differ in the radio characteristics (transmission range, susceptibility to interferences, possible data rate, …) and consequently also in their applications.

The frequency bands are divided into “channels” which are distributed on the respective band at a specific distance.

For instance, the 2.4 GHz range of the ISM band5 is divided into thirteen channels between 2.412 GHz and 2.472 GHz; the spacing between neighboring channels is 5 MHz so that theoretically thirteen transmitters can use the band simultaneously.6

---

4 Colloquially “bandwidth” generally refers to the transmission capacity.
5 “Industrial, Scientific and Medical”; see also Glossary.
2.5 Antennas

An antenna transforms electrical currents into electro-magnetic waves and vice versa. They send out electro-magnetic waves and receive them in the same way. Each antenna has a certain frequency range within which the coupling between the antenna current and the surrounding wave is at its maximum.

Electromagnetic waves

Electromagnetic waves consist of an electrical field vector $E_x$ and a magnetic field vector $H_y$, which are always at right angle with each other. The current is the cause of the magnetic field vector and the voltage causes the electrical field vector. (see graphic)

Figure 2-3

2.5.1 Characteristics of an antenna

Impedance

Impedance refers to a frequency-dependent resistor. For the WLAN components (antenna, cable) this resistor has 50 Ohm. It is important here that the impedance of an antenna, i.e. input/output at the antenna and at the antenna cable are matched to each other.

Polarization

The polarization specifies the direction of the vector of the electrical field intensity in the radiated electro-magnetic wave. It is differentiated between linear and circular polarization. For linear polarization the electrical field lines run in one plane. If they are directed vertical to the ground surface this is referred to as vertical polarization; if they run horizontal to ground level this is a horizontal polarization.

If the direction of the electrical field component is not fixed but runs continuously in form of a circle, this is referred to as circular polarization. Depending on the direction this is also referred to as clockwise and anticlockwise polarization.

IWLAN antennas usually have a vertical polarization.

Table 2-1

<table>
<thead>
<tr>
<th>Polarization</th>
<th>Electrical field direction</th>
<th>Magnetic field direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear vertical</td>
<td>Vertical</td>
<td>Horizontal</td>
</tr>
<tr>
<td>Linear horizontal</td>
<td>Horizontal</td>
<td>Vertical</td>
</tr>
<tr>
<td>Circular</td>
<td>Constantly circulating around the axis of propagation (clockwise/anticlockwise)</td>
<td></td>
</tr>
</tbody>
</table>

Since the frequency ranges of transmitters on close channels overlap, there are only three channels which do not interfere with each other, see also 0.
For optimal reception it is important that for corresponding antenna the polarization of both is identical. A damping by 20 dB, for one vertical and another horizontal antenna, is not rare.

### 2.5.2 Non-directional and directional antennas

The radiation of antennas can be either non-directional or directional. In general, directional antennas achieve higher transmission ranges; however, this is not the effect of a higher transmitter power but the result of the shape of the radio field.

**Antenna gain**

The antenna gain is a parameter which describes how strong an antenna sends and receives compared with a reference emitter.

An isotropic radiator, i.e. an idealized point source which continuously sends into and receives from all directions. The gain of the isotropic point source is set to zero.

The unit of the antenna gain is normally “dBi” (i = isotropic point source). A gain of 3 dBi corresponds approximately to a doubled send/receive line.\(^7\)

**Antenna diagrams**

An antenna describes the directional characteristic of an antenna in which the direction-independent antenna gain is measured. Normally, the representation of the directional diagram occurs in polar coordinates.

A horizontal antenna diagram is a front view of the electromagnetic field of an antenna with the antenna at the center. The gain is plotted as distance from the center of the coordinate system above the send/receive angle.

---

\(^7\) Since the antenna gain is measured in logarithms, 6 dBi correspond to 4 times the power, 9 dBi 8 times the power etc..
Figure 2-4: Example of a horizontal (left) and a vertical (right) antenna diagram of a non-directional antenna: the gain of the antenna in the horizontal diagram (blue line) is equally high in all directions, approx. zero. In the right diagram the line runs "180 – 0" at right angle to the antenna axis.

A vertical antenna diagram is a side view of the electromagnetic field of the antenna. The antenna gain is plotted above the angle to the symmetry plane of the antenna.

Aperture angle

The aperture angle refers to the angular distance at which the field intensity of the antenna has dropped to approximately half ≈ 3 dBi of the maximum.

Figure 2-5 Exemplary antenna diagram for determining the aperture angle. The -3 dBi circle is represented green, which marks half of the signal maximum (= 0 dBi). The intersections of the blue antenna gain diagram with the green circle define the aperture angle of the antenna. (Hier: Ca. 30°)

The horizontal and vertical aperture angles of an antenna usually differ depending on the geometry.
Omni-directional (non-directional) antennas

Omni-directional or non-directional antennas always have the form of a rod or a straight wire. The term is misleading in so far as the radiation intensity is not isotropic, i.e. not equal in all directions. The radio field of the antenna reaches the maximum intensity on a plane at a right angle to the antenna axis. (Compare Figure 2-6) The field intensity quickly decreases above and below the “vertical aperture angle” of this plane and no noteworthy signal can be expected vertically above and below the antenna.

The radio field is radial symmetrical; this means that the field intensity is identical in all directions when viewed from the top along the antenna axis. In this case, the “horizontal aperture angle” is 360°.

Directional antennas

Directional antennas, which typically have the form of a flat box, generate a radio field in the shape of a cone at a right angle to the box.

The cone is defined by a horizontal and a vertical aperture angle; outside this angle the field intensity decreases quickly.
In the maximum field intensity direction the transmission range of a directional antenna is typically ten times as large as the range of an omni-directional antenna.

**Antennas for SCALANCE W devices**

Section 13.3 provides an overview of antennas suitable for operation with the SCALANCE W devices.

**Leaky wave cables**

Leaky wave cables for which the developing radio field is limited to the micro-environment of the conductor are alternatives to conventional antennas.

The fields of application of such leaky wave cables are moved nodes which move along defined paths (monorail conveyors), tunnels and similar areas that are difficult to cover using cabling.

An example of a leaky wave cable is the RCoax cable from chapter 13.1.

### 2.6 Requirements for radio communication in the industrial environment

Requirements for industrial networks differ in some points from the networks of the office or home environment.

**Data volumes**

In the office environment files of several megabytes are typically moved, for the industrial application the data packets are often much smaller.

**Transmission speed and latency**

During communication between office devices a temporal delay, for example when sending a print job, generally does not cause any problems. However, in the industrial environment measured values and control commands (such as an emergency off) must often be exchanged in the milliseconds range.

**Fail-safety and reliability**

Data loss or data corruption during transmission in the office environment is normally uncritical, since the transmission can always be repeated. However, for
industrial plants the delays through failed transmissions and their repetition are often unacceptable.

**Interferences due to external sources**

The home and office environments are generally marked by a low degree of interference from objects which are not part of the radio network. In the industrial environment, however, there are naturally numerous partly very intensive interference sources such as arc or spot welders, frequency converters, RFIDs, relays and drives, which inhibit fast error-free communication.
3 IEEE 802.11 as a WLAN Standard

Here you can learn about...

… the IEEE 802.11 standard on which most of the currently installed WLANs are based. This section imparts background knowledge that is not necessarily required for installing a WLAN but which makes it easier to understand the reason for individual measures.

3.1 The network standards of the IEEE 802 series

The Institute of Electrical and Electronics Engineers IEEE\(^8\) has made it its job to develop, publish and promote electronic and electrotechnical standards and can be remotely compared to DIN.

Under the project number “802”, a number of task groups have been formed to develop standards for the installation and operation of networks. For instance, group “802.3” is concerned with the standards for Ethernet connections.

Task group “802.11” has now developed specifications for wireless LANs. Nowadays, these specifications are the de facto standard for radio networks, the most important variants being “802.11 a/h” and “802.11 b/g”.

The IEEE continuously develops the standards to adapt them to new requirements and technical conditions.

The following table gives an overview of the topics of some IEEE 802 standards regarding IWLANs.

Table 3-1: Overview of some areas defined by IEEE 802.11 or IEEE 802.1 substandards

<table>
<thead>
<tr>
<th>Substandard</th>
<th>Definition area</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 a</td>
<td>Communication</td>
</tr>
<tr>
<td>802.11 b</td>
<td>Communication</td>
</tr>
<tr>
<td>802.11 e</td>
<td>Quality of Service (see 6.3)</td>
</tr>
<tr>
<td>802.11 g</td>
<td>Communication</td>
</tr>
<tr>
<td>802.11 h</td>
<td>Communication (reduce interference)</td>
</tr>
<tr>
<td>802.11 i</td>
<td>Data security (see 5.2)</td>
</tr>
<tr>
<td>802.11 n</td>
<td>Communication</td>
</tr>
<tr>
<td>802.1 Q</td>
<td>Virtual LANs (see 4.4.1)</td>
</tr>
<tr>
<td>802.1 X</td>
<td>Data security (see 5.2)</td>
</tr>
</tbody>
</table>

---

\(^8\) See also [http://www.ieee.org/portal/site](http://www.ieee.org/portal/site).

Version 2.1 08.02.2011 21/131
3.2 Basics of IEEE 802.11 and Wi-Fi

3.2.1 The 802.11 standard

The original 802.11 standard9 (today often referred to as “802.11 legacy” for reasons of clarity) defines the connection of the network nodes via radio in the frequency band at 2.4 GHz or alternatively via infrared interfaces.

The gross data rate was up to 2 Mbps, however, the actually achieved net data throughput was considerably less.

The standard was improved by the expansions “b”, “a”, “g”, “h” and “n”, which were put on the market in this order. The transmission capacities were increased by more complex and more efficient modulation methods.

Over time other substandards were also defined each relating to certain aspects of operating wireless radio networks.

Expansion 802.11n is still in the development phase; this standard is expected to be released before the end of 2009. Devices which support the standard already or after a firmware update are already available on the market.

The following table lists the technical properties of the 801.11 substandards.

<table>
<thead>
<tr>
<th></th>
<th>802.11 “a”/“h”</th>
<th>802.11 “b”</th>
<th>802.11 “g”</th>
<th>802.11 “n”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency band</td>
<td>5 GHz</td>
<td>2,4 GHz</td>
<td>2,4 GHz</td>
<td>2,4 GHz</td>
</tr>
<tr>
<td>Gross data rate</td>
<td>54 Mbit/s</td>
<td>11 Mbit/s</td>
<td>54 Mbit/s</td>
<td>600 Mbit/s</td>
</tr>
<tr>
<td>Net data rate approx.</td>
<td>23 Mbit/s</td>
<td>4,3 Mbit/s</td>
<td>19 Mbit/s</td>
<td>74 Mbit/s</td>
</tr>
<tr>
<td>Modulation / multiplex method*</td>
<td>OFDM</td>
<td>DSSS</td>
<td>OFDM</td>
<td>MIMO</td>
</tr>
</tbody>
</table>

*) For the individual modulation methods, see 3.3
**) Recommended

If the connection quality is not good enough to maintain the maximum data rate, the transmission rate is successively reduced until a stable connection is achieved.

Basically, a 802.11 a device cannot communicate with a 802.11 b/g device, the “b” and “g” versions of the standards are not compatible.

Transmission range and special antennas

Within buildings the used antennas achieve ranges of typically 30m. Since reflections and shadowing have less effect in the exterior, ranges of up to 100m and more can be achieved. A connection with line of sight is particularly advantageous since the radio waves can then propagate without being disturbed.

The use of directional antennas allows to increase this value to a multiple of 100m.

“Turbo” mode for increased data throughput

The theoretical data rates can be doubled by using “Turbo” mode (i.e. up to 108 Mbps are achieved). This mode, however, is proprietary, not compatible with all devices and must also not be used in all countries so that its use is only advisable in exceptional cases.

9 See also http://grouper.ieee.org/groups/802/11/, http://standards.ieee.org/wireless/overview.html#802.11
3.2.2 Further standards

In the course of time a number of further substandards were defined for the 802.11 standard, mostly relating to individual aspects of radio communication:

- 802.11e: Introduction of “Quality of Service” features for increased transmission quality, see 3.5,
- 802.11h: Adaptation to 802.11a, to prevent interference with other devices in the 5 GHz band, see 3.6,
- 802.11i: Security functions for data encoding and authentication, see 5.2.

Furthermore, IEEE 802.1 standards exist important for operating WLANs:

- 802.1Q: Virtual LANs for separating a network, see 4.4.1,
- 802.1X: Security functions for WLANs and VLANs, see 5.2.

3.2.3 “Wi-Fi”

Devices for the end user using the 802.11 suite of technologies are frequently promoted under the “Wi-Fi” label. The “Wi-Fi Alliance”\(^\text{10}\) in overall charge of this label is an association of several hundred WLAN solution providers who guarantee the compatibility of their products among each other by assigning a Wi-Fi logo.

Occasionally, the popularity of “Wi-Fi” has led to the expression being used as a synonym for wireless networks in general. Strictly speaking, Wi-Fi is only one standard for compatible devices using the 802.11 technologies.

3.3 Modulation and multiplex method

To transmit a signal by means of an oscillation, the signal has to be “modulated” onto a carrier wave. The “sum” of carrier wave and signal is transmitted to the receiver which “subtracts” the carrier wave from the received oscillation and thus receives the pure signal.

When the radio transmission is analog, e.g. either the amplitude of the carrier wave or its frequency can change depending on the signal. Medium wave stations use the first method, frequency-modulation stations use the latter; this is the reason why these bands are referred to as “AM” (“amplitude modulation”) or “FM” (“frequency modulation”) in the Anglo-American language area.

More complex methods are used to transmit digital data, which will be described in the following.

“Orthogonal Frequency Division Multiplexing” (OFDM)

OFDM does not use one frequency to transmit its signal but it transmits on several hundred to several thousand channels very close to each other; however, only a narrow frequency band is available to each individual channel.

The massive parallel data transmission drastically reduces the data rate over each individual channel, i.e. much more time is available for transmitting the individual bits. Consequently, OFDM connections are significantly less susceptible to short-term noise or occurring echoes. Even in case of considerable path differences there is a high probability that a received echo is still associated to the same bit as the one currently transmitted via the “direct path”.\(^\text{11}\) The reduced transmission rate

\(^{10}\) [http://wi-fi.org](http://wi-fi.org)

\(^{11}\) In other words: The runtime difference remains lower than the duration of the transmission of one bit.
additionally ensures that the duration of short-term noise peaks is mostly shorter than the transmission of a bit.

The following figure shows the schematic principle of operation of OFDM (bottom) in contrast to conventional transmission (top): the use of several parallel channels (only 4 channels are shown for reasons of clarity; this number is significantly higher in practical operation) considerably increases the time interval $\Delta t$ available for the transmission of one individual character so that short-term noise or echoes by path differences are clearly of less importance.

**Figure 3-1: Orthogonal Frequency Division Multiplexing: Transmission of a “Hello, World” message**

The top of the figure shows the “conventional” way of transmitting, the bottom shows the transmission with OFDM. The representation clearly shows how the transmission time $\Delta t$ for an individual character is increased without compromising the overall data rate of the transmission.

OFDM is used in a large number of transmission methods, e.g. for ADSL, DAB (Digital Audio Broadcasting) or DRM (Digital Radio Mondiale).

**“Direct Sequence Spread Spectrum” (DSSS)**

DSSS, which at first glance takes the opposite way, is an alternative to OFDM: A sequence of pseudo random numbers (“chips”) is added to the data stream to be transmitted in such a way that the random numbers change much faster than the values of the data stream.

The receiver, which must know the “chips” (they can either have been generated by an encryption algorithm or previously transmitted separately), simply subtracts them from the received stream and obtains the unmodified signal.\(^\text{12}\)

This has several effects:

- Although only one carrier wave is used, the spectrum of the transmitted signal broadens superproportionally. Consequently, the effects of interferences that are limited to a very narrow range of the spectrum are less serious.
- Due to the use of pseudo random numbers, the transmitted signal, at first glance, appears as noise. In other words, it is not apparent to a listener that any transmission takes place at all.
- Even if a listener knows that a transmission is active, he can only listen in if he knows which sequence of chips was used by the transmitter.

Except for WLANs, DSSS is also used for GPS, UMTS and WirelessUSB.

---

\(^{12}\) This is of course a simplified representation and strictly speaking it is not an addition or subtraction but XOR operations of data with its keys.
The above figure illustrates the function of DSSS. A) The user data signal, B) the “chips” used for encryption. This is only a short sequence (red) that is continuously repeated. The bit string of the “chips” changes much faster than in the user data. C) The encrypted signal is identical to the chips as long as the user data signal is “1” (black sections); otherwise, it is created by inverting the chips (green).

In practical operation, the chips would be more complicated and a bit length which is a multiple of the chip length would not be used for the user data.

**Multiple Input/Multiple Output (MIMO)**

For this method, used for 802.11n expansion the sender and receiver must be equipped with at least two antennas. MIMO enables an increase of data throughput without more bandwidth or transmitter power being used.

There is a “smart” interconnection of antennas, i.e. not only does their signal correlate but also their phase. This enables creating specific constructive interferences which amplify the signal at the location (only there) of the receiver (called “beam shaped”). Multipath propagation of the radio waves is not interpreted as interference, but is used to yield a better reception.

Another option is using spatial multiplexing where both antennas send different signals on the same frequency. Using its own “smart” antennas enables the receiver to separate both signals; the interference pattern of the phase-correlated transmission causes the individual antennas to behave similar as directional antennas.
3.4 Comparison 2.4 GHz and 5 GHz band

3.4.1 The 2.4 GHz band

The frequency band at 2.4 GHz is a frequency range that can be used without a license in almost all nations. Since it is relatively inexpensive to manufacture transmitters and receivers, the 2.4 GHz technology is very popular and not only used for WLANs but also for numerous other applications.

Channel distribution

The 2.4 GHz band, as used in the 802.11 b/g standard, is normally divided into 13 channels, which have a distance of 5.5 MHz to one another. However, this does not at all mean that 13 independent frequencies are available for each WLAN.

For the used data rates of up to 54 Mbps, each individual transmitter uses a band with a width of more than 40 MHz. (See chapter 2.4.4) To exclude that the transmitters in the WLAN disturb each other, it is required that they keep at least this distance from each other. This reduces the number of frequencies that can be used independently of one another in practical operation to three: usually, only the channels 1, 7 and 13 (the “non-overlapping channels”) are simultaneously used for 802.11 networks.

![Figure 3-3: Schematic diagram of the envelopes of a transmitter in the 2.4 GHz band](image)

The above figure shows the envelope curve of a station transmitting on channel 7 of the 2.4 GHz band. The envelope of the spectrum taken up by it is displayed in blue. Non-overlapping transmission of other stations of the WLAN is only possible on the channels 1 or 13 (open envelope).

When many access points are used in a network, it is required that many channels that are independent of one another, i.e. non-overlapping channels, are used. In this case, it may be advisable to switch to the 5 GHz band of the 802.11 a/h standards, which offers a larger number of non-overlapping channels.

---

13 Compare the remarks on country approvals for the components; see chapter 8
14 Details of the permitted channels are different in every country. The topic is discussed in detail in chapter 8.
3.4.2 The 5 GHz band

For the 5 GHz band different numbers of non-overlapping channels are approved in the various regions of the world. The modulation method is OFDM (see 3.3). Generally 5 GHz waves are “harder”, i.e. the propagation behavior is similar to that of light beams: There is less diffraction around objects, the absorption is higher and the penetration depth lower than for 2.4 GHz waves. Generally, the practically achievable transmission range is a little less than in the 2.4 GHz band.

Compared with the 2.4 GHz band the 5 GHz band is clearly less “busy”, and there are only few interference sources in this range. An exception are military radar and satellite tracking systems, whose operators naturally are rather sensitive towards system interferences from a WLAN.

To harmonize the operation of 5 GHz WLANs with these systems the IEEE standard 802.11h (see 3.6) was created.

3.4.3 Comparison of the properties of the 2.4 GHz and 5 GHz band

Connection security, interference by other devices:

The great popularity of the 2.4 GHz band also results in the fact that a large number of devices that actually have nothing to do with WLANs also transmit in this range – these devices include microwave ovens as well as Bluetooth devices and cordless DECT telephones.

This may cause interferences and problems when setting up a WLAN. Depending on the interference source type, it may advisable to switch to the 5 GHz band.

In any case the optimal configuration of illumination, frequency band and antennas must be clarified by a radio field analysis prior to setting up the system. The tool to be used here is SINEMA E, see 11.1.

Data rate

The net data rate for both networks are in the same range of approx. 54 MBit/s. Since the 5 GHz band is less occupied by interference sources and has a higher number of overlap-free channels the 5 GHz band normally has a higher net data throughput.

Range

Mainly, the range of both systems is approximately equally high, within the range of 30 to 100 m; more when using directional antennas. However, 5 GHz systems suffer from severe dampening through obstacles, so that the actual range yield is slightly less than that of 2.4 GHz networks.

Size

Due to the shorter used wave length 5 GHz components of smaller size than 2.4 GHz modules can be produced. (This naturally does not apply for devices designed for operation in both bands (“dual-use”).)

Costs

Generally, 5 GHz devices are more expensive than 2.4 GHz devices due to the more expensive technology; however, today many components combine both technologies in one casing.

---

15 See also chapter 8. Current approval lists are available on the internet at http://www.siemens.com/simatic-net/ik-info
Licensing

2.4 Ghz as well as 5 GHz networks can be operated without license in most states.

3.5 IEEE 802.11e and WMM: “Quality of Service”

In the winter of 2005/2006, the IEEE adopted the 802.11e standard. This standard adds “Quality of Service” criteria to the existing network standards, i.e. a specific connection quality is guaranteed if this standard is complied with.

The quality is not only measured with the mean achievable data rate, but also upper limits for connection reliability, the duration of possible connection interruptions, etc. are defined. A convenient telephone connection, for instance, not only requires to transmit an appropriate quality of sound but also to ensure that dropouts and voice delays are within narrow limits.

While earlier 802.11 standards placed more emphasis on gross data rates than on “Quality of Service”, a standard explicitly including the concerns of QoS was created with the “e” variant.

WMM

“WMM” (“Wireless Multimedia Extensions”) are a subset of the 802.11e standard, which was defined by the “WiFi Alliance” to explicitly integrate multimedia services into the networks.

3.6 IEEE 802.11h and the 5 GHz band

The 5 GHz band is only used for few applications other than WLAN. One of these applications, however, is radar, whose operators are naturally quite sensitive towards possible interferences.

For this reason the IEEE 802.11h standard introduced modifications which can be used to minimize interferences between WLAN operated below 5 GHz and radar. The newly introduced technologies include “DFS” and “TPC”.

DFS (Dynamic Frequency Selection)

DFS describes the automatic switching to another channel if interferences, originating from a radar device, are detected on the current WLAN channel.

TPC (Transmit Power Control)

TPC reduces the transmission power of the nodes until the minimum for a reliable transmission with the configured data rate has been reached. TPC represents a compromise between secure communication and preventing overreach.
3.7 Other radio technologies

Apart from the IEEE 802.11 standard for WLANs there is also a number of different technologies which communicate using the radio network and which are used in the industrial environment.

3.7.1 Bluetooth

“Bluetooth” is the name for the IEEE 802.15.1 standard which describes the networking of small devices via short distances. Its main area of application is the application of cable connections between office devices such as PDAs, mobiles, computers, printers and other I/O.

Bluetooth works in the frequency range between 2.402 GHz and 2.480 GHz in the ISM band, hence collides with the 2.4 GHz band used by 802.11.

The Bluetooth networks (“Piconets”) are operated “ad hoc”, i.e. without infrastructure: stations log on or off according to demand and take on the role of a master or slave, however, they can swap these roles, and there is no station with a permanent management function comparable to that of an AP. A Piconet can comprise up to 8 active and 256 “parked” stations (i.e. stations in standby mode).

The maximal transmission power is 100 mW with a reach of maximal ca 100 m. (Most portable devices, however, transmit with a lower output in order to save batteries; typical ranges are therefore below 10 m). Data are here transmitted at a speed of up to 2 Mbit/s.

The standard is checked and further developed by the “Bluetooth Special Interest Group”16.

Further information

To obtain further information on this topic, please use the following URL:
http://german.bluetooth.com/bluetooth/

3.7.2 Wireless HART

HART (“Highway Addressable Remote Transducer”) is a fieldbus communication standard which as “WirelessHART” also defines the wireless communication (based on IEEE standard 802.15.4).

WirelessHART also uses the ISM frequency band (2.4 GHz with maximal 250 kBit/s) and builds automatically meshed networks whose extend can be considerably larger than the nominal radio reach of an individual station (ca 200 m). The network organizes itself by evaluating all connection information from one network manager, and this information is used to automatically provide redundant paths which can bridge individual failed nodes.

The focus during the development of WirelessHART was the simple commissioning and maintainance of the self-organizing networks, so that the configuration caused only minimal workload. This comes at the price of real-time capability; i.e. no response times are guaranteed with WirelessHART.

The main application area of WirelessHART here is the regular transmission of lower, non-time critical data volumes in large distances (typically between approx. 15 seconds and several hours) over relatively large distances. Through low energy consumption battery runtimes of several years can be reached, i.e. the

16 http://www.bluetooth.org
WirelessHART stations can be "left to themselves" once they have been installed. The protocol is very robust and at sufficient illumination of the meshed network it automatically "mends" the failure of intermediate stations. WirelessHART is managed by the “HART Communication Foundation”\(^\text{17}\) (HCF).

Further information
To obtain further information on this topic, please use the following URL:
http://www.hartcomm2.org/hart_protocol/wireless_hart/wireless_hart_main.html or

3.7.3 Zigbee

Like WirelessHART, Zigbee is also based on IEEE standard 802.15.4 and also uses the ISM band at 2.4 GHz. As opposed to HART the focus here is not on the industrial environment, but on the field of facility automation and household technology where the aim is to install devices in areas which are hard to access, which can remain in operation with out maintenance for years (electricity or heat meters, light switches, etc.).

The Zigbee protocol is less "robust" than that of WirelessHART, and if a central controller fails the communication of the entire network may be compromised. In return Zigbee offers lower reaction times and is therefore also suitable for real-time applications.

The Zigbee standard is under the control of the Zigbee alliance \(^\text{18}\), which also provides further information on this topic.

3.7.4 AeroScout

AeroScout is a technology which combines the classic application areas of RFIDs (locating, identification, tracking) with WLANs.

The AeroScout-RFID tags send signals in the 2.4 GHz band (IEEE 802.11 b/g), which are received by access points which manage a conventional WLAN. The tags can send their homing signal automatically in regular intervals or after request from an “exciter” where the exciters in return are controlled by the AeroScout engine, a software application whose PC is connected with the access points via cable based Ethernet. The access points then return the signals received by the AeroScout tags to the AeroScout engine. The engine can now compute back to the position of the AeroScout tag via runtime differences (TDOA) or the received signal strength (RSSI) of the various APs.

\(^{17}\) http://www.hartcomm.org/
\(^{18}\) http://www.zigbee.org/
Figure 3-4: Schematic function of an AeroScout system: 1) The AeroScout engine running on the PC sends a trigger signal to the exciters, 2) the trigger is transmitted to the AeroScout-RFID tag, 3.) the tag responds with signals received by the involved APs and 4.) are sent back to the engine, which determines the position of the tag from differences in runtime or signal strength.

The precision achieved this way – depending on how accurately the shape of the radio field is known – is between 5 and 10 meters; using exciters it can be increased up to 20 cm. If the tags are equipped with a sensor they can also transfer measured values such as temperature or humidity.

The main application area is the tracking of persons or objects moving freely within a limited area (detected by the radio field of the APs). This makes AeroScout suitable for tracking persons, simple logistic tasks (where is a certain object located?) and facility monitoring (is the temperature in this room within the permitted range?) especially in the manufacturing and health sector.

AeroScout is a proprietary product of AeroScout inc.19

The SCALANCE W access points W784/W786/W788 (see 9.2) are compatible with AeroScout as of firmware version V 4.0.14. For setting up an AeroScout network only the software engine as well as the exciters are necessary apart from the tags and access points. The configuration of the access points is literally restricted to activating a checkmark, which directs the APs to forward the data packages of the tags to the engine PC.

19 http://www.aeroscout.com/
4 Topology, Configuration and Organization of IWLANs

Here you can learn about...

... options to structure WLANs, the advantages and disadvantages of the networks set up as described and the possibly required hardware. You are introduced to the division of a network into radio cells and the use of clients and access points.

4.1 Radio Cells and the Transition between Cells: “Roaming” Method

Disadvantages of unstructured radio networks
As we have seen in section 2.4.3, the range of radio transmitters is limited in practical operation. Generally, the area you want to cover by a LAN will be too large to be reliably “illuminated” by one single transmitter.

Even if it was technically possible to set the transmitter power high enough for all nodes, this would not be desired in many cases. If the LAN nodes were, for example, arranged along a straight line, an unnecessarily large area on the left and on the right of the line would be illuminated, and it would be easy for third parties to install additional receivers and to listen in on the radio communication without being noticed.

Structuring radio networks by radio cells
Furthermore, it is more economic to divide the WLAN into individual cells since only one station can send on each channel at any time. If several cells are available, an active transmitter can be located in each cell and the actual data throughput increases.

Figure 4-1: Division of a WLAN into radio cells

The above figure shows the same WLAN without division into radio cells (left) and with division into two cells (right, the cells are red or green). The shaded areas show the respective necessary expansion of the radio transmission ranges. Third parties can theoretically listen in on and disturb the radio communication only within these areas; the area is significantly reduced by using radio cells (right).

---

A simple ad hoc network (see 4.3) is assumed without access points and clients (see below).

4.1.1 **Connection of individual radio cells: “Access points” and “clients”**

The use of “access points” is required to control the communication in a cell or to connect several radio cells. Their position within the WLAN is comparable to the position of switches for cable-based networks.

**Administrative function of access points**

If there is only one radio cell or if the communication occurs only within one cell, the access point can be used to coordinate the communication within this cell.

When using encryption methods, it can either grant or deny clients access to the network (see section 5). The access point can meet real-time requirements for the communication by controlling and coordinating the data communication in the network and by assigning periodic “time slots” to the individual clients within which they can transmit their data without being disturbed (see section 4.4).

**Access points as a “backbone” of the communication**

On the one hand, each of the access points in a WLAN that consists of several radio cells communicates with all regular nodes of its cell, the clients – regardless of whether they are stationary or mobile. On the other hand, the access points of a WLAN maintain the connection to one another either via cables or by means of a second, independent radio network\(^2\) and thus enable the communication beyond the limits of the radio cells.

Figure 4-2: Using access points and clients in radio cells

The figure shows the division of a WLAN into three radio cells (yellow, blue, green).

---

\(^2\) This is the reason why some access points have two radio interfaces via which they can simultaneously communicate via two different frequencies.
with a number of clients and one respective access point. The red arrows follow the communication path between a client of the yellow cell and a client of the blue cell.

4.1.2 Motion of clients between the radio cells: “Roaming”

The situation becomes more complicated if the clients are to be allowed to move: The clients do not only have to be located within one of the radio cells along their path at any time: what happens when they leave one radio cell and enter the other?

This process of roaming obviously requires an overlapping of the individual radio cells. If all radio cells used the same frequency, a client in the overlapping area would permanently have faulty reception. (See section 2.4.4)

To avoid this, adjacent radio cells should communicate on different channels.

Problems developing from roaming

A problem related to roaming is that a relatively long time is required to

- detect the leaving of the old radio cell by a client and
- to establish its connection to a new radio cell.

This “handover” typically lasts only several hundred milliseconds; this time is too long for many industrial applications. For this reason, the introduction of special methods (e.g. iPCF, see section 4.4) is required to enable “rapid roaming” with acceptable interruption intervals.
4.1.3 “Hidden node” problem

The expression “hidden node problem” refers to a configuration in a WLAN in which two nodes of a radio cell cannot “see” each other (i.e. they are not in the mutual range). If, however, both try to communicate with a third node which is located between them (and which simultaneously has contact with both transmitters), conflicts occur. In particular, the two transmitters cannot detect whether the respective other is also transmitting at the same time.

Figure 4-3: “Hidden node” problem

An illustration of the hidden node problem is shown above: nodes A and C are located outside the range of the respective other node, but both can communicate with a common partner B (radio transmission range: shaded circle).

While A, for instance, transmits to talk to B, C keeps the frequency free and possibly starts transmitting itself, which prevents the reception of both messages. Neither A nor C can easily determine that their transmission has failed.

The solution is to configure B as an access point and to adapt the protocol in such a way that B – the only node in contact with all transmitters – “assigns” transmission slots to the other network nodes within which they are allowed to transmit. See also the RTS/CTS method in section 4.4.4.

4.2 Infrastructure networks

The operation of WLANs with the aid of coordinating access points is referred to as “infrastructure mode”. This mode is thus contrary to the – rarely used industrially – ad hoc networks (see 4.3) which do not have a central access point.

The following sections show several examples of infrastructure network topologies.

4.2.1 Stand-alone networks

Stand-alone networks consist of a number of clients which are all located in the radio cell of one single access point. The function of the access point is limited to the coordination of the client communication.
Figure 4-4: Example of a stand-alone network.

The above figure shows such a stand-alone network. It includes an access point which coordinates the data communication of the other bus nodes and via which the entire traffic is directed. The access point determines the "SSID" ("Service Set Identifier") of the network, its "name". Only a client that knows the SSID of the access point can log on to it.\(^{22}\)

It is not necessary that all network nodes of a stand-alone network have direct contact; but hidden node problems (see 4.1.3) may occur if this is not the case. The maximum expansion of such a network is limited by the condition that all clients have to be located within the range of the access point (circle shaded in green).

### 4.2.2 Mixed Networks

In mixed networks, the access points are not only used for the communication of the clients but they additionally provide the connection to a cable-based network. (This cable-based network is normally Industrial Ethernet.)

Several access points can be connected to the cable-based network. This means that the access points generate several radio cells. If these cells cover a specific area completely, the clients located in this area can move from radio cell to radio cell (so-called "roaming", see 4.1.2).

\(^{22}\) This is only a very weak and by no means sufficient protection from unauthorized network access.
Mixed networks allow roaming, i.e. the change of a mobile node from one radio cell to a neighboring cell (see above, dotted arrow). WLANs set up as described above can theoretically reach any size. Interferences with reception may occur within the overlapping range of the radio cells since the access points operate on the same frequency.

### 4.2.3 Multi-channel configuration

The multi-channel configuration corresponds to the mixed network (see 4.2.2), however, the individual access points operate on different, non-overlapping radio channels (see 3.4). This ensures that interferences no longer occur where radio cells overlap.

At the same time, roaming, thus the change of a client from one cell to another, is facilitated, which results in a considerable increase in performance.

In this configuration, the individual access points form a backbone and are connected to one another via a cable-based network (e.g. Industrial Ethernet). It is possible that the access points are the only nodes of the Industrial Ethernet.

In practical operation, this configuration is most frequently used for WLAN and is normally selected.
The above figure illustrates the principle of operation, compare also Figure 4-5. The different frequencies on which the access points transmit are indicated by hatchings in different directions.

### 4.2.4 Wireless Distribution System (“WDS”)

WDS (“Wireless Distribution System”) corresponds to the multi-channel configuration (see 4.2.3) – except for one important difference: The access points do not maintain the connection to one another via a second medium (Industrial Ethernet cable in the case of the multi-channel configuration) but via the radio network.

Two properties ensue, which characterize the WDS:

- The distance between the access points must be small enough to ensure that every access point is located within the range of its communication partner.
- If there are two access points, the effective data rate is halved since the bandwidth has to be split between the client-access point communication and the communication among the access points. If more than two access points are used, the effective data rate continues to decrease.
4.2.5 Redundant wireless LANs

This mode requires the use of access points which feature two radio interfaces and which can thus simultaneously transmit on two frequencies.

Basically, the setup corresponds to the setup of the Wireless Distribution System (see 4.2.4), however, the access points not only communicate on the primary frequency but also on a second channel with a second set of antennas.

This ensures high connection reliability in combination with high data rates: Even if a frequency range is temporarily interrupted by interfering nodes or shadowing or interferences, it is highly probable that a connection is still possible via the other channel.
4.3 Ad hoc networks

For this form of network there is no access point as opposed to the infrastructure networks discussed in section 4.2. The clients communicate with a server or with each other and establish connections on demand.

An example for such an ad hoc network is shown below. The spatial expansion and security of the WLAN is narrowly confined by the fact that there is no higher-level management structure nor any forwarding of messages.

Ad hoc networks practically require no configuration load, however, they have a number of considerable disadvantages:

- Obviously, the expansion of such a network is limited to the fact that all clients are still located in the mutual range of the radio signals. There are no cells via which a message can be routed and no access point which would fulfill this function.
• Ad Hoc networks are limited to the IEEE 802.11b standard (see 3.2.1) and can communicate with a maximum of 11 Mbps. They are thus only suitable for networks with a small number of nodes and lower data volumes.

• Security options against unauthorized intrusion are poor. For example, only old and insufficiently evaluated WEP mechanisms – see 5 – are permitted as authorization methods.

• There are no mechanisms for access control or prioritizing of messages. Real-time capability or “Quality of Service” can therefore not be reached via ad hoc networks.

While the restrictions for home networks may be acceptable, it is urgently recommended for these reasons to only operate industrial WLANs in one of the infrastructure modes.

4.4 Advanced management functions

4.4.1 VLANs (“Virtual LANs”)

The segmentation of a physical network into several logic, “virtual” networks can be performed for cable-based as well as radio networks. Today VLANs normally follow the IEEE 802.1Q standard.23

Segmentation of the data traffic

Here the Ethernet data packages (“frames”) are expanded by one data block (a “tag”) which contains a VLAN-ID. The switches (or access points) of the network forward the message only to those respective receivers which are members of the VLAN to which the message is addressed. The assignment normally occurs “static” by means of the port via which a message leaves the switch: the ports of the switches are in this case assigned to individual VLAN. (Other options are “dynamic” assignment using the IP receiver address, the MAC address of the receiver, or the protocol (http, ftp, VoIP, etc.) served by the message.)

Advantages

Using VLANs has a number of advantages:

• Configurations errors remain restricted to the VLAN, in which they were made, and can no longer bring down the entire LAN.

• Broadcasts, i.e. transmissions to a general circle of receivers, are no longer performed via the entire LAN but only via the respective VLAN; this reduces the network load.

• The individual VLANs can have various priorities assigned to them for preferred transportation of messages from high-priority stations.

• In contrast to using IP subnets, the stations of different VLANs can have the same IP addresses. This makes better use of the restricted IP address space and production cells of identical structure can be configured with identical IP addresses, which reduces configuration and administration expenses.

23 Older protocols such as ISL (“Inter Switch Link”) and VLT (“Virtual LAN Trunk”) have become insignificant today.
4 Topology, Configuration and Organization of IWLANs

- The VLAN configuration is transparent for the end node, i.e. the end nodes do not know to which VLANs they belong and can neither listen in on their data traffic. This achieves a certain security of the network.

Further information in the SIEMENS I IA Portal

Regarding this topic the SIEMENS I IA Service & Support portal contains
- as well as an application with focus on Quality of Service in WLAN: http://support.automation.siemens.com/WW/view/en/32174160

4.4.2 VPNs (“Virtual Private Networks”)

VPNs serve as connection between two LANs, an end node with a LAN or two end nodes with each other or with a server, where a network of any different kind is located between both VPN nodes. Depending on the type of node the VPNs are referred to as “End-to-End-VPN”, “End-to-Site-VPN”, etc..

Prerequisite here is a gateway at the connection location between the VPN areas and the connecting network. The gateway “packs” the frames of the VPN nodes as user load of a frame as valid in the connecting network. At the target VPN in return the user load is unzipped by a second gateway.

VPN tunnel

The “piggyback” transport of the user load frames makes the VPN configuration transparent to end nodes. They cannot recognize the type of connecting network existing between them.

If the gateways encode the user load during the transmission, the data traffic can no longer be listened to from outside: this is referred to as a “tunneling” of VPNs. Common encoding methods are e.g. IPsec (“Internet Protocol Security”) or TLS/SSL (“Transport Layer Security/Secure Socket Layer”)

24 The role of such a gateway can, for example, be taken on by the SCALANCE S security modules.
Advantages

The on hand advantage of VPNs is of course that they allow establishing a connection between two subnets by using an existing network, even if it is set up differently: it is no longer necessary to create a new infrastructure.

However, even if the end nodes are located in a homogenous environment (when the connecting network has the same structure as that of the end nodes and a connection without VNP would be possible in principle), using the encoding and authentication measures enable establishing “secure” network sections, interconnected by potentially “unsecure” sections. An attack on the unsecure network can in this case no longer compromise the security of VPNs.

The nature of the tunnel method also enables directing any services (http, ftp, …) via the VPNs. The VPN has the same effect on the end nodes as if they were directly connected with each other.

Typical application cases from the office world

A typical application case for VPNs is the Home Office, for which the PC of the employee working from home tunnels into the company network via a VPN. There he has secure access to the intranet and local drives, even though the medium via which the access is provided is principally unsecure.

Also, several company locations can be interconnected via VPN, or servers tunnel via VPN to compare their common database. In both cases the tunnel procedure secures sensitive data traffic from unauthorized third-party access.

Further information in the SIEMENS I IA Portal

Further information on the topic of “VPNs in cable-based networks” is available in the SIEMENS I IA Service & Support-Portal under entry ID 22056713:

4.4.3 RSTP (“Rapid Spanning Tree Protocol”)

Redundant networks are networks in which messages are forwarded between the end nodes via switches, where the connection between each pair of end nodes is made via more than one path. Such a network can be cable-based or wireless; in the latter case the access points act as switches.

Forwarding the messages via each possible connection would cause unnecessary network load and clog the network. It makes more sense if the switches or access points determine the optimal paths between the end nodes and forward the messages only along this route. They only use an alternative path if the optimal route has been disrupted by interferences or device failures.

“Spanning Tree Protocol”

For this purpose the “Spanning Tree Protocol” STP was developed as IEEE standard 802.1D.

In addition to regular data traffic the switches interexchange particular BPDUs (“Bridge Protocol Data Units”). The BPDUs list the MAC addresses of the sender and the forwarding switches. By evaluating this information the self-learning switches can develop a “map” of the network and learn which data paths are available.

Which path is optimal is determined by means of two criteria:

- Principally the path is preferred which contains the lowest “path costs”. The path costs are here inverse proportional with the data rate of a connection.
- If the path costs of two connections are equal, the route with higher priority is selected. This priority of the individual ports is configured at the switches themselves.

In regular operation all messages run via the optimal path.

Rapid Spanning Tree Protocol

One advantage of the STP is that during an disruption or a device failure the network must reconfigure itself: the switches only start negotiating new paths at the moment of the disruption. This process takes up to 30 seconds; such a period is not acceptable for many automation processes.

For these reasons STP was expanded to the “Rapid Spanning Tree Protocol” (RSTP, IEEE 802.1w). The main difference compared with STP is that the switches already collect information of alternative routes at the time of undisrupted operation, which they then need not obtain after a failure has occurred.

This enables reducing the reconfiguration time for an RSTP controlled network to a few seconds.

Further information in the SIEMENS I IA Portal

Further information on the topic of “RSTP in wireless LANs” is available in the SIEMENS I IA Service & Support-Portal under entry ID 30805917: http://support.automation.siemens.com/WW/view/en/30805917
4.4.4 IWLAN management functions DCF and PCF

The abbreviations DCF and PCF describe two different methods of processing the data communication in radio networks, which are planned in the 802.11 standard. DCF can thereby be expanded by the RTS/CTS mechanism for preventing collisions.

DCF (“Distributed Coordination Function”)

In DCF, all nodes are always “responsible for themselves”. A node only starts transmitting if no other signal is pending on its frequency and a receiver, which has received a message intended for it, sends a confirmation message with which the transmitter detects the success of the transmission.

DCF does not guarantee that a specific data volume is transmitted within a maximum time interval. For this reason, it is primarily suitable for asynchronous data transmission (such as e-mail or web browsing).

The use of DCF does not prevent the occurrence of hidden node problems (compare section 4.1.3). The data throughput of some DCF network configurations can be increased by using the RTS/CTS method.

“RTS/CTS” method for collision avoidance

To avoid “collisions” – the attempt of two transmitters to simultaneously access the frequency – the RTS/CTS method is available.

A transmitter that wants to transmit a(n) (extensive) data frame registers this by sending a (short) “RTS” (“ready-to-send”) to inform on its request to transmit before sending the data frame. It only actually transmits the data frame if it receives a “CTS” (“clear-to-send”) as a response.

With the aid of this method, the number of necessary transmission repetitions is considerably reduced since the collision is detected already before sending longer data packets. However, the overhead produced by the RTS/CTS frames can reduce the achievable data throughput.

PCF (“Point Coordination Function”)

The abbreviation PCF describes an access method defined in the 802.11 standard; however, the implementation of this method is not mandatory. The method is suitable to avoid some of the disadvantages of the DCF method.

In PCF, not all network nodes have equal rights but one or several access points act as central administrators in the network. An access point then assigns time slots to the other nodes, the clients: within these slots the frequency is reserved for these clients and they can transmit without being disturbed.

PCF enables to assign regular network access to the clients and to ensure the transmission of data within a specific period. For this reason, PCF is preferably suitable for applications requiring continuous data flows. (Synchronous data transmission, e.g. video or audio streams and, of course, also process values.) The achieved transmission periods, however, are in the range of several hundred milliseconds and also the speed of the change from one radio cell to the next does not meet real-time requirements.

But it is possible to have networks change between DCF and PCF at intervals if this is required by the communication.

In practical operation, PCF is rarely supported by manufacturers.
5 Data Security and Data Encryption according to IEEE 802.11i and 802.1X

Here you can learn...

... about the aspects to be observed in the securing of IWLANs, and how to protect your radio networks from unauthorized listening or access by a third-party.

5.1 Basics on security in radio networks

WLANs can easily create a feeling of insecurity with the user, as it is not necessary for an intruder to access a factory site in order to connect to a switch and listen to the data: in principle, anybody located within the radio range can listen to the data traffic of a network. However, this assumption is misleading as today there are hardly any cable-based isolated LANs: in reality, most LANs are connected with the internet and so they are potentially subject to attacks from outside. Security must be intentionally configured for radio networks as well as for cable-based networks. Due to advances in security standards and capability of the components the radio networks today can be considered as secure as cable-based networks.

Simple measures

One of the simplest measures of securing a radio network consists, for example, in configuring the access points and their transmission performance so they actually only cover the required space and no overreach occurs. This restricts the radio network to the company site and prevents listening from outside.

VPNs (see 4.4.2) already provide an advanced protection from listening and manipulation from a third-party, however, increased configuration expenses and the use of special client software is cost-intensive and causes the usage of the network being complicated and impractical (due to the necessary separate login).

Advanced measures

A reduction of the radio power can of course only provide a limited protection and cannot be realized on any scale. An advanced, more effective and secure method is selecting a suitable infrastructure (for example not using ad hoc networks where principally any computer can gain access to the network 4.3 and 5.3), as well as the application of powerful encryption and authentication protocols as described below.

5.2 IEEE 802.11i and IEEE802.1X

Data traffic: 802.11i

Task group 802.11i of the IEEE is concerned with the security of data transmission via WLANs, in particular with the definition of encryption algorithms for wireless transmission.
The following table shows a simplified overview of the used methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Encryption</th>
<th>Stream cypher</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP</td>
<td>RC4</td>
<td></td>
<td>out of date</td>
</tr>
<tr>
<td>WPA</td>
<td>TKIP</td>
<td>RC4, AES</td>
<td></td>
</tr>
<tr>
<td>WPA2</td>
<td>TKIP + CCMP</td>
<td>AES</td>
<td></td>
</tr>
</tbody>
</table>

**Authentication: 802.1X**

Standard IEEE802.1X does not define the encryption of the data traffic between access point and client, but the login procedure as well as the assignment of access rights for clients. The RADIUS protocol is used for this (see 5.2.3). In form of “PSK” (“Pre-Shared Key”) this is used for smaller home/office networks and as “EAP” (“Extensible Authentication Protocol”) for larger networks.

### 5.2.1 WEP (“Wired Equivalent Privacy”)

WEP is the oldest and at the same time the least secure encryption method with which WLAN transmissions are protected against unauthorized intruders according to the 802.11i standard.

This method uses a user password that is used as a key to generate a sequence of pseudo random numbers. Each character of the message to be transmitted is then encrypted or decrypted with the next number from this sequence at the receiver.

The method is relatively simple and can be compromised comparatively easily in two ways: on the one hand, the key must be exchanged between sender and receiver when establishing the connection; this exchange is, of course, unencrypted.

On the other hand, statistical methods can be used to determine characteristics from the transmitted message traffic, which again enable to draw conclusions about the used key as long as there is an adequate number of messages for the analysis.25

Using appropriate tools the data traffic in WEP encrypted networks can be decrypted within a few minutes. For these reasons, WEP is generally no longer considered to be adequately secure.

### 5.2.2 WPA and WPA2

WPA (“Wi-Fi Protected Access”) and TKIP (“Temporal Key Integrity Protocol”)

WPA is the development of WEP and still considered as a standard despite several shortcomings. The protocol was adjusted and made more secure by various new methods:

- **TKIP**: for encoding the “Temporal Key Integrity Protocol” uses a key as well as an additional initialization vector. Various combinations of initial key and initialization vector makes the encoding work as if the key was continuously changed which make decryption difficult.
- The MAC address (i.e. the unique hardware identification) of the sender is incorporated into the key, which makes it additionally complicated to falsify the sender of messages.

25 Frequent manual change of the key by the user would increase security, however, in practice this is rarely pursued conscientiously.
The development of an encryption algorithm that was supposed to replace WEP by IEEE task group 802.11i was delayed so that the “Wi-Fi Alliance” recommended the application of WPA as a subset of the 802.11i standard as an interim solution. In the meantime, this has been rendered invalid with the adoption of the 802.11i standard and WPA2 or AES and TRIP are available as methods of first choice.

WPA2 and AES (“Advanced Encryption Standard”)  
After adopting the complete 802.11i standard, this standard was applied by the “Wi-Fi Alliance” as “WPA2”. The essential difference between WPA2 and WPA is the encryption method: the shortcomings that were identified in the meantime in WPA no longer exist in the AES method used in WPA2.

- **AES**: like WEP, “Advanced Encryption Standard” exercises the “adding up” of a key to the message. One block of the raw data is processed with the corresponding identical key, but several processing sequences with respectively varying block boundaries take place.

When selecting “reasonable” passwords with an adequate length that cannot be guessed, AES and TKIP encrypted messages are considered to be impossible to crack, according to the present state of the art (autumn 2009).

EAP (“Extensible Authentication Protocol”)  
EAP is a widely used framework for different authentication methods for network access. In other words, the actual EAP is not an authentication method but describes the mechanism according to which client and server can agree on a method.

One of the methods that can be used under EAP is “EAP-TLS” (“EAP-Transport Layer Security”) in which the network nodes have to be “certified” before they are authorized for the network communication, i.e. they must be authenticated at a central server. This method is comparable to SSL familiar from the internet. Aside from this method, a large number of other, partly manufacturer-specific, protocols exist that can be used under EAP.

Mac filters  
MAC addresses (“Media Access Control A.”) are codes with which hardware elements (such as network cards, modules, motherboards) can be uniquely identified worldwide.\(^{26}\) The addresses normally comprise 6 bytes (48 bits) and are “hard-wired” in the corresponding components; upon request, the components identify themselves by returning their MAC address.

In the network management, filter tables with mac addresses can be created which allow or forbid access to specific addresses. This way enables to implement a simple, albeit comparatively insecure access protection for the network.

\(^{26}\) The abbreviation “MAC” was originally used for managing the media access itself, hence for the protocol used for negotiating who, at what time has the send authorization – whereas the nodes were identified by their MAC addresses. Both meanings must be separated.
5 Data Security and Data Encryption according to IEEE 802.11i and 802.1X

It cannot be excluded that mac addresses are manipulated (so-called "spoofing") so that mac filters only offer adequate protection for a network in connection with other measures.

5.2.3 RADIUS protocol

The RADIUS protocol ("Remote Authentication Dial In User Service") for the authentication at the network was originally developed for cable-based systems, however, it has also proven itself especially in the radio sector.

For RADIUS there is a central so-called RADIUS server, which contains a lost with access authorizations of all nodes. If a client wishes to connect to the network, the access point forwards the request to the RADIUS server. It reacts be generating a “Challenge”, i.e. a request for which the client can only send the appropriate “Response” if he has the password saved on the RADIUS server.

This method has two advantages:

- The password is never sent via the network in plain text, neither can it be intercepted by somebody without authorization.
- Since the access authorizations are saved on a central server, the method is particularly suitable when using roaming clients. Not all access points need to store the access data of the clients, but they can request them any time at the RADIUS computer.

Further information in the SIEMENS I IA Portal

Further information on this topic is available in the SIEMENS I IA Service & Support-Portal under entry ID 30805917:


5.2.4 Security functions and data rate

Please note that the increasing complexity of the encryption methods generates an increasing transmission overhead and consumes more computing time of the nodes which may reduce the effective data rate.

If a WLAN has to be operated with a very high performance (data throughput and response times, e.g. PROFINET I/O), it may become necessary to use an encryption method that is less secure but resource-saving.

Further information regarding SCALANCE w devices is available in chapter 9.1.3
5.3 Attack scenarios

Compromising the safety concept

The security concept of a WLAN can unintentionally be compromised in several ways:

- **Access Points configured with errors**. Access Points which were connected with the cable-based network by an internal user, but contain a configuration error. If, for example, no security settings were made, the respective access point provides a free network access for all.

- **Ad hoc wireless network**. Operating systems such as Windows enable configuring networks consisting of several wireless clients without the access point in between. If one of the computers is configured so that it forms part of an ad hoc network and also establishes connections with the company WLAN it may provide unintentional access for hackers.

- **Faulty client connections**. If companies are located within direct physical vicinity, the company WLANs most probably use the same network information. In this case a wireless client connects with the first accessible access point. However, if it is part of a neighboring WLAN, this may cause a security risk.

Attack methods

Malicious users can often benefit from the above described security gaps. However, the following examples also describe scenarios in which you can create your own WLAN accesses:

- **Rogue Access Points**. An illegal access point connects with the cable-based network and creates free LAN access for malicious or unauthorized users.

- **Honeypot Access Points**. Some hackers are capable of determining the configuration settings of WLANs and use an access point with the same settings within network reach. Through this intentional faulty connection the clients create a connection with these "honeypots" assuming that they are contacting an official access point. Intelligent hackers can make use of this by connecting network resources with the AP, which act as bait so that the users log on as usual and so give the hacker the opportunity to take unauthorized possession of passwords or confidential documents.

- **Access Point MAC Spoofing**. Wireless client computer can be configured as access points. This way a hacker can abuse a normal PC as honeypot.

Manipulation options

If a hacker has found its way into the network – either through an existing gap or by creating a gap – there are various options of manipulating the company network:

- **Unauthorized client accesses**. Hackers search permanent access options in wireless networks. If a network has a weak, or non-existent user authentication, access to the company network is made very easy and the hackers can retrieve information or attack resources, leading to failures.

- **Denial of Service ("DoS")**. Networked devices must react to all client requests. Hackers use this property by flooding a network resource with more requests than they can handle. Distributed DoS attacks increase the problem by preparing a number of “ignorant” computers using a hidden code, which then simultaneously perform DoS attacks of a possibly enormous extent.
• “Man in the Middle”. For unprotected data hackers can intercept messages and manipulate contents by disguising themselves as nodes on the travel path of a communication connection.

• IP Spoofing. By manipulating the source IP address in the package header a hacker can access traffic of a correctly authenticated user and pretend that the user uses the computer of the hacker. Subsequently all data and messages of the server go back to the hacker.

• Hijacking. Using software secretly installed on the PC of a company user, a hacker can take control over the affected computer and gain access to the resources which the user can access, or damage servers or other computers.
6 Proprietary Expansions of the IEEE 802.11 Standard

Here you can learn…

...which expansions of the WLAN standard IEEE 802.11 is provided to you by the SCALANCE devices of SIEMENS. The chapter describes the new application options and capabilities of radio networks resulting from the application of these technologies.

6.1 “iPCF” ("Industrial Point Coordination Function") and Rapid Roaming

iPCF developed by SIEMENS provides a proprietary alternative to PCF, which solves a number of problems related to PCF and allows rapid roaming.

Rapid roaming is a change of a client from one radio cell to another, during which the log-off and new logon of the client ("handover") happen so quickly that the real-time requirements of the communication are still complied with.

In iPCF, the access points poll the clients in their radio cell at regular, very short intervals. They can register their requirement to send longer data frames, however, they only start sending after having received the permission by the access point.

These properties result in the following effects:

- The access point can be parameterized to perform the pollings in a very fast sequence. This results in very short guaranteed response times (deterministic transmission): The response times can be reduced to about 2 ms per network node, i.e. a response time of less than 10 ms is guaranteed for 4 clients.
- The transmission of larger, non-time critical messages is delayed until free cycle time is available.
- Due to the short polling cycle times, a client detects very quickly if it has lost contact with its access point and it can reestablish the connection to an alternative access point very quickly. The "handover" times when changing from one access point to another are typically 20 ms – 30 ms and thus approximately one tenth below the period required by PCF.
- Quick handover is further accelerated by simplified re-logon or authentication methods.

iPCF provides particularly industrial applications with medium real-time requirements in the two-digit millisecond range with WLAN-capability. This field also includes the wireless connection of PROFINET IO devices.

A disadvantage of iPCF is merely the loss of compatibility with components which are not iPCF-capable. "Mixed networks", in which a part of the devices is connected via DCF/PCF, are no longer possible with iPCF.

Optimal performance with iPCF is achieved when using RCoax cables. For movable nodes in communication with stationary RR access points the application of iPCF-MC is recommended (see 6.4).

Further information

Further information on this topic with particular regard to SIMATIC products is given in chapter 9.5
6.2 “iHOP” (“industrial Hopping”)

iHOP is an adaptive frequency jump method, where the access points and their clients simultaneously change the used transmission channels in regular intervals. The pattern of the jumped channels is given by the access point here. This ensures that the failure of a single channel – no matter how long it lasts – can only interrupt the communication for a short time, i.e. until the next planned frequency jump. The mechanism yields a maximal data throughput in environments where it is difficult to foretell how the reception conditions of individual frequencies change.

iHOP is controlled by the access point. It monitors the connection quality to the individual channels and agrees a time schedule with the client regarding the frequency usage, for which channels with high connection quality are preferably used. During an unexpected failure on the currently used channel the client and the access point simply let the affected transmission interval pass and communicate again after the next frequency jump. This means that an interruption takes rarely longer than a transmission interval.

Figure 6-1: Scheme of the iHOP channel jump method

The iHOP method is available in 2.4 GHz as well as 5 GHz, and the channel jumps also change between both bands.

“Mixed networks”, in which one part of the senders support iHOP and the other part is connected via DCF/PCF, are no longer possible. Either all nodes are configured or iHOP or none.

iPCF and iHOP cannot simultaneously be operated on the same frequencies. (The underlying objectives are also different – minimal roaming times for iPCF, optimal data throughput for iHOP.)
Restrictions

While iHOP generally improve the capacity of the radio connection, it still cannot guarantee minimum roaming times (see below). For this reason iHOP is not suitable for the operation with PN I/O. At the same time iHOP is restricted to a maximum of 8 clients per access point.

All SCALANCE W devices with rapid roaming capability (“RR”, see 6.1) can also be operated in iHOP. The IWLAN PB link (see 10.3) works with iHOP however, not together.

Roaming in iHOP

In iHOP the roaming method differs in some points from the normal procedure in 802.11:
Roaming is initiated by the client as soon as

- the signal strength of its access point falls below a certain threshold value, or
- neither regular data frames nor synchronization frames point are received by the access point for a certain period of time.

The client then connects with the first access point from which it receives a signal. (It does not optimize in searching the best access point.)

6.3 “iQoS” (“industrial Quality of Service”)

“Quality of Service” generally refers to a guaranteed certain minimal data throughput and a maximal interruption period for a connection; these guarantees can not be given in conventional 802.11 connections. QoS is reasonable for applications where data flows are transferred (Multimedia, VoIP), but also in the industrial environment where each connection interruption is valued as security risk an may lead to the immediate shutdown of a plant.

iQoS (“QoS in the industrial environment”) is a 802.11 compatible expansion with which certain data rates and reaction times can be secured.

In conventional IEEE 802.11 networks the individual clients send their data according to demand:

**Figure 6-2: Data traffic in conventional IEEE 802.11 networks without prioritizing**

<table>
<thead>
<tr>
<th>No data rate reservation</th>
<th>IEEE 802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client 1</td>
<td></td>
</tr>
<tr>
<td>Client 2</td>
<td></td>
</tr>
<tr>
<td>Client 3</td>
<td></td>
</tr>
<tr>
<td>Client 4</td>
<td></td>
</tr>
<tr>
<td>Client 5</td>
<td></td>
</tr>
<tr>
<td>Client 6</td>
<td></td>
</tr>
</tbody>
</table>

This means that access by nodes with critical data cannot be predicted.

All nodes access the radio channel without prioritization.

In iQoS the access point is now configured to reserve a preset transmission capacity for certain clients. To achieve this the access point creates a cyclic
transmission plan, which contains the time slots for the reserved transmissions of the individual clients:

Figure 6-3: iQoS transmission plan with reserved data rates for all clients

If one of the clients is authorized to send, but has no transmission, the frequency remains free; the unassigned channel is not used by the other nodes.

In contrast to this example iQoS is mostly configured so that data transmissions are not reserved for all, but only for some selected nodes, while the other clients share the remaining capacity according to the “first come first serve” principle:

Figure 6-4: iQoS in “mixed” operation with clients with reserved time slots (clients 1 - 3) and “free” transmissions (clients 4 – 6)

In Figure 6-4 such a mixed operation is illustrated in which clients 1 to 3 can rely on having a send interval assigned to them in regular intervals. The other clients 4 to 6 share the rest of the send time. This can lead to a shifting of individual transmissions (as that of client 4 marked orange in this example); however this is not severe, since this is not a time-critical transmission.

iQoS represents a compromise which firstly ensures the connection quality for critical nodes, and secondly makes optimal use of the available bandwidth.
Configuration of iQoS with SCALANCE W devices

iQoS is – as virtually all settings for SCALANCE W devices – configured via the Web Based Management (see 9.1.1). In the access point the project engineer defines the following for the respective clients:

- The MAC address,
- the data transmission rate to be reserved, and
- the maximum reaction time for the access point to wait for a reaction of the client.

After the reaction time has elapsed, the access point assumes that the client in this cycle does have nothing to send and clears the frequency.

Figure 6-5: Screenshot of the WBM interface for the configuration of iQoS. In this example a bandwidth of 200 kBit/s is reserved for a node.

Restrictions of iQoS

iQoS cannot be operated together with iPCF.

Principally iQoS can be performed with any number of clients. However, to ensure a smooth operation no more than four clients per access point should be employed.

Since iQoS keeps the roaming protocol unchanged, the connection may be disrupted if a client moves from the area of an access point into a neighboring cell. These interruptions typically last 200-300 ms.
6.4 “iPCF-MC” (“Industrial Point Coordination Function – Management Channel”)

iPCF and iPCF-MC

iPCF (see 6.1) was developed to achieve short handover times during change between radio cells ("roaming"). However, iPCF only achieves optimal performance with RCoax cables. The iPCF-MC procedure enables short handover times even for freely movable clients and many cells or a large number of used channels. iPCF-MC is a internal development of Siemens AG and works only with nodes where iPCF-MC has been implemented.

Functionality of iPCF-MC

iPCF-MC uses both radio interfaces of the access points differently: One interface works as management interface and sends a "Beacon" with administrative information every five milliseconds. The other interface transfers the user data. The following prerequisites must be fulfilled in order to use iPCF-MC:

- The access point must provide "RR" functionality and be equipped with two radio interfaces. All SCALANCE W-700 "RR" variants are suitable as client.
- Management interface and data interface must be operated in the same frequency band and their radio coverage must match. iPCF-MC will not function if both radio interfaces are equipped with directional antennas which cover different areas.
- The management interfaces of all access points between which a client should change must use the same channel. A client only scans this one channel to find an accessible access point.
- For the management interface the transmission method according to IEEE 802.11h cannot be used. However, 802.11h is possible for the data interface.

6.5 “Dual client” technology

The dual client method was developed to achieve a higher data throughput as compared with standard WLANs while achieving very short handover times, while at the same time using security mechanisms according to IEEE 802.11i (see 5.2).

Requirements

The Dual Client procedure is a proprietary development of Siemens AG. Therefore the clients as well as the involved access points must support this procedure. Dual Client can only be used with devices activated for layer 2 tunneling.

Principle of Operation

With the Dual Client procedure the devices are not connected to a radio network via one WLAN client, as usually, but two client devices simultaneously. Both clients take on different functions. The so-called “active client” handles the regular data
traffic with the access point as this would be the case without the connected second client.

Figure 6-6: Clients ❶ and ❷ are employed in Dual Client operating mode. Between the client ❷ and the access point ❸ there is an active connection ❹, via which the data exchange occurs. Between the client ❶ and the access point ❹ there is a connection ❸, however without data exchange (stand-by connection).

The second client, the so-called “standby client”, meanwhile permanently scans the radio field for alternative access points and always establishes a connection with the access point providing the best transmission quality, however without performing a data transfer. Furthermore, the stand-by client regularly receives information on the quality of the connection between active client and access point.

As soon as the connection quality of the stand-by client with the connected access point is better than the quality of the connection between active client and access point, the roles are exchanged within few milliseconds, and the previous stand-by client takes on the data transfer. The previously active client now takes on the role of the stand-by client and scans the radio field for access points.

For each Dual Client connection two client devices must exist which are interconnected via Ethernet. Both clients need not necessarily be of the same type.
Compatibility with other i-features

Dual Client cannot simultaneously be used with other i-features (iQoS, iPCF, iPCF-MC, iHOP).

Conditions for the application of RSTP

Within the context of the Rapid Spanning Tree Protocol (RSTP, see 4.4.3) please note the following:

- The subnet with the clients in Dual Client mode must not contain any network components with activated (R)STP functionality.
- All bridge ports of a SCALANCE W-700 access point, which represents a node in Dual Client mode are automatically defined as Edge ports when using (R)STP. The generation of redundant network paths is prevented by the internal functioning of the Dual Client function.

Further information

Further documents on the topic of “Current IWLAN technologies” is available on the SIEMENS automation portal under URL:

7 Coexistence of IWLANs with other Radio Networks

Here you can learn...

... what to do to make your industrial WLAN work smoothly in an environment where other radio transmitters are also operated.

Possible sources interfering with the operation

In the industrial environment there are basically two sources of interference which can affect the function of an IWLAN:

- Other radio transmitters using the same frequency band (other WLAN nodes, but also Bluetooth, etc.),
- Devices sending unspecific interference pulses (welding devices, switching devices)

Since the 2.4 GHz band is also used by more radio systems than the 5 GHz band, larger operational difficulties must be expected in the 2.4 GHz band.

Coexistence management

"Radio" as such is no limited resource. Due to its nature as a "shared medium" it is not possible to increase the capacity by simply installing more cables, for example. Due to a proactive coexistence management it is possible to use this resource optimal, which in most cases meets the requirements of industrial application.

An expert should always be consulted for the coexistence management. Planning and design of a radio system can already be supported beforehand by using the SINEMA software (see chapter 11).

Radio analysis

The first step should always be a radio analysis of the environment. It evaluates the individual transmitters according to the various criteria:

- On which frequency does the transmitter work?
- Is its application time or security critical?
- How large is the data volume to be transferred?
- Does the transmission occur cyclically, sporadically or continuously?

The principle of decoupling

The individual radio fields can work independent of one another if they are "decoupled" in at least on of the three domains

- space
- frequency
- time

i.e. separated from each other.
7 Coexistence of IWLANs with other Radio Networks

Figure 7-1: Example for decoupling in the frequency range: The MP277 Mobile Panel (left, see 10.1) can communicate with the robot (center), even though it is simultaneously within the transmission range of the mobile phone (right), since both communicate on different frequencies (orange 5 GHz, green: 2.4 GHz).

Even though the fields overlap in space and time they are decoupled in the frequency domain.

- **Spatial decoupling** is achieved by keeping the overlap between the various radio systems as low as possible. This is achieved by reducing the transmission power to the required minimum (no overreach), by selecting suitable antennas (directional antennas or omni-directional, see 13.3), as well as optimizing the setup location of access points and clients, as far as possible within the framework of the function of the plant.

- For the **frequency decoupling** it is decisive that the frequency ranges of the individual radio systems overlap as little as possible. In the most simple case this is achieved by selecting the respective radio channels, in the advanced case this is achieved by the modulation and multiplex methods (see 3.3) such as MIMO or also the application of iHOP (see 6.2).

- For the **temporal decoupling** the configuration of the individual nodes is decisive. These must be selected so that the probability that a time-critical transmission such as PROFINET IO overlaps with another transmission becomes as low as possible. (It is possible, for example, to reserve a channel exclusively for time-critical transmissions, as far as practical)

Further information

For further information on this topic please refer to the web at:

[ZVEI Koexistenz von Funksystemen in der Automatisierungstechnik](http://www.zvei.org)

Published by “ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.”

Further information

The individual steps of the coexistence management are summarized in the VDI/VDE guideline 2185

"Radio-based communication in automation technology"

(Download liable to charge)

27 www.zvei.org
8 Country Approvals

Here you can learn...

... about the requirements necessary for operating WLAN components in various countries and which restrictions may exist.

8.1 General information

Not all radio modes are approved in all countries. Among other things, nationally different restrictions for approved configurations can refer to

- permitted frequency bands and channels,
- maximum transmitter power,
- indoor/outdoor operation,
- 802.11 substandards (“a”, “b”, “g”, “h”, “n”, “Turbo”),
- specific methods for improving the transmission quality such as DFS and TCP. (see 4.4.4)

If you require a specific configuration when configuring your network, please consult your Siemens customer adviser.

Respective components

A radio network is considered as an “entity” in which the respective approvals must exist for all participating components, which include –

- access points
- clients, including interface modules (see 10.2, 10.3)
- possibly mobile operator panels (see 10.1).
- Antennas (13.3), this also includes RCoax leaky wave cables (13.1).

8.2 Approval methods and responsibility

Principally, the responsibility for proper operation of a radio system lies with the operator, and not the manufacturer. Technically, it is now possible at any time to configure a device approved in a country in such a way that in actual operation is violates the standards of this country.

8.3 Country approvals in the SCALANCE W devices

The national standards that were current at the time the firmware was published are stored in the firmware of each SCALANCE W device (compare chapter 9). These standards can be read out via the web interface of the access point or client by calling this page

http://<IP-Adresse>/countrylist.log

with a web browser connected to the corresponding radio network.

<IP address> stands for the internet address of the corresponding device; the called page provides a tabular overview of the approved configurations.

Please note that this list is for your information only; it is not related to a functional restriction of the respective device: operating an access point or client in a radio mode that is not approved in the respective country does not require additional
measures. Operating SCALANCE W devices is not permitted in countries that are not listed in the country list.

Figure 8-1: Example of a possible country approval list from an access point. The excerpt below shows the entries of the radio modes permitted in Italy.

| Country | Mode | CH | MHz | PWR (dBm) | Usage
|---------|------|----|-----|-----------|------
| ITALY   |      |    |     |           |      
|         | 11b  | 2412 | 100mG | Indoor-Outdoor |
|         | 11a  | 2417 | 100mG | Indoor-Outdoor |
|         | 11b  | 2422 | 100mG | Indoor-Outdoor |
|         | 11a  | 2427 | 100mG | Indoor-Outdoor |
|         | 11b  | 2432 | 100mG | Indoor-Outdoor |
|         | 11a  | 2437 | 100mG | Indoor-Outdoor |
|         | 11b  | 2442 | 100mG | Indoor-Outdoor |
|         | 11a  | 2447 | 100mG | Indoor-Outdoor |
|         | 11b  | 2452 | 100mG | Indoor-Outdoor |
|         | 11a  | 2457 | 100mG | Indoor-Outdoor |
|         | 11b  | 2462 | 100mG | Indoor-Outdoor |
|         | 11a  | 2467 | 100mG | Indoor-Outdoor |
|         | 11b  | 2472 | 100mG | Indoor-Outdoor |

Further information in the SIEMENS IIA-Portal

Updates lists with country approvals for the individual SCALANCE W products are available in the SIEMENS automation portal:

SIEMENS NET Products for Setting up an IWLAN

Content

This section provides you with an overview of the products offered by SIEMENS for setting up a secure and reliable WLAN.

The current product range with its properties is presented and you are provided with an introduction to the application and the practical benefits.

Overview of the some of the most important SCALANCE Wireless products. Top row left to right: Access Points W784, W788, W786; bottom row: IWLAN interface IM 154-6 PN HF, Mobile Panel 277F, IWLAN/PB Link PN IO, in between various antennas and RCoax cables (figure not to scale)
## Structure

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>The introductory chapter presents the access points and clients of the SCALANCE W family.</td>
</tr>
<tr>
<td>10</td>
<td>This section represents further SIMATIC-IWLAN components, including the Mobile Panels 277/277 F as well as the ET200 Pro IWLAN Interface Module IM 154-6 PN HF and the IWLAN/PB Link PN IO; a module, which can be used for creating a connection between wireless networks and PROFIBUS networks.</td>
</tr>
<tr>
<td>11</td>
<td>This chapter deals with SINEMA E. This is a software package which enables the user to plan, simulate and configure WLANs.</td>
</tr>
<tr>
<td>12</td>
<td>The subsequent section describes the HiPath portfolio of multi-functional communication and security solutions.</td>
</tr>
<tr>
<td>13</td>
<td>Finally, you are provided with information on different accessories for wireless networks such as antennas, etc.</td>
</tr>
</tbody>
</table>
9 SCALANCE Access Points and Clients

Here you can learn...

... about the specific SCALANCE family access points and clients provided by SIEMENS to establish the connection between wire-bound networks and WLANs and to connect WLAN nodes.

SCALANCE product overview

PROFINET is an open, cross-vendor product standard based on Industrial Ethernet which facilitates the vertical integration of the automation, i.e. the networking of all levels of the course of manufacture. SCALANCE products are the latest generation of network components for PROFINET which are divided into three product lines:

- SCALANCE X are switches for Industrial Ethernet,
- SCALANCE S is a series of security modules, and
- SCALANCE W provides functions for wireless communication. These functions are mainly access points and client modules (see chapter 9) and "communications processors" (radio network cards).

9.1 SCALANCE W: General information

The following table provides an overview of the positioning of SIEMENS products of the SCALANCE W family.

Figure 9-1: Positioning of the SCALANCE W products. More information on the IWLAN/PB Link PN IO is available in section 10.3, the antennas are described in detail in chapter 13.

Note: the expanded temperature range of -40°C ... +70°C cannot be used if the 100 V ... 240 V power supply is used. In this case the maximum operating temperature is reduced to +60°C.
SCALANCE W-780 and W-740

The SCALANCE W product series ("wireless") consists of components for connecting Industrial Ethernet and WLAN in industrial environments.

In this series, the "W-780" modules are access points which are used as network switches of the individual radio cells and as transitions between Industrial Ethernet and WLAN segments.

The client modules have the designation "W-740". They are connected to mobile end nodes via Ethernet and communicate via the access points.

Table 9-1: Overview of the SCALANCE W700 product range

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Device name</th>
<th>Special features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Points</td>
<td>W788-1PRO</td>
<td>&quot;Standard&quot; access points</td>
</tr>
<tr>
<td></td>
<td>W788-2PRO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>W788-1RR</td>
<td>Access points with expanded function range (see &quot;RR features below&quot;)</td>
</tr>
<tr>
<td></td>
<td>W788-2RR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>W786-1PRO</td>
<td>Particularly rugged devices for use in mechanically and climatically demanding environments</td>
</tr>
<tr>
<td></td>
<td>W786-2PRO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>W786-3PRO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>W786-2RR</td>
<td>Robust access points with expanded function range (see &quot;RR features below&quot;)</td>
</tr>
<tr>
<td></td>
<td>W784-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>W784-1RR</td>
<td></td>
</tr>
<tr>
<td>Clients</td>
<td>W744-1PRO</td>
<td>Client for connecting an end node</td>
</tr>
<tr>
<td></td>
<td>W746-1PRO</td>
<td>Client for up to eight end nodes *)</td>
</tr>
<tr>
<td></td>
<td>W747-1RR</td>
<td>Client for up to eight end nodes *) with expanded function range (see &quot;RR features below&quot;)</td>
</tr>
<tr>
<td></td>
<td>W744-1</td>
<td>As above, however with small form factor and reduced hardware configuration</td>
</tr>
<tr>
<td></td>
<td>W746-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>W747-1</td>
<td></td>
</tr>
</tbody>
</table>

*) One of them a PROFINET I/O client

"RR" features

Access points and clients with "RR" in the name have an expanded function scope. This includes the following:

- "Rapid roaming" with iPCF (see chapter 6.1 and 9.5)
- "iHOP" (see 6.2)
- iPCF MC (only W78x-2RR access points and W747 clients, see 6.4)
- Dual Client (see 6.5)

For using the RR features the involved access points as well as the clients must be RR devices.

28 Access Points can also be configured so they are limited to the functionality of clients
Further information in the SIEMENS IIA-Portal

Further, continuously updated information on SCALANCE W products are available at:
http://www.automation.siemens.com/net/html_76/produkte/050_scalance_w700.htm

9.1.1 Installation and configuration

The basic settings of the SCALANCE W-700 access points and client modules can be made via “Web Based Management” (WBM) or with telenet via the command line (“Command Line Interface”, CLI).

Figure 9-2: Web interface (“WBM”) for configuring an access point. A standard web browser is used for operation that communicates the input data to a web server running on an access point.

For WBM the SCALANCE W configuration data is accessed via the Ethernet interface or an existing WLAN connection. A web browser on the PC of the configurator communicates with an HTTP server that runs on the SCALANCE W. With the aid of the HTTP server, the configuration data can be read and changed with forms as known from conventional websites. A number of wizards are available in web-based management for user-friendly installation and configuration of both access points and client modules. Using these wizards, the modules can be optimally adapted to the communication task. Both network mode (see chapter 4) and the required WLAN security level (see 5) can easily be set.
9.1.2 Power supply

For the power supply of SCALANCE W devices there is a number of options. These can be combined and provide a highly available power supply.

SCALANCE W-700 general:

Power over Ethernet ("PoE")

Power over Ethernet is supported by all SCALANCE W-700 and is defined in the IEEE standard 802.3af. Since normally not all eight lines of an Ethernet cable are used for signal transfer, the power supply can be directed via the vacant lines. The advantage is that with this method devices are supplied with power without having to install separate lines, which saves installation and maintenance costs.

Phantom feed

A PoE variant is the voltage feed via the signal lines themselves, the so-called "phantom feed", via which all SCALANCE W-700 can be supplied. In this case a four-line cable is sufficient, however, this mode must be supported by the power source.

Figure 9-4: Redundant power supply of an access point or client via PoE or phantom feed and external power supply

SCALANCE W788-xPRO/RR and SCALANCE W74x-1PRO/RR:

Power supply via hybrid connector

The device variants W788-xPRO/RR and W74x-1PRO/RR are connected to an FC RJ 45 modular outlet with power insert using an eight-line industrial Ethernet cable. Two additional cables branch off of this cable; one cable leads to the actual power supply unit (e.g., a PS307 module), the other cable is an Ethernet hybrid cable leading to the bus nodes to be managed. (See figure below.)

29 It must generally be observed that the configurations described here can also be used with the DC 24 V common in automation technology which, however, does not conform with the specification in the IEEE 802.3af standard. If the application of this IEEE standard is desired, the products of the SCALANCE W-700 family will also be capable of this.
The power supply is directed here via separate lines in the hybrid cable. See also 13.5.

**Power supply via M12 connection**

For device variants W788-xPRO/RR and W74x-1PRO/RR a separate power supply can be used simultaneously that is connected to the SCALANCE W-700 device via an M12 connection (see below).

When both methods are used simultaneously, a redundant power supply develops in which the device switches over to the other source immediately and without interrupting the communication in the event of a failure of one of the two power supplies. This ensures the high availability of the SCALANCE W devices.
Different models:

**Power supply adapter W786-xPRO/RR**

The device variants W786-xPRO/RR can additionally be supplied with DC 48V for direct feed via power supply adapters with DC 12-24V or AC 100-240V.

**Power supply W784-1xx/W74x-1**

The device variants W784-1xx and W74x-1 have a 24V direct feed in addition to PoE.

**9.1.3 Security aspects**

The SCALANCE W devices are flexible and master the WPA and WPA2 procedures with encryption according to AES or TKIP. (To refer to the individual procedures, see 5.2). Clients be configured to adapt to the encryption given by the access point and vice versa.

On this basis it is possible for an access point to communicate with a client via WPA, for example, and with the others via WPA2 at the same time. This supports the application case where a client roams from one access point to another which uses a different encryption method. Furthermore, an AP can communicate with different clients and serve the respectively highest security standard supported by the component. This applies for WPA and WPA2 as well as for WPA-PSK and WPA2-PSK.

This is relevant if older devices by third-party manufactures shall be integrated into the radio network.
9.2 Access Points of the SCALANCE W product line

Figure 9-5: Product overview: SCALANCE W Access Points

Note: the expanded temperature range of -40°C ... +70°C cannot be used if the 100 V ... 240 V power supply is used. In this case the maximum operating temperature is reduced to +60°C.

### 9.2.1 Access Points SCALANCE W788-xPRO/RR

Currently four different W788xPRO/RR access points are offered:
- SCALANCE W788-1PRO
- SCALANCE W788-2PRO
- SCALANCE W788-1RR
- SCALANCE W788-2RR

Each of the W788-2PRO and W788-2RR models is equipped with two radio modules that are independent of one another; the other models only feature one such module. Only W788-2PRO and W788-2RR are thus suitable for redundancy mode (see section 4.2.5).
Table 9-3. Properties of the SCALANCE W780 Access Points

<table>
<thead>
<tr>
<th></th>
<th>W788-1PRO</th>
<th>W788-2PRO</th>
<th>W788-1RR</th>
<th>W788-2RR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundancy-Modus</td>
<td>--</td>
<td>Yes</td>
<td>--</td>
<td>Yes</td>
</tr>
<tr>
<td>Rapid Roaming (IPCF)</td>
<td>--</td>
<td>--</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Further information in the SIEMENS IA-Portal

Application examples for using W788 access points are available in the SIEMENS IA portal


9.2.2 Access Points SCALANCE W786

Figure 9-7: SCALANCE W786-3PRO access point

The SCALANCE W786-xPRO/RR access points are designed for use in particularly demanding ambient conditions or in public areas. The most important properties include insensitivity to extreme effects of the weather such as salt water spray, but also the rugged design in an impact-resistant and shock-proof plastic housing without destructible parts facing outwards.

Five variants of access points exist:

- SCALANCE W 786-1PRO
- SCALANCE W 786-2PRO
- SCALANCE W 786-2RR
- SCALANCE W 768-2HPW
- SCALANCE W 786-3PRO
They essentially differ in the number of available interfaces (except for the W786-2HPW, see below):

Table 9-4: Interface equipment of the W788-xPRO/RR access point

<table>
<thead>
<tr>
<th></th>
<th>W 786-1PRO</th>
<th>W 786-2PRO</th>
<th>W 786-3PRO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio interfaces</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Internal antenna sockets</td>
<td>(internal or external)</td>
<td>(external)</td>
<td>(external)</td>
</tr>
<tr>
<td>Ethernet interfaces</td>
<td>(RJ45 or BFOC)</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The Ethernet interfaces are either electrical (RJ45) or optical (BFOC bayonet fiber optic connector).

The access point W786-2RR furthermore has the “RR features” (see page 72)
The other technical data correspond to the W-788 access points (see 9.2.1).
Figure 9-8: Application options of the SCALANCE W780 access points. Use in docks is only enabled by the resistance to salt water spray.

SCALANCE W786-2HPW ("HighPath Wireless")
Access point W786-2HPW is suitable for using HighPath networks. Further information is available in chapter 12.4

9.2.3 Access Points SCALANCE W784-1xx

Figure 9-9: SCALANCE W784-1xx Access Point
The W784-1xx access points are cost-effective models intended for application in less demanding environment connections, such as in switching cabinets. Their compact form factor makes them particularly suitable for installation in areas with difficult access such as integration into a device or machine. The reduction of the hardware installed on the access point to necessary components ensures an optimum price/performance ratio.

Figure 9-10: Mounting and connection options of the access point W-784

The W-784-1xx access point is offered in two models:
- SCALANCE W784-1
- SCALANCE W784-1RR

Except for the rapid roaming capabilities, which are only available for the W784-1RR device, the technical equipment of both models is largely identical.

Further information in the SIEMENS I IA-Portal

Manuals on the SCALANCE access points are available in the SIEMENS I IA Service & Support portal under entry ID 19384623:

Further information in the SIEMENS Industry Mall

Further information on this product is available in the SIEMENS Industry Mall at:
SCALANCE W-780 Access Points
9.3 WLAN client modules of the SCALANCE W740 series

The design of the WLAN clients of the W-740 series is identical with that of W788-xPRO/RR or W784-xPRO/RR access points. The difference consists in the software complement that does not allow the client modules to perform management tasks in the scope of the radio network. The clients rather work together with one or several access points which they adopt for the connection to a WLAN with infrastructure (see 4.2). 30

It is possible to operate the clients in ad hoc mode (see 4.3) which however is not recommended for security and performance reasons.

---

30 It is possible to operate the clients in ad hoc mode (see 4.3) which however is not recommended for security and performance reasons.
These clients come in six different versions which amongst other things differ in the protection class:

<table>
<thead>
<tr>
<th>Class of protection</th>
<th>IP 65</th>
<th>IP 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>W744-1PRO</td>
<td>W744-1</td>
<td></td>
</tr>
<tr>
<td>W746-1PRO</td>
<td>W746-1</td>
<td></td>
</tr>
<tr>
<td>W747-1RR</td>
<td>W747-1</td>
<td></td>
</tr>
</tbody>
</table>

- The individual variants also differ in the number of Ethernet addresses they can manage and in the “rapid roaming” capability, as well as the protection class which determines the environment conditions for which they are suitable.
- The clients form the interface between Ethernet-connected devices and WLAN. However, they do not transmit the complete network communication, but only the messages of a limited number of Ethernet nodes. W744-1xx can only connect one single node, the models W746-1xx and W747-1xx supply up to 8 nodes.
- In addition, the W747-1xx supports rapid roaming by means of iPCF (i.e. the practically uninterrupted link between the radio cells of changing nodes, see 4.4 and 9.5).
- Each client module has only one radio interface.

Other clients

The functionality of a client is also filled by the
- mobile panels 277, 277F (see 10.1),
- ET200pro WLAN interface modules (see 10.2),
- the IWLAN/PB link PN IO (see 10.3).

Further information in the SIEMENS I IA-Portal

Manuals on the SCALANCE client modules are available in the SIEMENS I IA Service & Support portal under entry ID 19386812:


Further information in the SIEMENS Industry Mall

Further information on these products is available in the SIEMENS Industry Mall at:

SCALANCE W-740 Client Module
9.4 Application Examples

Simple example configuration

Figure 9-12: Example for the simple setup of a WLAN: Monorail overhead conveyor

In the above simple example hangers 1 to 6 move on a monorail overhead conveyor. Each hanger is equipped with a W747-1 client module. Along the path of the monorail overhead conveyor there is a RCoax cable which forms the antenna of the W788-2RR access point, which in return mediates the connection with Ethernet LANs or – as in this example – with a field PG with radio card.

Complex application example

The figure below shows a more complex application example of the SCALANCE products in which W788-1PRO access points span several neighboring radio cells. Interconnected via a cable-based Ethernet string it mediates the communication between the automated guided vehicle system on which a client module W744-1PRO and a mobile S7-300 CPU are located, and a stationary S7-300 CPU as well as an HMI panel and a field PG on the other hand.

This configuration enables the FTS to change from radio cell to radio cell (“roaming”) without losing contact.
Figure 9-13: Setup of a complex WLAN

Application of a W747-1 client in a RCoax system

Figure 9-14: Application of a W784-1RR access point and a W747-1 client in a RCoax system
This example shows an automation cell with a nutrunner controller. An operator panel as well as an ET200S, which are connected at the cable-based Ethernet line via client, RCoax cable and access point, are attached at the cell.

9.5 Deterministic data communication and rapid roaming: iPCF

"Rapid roaming" is the fast reestablishment of a connection when a mobile network node changes from one radio cell to the other. (See, for example, section 4.1.2) Conventional roaming methods frequently require several hundred milliseconds to reestablish the connection in this case; this value is too large for numerous applications.

To avoid this the W-700 RR variants (access points and client modules) use the iPCF-method, a variant of the PCF (see section 5). iPCF reduces the handover times (i.e. the period between the interruption of the communication in one radio cell and the resumption of the communication in the other cell) to less than 50 ms and thus guarantees an almost uninterrupted communication within the entire radio network, also for moved nodes.

However, it proprietarily changes the protocol structure of the data frames and no longer allows a coexistence with DCF ("Distributed Coordination Function"). All network nodes have to use iPCF and it is no longer possible to operate mixed networks.

Figure 9-15: Application example for rapid roaming with RCoax

Represented above an example for performing RR with RCoax cables. The automated guided vehicle system moves from one RCoax segment to the other and changes the access point without a resulting noticeable interruption of the connection.

9.6 PROFIsafe with SCALANCE W

PROFIsafe is a protocol extension for the PROFINET Industrial Ethernet variant. PROFIsafe introduces features for fail-safe communication in both bus/network systems. The achieved properties include:
- protection against corrupted addresses,
- protection against loss of data,
guaranteed response times
Since PROFIsafe is a protocol extension, mixed traffic of "secure" and standard messages can take place on the same network.

Figure 9-16: Failsafe wireless communication with PROFIsafe

The SCALANCE W access points and clients, of the SIMATIC Mobile Panel 277F, the ET200pro IWLAN Interface Module as well as the IWLAN/PB Link PN IO are suitable for the operation with PROFIsafe. (See chapter 10)

The method is primarily designed to compensate for internal error sources. To ensure secure transmission also for a network that is subject to external danger (for example, attempts to disturb the network or manipulation by unauthorized third parties), it is required to use the additionally available security mechanisms (section 5).

9.7 Increase in performance by HiPath Wireless

In conjunction with a HiPath Wireless Controller (compare chapter 12), it is particularly easy to realize larger radio infrastructures in which voice (Voice over WLAN) is transmitted via the radio network in addition to data. The HiPath Wireless Controller provides a central management. It connects, manages and coordinates all access points and clients in such a way that the WLAN environment appears as several individual, centrally managed IP subnets. In addition, the individual connections are managed so that the nodes can securely move in the entire radio network without problems.
10 Further SIMATIC IWLAN products

Here you can learn...

... which further SIMATIC products exist which you can use for configuring and operating IWLANs. This includes the “mobile panels” 277, 277F, which are portable devices for operating and monitoring plants, as well as the ET200 Pro and IWLAN/PB link-interface modules, which provide interfaces between ET200 controllers and PROFIBUS on the one hand and IWLAN on the other.

10.1 SIMATIC Mobile Panels

SIEMENS offers a wide range of HMI devices for automation (“panels”), which can be used to monitor, surveil and operate individual devices within the series. This also includes “mobile panels” with integrated radio interfaces which can be used in the course of an IWLAN. These panels are no longer stationary, but can be moved throughout the plant and used at the required location.

They combine capabilities of an IWLAN clients with the function scope of an HMI panel. This includes archives (storing of measured values and input in temporal context), recipes (sentences of connected process data which are managed “as a whole”) as well as highly developed message, logging and alarm systems.

Operation occurs via touch screen, the configurable function buttons or via hand wheel, key switches and illuminated push-button. The mobile panels are configured with the configuration software WinCC flexible.

Protection type IP 65 has been designed for industrial environments.

Technical properties

The SIMATIC mobile panels 277(F) IWLAN communicate via the WLAN standard IEEE 802.11 a/b/g/h via PROFINET. The devices Mobile Panel 277F IWLAN additionally support the fail-safe PROFIsafe communication. (see 9.6)

There are four device variants:

- For mobile operation and monitoring via WLAN:
  - Mobile Panel 277 IWLAN
  - Mobile Panel 277 IWLAN with hand wheel, key switch and illuminated push-button
- As fail-safe device also for fail-safe operation:
  - Mobile Panel 277F IWLAN with enabling button and emergency stop button
  - Mobile Panel 277F IWLAN with enabling button, emergency stop button, hand wheel, key switch and illuminated push-buttons.

The mobile panels 277(F) IWLAN will as of version 2 (delivered presumably by mid 2010) also come with iPCF-MC (see 6.4).

For variants Mobile Panel 277F IWLAN (PROFIsafe) the following system requirements are mandatory:

- The mobile panel must be integrated as a secure device (PROFIsafe, Distributed Safety)
- Using a SIMATIC F-CPU

31 For safety operation the B standard is recommended.
Application of effective areas and transponders

For Mobile Panel 277F IWLAN an effective area restriction was realized. Depending on its location the operator receives a secure, electronically monitored operator enable.

An effective area is the area in which parts of the plant, e.g. a machine, can be operated with the enabling button of the operator panel. An effective area is formed physically with transponders, which are mounted in the vicinity of the machine and send unique IDs in a club-shaped area. The ID is received by the operator panel and enables it to determine its distance from the transponder.

As soon as the operator panel detects that it is located within an effective area, the operator can log the operator panel on at the effective area. A secure operating of the plant component separated by the effective area is only possible after successful logon.

This can, for example, automatically prevent a plant component being put into operation, while the operating staff is still within the hazard area.
The above example illustrates the application of a mobile panel 277F and the concept of effective area: the operator takes the mobile panel and goes from robot cell to robot cell. Whenever he is located within the reception area (i.e., effective area) of a transponder, the appropriate robot cell connected to the fail-safe CPU 317F is switched to fail-safe mode.

The following requirements have to be met for the application of effective areas:

- The effective areas must not overlap,
- The space covered by the effective area must be illuminated completely by the transponder,
- The diameter of the effective area must not exceed 8m. (This is the practical range of the transponder signal.)

Further information on this product is available in the SIEMENS Industry Mall at:

SIMATIC Mobile Panel 277(F) IWLAN

Further information on the topic “Fail-safe operation of the mobile panel 227F IWLAN” is available in the function manuals of the SIEMENS I IA Service & Support portal at entry ID 31255853:


10.2 SIMATIC ET 200pro IWLAN interface module IM 154-6 PN HF

SIMATIC ET 200pro is a new modular I/O system with high protection type IP65/66/67 for machine-based application without cabinet. ET 200pro is marked by a low size and a modular concept. IM 154-6 PN HF is an interface module for communication handling between ET 200pro and a higher-level PROFINET I/O controller via Industrial Wireless LAN. This makes ET 200pro IWLAN-capable.
Further SIMATIC IWLAN products

Figure 10-5

Figure 10-6 shows an application example for the application of this module:
A SIMATIC S7-400 CPU is used as controller which is connected with several access points via Industrial Ethernet. ET 200pro with the interface module is attached to an automated guided vehicle system (AGVS) which provides the communication between ET 200pro and the controller CPU. Here the interface module works as client of the access points. The connection is transparent for the ET 200pro. The AGVS can roam between the radio cells spanned by the various access points without disturbing the connection.

Figure 10-6: Application example for an IM 154-6 PN HF module
Properties

The interface module communicates according to the IEEE 802.11 a/b/g/h standards (see 3.2.1) on 2.4 GHz and 5 GHz and provides the security features according to IEEE 802.11 e/i (see 5.2) for protection from unauthorized access, espionage, bugging and falsification (e.g. WPA2 with AES). Furthermore it enables rapid roaming with iPCF (see 6.1), the free undisrupted motion of a node within the radio field.

This enables the application of an ET 200pro for applications where a cable-based solution can only be realized at great expense (wear, distance, unaccessible terrain).

Possible application areas are:
- automated guided vehicle systems
- escalators
- storage logistics
- material transport
- electrical overhead conveyors
- facility management
- service applications

Structure

The interface module IM 154-6 PN HF IWLAN consists of the following components:
- an interface unit (IWLAN radio card) and
- an connection unit

Interface unit and connection unit are delivered together with the terminating module.

Antennas can be connected directly or removed at the interface module via screw connection (R-SMA). The application of two antennas leads to optimized data transmission even in difficult environments regarding radio technology (shadowing, interferences).

Device names as well as user and configuration data can be stored on a SIMATIC Micro Memory Card.

Further information on this product is available in the SIEMENS Industry Mall at:
Interfacemodule IM 154-6 PN IWLAN
10.3 IWLAN/PB Link PN IO

The IWLAN/PB link module provides a high-performance and flexible interface between Industrial Wireless LANs on the one hand and PROFIBUS networks on the other, which saves using a decided clients here.

Figure 10-7: IWLAN/PB Link PN IO with connected PROFIBUS cable (violet, top) and antenna cable (turquoise, bottom)

Application options

The IWLAN/PB Link PN IO is a network transition which connects the two network types Industrial Wireless LAN (control level) and PROFIBUS (cell level/field level).

The IWLAN/PB Link PN IO supports access to all PROFIBUS DP slaves connected to the lower-level PROFIBUS; DP slaves higher than PROFIBUS DP-V0 are supported and, from firmware revision level V1.1.0, also DP slaves according to the DP-V1 standard and Siemens DP slaves.

Since the IWLAN/PB Link PN IO is rapid roaming-capable, it is also suitable for use with real-time requirements.
In addition, far-reaching options open up for mobile applications by using Industrial Wireless LAN (IWLAN) with RCoax and WLAN antennas for wireless or contactless data transmission. Fields of application include monorail conveyors or stacker crane systems.

The IWLAN/PB Link PN IO can be used in the following modes:

- Network transition as a PROFINET IO proxy
- Network transition in standard mode
- Network transition in mobile applications

### 10.3.1 Network transition as a PROFINET IO proxy

The IWLAN/PB Link PN IO is an essential component in the field of application of PROFINET IO. It provides the connection between the PROFINET IO controllers on Industrial Ethernet and the PROFINET IO devices (DP slaves on PROFIBUS).

From the point of view of the PROFINET IO controller on Industrial Ethernet, no difference ensues when accessing PROFINET IO devices which are connected to Industrial Ethernet via Industrial Wireless LAN and the IWLAN/PB Link PN IO and when accessing PROFIBUS DP slaves connected to PROFI Bus DP.

The IWLAN/PB Link PN IO takes the role of a proxy for the DP slaves connected to PROFIBUS DP.
10.3.2 Network transition in standard mode

The following services are available in standard mode:

PG/OP communication

PG/OP communication is used for downloading programs and configuration data, for performing test and diagnostic functions and for operator control and monitoring (HMI systems) of a plant.

Parameterization of field devices (data record routing)

The IWLAN/PB Link PN IO can additionally be used as a router for data records directed at devices (DP slaves). This enables devices which are not directly connected to PROFINET and thus do not have direct access to the field devices (DP slaves) to transfer data records to the field devices via the IWLAN/PB Link PN IO.

A tool generating such data records for parameterizing field devices is, for example, SIMATIC PDM (“Process Device Manager”).

Network transition to a DP master system with constant bus cycle time

The IWLAN/PB Link PN IO is used as a network transition between Industrial Wireless LAN and the field devices on a DP master system. The IWLAN/PB Link PN IO is operated as an active node together with a DP master on a PROFINET with equidistant parameterization.

Cross-subnet S7 connections for HMI operation

The IWLAN/PB Link PN IO routes the communication via S7 connections. This service is, for example, used in HMI applications (PC nodes).

10.3.3 Network transition in mobile applications

The IWLAN/PB Link PN IO additionally enables wireless communication to automation systems in mobile applications such as automated guided vehicle systems (AGVS), stacker crane systems or monorail conveyors (EMC). This way solutions with Power Rail Booster for PROFINET via sliding contact are replaced by a contactless and thus wear-free data transmission technology.

The connection is made alternatively via a WLAN antenna or an antenna for operation with RCoax cable (leaky wave cable, see 13.1).
Figure 10-10: Application of the IWLAN/PB Link groups to connect a roaming monorail conveyor to an Ethernet network stretching over several RCoax segments.

Further information in the SIEMENS Industry Mall:
IWLAN/PB Link PN IO

Further continuously updated product information on the IWLAN PB link PN IO is available at:
11 SINEMA Software for WLANs

Here you can learn...

... how you can use the SINEMA software to monitor and diagnose wireless and cable-based Ethernet networks, and forecast the complex behavior of the radio fields of a WLAN in different environments.

This chapter shows you the essential properties of the software and introduces you to the functional scope of SINEMA.

11.1 The SINEMA E configuration software

Problem

The exact prediction of the propagation of a radio field depends on a large number of factors: Conducting and non-conducting objects in the transmitting range can reflect, absorb, accept or scatter radio waves. (For a detailed examination, see chapter 2.3) If a specific range is to be securely illuminated with a radio field, two easy options exist:

- The transmitting power of the access points is increased until they can be received at any point, or
- the access point positions are moved and the access points are reconfigured in a method of trial and error until the desired effect is achieved.

When using the first method, the actually illuminated area will almost certainly be significantly larger than actually required. This facilitates listening in by third parties and interferences can occur in neighboring WLANs. The amount of work required by the second method is considerable and it remains questionable whether the optimum solution can be found with this approach. Particularly the probability that the installed hardware is clearly more comprehensive than the actually required hardware is very high.

Our solution

SINEMA E (“SIMATIC NEtwork MAnager Engineering”) is a Windows application that avoids the above-mentioned problems already during the planning phase. At the core, SINEMA E is used for simulating a radio field before actually installing hardware.

Application of SINEMA E

- Minimizes the required hardware,
- ensures at a very early stage that the connection to the radio network nodes will be reliable at any time also if they are mobile and
- allows specific statements on the required hardware before the installation.

License model

SINEMA E is offered in two different versions, depending on the planned application of the software:

- SINEMA E Standard with the full functional scope and
- SINEMA E Lean with a reduced functional scope.
In addition, the
- SINEMA E PowerPack

is available. With the PowerPack a SINEMA E Lean version can be upgraded to a standard version.

Integration of SINEMA E into the project handling

Figure 11-4 shows how SINEMA E is integrated into the process of a WLAN project. The application is used in both the preliminary stages, i.e. in the planning and configuration phase, and during commissioning and maintenance.
11.1.1 Functional scope of SINEMA E

Modeling the environment and the radio field

For the purpose of the simulation, the user models the environment within which the WLAN is to be set up. This environment includes walls, windows, doors, ceilings and floors of the buildings for which thickness, composition, etc. and also larger fixtures are considered.

In a further step the active components, the access points and clients, are placed in the thus modeled office or industrial environment.

Devices, antennas and radio obstacles can be selected from a component catalog and adapted to the requirement. A subsequent simulation enables the planner to get a quick idea of the signal quality to be expected in the individual configured areas. The integrated consistency check ensures the validity of the configuration and reduces possible errors already before installing the network.

By means of the graphical user interface, even complex environments can easily be simulated.

Simulation of the developing radio field

Figure 11-5: Exemplary screen shot of the SINEMA E application that shows the configuration of a part of a building. The simulation covers the three-dimensional arrangement of parts of buildings and fixtures as well as the active and passive components of the radio network.

With the access points and clients distributed by the user in the modeled building, SINEMA E simulates the resulting radio field and graphically represents it so that it is immediately clear whether the illumination and the data rate of the radio cell are...
adequate. Both the frequency of the used transmitters and the characteristics of the used antennas or RCoax cables are considered (see section 13.1).

Three-dimensional evaluation of interiors and exteriors

The simulation is three-dimensional and thus also allows to evaluate the effects of ceilings and floors and the radiation behavior over several stories. In addition, SINEMA E is not limited to the interior of office or industrial buildings, it can also evaluate the exterior. This is, for example, relevant to evaluate possible radio leaks to the outside world or the connection of two blocks of buildings.

Figure 11-6: Simulation mode of SINEMA E. In the environment configured in the previous step the signal strengths to be expected are calculated for each point and displayed in a false-color image.

Product catalogs

The comprehensive product catalogs included in the delivery make this simulation particularly convenient. They offer the option to use SIEMENS or non-SIEMENS products for the simulated hardware. Modules are simply selected from the catalog which contains a precise directory of the technical characteristics and set up in the simulated building.

The catalog can be extended by the customer to enable the consideration of newly developed future models and functionalities.

The simulation mode shown in Figure 11-6 displays a ground plan of a building in which several access points generate a radio field. The signal strengths achieved at different points in the area are represented by different colors.
It has to be observed that the geometry of the room (e.g., the corridor shown in the bottom center) is considered and that it is included in the realistic forecast of the radio field.

Report module

A report module is integrated into the simulation and diagnostic functions of both SINEMA E versions, Lean and Standard.

From the configuration developed during the simulation, this module generates a list of components that includes the ordering data of all devices from the module catalog. This facilitates an early tendering, planning and cost forecast for a project.

Figure 11-7: Example of a report file excerpt generated by SINEMA E

When setting up the radio network, the coordinates at which the individual devices are to be installed can also be taken from the report. This facilitates fast, smooth and reliable installation of the individual components.

The performed simulations are also embedded in the report as informative charts which indicate the signal strength, data rate and interferences. The report is now also the acceptance document for the commissioning and can be used for warranties concerning guarantee and servicing.

11.1.2 Extended functionality for SINEMA E Standard

The functions described above are available in both SINEMA E versions. Furthermore, the Standard version features two additional useful functions: “Autoplacement” and “Site Survey”.

“Autoplacement”: Automatic optimization

After the environment has been configured, it is possible to have the actual SINEMA E application search for the optimum place of installation of the access points in another additional step: After configuring the building geometry and after defining the sections of the building which absolutely have to be covered by the
WLAN, SINEMA E independently calculates the optimum (and resource-saving) placing of the individual access points.

“Site Survey” mode: Analysis and diagnostics of existing networks

In “Site Survey” mode, existing WLAN radio fields can be “mapped”: The user walks around the relevant area with a laptop equipped with SINEMA E and a radio network card. The SINEMA E application permanently receives the radio signals of the installed access points and uses them to generate a “map” of the existing radio fields. With this mode it is easily possible to verify the planning/simulation and to identify weak spots such as overreaches or low signal strengths or data rates.

Further properties

The Material/Regions Builder, another SINEMA E module, enables the user to measure and store complex radio obstacles or other parts of buildings (for instance, large transformers or turbines) in reality and to reuse this data in both current and future simulations.

This avoids the unnecessary repetition of time-consuming measuring processes and allows the creation of user-specific libraries of radio obstacles with their exact geometries and characteristics.

For further information on this product please refer to the SIEMENS website at:

SINEMA E
Here you can learn...

... HiPath and the support provided by HiPath products in the vertical integration of networks, particularly when connecting VoIP and Industrial Ethernet.

12.1 Basic information

HiPath is a modular product and service portfolio consisting of multi-functional communication and security solutions. It enables the setup of a modern real-time communication environment and provides, for example, the permanent availability of the employees, the access to company resources from every site and the use of innovative business communications applications to increase productivity.

Figure 12-1: Central management of the WLAN infrastructure in mixed office and industrial networks

HiPath offers solutions in six sectors:

1. Communications systems
   This sector includes scalable telecommunications systems for companies with less than ten to more than 100,000 employees based on ISDN or IP, "HiPath Cordless" (cordless telephones), access points to link analog telephones with Voice over IP and HiPath CAP ("Common Application Platform") middleware for communications systems. This includes especially the HiPath Wireless Portfolio, the mobility management for wireless voice and data connections (see 12.2).

2. Applications
   The applications developed under HiPath comprise HiPath MobileOffice for the realization of the idea of the "mobile office", HiPath OpenScape for the management of company communication resources and HiPath ProCenter, a software suite for customer management and after sales service.

3. Clients & Devices
   Mobile and stationary, cordless and cable-based telephones and accessories

4. Security Solutions
   All-in package solutions for the protection of company data and resources

5. Management Solutions
   Comprehensive solutions for the central administration of heterogeneous networks, systems and applications
6. Services
Consulting, outtasking and support for the availability of networks and applications

Figure 12-2: Example for roaming without transition between the office network and IWLAN with HiPath
12.2 **HiPath Wireless Portfolio as part of HiPath**

The HiPath Wireless Portfolio is of greatest importance to WLAN applications. This portfolio enables the setup, management and combination of radio networks and their connection to cable-based networks.

Parts of the portfolio are the
- HiPath Wireless Controllers,
- HiPath Wireless Access Points and
- HiPath Wireless Convergence Software.

In “conventional” WLANs, all access points have the same responsibility and are jointly responsible for the access and forwarding of information. They all include the full functionality required for the processing of the data communication (“fat access points, however, they do not control and coordinate one another.

**Central intelligence**

HiPath now introduces a central wireless controller, which takes the intelligence from the access points and thus turns them into “fit access points” which only operate the functions they actually require. That way all messages received at the individual access points are forwarded to the controller located in a line of an Ethernet section and the controller then provides the distribution of the messages to the actual recipients.

Furthermore, the wireless controller performs a large number of other configuration and administration tasks in the network and records interferences, network operation and statistics for later evaluation.

**Increase in value of the access points**

At the same time, the access points in HiPath feature many capabilities missing in other WLANs. Their coordinated function ensures that they can connect, for example, clients located within the range of reception of several access points always to the least loaded AP so that a well balanced load distribution develops on the network. In addition, the access points can dynamically adjust their transmitter power: If one of them has to be removed from the network, the other access points can thus increase their power and ensure that the entire area is still covered by the WLAN.

“Dynamic routing” – i.e. the automatic adaptation of the paths via which the messages are routed during operation – also enables to bridge the failure of individual components without interrupting the network.

Using the HiPath technology, it is finally not only possible but planned to integrate also “conventional” modules (such as SCALANCE W components) and networks. The example shown in the figure below shows how SCALANCE Access Points can be used within HiPath Wireless networks.
“Quality of Service” and integration of multimedia

HiPath WLANs support the IEEE 802.11e protocol and the WMM standards. (see 3.5)

This means that voice and multimedia services have already been seamlessly integrated into the data network.
12.3 Properties and customer benefits of HiPath Wireless WLANs

The central function of the HiPath Wireless Controller and the use of HiPath Wireless Access Points result in the following superior advantages of the WLAN modified as described:

Central administration

The controller is not only capable of delivering messages to the HiPath Wireless Access Points, but it can also reconfigure them. This means that the network administration can be performed for WLANs of virtually any size from a central point and implemented automatically if required.

VoIP in conjunction with the WLAN

The central controller enables the combination of several (physical) WLANs to form one logical WLAN. In particular, it can combine industrial radio networks with VoIP (“Voice over IP”) services, i.e. the access points are simultaneously used for the transmission of data and voice services. This is enabled by the high availability and reliability of HiPath networks by which the necessary short failure times (e.g., during changes between radio cells) are achieved.

This enables uninterrupted roaming with WLAN telephones also between individual cells of the WLAN spanned by SCALANCE.

Division into logical subnets by VNS

Just as different physical WLANs can be combined to form one logical WLAN, the reverse is also possible: Several logical networks can be “put” over one physical network.

These Virtual Network Services (VNS) enable the reliable assignment of different services, security requirements and access options to users.

This facilitates the network access for different user groups. For instance, one network can be created for “guests” with low privileges but open access and one for maintenance staff with high security requirements and almost unrestricted options.

Fault tolerance by “hot standby”

The function of the controller is critical for the entire WLAN. Its failure, however, has no consequences if a second controller is kept in “hot standby”: As soon as the first controller switches off due to a malfunction, it is removed from the network and the second controller, which has a permanently updated copy of the network data, performs its work.

Scalability

HiPath additionally facilitates the scalability of the networks. A number of different models are available for wireless controllers and access points; the performance of these models is adapted to the requirements of small and medium-sized to very large networks.
12 HiPath Wireless Products by SIEMENS

Security

HiPath Wireless immediately supports all relevant and modern mechanisms for authentication and access control such as WEP, WPA, WPA2 and RADIUS (see also 5), additionally VPN ("Virtual Private Networks") and the detection and handling of "rogue access points", i.e. other access points that try to log on to the network without authorization.

12.4 SCALANCE W786-2HPW access point for HiPath

SCALANCE W786-2HPW is a variant of the W-786 access points (see 9.2.2) and can be used as so-called fit access point for operation with the HiPath wireless controller, thus opening up the advantages of this architecture to industrial and outdoor areas.

It is used for application with a HiPath Wireless LAN controller as comprehensive solution in office and production environments and with the other W-786 access points it shares the robust setup and resistance towards extreme environment conditions.

The SCALANCE W786-2HPW can be exclusively operated at the HiPath WLAN controller, and is approved for operation in areas subject to explosion hazards of zone 2.

Figure 12-3: SCALANCE W786-2HPW access point for operation at the HiPath

Further information in the SIEMENS Industry Mall

Further information on this product is available in the SIEMENS Industry Mall at:

SCALANCE W786-2HPW

Further information

For further information on HiPath product please refer to the SIEMENS HiPath portal at:

http://www.siemens.de/hipath
13 Accessories for Wireless Networks (WLANs)

Here you can learn...

... which additional products SIEMENS offers you to optimally configure your WLANs.

13.1 RCoax leaky wave cables

RCoax cables are flexible antenna cables – strictly speaking they are coaxial cables whose outer shield has been interrupted on a defined basis (so-called “leaky wave cables”) so they generate a spatially defined radio field. This field is wedge shaped and runs parallel with the antenna axis.

Figure 13-1: Schematic representation of a radio field generated by an RCoax cable

The RCoax cables replace the standard radio antennas at selected access points by an antenna segment with a selectable length. They transmit and receive in the 2.4 GHZ or 5 GHZ band. They are preferably used in environments in which the nodes move in limited areas or exclusively on defined paths (monorail conveyors, high-bay racking systems) and where many shadings or reflections are to be expected.

The RCoax cable can be bent during installation of the plant and hence be adjusted to the local conditions: it can, for example, directly follow the course of a monorail overhead conveyor. In difficult environments, this offers the option to reliably illuminate sections of the radio cell that are difficult to access. High-maintenance sliding contacts or trailing cables can thus be saved.
Figure 13-2: Picture of an RCoax cable.

At the bottom left, the above figure shows the access point with IE cable, then the connecting cable available at various lengths, and finally horizontally the actual RCoax antenna segment with a terminal resistance.

Each SCALANCE W access point can be equipped with a RCoax cable. Typically, the length of a RCoax segment is up to 100 m. To be able to create seamless radio areas, several leaky wave cable segments (with one assigned access point respectively) can be aligned in succession. RCoax cables are suitable for rapid roaming and enable a virtually disruption-free transition from one cable segment to the next.

13.1.1 Data rate and segment length

Dampening of the RCoax cable increases along the leaky wave cable and the signal strength is reduced. At increased cable length and increasing distance from the cable the achievable data rate is also reduced.

Further information on this topic and performance data are available in the “System manual RCoax” in SIEMENS I IA Service & Support portal at entry ID 21286952:

13.1.2 Principle of operation

The above figure illustrates the principle of operation of the RCoax cable. Several RCoax segments, each of which features its own access point, are arranged along the travel path of a monorail conveyor. The path can change from one RCoax segment to the next RCoax segment practically without interruption.

The IEEE 802.11 protocol of the access point is not influenced by the use of the RCoax cables, particularly the data rates and the protocols for data backup are not changed. The example in the above figure shows the connection of PROFINET IO via RCoax cables. As before, rapid roaming – assuming that the corresponding access points and clients exist – is possible.
Application Examples

In this application example a high-bay racking system with WLAN components is controlled. RCoax cables connect the central control cabinet in which the storage computer is located, with a number of read systems (1), which read the information of the shelve contents, and with the lift forks (2) which control the motion of the storage.32

Another application example is controlling a nutrunner station at the mobile hangers:

---

32 Please note that for optimal usage of the storage the various frequency bands of 2.4 GHz and 5 GHz are used simultaneously.
Figure 13-5: Nutrunner control at the mobile hangers with RCoax cable

Updated product information on RCoax leaky wave cables is available on the web at:

Further information in the SIEMENS Industry Mall:
RCoax leaky wave cables

An application example for using RCoax cables in a PROFINET I/O environment is available at entry ID 23488061:
13.2 "C-PLUG" and PRESET-PLUG

13.2.1 C-PLUG

A "C-PLUG" ("Configuration Plug") is an ideal swap medium which, plugged into a respective slot of the hardware, stores the complete configuration of this module. SCALANCE W components and IWLAN/PB link PN/IO are designed for use with C-PLUGS.

Figure 13-6: C-PLUG

Swap medium C-PLUG as an alternative to flash memory

All SCALANCE W-700 devices as well as the IWLAN/PB link PN IO have an internal flash memory as well as C-PLUG slots for storing the configuration data. The flash memory existing in the device is only used if no C-PLUG has been plugged.

If a C-PLUG has been plugged, the configuration data and their changes are always stored on it. This simplifies the substitute case. A simple exchange of C-PLUG enables adopting all data to a substitute device without programming device.

There are two operating modes for this:

- During startup the device automatically secures the configuration data on an empty C-PLUG (delivery state), which is plugged into a SIMATIC NET component. Configuration changes are also secured during runtime without additional operator intervention.

- During startup an unconfigured device automatically adopts the configuration data of a plugged, written C-PLUG, provided that the data were written to the C-PLUG by a compatible device type.
Figure 13-7: Application cases of the C-PLUG. A) An empty C-PLUG is plugged to a device with an existing configuration. In this case, the configuration is stored on the C-PLUG during startup. B) There is no configuration on the device; upon switching on a possible existing configuration is read from the C-PLUG and used, but not written to the internal memory. All configuration changes are stored on the C-PLUG again.

A

B

Device C-PLUG Device C-PLUG

Several applications are possible for the C-PLUG:

- If, for some reason, the configuration of a device is lost, the stored configuration can be restored by using the C-PLUG.
- If a device fails, a back-up device can be made ready for use by inserting the C-PLUG of the failed device in the back-up device. A manual configuration of the back-up device is no longer required.

In this way, the configuration data can be transferred quickly, conveniently and securely from one device to the other. This considerably reduces failure and maintenance periods and complex, error-prone manual reconfiguration is no longer required.

Details on the operation

The devices only use your internal memory if no C-PLUG has been plugged; otherwise changes are always stored on the C-PLUG. This means that in case of a necessary device exchange the current backup of the configuration is always on the C-PLUG.

C-Plugs can take the configuration data for a large number of different modules. When plugged in a new module, they detect whether this module is of the same type as the one whose data is stored on the plug and thus automatically prevent misconfigurations.
13 Accessories for Wireless Networks (WLANs)

Figure 13-8: Demonstration of the change of the C-PLUG for a SCALANCE W-788 Access Point (rear view). The small form factor of the memory medium is distinctly recognizable.

Diagnose

A faulty C-PLUG operation such as plugging a C-PLUG, which contains the configuration of another device group, or general malfunctions of the C-PLUG are signaled via the diagnostic mechanism of the respective end-device (LEDs, PROFINET, SNMP, Webbased Management, etc.).

13.2.2 PRESET-PLUG

PRESET-PLUG is related to the C-PLUGs and uses the same slots, however is not used as backup. This rather gives SCALANCE W devices or IWLAN/PB Link PN IO defined presettings in the most simple way. A particular application case is the duplication of a configuration to install identical configurations on a larger number of devices.

PRESET-PLUG is initially configured in a SCALANCE W-700 with the desired WLAN parameters, and then plugged into the C-PLUG slot of the target device for commissioning.

This procedure is an advantage when commissioning many equally configured WLAN clients, since each client then needs not be configured separately.

Further information on both if these products is available in the SIEMENS Industry Mall at:
C-PLUG
PRESET-PLUG
Further information on the application of C-PLUGs and PRESET-PLUGs with SCALANCE W devices is available in the SIEMENS I IA Service & Support portal at entry IDs 19015713, 24030688 and 29823212:

Part 2 of the manual “Network transition IWLAN/PB Link PN IO” contains information on configuring and using C-PLUG and PRESET-PLUG:

13.3 Antennas

Aside from the antennas of the ANT795-4MR type included in the standard delivery of the access points and client modules of the SCALANCE W788 series (see below) and aside from the RCoax cables (see section 13.1), a number of other omni-directional antennas and directional antennas are also available. (Regarding the radiation characteristics of the antennas see also section 2.5) They can be mounted remotely from the device on a mast or a wall to achieve an optimum illumination of the space to be covered.

Figure 13-9

The properties of the most important antenna types are listed in the following table:
Table 13-1: Overview of the most important data of the various antenna types

<table>
<thead>
<tr>
<th>Type</th>
<th>Installation</th>
<th>Directional char.</th>
<th>Typical range *)</th>
<th>Frequency band:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANT795-4MR **)</td>
<td>Directly on the device</td>
<td>Omnidir.</td>
<td>100 m</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>ANT795-4MS</td>
<td></td>
<td></td>
<td></td>
<td>5 GHz</td>
</tr>
<tr>
<td>ANT792-6MN</td>
<td>Wall or mast</td>
<td>Omnidir.</td>
<td>200 m</td>
<td></td>
</tr>
<tr>
<td>ANT793-6MN</td>
<td>Wall or mast</td>
<td>Omnidir.</td>
<td>200 m</td>
<td></td>
</tr>
<tr>
<td>ANT795-6MN</td>
<td>Ceiling</td>
<td>Omnidir.</td>
<td>200 m</td>
<td></td>
</tr>
<tr>
<td>ANT795-6DN</td>
<td>Wall or mast</td>
<td>Omnidir.</td>
<td>200 m</td>
<td></td>
</tr>
<tr>
<td>ANT792-8DN</td>
<td>Remote</td>
<td>Directed</td>
<td>1000 m</td>
<td></td>
</tr>
<tr>
<td>ANT793-8DN</td>
<td>Remote</td>
<td>Directed</td>
<td>1000 m</td>
<td></td>
</tr>
<tr>
<td>ANT793-4MN ***)</td>
<td>Remote</td>
<td>Directed</td>
<td>&lt; 10 m</td>
<td></td>
</tr>
<tr>
<td>ANT792-4DN ***)</td>
<td>Remote</td>
<td>Directed</td>
<td>&lt; 10 m</td>
<td></td>
</tr>
</tbody>
</table>

*) depending on the respective environmental conditions
**) delivered with the access points/clients W788-1PRO, W788-2PRO, W788-1RR, W788-2RR, W744-1PRO, W746-1PRO, W747-1RR
***) Used with RCoax cables, see chapter 13.1

Table 13-2: The various antennas for operation with SCALANCE W devices (not to scale)

ANT795-4MR (left) and ANT795-4MS (right), omni-directional antennas for installation directly at the access point or client. ANT795-4MS resembles ANT795-4MS, however, it is characterized by an additional joint with which the antenna can be oriented around two axes and opposed to ANT795-4MR with IP 65 has a lower protection type IP 30.

ANT792-6MN (left) and ANT793-6MN (right), omni-directional antennas for remote installation at mast or wall.
### Omni-directional antennas
ANT795-6MN for ceiling installation (left) and remote universal directional antenna ANT 795-6DN (right)

### Directional antennas
ANT792-8DN (left) and ANT793-8DN (right) for remote installation

### Directional antennas
ANT792-4DN/793-4MN for operation with RCoax leaky wave cables

---

**Further information in the SIEMENS Industry Mall**

Further information on these products is available in the SIEMENS Industry Mall at:

[Product catalog for antennas](http://www.automation.siemens.com/net/html_76/produkte/antennen.htm)

**Further information in the SIEMENS I IA-Portal**

Further product information on antennas is available in the SIEMENS I IA Service & Support portal at:

13.4 Connections and cabling

In the industrial sector R/SMA as well as N-Connect connections are common for transmission of high-frequency signals (up to approx. 10 GHz, depending on the application). These applications are marked by high-class transmission, reliable connections and the application of cap nuts and a low form factor.

Figure 13-10: Example for the connection of various I/O devices to the access points W-786 (left) and W-784 (right)

SCALANCE W products also use these technologies:
- Access points and clients have connections in R/SMA design,
- Removed antennas are delivered with N-Connect connectors.

The antenna connection cables come as adapters, which have one R/SMA and one N-Connect end each. So the connection between various components can be realized anytime without greater workload.
Figure 13-11: Connections of IWLAN/PB Link PN IO in connection with one access point and a RCoax antenna (see 13.1)
13.5 Additional accessories

The entire SIEMENS product range is very comprehensive. Additional accessories increasing the customer benefit when setting up a WLAN include, e.g. —

Lightning protection element

The LP798-1PRO lightning protection element expands the applications of SCALANCE W-700 products with remote antennas particularly for the exterior.

Figure 13-13: Lightning protection element LP798-1PRO

Terminating resistor

If only one antenna is mounted, the TI795-1R antenna terminating resistor has to be used for SCALANCE W-700 products to neutralize the second antenna socket.
Antenna extension cable

The FRNC IWLAN antenna extension cable is a preassembled extension cable with two R-SMA connectors (R-SMA male / R-SMA female). The cables are delivered at a length of 5 m and 15 m and are used for the connection between access point or client and remote antenna.

Alternating voltage power supply with IP 65

The W788, W744-1PRO, W746-1PRO and W747-1RR devices can be supplied with power directly from the socket via the PS791-1PRO power supply unit designed according to IP 65 protection type (i.e. protection against ingress of dust and water jets).

Figure 13-14: Power supply unit PS791-1PRO

FC Modular Outlet Base with Power Insert

Expands the power supply alternatives of the W788, W744-1PRO, W746-1PRO and W747-1RR devices by the option of using the same cable for data and power transmission simultaneously. (See also 9.1.2)

Figure 13-15: Modular outlet with power insert for power supply

Power splitter

Power splitter for use with the RCoax cable.
Appendix and List of Further Literature

14 Glossary

802.11
A series of standards for wireless network protocols developed by the → IEEE. See 3

Access Point
“Access point”, a node of a → WLAN which simultaneously performs administrative functions in the network and which – for example for → clients – provides the connection to wire-bound networks, other clients in the same radio cell or in other radio cells. See 4.1.1

Ad hoc network
An unstructured → WLAN without → access points. The → clients communicate “at their own responsibility” without higher-level coordination. The opposite is a network in → infrastructure mode. See 4.3

AeroScout
A technology for locating nodes using radio networks and RFID tags. See 3.7.4

AES
“Advanced Encryption Standard”, an encryption method, see 5.2.2

Antenna Diversity
The simultaneous availability of two radio interfaces on one device. Enables to dynamically change to the interface with the frequency currently providing the best reception conditions in difficult radio environments.

Bandwidth
Can be described as “maximum available data rate”. The term derives from the fact that a proportionally wide section of the radio spectrum is used by the transmission at a specific data rate. See also 2.4.4.

Bluetooth
A short-range radio standard for communication between office devices and mobile phones, see 3.7.1.

CCMP
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, an encryption algorithm used in within the framework of → WPA2, see 5.2.2.

Client
Here: a node of a → WLAN which has no own infrastructure capabilities but which accesses a radio network via an → access point.
CSMA/CA

“Carrier Sense Multiple Access with Collision Avoidance”, a method for the detection of “collisions”, i.e. the attempt of several transmitters to simultaneously start their transmission on one frequency. If this happens, both transmitters abort their transmission and wait until a more or less random period expires. They only start their repetition if the other transmitter has not again started transmitting during this period. A second collision occurs only if the two randomly selected delays are identical.

DCF

“Distributed Coordination Function”, an organization model for radio networks. See 4.4

DFS

“Dynamic Frequency Selection”, similar to an extension of the → 802.11h standard. If, during operation, another (non-network) user is detected on a channel, the → access point changes the used channel. Influencing by other systems using the 5 GHz band (radar, satellite radio and satellite navigation) is to be avoided. See 3.6.

DoS

“Denial of Service”, an attack method against a network. See 5.3.

EAP

“Extensible Authentication Protocol”, a method within the framework of the → RADIUS protocol with which server and client can agree on one method of authentication before the actual authentication, see 5.2

Enabling button

During handling in hazardous environments the staff could use handheld enabling buttons which have three button positions. Operation of the device controlled by the enabling button is only possible in the central position by means of a moderately firm grip. If the enabling button is released or held very firmly (“panic switch”) the emergency stop of the device is triggered.

GPRS

General Packet Radio Service”, a data transmission service used for mobile phones communication.

Handover

The transition of a mobile client from one access point and its radio cell to the next (→ roaming); particularly the re-integration into the network. See 4.4

Hidden node problem

Same as → Hidden station problem

Hidden station problem

A connection problem which occurs if one receiver is simultaneously addressed by two senders, which cannot hear each other, which results in collision at the receiver. See 4.1.3.
HMI

“Human/Machine Interface”, display and operating devices for the plant control, such as SIMATIC mobile panels (see 10.1)

IEEE

“Institute of Electrics and Electronics Engineers” (pronounced “I – triple E”), a US association which, among other things, develops guidelines and technical recommendations; in the broader sense comparable to DIN (German Standards Institution). See 3.1

iHOP

“Industrial Hopping”, one method for optimizing the data throughput in radio networks. Access points and clients jump from frequency to frequency following a previously agreed plan. This ensures that the failure of one individual channel can only disrupt the communication for a short period of time. See 6.2.

Infrastructure mode

A radio network organized in such a way that one or several → access points form cells giving the network a “structure”. The opposite is an → ad hoc network. Compare 4.2

IP 30

A degree of protection indicating that a component categorized accordingly is protected against ingress of solid foreign bodies (with a diameter of 2.5 mm and more) but not against ingress of water. This corresponds to a conventional electrical household appliance.

IP 65

A degree of protection indicating that a component categorized accordingly is completely protected against dust and jet-water. This corresponds to an almost airtight enclosure.

iPCF

“Industrial Point Coordination Function”, a proprietary network protocol supported by SIEMENS which enables short → handover times (in the range of 30 ms) during → roaming of the mobile nodes. iPCF is not compatible with → iQoS. See 6.1

iQoS

“Industrial Quality of Service”, a method in which a specific → bandwidth is reserved for individual → clients. The result is a response time that is complied with with a high probability but not with certainty. iQoS thus meets less strict real-time requirements than → iPCF; it is not compatible with → iPCF. See 6.3

ISM

“Industrial, Scientific and Medical”, a band of the radio spectrum which, among other things, also includes the 2.4 GHz frequency range used by the → 802.11 protocol. See 2.4.4

LAN

“Local Area Network”, locally defined network, in contrast to, for example, the internet
Leaky wave cable
A coaxial cable whose outer shield is interrupted at defined distances. As a consequence, the cable generates a spatially limited short-range radio field that can be “formed” since it follows the cable bend. See 13.1

Link Check
An access point functionality for monitoring the connection to the clients. Different events (logging on, logging off of the clients, etc.) can cause automated reactions of the access point (sending mails/traps, turning on Fault LED, etc.). All SCALANCE W Access Points support L.

MAC
“Media Access Control”, a protocol used to control the access to a transmission medium (cable, radio) that cannot be used simultaneously by all nodes, see 5.

Mac Address
An identification number for each hardware component of importance in a network that is unique worldwide. → MAC and 5.

Middleware
Software performing a mediating function between operating systems and drivers on the one hand and user applications on the other hand.

MIMO
“Multiple Inputs, Multiple Outputs”, a method where each radio node sends and receives simultaneously with several antennas. MIMO is part of the → IEEE → 802.11n standard. (See 3.2.1 and 3.3)

MPI
“Multi-Point Interface”, a Siemens-proprietary RS-485-based bus for serial → PROFIBUS communication with a larger number of nodes.

N-Connect
A connection system for WLAN antennas, see 13.4

PCF
“Point Coordination Function”, an organization model for radio networks. See 4.4

PoE
“Power over Ethernet”, power supply of bus nodes via the Industrial Ethernet cable. See 9.1.2

Polling
Regular polling of status data or variables from a data source (“server”) by a client. (This client is not necessarily the client of a WLAN.) An alternative to polling is event-controlled transmission in which the server, without being polled, transmits data to the client as soon as it changes.

PROFIBUS
A field bus system for serial data transmission in automation technology based on → MPI hardware specifications.
PROFINET
An extension of the Ethernet communications standards to meet the “Industrial Ethernet” requirements, i.e. the use in an industrial environment. New properties are the measures to increase the transmission security and fault tolerance and the use of sturdy components, etc. The SCALANCE product generation is designed for use with P.

PROFIsafe
A protocol extension for \rightarrow PROFIBUS and \rightarrow PROFINET with which the transmission security is considerably increased, see 9.6

PSK
“Pre-Shared Key”, a method for authentication within the framework of the \rightarrow WPA/WPA2 protocols, see 5.2.2

Quality of Service
Transmission quality guaranteed in the framework of a network, see 3.5

RADIUS
“Remote Authentication Dial In User Service”, an access control method in which the authentication between client and access point is handled via a third, separate server on which the access data is stored. See 5.2.3

Rapid Roaming
\rightarrow Roaming during which the resumption of the connection occurs so rapidly that no noteworthy interruption of the connectivity (\rightarrow handover) takes place. See 4.4

Rapid Spanning Tree
A method for optimizing the data paths in networks, similar to \rightarrow Spanning Tree. Rapid S.T., however, was configured to keep the reconfiguration time as short as possible in the event of a failure of an access point.

RC4
An encryption algorithm used within the framework of the \rightarrow WEP and \rightarrow WPA standards. See 5.2

RCoax
A \rightarrow leaky wave cable, used for setting up realtime-capable radio networks with low reach, particularly suitable for \rightarrow clients with fixed motion paths (e.g. automated transport systems) or in heavily shaded environments (e.g. tunnels). See 13.1

RFID
“Radio Frequency IDentification”, a method where objects (e.g. books in a library) are fitted with passive radio transponders. The transponder responds to the request of a sender (e.g. read device at the borrowing section of the library) with an ID to track them. The transponders are small, cheap and are fed by the energy of the read device. Reach and data capacity, however, are low.

Roaming
The motion of a \rightarrow WLAN node from one radio cell to the next, see 4.1.2 and 4.4
R/SMA

“Reverse (Polarity) SubMiniature (version) A (Connector)”, a connection system for WLAN antennas, see 13.4

RSSI

“Received Signal Strength Indication”, strength of a receiving signal. RSSI is used for → AeroScout for triangulation and location determination of a node. See 3.7.4

RSTP

“Rapid Spannung Tree Protocol”, an algorithm used by switches in a network to automatically determine the optimal travel to the data transmission between two end nodes, and also to determine alternatives for the event of a failed transmission point. See 4.4.3

RTS/CTS

“Read-to-Send/Clear-to-Send”, a method for the avoidance of network collisions and for avoiding the → Hidden Station problem. See 4.4

SINEMA E

“SIMATIC NEwork MAnager Engineering”, software for simulating and configuring → WLANs with SIMATIC components. See 11

Spanning Tree

A method for optimizing the data paths in (radio) networks. The Spanning Tree method determines physically redundant network structures and prevents the generation of loops by disabling redundant paths. The data communication then takes place exclusively on the remaining connection paths. If the preferred data path fails, the Spanning Tree algorithm searches for the most efficient way possible with the remaining network nodes. See also → Rapid Spanning Tree

Spoofing

“Parody, swindle”, a general term for attacks to networks where the attacker disguises his own IP or MAC address (“IP spoofing”, “MAC spoofing”), faking the “identity” of a (authorized) network node. See 5.2.2 and 5.3

SSID

“Service Set Identifier”, in the framework of a → “Wi-Fi” WLAN the name of a network which, at the same time, must be known to all of its network nodes and which is part of each transmitted message. SSIDs alone only provide extremely weak access protection against third parties and should, in any case, be completed by other encryption methods. See 4.2

SSL

“Secure Sockets Layer”, a protocol for encrypted data transmission on the internet which receives its security by using “public key” algorithms.

TDOA

“Time Difference of Arrival”, runtime difference of a signal. TDOA is used for → AeroScout for triangulation and location determination of a node. See 3.7.4
TKIP

“Temporary Key Integrity Protocol”, a method for the dynamic change of the keys in a → WLAN, see 5.2.2.

TPC

“Transmit Power Control”, an extension of the → 802.11h standard in which only the transmitter power required for interference-free reception of the known clients is radiated. This prevents the generation of overreaches. See 3.6.

UMTS

“Universal mobile telecommunication system”, a mobile radio standard for data transmission with high capacity.

VLAN

“Virtual LAN”, a protocol extension for cable-based and wireless networks used for dividing a physical network into several logic subnets. See 4.4.1 and → VPN

VNS

“Virtual Network Services”, the organization of logical networks within one or several physical networks, see 12.3

VoIP

“Voice over IP”, the transmission of telephone conversations over the internet or other IP-based networks.

VPN

“Virtual Private Network”, a protocol expansion where protocol extensions closely related to → VLANs where the data traffic of a (virtual) subnet is “tunneled” within a larger network, i.e. invisible for the other nodes. This property makes VPNs suitable for increasing the security of network. See 4.2.2

WAN

“Wide Area Network”, a limited network with a larger expansion than a → LAN.

WBM

“Web Based Management”, configuration of an access point or client via a web interface, see 9.1.1

WDS

“Wireless Distribution System”, an → infrastructure mode for → WLANs, where the → access points set up a redundant network. S. 4.2.4

WEP

“Wire Equivalent Protocol”, an encryption method in wireless data communication, see 5.2.1

Wi-Fi

Designation introduced by the “WiFi Alliance” group of manufacturers for → WLAN products which are compatible with a specific subset of the → 802.11 standard; occasionally also (incorrectly) used as a synonym for WLAN in general. See 3.2
Wireless HART

("Highway Addressable Remote Transducer"), the wireless variant of a field bus standard, see 3.7.2.

WLAN

"Wireless Local Area Network", a "local radio network", thus a radio-based→ LAN.

WMM

"Wireless Multimedia Extensions", a subset of the → IEEE → 802.11e standard. See 3.5.

WPA, WPA2

"WiFi Protected Access", two encryption methods in wireless data communication, see 5.2.2

Zigbee

A radio standard similar to → WirelessHART, however, it is used for operation in home or facility automation. See 3.7.3
# 15 Internet Links

Note: Websites with relevant material have, where reasonable, already been linked directly in the text.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. SIEMENS I A Customer Support</td>
<td><a href="http://support.automation.siemens.com">http://support.automation.siemens.com</a></td>
</tr>
</tbody>
</table>
16 Index

2.4 GHz band ............................................ 13
2.4 GHz-Band ........................................ 26
5 GHz band ........................................ 26, 27
5 GHz-Band ........................................ 26
802.11 .................................................. 22
802.11 b/g .............................................. 30
802.11a .................................................. 22
802.11b .............................................. 22, 41
802.11e ............................................... 28, 101
802.11g .................................................. 22
802.11h .................................................. 22
802.11i .................................................. 46
802.11n .................................................. 22
802.15.1 (Bluetooth) .................................. 29
802.15.4 (WirelessHART) .......................... 29
802.15.4 (Zigbee) ..................................... 30
802.1D (STP) .......................................... 44
802.1w (RSTP) ........................................... 44
802.1x .................................................. 46
absorption (radio waves) .................................. 11
access points .......................................... 33
active components ..................................... 93
ad hoc network ....................................... 50
ad hoc networks ...................................... 46
Ad hoc networks ...................................... 40
ADSL .................................................. 24
Advanced Encryption Standard ................... 48
AES .................................................... 48, 71
antenna extension cable ............................. 117
antenna gain .......................................... 16
aperture angle .......................................... 17
  horizontal ........................................... 18
  vertical .............................................. 18
audio streams ......................................... 45
authentication ........................................ 47, 49
authentication methods ............................. 52
automated guided vehicle system 79, 81, 90
autoplacement ........................................ 96
backbone ............................................. 33
beam shaped ......................................... 25
BFOC bayonet fiber optic connector .............. 74
Bluetooth ............................................. 10, 13, 27
BPDU .................................................. 44
Bridge Protocol Data Unit .......................... 44
Broadcast ............................................. 41
carrier frequency ..................................... 14
CCMP .................................................. 47
cell level ............................................ 88
cellular phones ..................................... 13
channels ............................................. 14
chips ............................................... 24
DSSS .................................................. 24
clear-to-send ....................................... 45
CLI ...................................................... 68
coexistence management ........................... 60
clients .................................................. 33
collision ............................................... 14
collision avoidance ................................. 45
Command Line Interface ........................... 68
connection reliability .............................. 10, 28
consistency check ................................... 93
control level ......................................... 88
country approvals ................................... 62
C-PLUG .............................................. 109
DAB ..................................................... 24
data rate ............................................. 13
data transmission ................................. 45
  asynchronous .................................... 45
  synchronous .................................... 45
DCF ................................................ 45, 81
DECT telephones .................................... 27
Denial of Service .................................... 50
deterministic data communication .............. 52, 81
DFS ................................................ 28, 62
diffraction .......................................... 12
Direct Sequence Spread Spectrum .............. 24
directional antennas ............................... 18
Distributed Coordination Function ............. 45, 81
DoS ................................................ 50
DRM ............................................... 24
dynamic data communication ..................... 52, 81
Dynamic Frequency Selection .................. 28
dynamic routing ..................................... 100
EAP .................................................. 47, 48
effective area ....................................... 84
e-mail .................................................. 45
encryption methods ............................... 33
ET 200pro .......................................... 85
Exciter (AeroScout) ................................ 30
Extensible Authentication Protocol ............ 47, 48
fail-safe communication ........................... 81
fat access points .................................. 100
FC Modular Outlet Base .......................... 118
FC RJ 45 modular outlet ......................... 69
field level .......................................... 88
fit access points .................................. 100
frequency bands ................................... 14
FRNC .................................................. 117
Gateway .............................................. 42
GPRS ............................................... 10
GPS .................................................. 24
half duplex ......................................... 14
handover .......................................... 34, 52, 81
HART ................................................. 29
high-bay racking systems ....................... 104
high-bay warehouse ............................... 11
Highway Addressable Remote Transducer ...... 29

128/131
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>hijacking (Computer)</td>
<td>51</td>
</tr>
<tr>
<td>HiPath CAP</td>
<td>98</td>
</tr>
<tr>
<td>HiPath Cordless</td>
<td>98</td>
</tr>
<tr>
<td>HiPath Wireless</td>
<td>82</td>
</tr>
<tr>
<td>HiPath Wireless Controller</td>
<td>82, 100</td>
</tr>
<tr>
<td>HMI operation</td>
<td>90</td>
</tr>
<tr>
<td>Honeypot Access Point</td>
<td>50</td>
</tr>
<tr>
<td>hot standby</td>
<td>102</td>
</tr>
<tr>
<td>IEEE 802</td>
<td>21</td>
</tr>
<tr>
<td>IEEE 802.1Q</td>
<td>41</td>
</tr>
<tr>
<td>iHOP</td>
<td>53, 67</td>
</tr>
<tr>
<td>illumination</td>
<td></td>
</tr>
<tr>
<td>radio field</td>
<td>32, 92, 112</td>
</tr>
<tr>
<td>Impedance</td>
<td>15</td>
</tr>
<tr>
<td>Industrial Point Coordination Function</td>
<td>52</td>
</tr>
<tr>
<td>Industrial Point Coordination Function – Management Channel</td>
<td>57</td>
</tr>
<tr>
<td>infrastructure networks</td>
<td>35</td>
</tr>
<tr>
<td>Institute of Electrical and Electronics Engineers</td>
<td>21</td>
</tr>
<tr>
<td>interference</td>
<td>12</td>
</tr>
<tr>
<td>interference immunity</td>
<td>10</td>
</tr>
<tr>
<td>IP Spoofing</td>
<td>51</td>
</tr>
<tr>
<td>iPCF</td>
<td>34, 52, 67, 81</td>
</tr>
<tr>
<td>iPFC</td>
<td>67</td>
</tr>
<tr>
<td>IPsec</td>
<td>42</td>
</tr>
<tr>
<td>ISM band</td>
<td>14</td>
</tr>
<tr>
<td>LAN</td>
<td>10, 32</td>
</tr>
<tr>
<td>leaky wave cable</td>
<td>90, 104</td>
</tr>
<tr>
<td>leaky wave cables</td>
<td>19</td>
</tr>
<tr>
<td>lightning protection element</td>
<td>117</td>
</tr>
<tr>
<td>load distribution</td>
<td>100</td>
</tr>
<tr>
<td>Local Area Network</td>
<td>10</td>
</tr>
<tr>
<td>login procedure</td>
<td>47</td>
</tr>
<tr>
<td>mac address</td>
<td>47, 48</td>
</tr>
<tr>
<td>mac filters</td>
<td>48</td>
</tr>
<tr>
<td>MAC Spoofing</td>
<td>50</td>
</tr>
<tr>
<td>Man in the Middle-Angriff</td>
<td>51</td>
</tr>
<tr>
<td>microwave ovens</td>
<td>13, 27</td>
</tr>
<tr>
<td>MIMO</td>
<td>25</td>
</tr>
<tr>
<td>mixed networks</td>
<td>36, 52, 81</td>
</tr>
<tr>
<td>mobiles monitoring and operation</td>
<td>73</td>
</tr>
<tr>
<td>modeling</td>
<td></td>
</tr>
<tr>
<td>radio field</td>
<td>93</td>
</tr>
<tr>
<td>monorail conveyors</td>
<td>11, 19, 89, 90, 104</td>
</tr>
<tr>
<td>monorail overhead conveyor</td>
<td>79</td>
</tr>
<tr>
<td>MPI</td>
<td>13</td>
</tr>
<tr>
<td>multi-channel configuration</td>
<td>37</td>
</tr>
<tr>
<td>multimedia services</td>
<td>28</td>
</tr>
<tr>
<td>Multiple Input/Multiple Output</td>
<td>25</td>
</tr>
<tr>
<td>N-Connect connections</td>
<td>115</td>
</tr>
<tr>
<td>non-overlapping channels</td>
<td>26</td>
</tr>
<tr>
<td>nutrunner controller</td>
<td>80</td>
</tr>
<tr>
<td>OFDM</td>
<td>22, 23</td>
</tr>
<tr>
<td>omnidirectional antennas</td>
<td>13, 18</td>
</tr>
<tr>
<td>operating and monitoring</td>
<td>83</td>
</tr>
<tr>
<td>Orthogonal Frequency Division Multiplexing</td>
<td></td>
</tr>
<tr>
<td>Panel</td>
<td>83</td>
</tr>
<tr>
<td>PCF</td>
<td>45</td>
</tr>
<tr>
<td>PG/OP communication</td>
<td>90</td>
</tr>
<tr>
<td>phantom feed</td>
<td>69</td>
</tr>
<tr>
<td>planning phase</td>
<td>92</td>
</tr>
<tr>
<td>Point Coordination Function</td>
<td>45</td>
</tr>
<tr>
<td>point-to-point networks</td>
<td>41</td>
</tr>
<tr>
<td>polarisation</td>
<td>15</td>
</tr>
<tr>
<td>Power over Ethernet</td>
<td>69</td>
</tr>
<tr>
<td>Power Rail Booster</td>
<td>50</td>
</tr>
<tr>
<td>power splitter</td>
<td>118</td>
</tr>
<tr>
<td>power supply unit</td>
<td>117, Siehe Netzteil</td>
</tr>
<tr>
<td>PRESET-PLUG</td>
<td>111</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>47</td>
</tr>
<tr>
<td>Process Device Manager</td>
<td>90</td>
</tr>
<tr>
<td>PROFIBUS</td>
<td>81, 88</td>
</tr>
<tr>
<td>PROFIBUS DP slave</td>
<td>88</td>
</tr>
<tr>
<td>PROFINET</td>
<td>66, 81</td>
</tr>
<tr>
<td>PROFINET IO</td>
<td>49, 52, 89, 106, 108</td>
</tr>
<tr>
<td>PROFIsafe</td>
<td>81</td>
</tr>
<tr>
<td>PSK</td>
<td>47</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>28, 41, 101</td>
</tr>
<tr>
<td>R/SMA connection</td>
<td>115</td>
</tr>
<tr>
<td>radar</td>
<td>27</td>
</tr>
<tr>
<td>radio field</td>
<td>18</td>
</tr>
<tr>
<td>radio leaks</td>
<td>94</td>
</tr>
<tr>
<td>RADIUS</td>
<td>49, 103</td>
</tr>
<tr>
<td>rapid roaming</td>
<td>34, 67, 76, 81, 88, 106</td>
</tr>
<tr>
<td>Rapid Roaming</td>
<td>52</td>
</tr>
<tr>
<td>Rapid Spanning Tree Protocol</td>
<td>44</td>
</tr>
<tr>
<td>RC4</td>
<td>47</td>
</tr>
<tr>
<td>RCox</td>
<td>89</td>
</tr>
<tr>
<td>RCox cable</td>
<td>79</td>
</tr>
<tr>
<td>RCox-Kabel</td>
<td>90, 104</td>
</tr>
<tr>
<td>ready-to-send</td>
<td>45</td>
</tr>
<tr>
<td>real-time requirements</td>
<td>33, 45</td>
</tr>
<tr>
<td>redundancy mode</td>
<td>72</td>
</tr>
<tr>
<td>redundant power supply</td>
<td>69</td>
</tr>
<tr>
<td>redundant wireless LANs</td>
<td>39</td>
</tr>
<tr>
<td>reflection (radio waves)</td>
<td>11</td>
</tr>
<tr>
<td>Remote Authentication Dial In User Service</td>
<td>49</td>
</tr>
<tr>
<td>RFID</td>
<td>10, 20, 30</td>
</tr>
<tr>
<td>roaming</td>
<td>34, 106</td>
</tr>
<tr>
<td>Rogue Access Point</td>
<td>50</td>
</tr>
<tr>
<td>rogue access points</td>
<td>103</td>
</tr>
<tr>
<td>RR features</td>
<td>67</td>
</tr>
<tr>
<td>RSSI</td>
<td>30</td>
</tr>
<tr>
<td>RSTP</td>
<td>44</td>
</tr>
<tr>
<td>RTS/CTS</td>
<td>45</td>
</tr>
<tr>
<td>SCALANCE</td>
<td>66</td>
</tr>
<tr>
<td>SCALANCE W</td>
<td>66</td>
</tr>
<tr>
<td>scattering</td>
<td></td>
</tr>
<tr>
<td>radio waves</td>
<td>11</td>
</tr>
<tr>
<td>Service Set Identifier</td>
<td>36</td>
</tr>
</tbody>
</table>
Index

shared medium.................................10
signal quality.....................................93
silent listeners..................................10
SIMATIC NETwork MAnager Engineering 92
SIMATIC PDM....................................90
simulation of a radio field....................92
site survey.......................................96
sliding contacts...............................11
smart antenna..................................25
Spanning Tree Protocol.......................44
spatial multiplexing............................25
spoofing..........................................49
spot welders....................................20
SSID.................................................36
SSL..................................................42, 48
stacker crane systems.........................89, 90
Stand-alone-Netzwerke.......................35
switch..............................................33
TCP.................................................62
TDOA...............................................30
Temporal Key Integrity Protocol..............47
terminating resistor............................117
time slots.........................................33
TKIP.................................................47, 71
TLS..................................................42, 48
TPC..................................................28
trailing cables..................................11
transmission range.............................13
Transmit Power Control.......................28
transmitter power
  dynamic adjustment..........................100
Transport Layer Security....................48
UMTS.............................................10, 24
Virtual LAN......................................41
Virtual Network Services.....................102
Virtual Private Network......................42
VLAN..............................................41
VNS...............................................102
Voice over IP...................................98, 102
Voice over WLAN...............................82
VPN...............................................42, 103
W-740.............................................67
W-780.............................................67
WBM...............................................68
WDS...............................................38
Web Based Management.......................68
web browsing....................................45
WEP...............................................41, 47, 103
Wi-Fi..............................................23
Wi-Fi Protected Access.......................47
Wired Equivalent Privacy.....................47
wireless controller............................100
Wireless Distribution System................38
WirelessUSB.....................................24
WMM...............................................28, 101
WPA...............................................47, 71, 103
WPA2.............................................48, 71, 103
## 17 History

### Table 17-1

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.04.2006</td>
<td>First edition</td>
</tr>
<tr>
<td>1.1</td>
<td>07.11.2007</td>
<td>Various updates</td>
</tr>
<tr>
<td>2.0</td>
<td>01.01.2010</td>
<td>Various updates</td>
</tr>
<tr>
<td>2.1</td>
<td>08.02.2011</td>
<td>Various updates</td>
</tr>
</tbody>
</table>