SIEMENS
Ingenuity for life

Basic information on configuring an Industrial Wireless LAN

SCALANCE W

https://support.industry.siemens.com/cs/ww/en/view/22681042

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cert.

Table of contents

Legal information **2**

Foreword **6**

1 Radio waves as the basis of a "shared medium" network **7**

1.1 Overview of radio standards 7

1.2 Introduction to radio networks 7
1.2.1 Comparing radio waves and cables 7
1.2.2 Complexity of the radio field 7
1.2.3 Access rules in a shared medium network 8

1.3 Preferred areas of application 8

1.4 The physics of radio waves 9
1.4.1 Propagation 9
1.4.2 Interferences 10
1.4.3 Transmission range and data rate 10
1.4.4 Frequencies, frequency spacing and channels 11

1.5 Antennas 12
1.5.1 Properties of an antenna 12
1.5.2 Omnidirectional and directional antennas 13
1.5.3 Fresnel zone 17

1.6 Modulation and multiplex methods 19

1.7 Requirements for radio communication in industrial environments ... 19

2 The WLAN standard IEEE 802.11 .... **20**

2.1 The network standards for the IEEE 802 series 20

2.2 Communication standard of IEEE 802.11 21
2.2.1 IEEE 802.11a 21
2.2.2 IEEE 802.11b 22
2.2.3 IEEE 802.11g 24
2.2.4 IEEE 802.11n 24
2.2.5 IEEE 802.11ac 26
2.2.6 IEEE 802.11ad 27
2.2.7 IEEE 802.11ax 27
2.2.8 Transmission range and special antennas 27

2.3 Additional IEEE 802.1x standards 28
2.3.1 IEEE 802.11e and WMM: "Quality of Service" 28
2.3.2 IEEE 802.11h and the 5 GHz band 28
2.3.3 IEEE 802.11r 29

2.4 Channel distribution in the IEEE 802.11 standard 31
2.4.1 The 2.4 GHz band 31
2.4.2 The 5 GHz band 31
2.4.3 The 6 GHz band 32
2.4.4 Comparison of the properties of the 2.4 GHz and the 5/6 GHz band 32

3 Alternative radio technologies with IWLAN **33**

3.1 Bluetooth 33

3.2 Wireless HART 33

3.3 Zigbee 34

3.4 WiMAX 34

4 Topology, configuration and organization of IWLANs 35

4.1 The structure of a WLAN 35
4.1.1 Structuring by cell distribution 35
4.1.2 Connecting individual wireless cells: Access points and clients 36

4.2 The "roaming" method 38

4.3 Infrastructure networks 39
4.3.1 Standalone networks 39
4.3.2 Mixed networks 39
4.3.3 Multichannel configuration 40
4.3.4 Wireless Distribution System (WDS) 41
4.3.5 Redundant wireless link 42

4.4 Coordination of data transfer 44
4.4.1 Distributed Coordination Function (DCF) 44
4.4.2 OFDM 45
4.4.3 OFDMA 45
4.4.4 Hidden Station and RTS / CTS methods for collision avoidance 46
4.4.5 Point Coordination Function (PCF) 46

4.5 Functions for network management 47
4.5.1 Virtual LANs (VLANs) 47
4.5.2 Spanning Tree Protocol (STP) 47
4.5.3 Rapid Spanning Tree Protocol (RSTP) 48
4.5.4 Multiple Spanning Tree Protocol (MSTP) 48

4.6 Proprietary extensions of the IEEE 802.11 standard: iFeatures 49
4.6.1 Industrial Point Coordination Function (iPCF) 49
4.6.2 iPCF – Management Channel (iPCF-MC) 51
4.6.3 iREF 53
4.6.4 Inter AP blocking 54
4.6.5 iPRP 55
4.6.6 Sleep Mode 57
4.6.7 TCP event roaming 57
4.6.8 Usable IWLAN devices 58
4.6.9 iFeatures and PROFINET I/O 59

5 Data Security and Encryption 60

5.1 Attack scenarios and security mechanisms 60
5.1.1 Basics of WLAN security 60
5.1.2 Attack scenarios 60
5.1.3 IEEE 802.11 security mechanisms 62

5.2 Measures for increasing the WLAN security 63
5.2.1 The IEEE 802.11i extension - encryption methods 63
5.2.2 Wi-Fi Protected Access security standard (WPA) 64

5.3 Authentication and key management 66
5.3.1 IEEE 802.1X authentication 66
5.3.2 Pre-Shared Key (PSK) 66

5.4 Safety functions and data rate 67

6 Coexistence of IWLANs with other wireless networks 68

7 Country approvals 70

7.1 General remarks 70

7.2 Country approvals in the SCALANCE W devices 71

8 SIMATIC NET products for setting up an IWLAN 73

8.1 General information 73
8.1.1 Overview of product range 73
8.1.2 Division of SCALANCE W products 73

8.2 SCALANCE W access points 75
8.2.1 IEEE 802.11 ax access points 75
8.2.2 IEEE 802.11 ac access points 76

8.3 SCALANCE W clients 78
8.3.1 IEEE 802.11 ax client modules 79
8.3.2 IEEE 802.11ac client modules 80

8.4 Configuring the SCALANCE W devices 82

9 Accessories for wireless networks (WLANs) 84

9.1 Optional storage media 84
9.1.1 SCALANCE CLP 84
9.1.2 KEY-PLUG 84
9.1.3 C-PLUG 85

9.2 RCoax radiating cables 85

9.3 Antennas 87
9.3.1 Overview of WLAN antennas 87
9.3.2 Antennas with an omnidirectional property 89
9.3.3 Antennas with directional effect 93
9.3.4 Antennas for RCoax 95

9.4 Connections and cabling 96

9.5 Additional accessories 97

9.6 Useful tools 103
9.6.1 Industrial Wireless LAN – Distance Estimation Tool 103
9.6.2 TIA Selection Tool 104
9.6.3 Signal recorder 105
9.6.4 Spectrum analyzer 107
9.6.5 Remote capture 108
9.6.6 Network management with SINEC NMS 109

10 IWLAN in use 110

11 Glossary 114

12 Appendix 121

12.1 Service and support 121

12.2 Industry Mall 121

12.3 Links and literature 122

12.4 Change documentation 123

Foreword

Aim of the document

This document provides an overview of the special requirements for setting up an Industrial Wireless LAN and offers an introduction to the properties of the relevant SIEMENS products.

You will first be introduced to the topic of wireless local area networks (WLANs) in an industrial environment and the main technical principles will be presented. We will then show you various SIEMENS products, highlight their possible uses and provide you with decision-making tools for the process of choosing the best solution for your task.

Key topics in this document

This document deals with the following key topics:

- Properties of WLANs in general,
- Siemens products for the installation of wireless networks with a particular focus in industrial environments.

Exclusions

This document does not contain a detailed description for the software installation or for the commissioning of the individual components.

Current and detailed information on these topics can be found in the manuals and operating instructions for the corresponding products.

1 Radio waves as the basis of a "shared medium" network

1.1 Overview of radio standards

There are currently a number of different technologies for constructing radio networks, such as Bluetooth, GPRS and UMTS for mobile telephone networks, RFID tags for identification and product tracking, etc. (see also chapter 3).

For the purposes of this document, we limit ourselves to WLANs in the narrower sense, meaning radio networks that comply with the IEEE 802.11 standard (see chapter 2). We refer to WLANs that have been "hardened" by special measures as IWLANs (Industrial WLANs). In other words, they can be used for the industrial sector’s requirements and environments.

1.2 Introduction to radio networks

1.2.1 Comparing radio waves and cables

The use of cables and lines for communication has certain advantages because an exclusive medium is available: The transmission properties 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 (abbrev. 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. Ultimately, the use of wired methods for communication with freely moving nodes is only feasible in exceptional cases. Radio links also enable bridging zones for sections for which cabling would otherwise be difficult (streets, waters).

Radio-based networks can show their advantages in these applications (advantages that are generally less bound to a specific location). In these cases, the potentially higher investment costs are compensated by increased customer benefits.

1.2.2 Complexity of the radio field

Radio waves propagate through space, are diffracted or reflected by obstacles, or attenuated while passing. They generate a complex radio field that even undergoes changes when obstacles move. It remains clear that the range illuminated by one or several transmitter(s) is not sharply defined. Thus, there is no clear delimitation of the radio field which causes a fluctuation of the transmission properties 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 eavesdropping security or interference immunity of a network. Assuming responsible administration, careful planning and the availability of trained employees who are aware of the specific concerns pertaining to wireless networks, they are as reliable, secure and robust as wired networks.

1.2.3 Access rules in a shared medium network

Radio networks are so-called "shared medium" networks, i.e. all stations share the network. To prevent multiple accesses to the network, there has to be a rule, which node is allowed to transmit when.

This is achieved using CSMA (Carrier Sense Multiple Access). This protocol requires a check from each station before transmission to determine whether the medium is free. Only then may data be transmitted.

If two stations are checked at the same time, it is possible for both to recognize the medium as free and transmit data simultaneously. This results in a collision, making the data unusable. A wireless transmitting station is not able to detect a signal collision itself. Its own signal covers the signals from other stations, and it is impossible for collisions to be distinguished from interference.

In order to avoid these non-recognizable collisions as well as possible, the CA (Collision Avoidance) system is also used. If the occupied medium is now free, a station ready to transmit will not start straight away with the data transmission but will wait for a randomly determined period of time. After the lapse of this wait time, the station will again check the status of the medium. Because of this random wait time, it is very unlikely that both will start to transmit at the same time.

1.3 Preferred areas of application

In many environments, the special qualities of radio networks mean that they are the preferred, and in some cases, the only practical medium.

These areas of application for which radio networks are intended 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 cable-based subnets (different buildings, streets, waters),
- Communication with nodes in areas that are difficult to access.

1.4 The physics of radio waves

1.4.1 Propagation

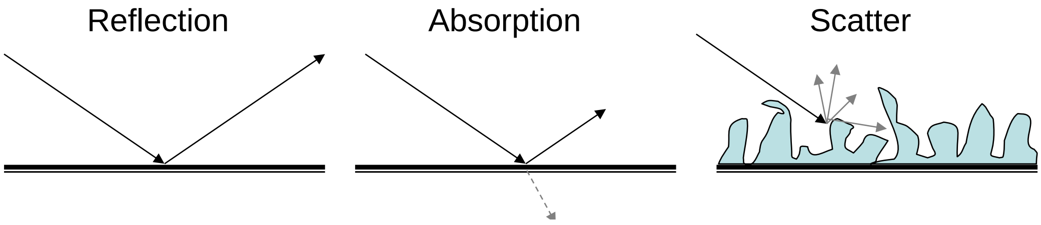
Unlike signals in a line, radio signals propagate three-dimensionally in space as electromagnetic waves.

Obstacles and objects influence the propagation of radio waves, effects such as reflexion, diffusion, absorption, interference and diffraction occur.

Reflection and absorption

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 the rest is finally allowed through the object. When hitting edges, radio waves are scattered into practically all directions.

Figure 1-1



Fading and diffraction

Two additional properties are important for the propagation of radio waves:

- On the one hand, radio waves (unlike incoherent light) can amplify or even extinguish each another (called "fading or interference"). If a receiver is located in both the direct beam and the reflection of a transmitter, it does not necessarily detect double the signal strength, 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 a 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 radiation used. 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 transmission and reception behavior to change.

Frequency sensitivity of radio wave properties

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 are then not able to reach receivers located behind objects. On surfaces, they are almost completely absorbed or reflected.

Signals of a longer wavelength, however, are also able to "go around objects" and penetrate deeper into non-conducting objects or pass through them.

1.4.2 Interferences

Each object that is located spatially within a radio network is capable of interfering with 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 proximity which, intermittently or continuously, can radiate on strictly limited channels or emit broadband radiation.

These devices include those designed as transmitters such as cordless phones and Bluetooth devices, microwave ovens, welding devices, etc.

However, such interferences can already be counteracted before they occur by carefully planning the radio network.

1.4.3 Transmission range and data rate

The transmission range and achievable data rate of a radio transmitter depend on several aspects, including the frequency used.

Transmission range

Essentially, the transmission range for transmitters of short wavelengths (higher frequency) is shorter than the range for long wavelengths: The shortwave signals behave similarly to light, can only propagate in a straight line and are completely absorbed or reflected by objects. This results in a considerable decrease of the signal quality if the free line of sight between transmitter and the receiver is impaired. However, the transmission range can be significantly increased with the use of directional antennas.

With the "SIEMENS IWLAN Distance Estimation Tool" (see chapter 9.6.1), it is possible to calculate the theoretical range as a function of multiple parameters, such as frequency and transmit power.

Data rate

The maximum data rate that can be transmitted on a carrier wave is proportional to the bandwidth that is available, i.e. the larger the bandwidth, the larger the attainable data rate.[1]

Transmitters on a frequency of 2.4 GHz (as used by the IEEE 802.11 method) can typically achieve ranges between approx. 30 m to 100 m (indoors or outdoors) with omnidirectional antennas (see also Table 2-2). The data rates that can be transmitted on this band amount to up to 450 Mbit/s.

[1] The theoretically attainable gross data rate (in bit/s) is proportional to the bandwidth. This dependency is described by the Shannon-Hartley theorem.

Relevance of the data rate

Which data rate is actually necessary or sufficient for a specific application does not only depend on the quantity of user data – even if the connections are optimal. Depending on the protocol, a smaller or larger overhead results for the handling of the radio communication, and interconnected devices such as access points, routers, etc., also cause delays that 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 actual existing radio network.

1.4.4 Frequencies, frequency spacing and channels

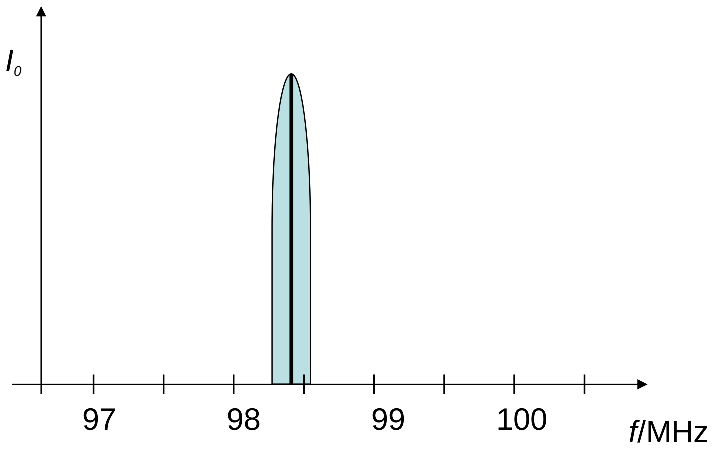
Only one node can transmit on each radio frequency at any given time. If several stations transmit on the same frequency simultaneously, none of them can be received. This case is referred to as a "collision".

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

Frequencies and required spectrum

Strictly speaking, stating that a transmitter emits on exactly one frequency is not correct: This would only be true in the case of a pure sinusoidal signal. The transmitter also assumes a range of frequencies above and below the carrier frequency. This is the reason why the transmitters have to maintain a frequency spacing in relation to each other that is proportional to the data rate used: This is referred to as the "bandwidth" of the transmitter.[2]

Figure 1-2



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

Bands and channels

To maintain clarity, the radio spectrum, i.e. the entire frequency range of the radio communication, is divided into individual "bands". The various bands differ in their

[2] The general colloquial term for transmission capacity is "bandwidth".

radio properties (transmission range, susceptibility to interferences, possible data rate, etc.) and consequently also in their applications.

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

The 2.4 GHz range of the ISM band,[3] for example, is divided into thirteen channels with a center frequency between 2.412 GHz and 2.472 GHz, where the distance between the neighboring channels is 5 MHz each. Theoretically, thirteen transmitters are able to use the band simultaneously.[4]

1.5 Antennas

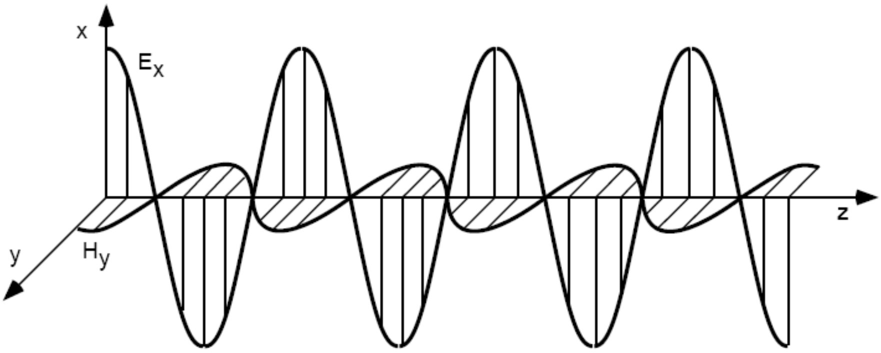
Task

Antennas transform 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 electric field vector *E_x* and a magnetic field vector *H_y* that always face each other at a right angle. The current is the cause of the magnetic field vector and the voltage causes the electric field vector (see graphic).

Figure 1-3



1.5.1 Properties of an antenna

Impedance

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

[3] "Industrial, Scientific and Medical"; also see glossary.
[4] However, since the frequency ranges of transmitters from neighboring channels overlap, there are only three channels that are mutually interference-free (also see chapter 2.4.1).

Polarization

The polarization specifies the direction of the vector of the electric field intensity in the radiated electromagnetic wave. A distinction is made between linear and circular polarization. With linear polarization, the electrical field lines run in one plane. If they are aligned vertically to the surface of the earth, we talk of vertical polarization. If they run horizontally to the surface of the earth, this is horizontal polarization.

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

Table 1-1

Polarization	Electrical field direction	Magnetic field direction
Linear vertical	Vertical	Horizontal
Linear horizontal	Horizontal	Vertical
Circular	Constantly circulating around the axis of propagation (clockwise or anticlockwise)	

For optimum reception, it is important for the polarization of both corresponding antennas to be identical. If the polarization levels differ by, e.g. 90°, an attenuation of 20 dB is not uncommon.

This is why it is especially important to pay attention to the alignment of the polarization levels for antennas with several beams in one housing (dual / MIMO).

1.5.2 Omnidirectional and directional antennas

The radiation of antennas can be either omnidirectional or directional. In general, directional antennas achieve higher transmission ranges. However, this is not the effect of higher transmission power but caused by the shape of the radio field.

Antenna gain

The antenna gain is a measured variable that describes how strongly an antenna sends and receives as compared to an reference emitter.

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

The unit used for the antenna gain is normally "dBi" (i = isotropic radiator). A gain of 3 dBi approximately corresponds to a doubled send/receive line.[5]

Antenna patterns

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

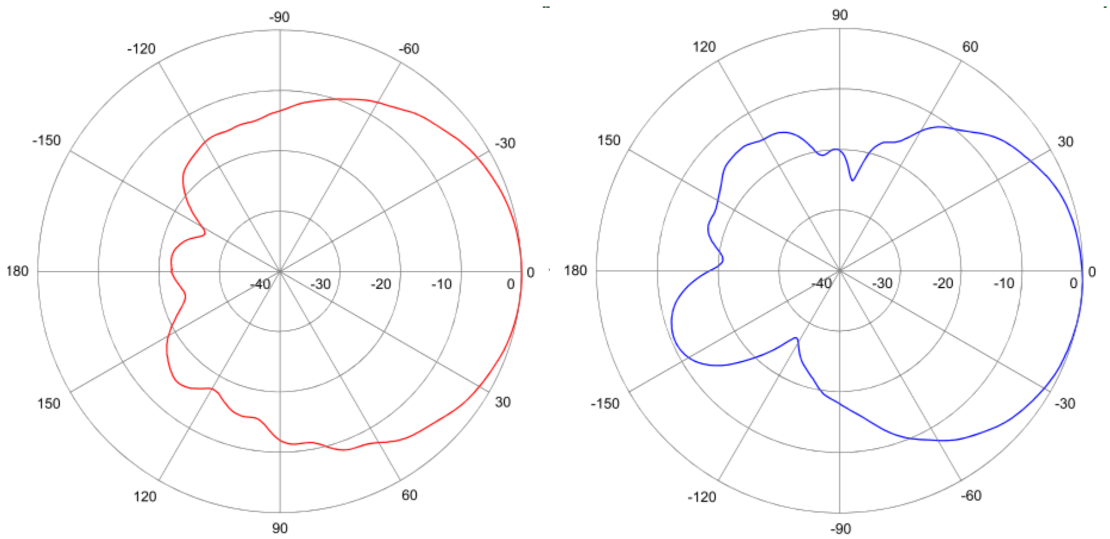
A horizontal antenna pattern is a front view of the electromagnetic field of an antenna with the antenna at the center. The gain is plotted as distance from the center of the coordinate system above the send/receive angle.

A vertical antenna pattern 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.

The following graphic shows a horizontal (left) and a vertical (right) antenna pattern for a directional antenna.

[5] Since the antenna gain is measured in logarithms, 6 dBi corresponds to four times the power, 9 dBi to eight times the power, etc.

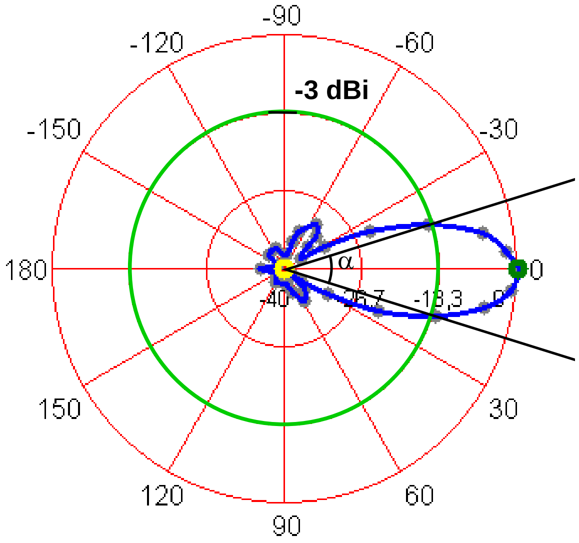
Figure 1-4


-90
-120
-60
-150
-30
180
0
-40
-30
-20
-10
0
150
30
120
60
90
90
120
60
150
30
180
0
-40
-30
-20
-10
0
-150
-30
-120
-60
-90

Opening angle

The opening angle refers to the angular distance at which the field intensity of the antenna has dropped to approximately half ≈ 3 dBi of the maximum. The following graphic shows how the opening angle can be determined using an example of an antenna pattern. The -3 dBi circle is represented in green, and marks half of the signal maximum (= 0 dBi). The intersections of the blue antenna gain pattern with the green circle define the opening angle of the antenna. (Here: approx. 30°)

Figure 1-5



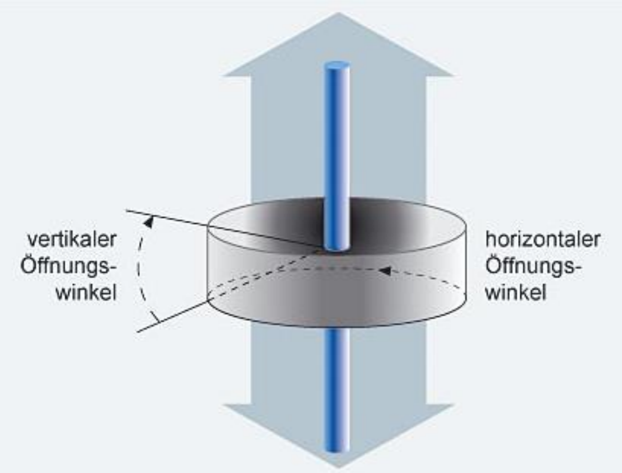
The horizontal and vertical opening angles of an antenna usually differ depending on the geometry.

Omnidirectional antennas

In general, omnidirectional 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. it is not equal in all directions. The radio field of the antenna reaches the maximum intensity on a plane, running at a right angle to the antenna axis (compare Figure 1-6). The field intensity quickly decreases above and below the "vertical aperture angle" of this plane and most of the time, no noteworthy signal can be expected vertically above and below the antenna.

The radio field is has radially symmetric form, meaning that the field intensity is identical in all directions when viewed from the top along the antenna axis. In this case, the "horizontal opening angle" is 360°.

Figure 1-6

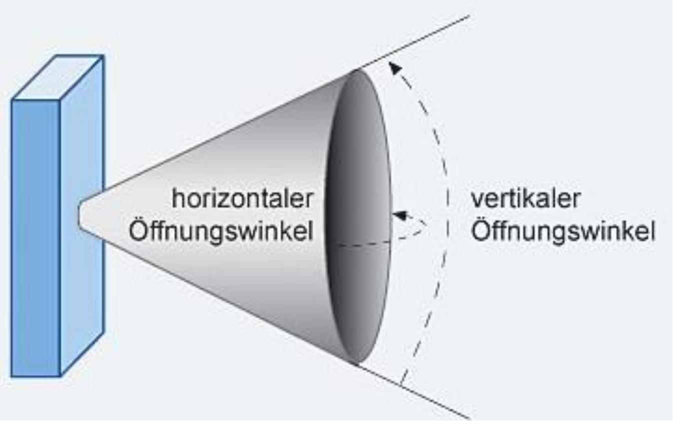


Directional antennas

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

The cone is defined by a horizontal and a vertical opening angle; the field intensity decreases quickly outside this angle.

Figure 1-7



In the direction of maximum field intensity, the transmission range of a directional antenna is typically ten times larger than the range of an omnidirectional antenna.

Antennas for SCALANCE W devices

Chapter 9.3 provides an overview of antennas suitable for operation with the SCALANCE W devices.

Radiating cables

An alternative to conventional antennas cables are radiating cables, where the developing radio field is limited to the immediate proximity of the conductor.

The fields of application for this type of radiating cables are moving nodes that travel along defined paths (e.g. monorail conveyors, automated guided vehicle systems), tunnels and similar areas that are difficult to cover using cabling.

An example of a radiating cable is the RCoax cable from chapter 9.1.

1.5.3 Fresnel zone

As described in the previous chapter, obstacles and objects have an influence on the propagation of radio waves and therefore on the attainable range.

The Fresnel zone has been defined in order to be able to specify the possible range. The Fresnel zone describes certain spatial areas between the transmitter and receiver antennas and therefore indicate the signal propagation. For calculating the free space loss, the following is required

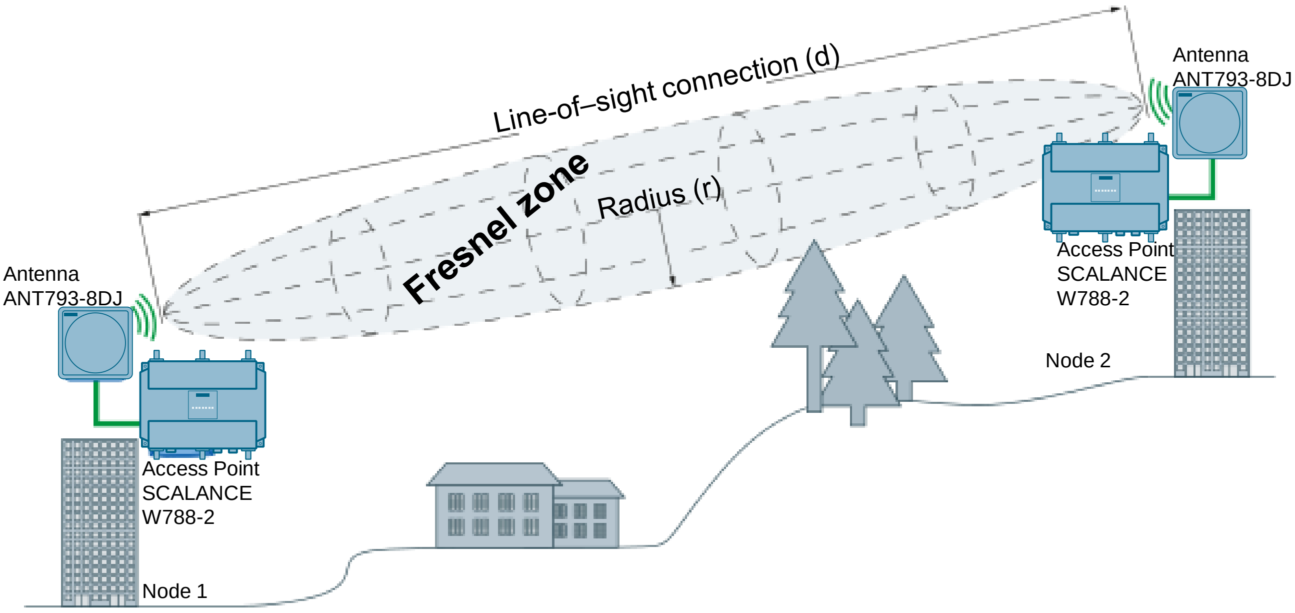
1. direct line-of-sight connection between the transmission path of the transmitter and receiver and
2. the presence of another area around this line-of-sight contact that must also be free of obstacles.

It is divided into several subzones. The first subzone[6] is the most significant, as this is where the majority of the signal energy is transmitted.

The above-mentioned conditions for the applying the free space loss are met if the first Fresnel zone is free of obstacles.

The Fresnel zone is in the shape of an ovoid and is dependent on the frequency of the radio waves and the distance between the transmitter and receiver. The diameter of these zones becomes smaller as the frequency increases, and becomes larger as the distance between the transmitter and receiver station increases.

Figure 1-8



[1] The first Fresnel zone is the area where the sum of the distance of the two antennas is λ/2 larger than the line-of-sight connection d (λ corresponds to the frequency wave length).

1.6 Modulation and multiplex methods

In order to transmit a signal using oscillation, the signal has to be "modulated" onto a carrier wave. The "sum" of the carrier wave and the signal is transmitted to the receiver, which then "subtracts" the carrier wave from the received oscillation, thus receiving the pure signal.

If the radio transmission is analog, the amplitude of the carrier wave or its frequency can change depending on the signal, for example. Medium wave stations use the former method while VHF uses the latter; this is the reason why these bands are referred to as "AM" ("amplitude modulation") or "FM" ("frequency modulation") in Anglo-American regions.

For the transmission of digital data, more complex methods such as the "Orthogonal Frequency Division Multiplexing" (OFDM) and "Direct Sequence Spread Spectrum" (DSSS) modulation methods are used (see chapter 2.2).

1.7 Requirements for radio communication in industrial environments

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

Data volumes

In office environments, it is common to move files that are several megabytes in size, whereas in industrial applications, the data packets are often much smaller.

Transmission rate and latency

Temporal delays in the communication between office devices, such as between sending and executing a print job, do not generally cause any issues. In industrial environments, however, measured values and control commands (e.g. emergency off) must often be exchanged within milliseconds.

Fail-safety and reliability

Data loss or data corruption during transmissions in an office environment is not normally critical, since the transmission can always be repeated. However, for industrial plants, the delays caused by failed and repeated transmissions are often unacceptable.

Additional interferences in industrial sectors

Office and home environments are usually characterized by a low degree of interference from objects that are not part of the radio network. Industrial environments, on the other hand, exhibit numerous inherent and highly intensive interferences that have an adverse effect on the propagation of electromagnetic waves. Metal parts or other signal sources, such as RFID, can be found virtually everywhere, which can lead to transmission disturbances or interruptions.
Metal surfaces reflect radio waves, for example, which can result in packet loss or even cancel the radio signal.

2 The WLAN standard IEEE 802.11

2.1 The network standards for the IEEE 802 series

The *Institute of Electrical and Electronics Engineers* IEEE[7] is tasked with developing, publishing and promoting electronic and electrotechnical standards.

Under the project number "802", a number of working groups were given the task of developing standards for setting up and operating networks. Group "802.3" is responsible, for example, for the standards relating to Ethernet connections.

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

The IEEE develops the standards on an ongoing basis in order to adapt them to new requirements and technical conditions.

The following table provides an overview of some of the IEEE 802 standards regarding IWLANs:

Table 2-1

Standard	Definition area
802.11a	Communication
802.11ac	Communication
802.11ad	Communication
803.11ax	Communication
802.11b	Communication
802.11e	Quality of Service (see chapter 2.3.1)
802.11g	Communication
802.11h	Communication (interruption reduction)
802.11i	Data security (see chapter 5.2.1)
802.11n	Communication
802.1Q	Virtual LANs (see chapter 4.5.1)
802.1X	Data security (see chapter 5.2.1)

Note

The 11a/b/g/h/n/ac/ad/ax standards cannot ensure deterministic communication. If you require deterministic communication, for example with PROFINET IO, use the iPCF proprietary protocol (see chapter 4.6.1).

[7] For more information, see also http://www.ieee.org/portal/site,

2.2 Communication standard of IEEE 802.11

The original 802.11 standard[8] (often referred to today 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.

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

The standard was improved with the extensions "b", "a", "g", "h", "n" and "ax", which were introduced to the market in this order.

Concerning the frequency bands used (2.4 GHz, 5 GHz and 6 GHz), the different standards vary with regard to the channels that can be used simultaneously and the maximum data rate.

Increases in the transmission capacities were achieved by using more complex and efficient modulation methods.

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

The following table lists the technical properties of the current prevailing 801.11 standard.

Table 2-2

	802.11a/h	802.11b	802.11g	802.11n	802.11ac	802.11ad	802.11ax
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz and 5 GHz	5 GHz	60 GHz	2.4 GHz and 5/6 GHz
Theoretical max. gross data rate	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s	7 Gbit/s	7 Gbit/s	10 Gbit/s
Modulation and multiplex methods*)	OFDM	DSSS	OFDM	MIMO and OFDM	MIMO and OFDM	OFDM/ QAM	MU-MIMO and OFDMA

*) for the individual modulation methods, see chapter 1.6

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

In principle, an 802.11a device is not able to communicate with an 802.11b/g device, as they are transmitting on different frequency bands. However, the "b", "n" and "g" versions of the standard are compatible.

2.2.1 IEEE 802.11a

Description

The IEEE 802.11a standard was adopted in 1999. It uses the 5 GHz frequency band and the Orthogonal Frequency Division Multiplexing (OFDM) modulation method and SISO technology. This can be used to achieve a maximum gross data rate of 54 Mbit/s.

This frequency band is mainly used by the military for radar purposes in air and marine traffic. WLAN tends to be a secondary user here.

In order to prevent interferences between WLAN and radar, the Transmit Power Control and Dynamic Frequency Selection (see chapter 2.3.2) also has to be implemented in some countries. For this purpose, the IEEE 802.11h standard was developed as an extension to IEEE 802.11a.

[8] See also http://grouper.ieee.org/groups/802/11/, http://standards.ieee.org/wireless/overview.html#802.11

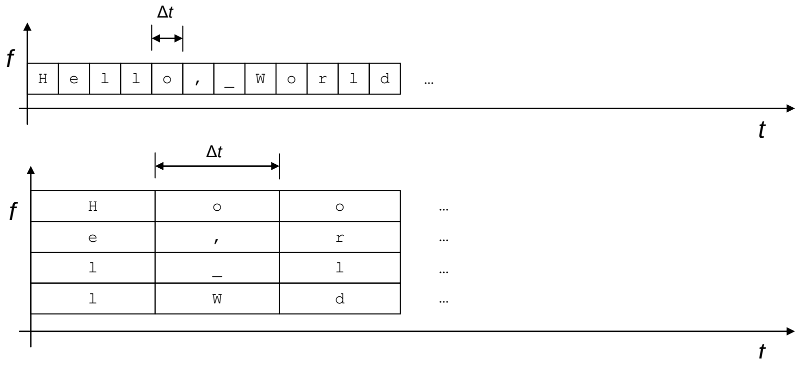
Orthogonal Frequency Division Multiplexing (OFDM) modulation method

OFDM does not use only one frequency to transfer a signal, but rather transmits on several hundred to several thousand channels in very close proximity 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. there is much more time available for transmitting the individual bits. Consequently, OFDM connections are significantly less susceptible to any short-term noise or occurring echoes. Even in the case of considerable path differences, there is a high probability that an echo received is still associated with the same bit as the one currently transmitted via the "direct path".[9] The reduced transmission rate also ensures that the duration of short-term noise peaks is generally shorter than the transmission of a bit.

The following figure shows the schematic operating principle for OFDM (bottom) in contrast to conventional transmission (top): The use of several parallel channels (here, only 4 channels are shown for reasons of clarity; this number is significantly higher in practice) considerably increases the time interval Δ*t* available for the transmission of one individual character so that short-term noise or echoes due to path differences become much less relevant.

Figure 2-1



The top of the previous figure shows the "conventional" way of transmitting, the bottom shows transmission with OFDM. The figure clearly shows how the transmission time Δ*t* for an individual character is increased without compromising the overall data rate for 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).

2.2.2 IEEE 802.11b

Description

The IEEE 802.11b standard was also developed in 1999 and operates in the 2.4 GHz frequency band. Here, the Direct Sequence Spreading Spectrum (DSSS) is used together with the Single Input Single Output (SISO) technology as the modulation method. This makes a maximum data rate of 11 Mbit/s possible.

[9] In other words: The travel time difference remains lower than the duration for transmitting one bit.

The Direct Sequence Spread Spectrum (DSSS) modulation method

DSSS, which at first glance goes the opposite way, is an alternative to OFDM: The data stream to be transmitted is multiplied by a series of pseudo random numbers (so-called "chips"), which have a greater data rate than the data stream.

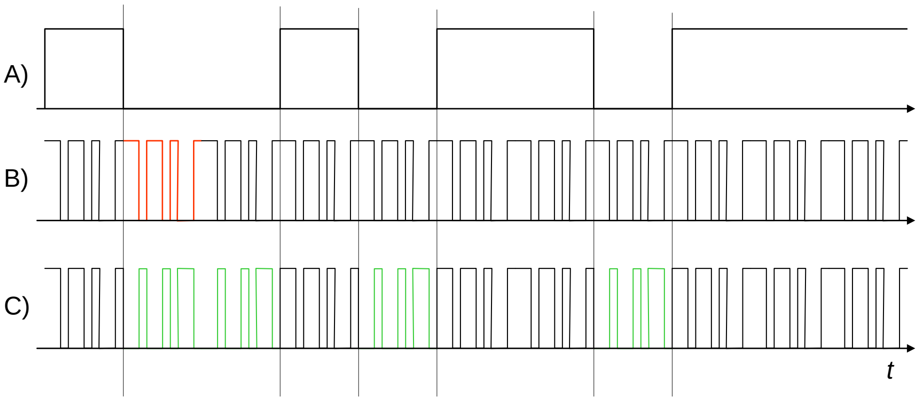
The receiver, which must recognize the "chips" (they could have either been generated by a cryptographic algorithm or separately transmitted previously), simply subtracts them from the stream received, obtaining the unmodified signal.[10]

This has several effects:

- Although only one carrier wave is used, the spectrum of the transmitted signal broadens disproportionally. Consequently, interferences that are limited to a very narrow range of the spectrum have a less significant effect.
- Due to the use of pseudo random numbers, the transmitted signal initially appears as noise. In other words, it is not apparent to someone monitoring that any transmission is taking place at all.
- Even if the individual is aware of an active transmission, it can only be monitored if the sequence of chips used by the transmitter is known.

Other than WLANs, DSSS is also used in GPS, UMTS and WirelessUSB.

Figure 2-2



The figure above illustrates the function of DSSS.

A) The user data signal,

B) The "chips" used for encryption. This only involves a short sequence (in red) that is continuously repeated. The bit sequence for the "chips" changes much faster than with 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 practice, the chips would be more complicated, and a bit length that is a multiple of the chip length would not be used for the user data.

[10] This is certainly a simplified representation and strictly speaking, it does not involve an addition or a subtraction, but rather uses XOR operations of data with its keys.

2.2.3 IEEE 802.11g

Description

This standard is the extension of IEEE 802.11b and also operates in the 2.4 GHz frequency band. IEEE 802.11g works with the OFDM modulation method and SISO technology, therefore reaching a maximum data rate of 54 Mbit/s. This standard is backward compatible to IEEE 802.11b. If both standards are used in one network, the DSSS modulation method with the corresponding lower data transmission rate is used.

OFDM modulation method

See chapter 2.2.1/4.4.5

2.2.4 IEEE 802.11n

Description

The IEEE 802.11n is the latest standard and is able to use both the 2.4 GHz as well as the 5 GHz bands. In addition to the OFDM modulation method, Multiple Input Multiple Output (MIMO) technology is used. This considerably increases the transmission rate as compared to the previously mentioned standards and can be up to 600 Mbit/s.

WLANs in accordance with 802.11n are compatible to 802.11a, 802.11b, 802.11g and 802.11h networks.

OFDM modulation method

See chapter 2.2.1/4.4.5

Diversity systems

Diversity is a technology used to increase transmission reliability in a radio system. The principle is based on transmitting and receiving information in one radio channel multiple (redundant) times. All diversity systems are based on transmitting signals over multiple parallel paths that are independent from each other. The separation can be achieved in terms of time, frequency or space.

Separation in terms of space is the primary method used in today’s radio systems.

Space diversity is distinct due to the fact that it can be implemented without the need for additional resources such as transmission time and bandwidth. The spatial differences in the channel are utilized here. For this purpose, several antennas are either used on the transmitter (MISO; Multiple Input Single Output) or on the receiver (SIMO; Single Input Multiple Output).

The information that is to be evaluated by each antenna is decided using test measurements that are carried out while the connection is being established. The antenna that receives the data with the best signal-to-noise ratio will be used for further data transmission. The signal from the other antenna is ignored. In concrete terms, only the data of one transmission path is used.

Multiple Input / Multiple Output Systems

In order to increase the receiving field intensity, and therefore the reception quality and data rate to be transmitted, MIMO technology is used. This technology is used in the IEEE 802.11n extension.

MIMO systems differ from diversity systems due to the fact that they not only use one channel for redundant signal transmission, but several parallel subchannels. These additional data channels make it possible to transfer different data independently from each other using the same antennas on the same frequency band and at the same time, in a process called multiplexing ("spatial multiplexing"). This technology requires the transmitter as well as the receiver to be equipped with a minimum of two and a maximum of four antennas.

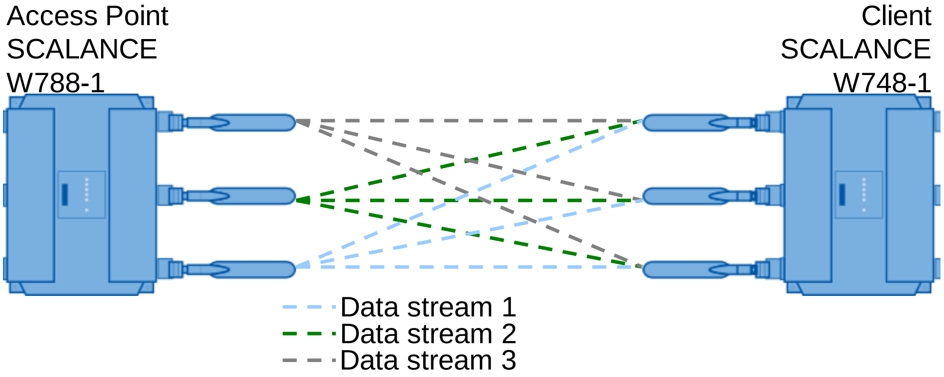
Beamforming enables the transmitter and receiver to block out interferences in the channel, therefore establishing a reliable, high-quality connection.

The principle is based on combining the signals of the individual antenna elements via enhancement factors and adjustable phase shifters. This results in "beamforming", which can be adjusted electronically using so-called smart antennas.

This MIMO method makes it possible to significantly increase the data throughput. A max. gross total of 150 Mbit/s is transferred per data stream with IEEE 802.11n. When utilizing the maximum total of four possible data channels, 600 Mbit/s can be achieved.

The following graphic illustrates MIMO technology when three antennas and three data streams are used:

Figure 2-3



Shortened guard interval

The guard interval prevents different transmissions from interfering with each other. After the transmission time lapses, there is a pause (guard interval) between the two transferred OFDM symbols before the next transmission starts.

The guard interval for IEEE 802.11a/b/g is 800 ns. IEEE 802.11n is able to use the shortened guard interval of 400 ns.

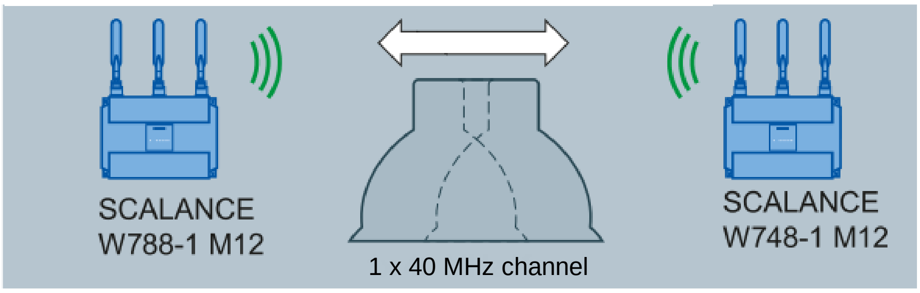
Channel Bonding

Channel bonding describes the linking of multiple channels in order to achieve higher data throughput.

With IEEE 802.11n, data can be transmitted via two directly adjacent channels. The two 20 MHz channels are combined into one channel at 40 MHz. This makes it possible to double the channel bandwidth and increase the data throughput. In order to use channel bonding, the receiver has to support 40 MHz transmissions. If this is not the case, it is automatically reduced to 20 MHz. This guarantees compatibility between IEEE 802.11n and IEEE 802.11a/b/g devices.

Figure 2-4

Communication via Standard IEEE 802.11n



Maximal data rate: 450 Mbit/s

Frame aggregation

With IEEE 802.11n, it is possible to combine individual data packets into one larger data packet (frame aggregation).
This method minimizes packet overhead and shortens the wait times between the data packets, thus increasing data throughput.
There are two types of frame aggregation:

- Aggregated MAC Protocol Data Unit (A-MPDU) and
- Aggregated MAC Service Data Unit (A-MSDU).

Frame aggregation can only be used if the individual data packets are intended for the same receiver station (client).

MCS ("Modulation and Coding Schemes")

The IEEE 802.11n standard supports different data rates.
The data rates are based on the number of transmitter and receiver streams (spatial streams), the modulation method and the channel coding. The different combinations are described in "Modulation and Coding Schemes".

The Web Based Management page for the SCALANCE W devices (IEEE 802.11n) displays the available data transmission rates for the WLAN 802.11n mode. They can be combined and selected as desired. Only the selected data transmission rates are then used by the access point for communication with the clients.

2.2.5 IEEE 802.11ac

Description

IEEE 802.11ac is a radio network standard adopted in November 2013 for WLAN with data rates in the gigabit range. By improving the transmission protocol and the WLAN technology as well as using the OFDM modulation method, data rates of up to 7 Gbit/s are possible. Data transmission is only achieved in the 5 GHz band.

IEEE 802.11ac offers high bandwidths for high network density and demanding transmission, such as with video data.
From a technical point of view, this standard does not make any significant changes as compared to its predecessor IEEE 802.11n. The higher transmission rate is mainly achieved using wider channels (up to 160 MHz), up to eight transceiver units that can be used simultaneously, high-quality modulation and a multi-user (MU) MIMO.
WLANs in accordance with 802.11ac are compatible with the 802.11a, 802.11h and 802.11n networks.

OFDM modulation method

See chapter 2.2.1/4.4.5

2.2.6 IEEE 802.11ad

Since 2012, there has been a new standard for wireless gigabit. This involves an IEEE 802.11ad specification for a wireless connection between digital video systems in the gigabit range. High data rates are achieved by changing the frequency range to the 60 GHz band and optimizing the access protocol.

Due to the change in frequency band, WLANs in accordance with 802.11ad lose their backwards compatibility to the other IEEE 802.11 standards.

2.2.7 IEEE 802.11ax

The IEEE 802.11ax standard is the direct successor to the 802.11n standard for the 2.4 GHz frequency range, and to the 802.11ac standard for the 5 GHz frequency range. An extension to the 6 GHz frequency range was also implemented. The 802.11ax standard is the sixth Wi-Fi standard and is thus known as Wi-Fi 6.

The focus during development of the 802.11ax standard was on increasing efficiency. Parallel data transmission is aimed at increasing data throughput in order to meet requirements for faster data transmission with high data volumes. The new standard is intended to quadruple data throughput when compared to the predecessor standards.

The 802.11ax standard contains the following additional specifications:

- The OFDMA modulation method (see chapter 4.4.5).
- Fast Transition over Air enables rapid, as well as secure, roaming of a client.
- Multi-user MIMO (Mu-MIMO) relies on multiple antennas to transmit and receive via multiple data streams simultaneously.
- Target Wake Time (TWT) is used to reduce energy consumption of the end devices until they are re-activated by a TWT signal.
- A channel width of 160 MHz increases bandwidth and enables greater performance at lower latencies.

2.2.8 Transmission range and special antennas

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

By using directional antennas, this value can be increased by many hundreds of meters. Depending on the country of use, line-of-sight and the Fresnel zone (see chapter 1.5.3), can even cover ranges over several kilometers.

2.3 Additional IEEE 802.1x standards

Over time, a number of additional standards have been defined for the IEEE 802.11 standard, mostly relating to individual aspects of radio communication:

- 802.11e: Introduction of "Quality of Service" features for increased transmission quality.
- 802.11h: Modifications to 802.11a, in order to prevent interference with other devices in the
  5 GHz band.
- 802.11i: Security functions for data encryption and authentication.
- 802.11r: Allows clients to switch from one access point to another without requiring total interruption of the secure network connections.

Furthermore, there are also IEEE 802.1 standards that are important for the operation of WLANs:

- 802.1Q: Virtual LANs for separating a network
- 802.1X: Security functions for WLANs and VLANs

2.3.1 IEEE 802.11e and WMM: "Quality of Service"

IEEE 802.11e

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. compliance with this standard guarantees a specific connection quality.

Quality is not only measured at the mean achievable data rate but lower limits for connection reliability are also defined, such as the duration of possible connection interruptions. A good telephone connection, for example, not only requires the transmission of appropriate sound quality but also reliability in ensuring that dropouts and voice delays stay within narrow limits.

While earlier 802.11 standards placed more emphasis on gross data rates than on "Quality of Service", the "e" variant introduced a standard that explicitly included issues concerning QoS.

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.

2.3.2 IEEE 802.11h and the 5 GHz band

IEEE 802.11h

Although the 5 GHz band is only used for a few applications outside of WLAN, one of these applications includes radar, whose operators are inherently quite sensitive to possible interferences.

For this reason, the IEEE 802.11h standard introduced modifications that can be used to minimize interferences between radar and WLANs operated below 5 GHz. The newly introduced technologies include "DFS" and "TPC".

DFS (Dynamic Frequency Selection)

DFS describes the process of automatically switching to a different 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 has been reached for achieving reliable transmission with the configured data rate. TPC represents a compromise between reliable communication and overshoot prevention.

2.3.3 IEEE 802.11r

Fast Transition (FT) over Air

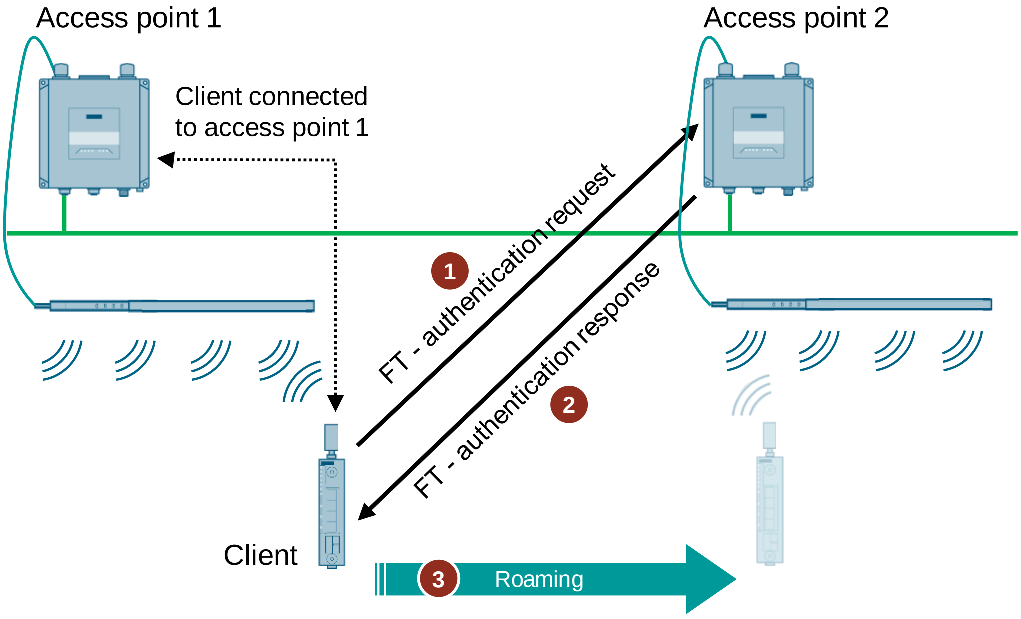
IEEE 802.11r, or "Fast BSS Transition (FT)" is an extension of the IEEE 802.11 standard that ensures continuous connection of clients with rapid and secure roaming from one access point to the next. The standard has 2 properties: Over-the-Air, and via a distributed system (over DS).

Note

The SCALANCE W 802.11ax devices have previously only supported "Over-the-Air"!

To speed up registration with the new access point, access points have been assigned to a mobility domain. Within this domain, the access points exchange certain registration information about the clients. This makes it possible to skip the key generation step and re-encryption. This reduces packet exchange between the client and the new access point during roaming, and speeds up authentication.

Figure 2-5


Access point 1
Access point 2
Client connected
to access point 1
1
FT - authentication request
2
FT - authentication response
Client
3
Roaming

2.4 Channel distribution in the IEEE 802.11 standard

The 802.11 standard uses the 2.4 GHz, 5 GHz and 6 GHz ISM bands as frequency channels.

2.4.1 The 2.4 GHz band

The frequency band at 2.4 GHz is a frequency range that can be used without a license in virtually every country.[11] Since it is relatively inexpensive to manufacture transmitters and receivers, 2.4 GHz technology is very popular and is used for a number of other applications besides WLAN.

The 2.4 GHz band, as used in the 802.11b/g standard, is normally divided into 13 channels,[12] which are at a distance of 5 MHz from each other and have a bandwidth of approx. 20 MHz (see chapter 1.4.4). However, this certainly does not mean that 13 non-overlapping channels are available for each WLAN.

In order to exclude the possibility of the transmitters in the WLAN interfering with each other, maintaining this minimum distance between the transmitters is required. This reduces the number of frequencies that can be used independently of one another in practice to three: In general, only channels 1, 7 and 13 (the so called "non-overlapping channels") are used simultaneously with 802.11 networks.

With the 802.11n standard, extending the bandwidth to 40 MHz per channel is possible (channel bonding; see chapter 2.2.4). This achieves higher data rates.

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

2.4.2 The 5 GHz band

For the 5 GHz band, different numbers of non-overlapping channels are approved around the various regions of the world.[13]

In general, 5 GHz waves are "harder", i.e. their propagation behavior is similar to that of light beams: There is less diffraction around objects, absorption is higher and the penetration depth is lower than for 2.4 GHz waves. In most cases, the achievable transmission range in practice is a little less than in the 2.4 GHz band.

Compared with the 2.4 GHz band, the 5 GHz band is significantly less "busy", and there are only a few sources of interference within this range. Military radar and satellite tracking systems are exceptions, as their operators have an inherent sensitive reaction towards system interferences from a WLAN.

In order to harmonize operations between the 5 GHz WLANs and these systems, the IEEE standard 802.11h (see chapter 2.3.2) was created.

[11] Updated lists of country approvals for individual SCALANCE W products are available at http://www.siemens.de/funkzulassungen.

[12] Details pertaining to approved channels differ from country to country. The topic is discussed in detail in chapter 7.

[13] Compare with the remarks on country approvals for components, see chapter 7.
Current approval lists can be found on the internet at http://www.siemens.de/funkzulassungen.

2.4.3 The 6 GHz band

The continual increase in Wi-Fi applications in the 2.4 and 5 GHz range has crowded available bandwidth.

Since 2020 in the USA and European Union, an additional 1200 MHz / 500 MHz in the 6 GHz band have been approved for license-free use. This extension is also known as Wi-Fi 6E and allows for double the available channels.

It only makes sense to use the 6 GHz band for industrial applications since there is no competition from office communication in this region.

Since there are no legacy systems in the 6 GHz, it is not necessary to consider backwards compatibility. All functions of the previous IWLAN standard, IEEE 802.11ax, can be used.

The current WPA3-SAE encryption protocol, the subject of the IEEE 801.11ax standard, is recommended for all nodes, particularly for the 6 GHz band.

More information on Wi-Fi 6 and the 6 GHz band can be found in \10\.

Note

The first implementations of the 6 GHz band for the family of the SCALANCE W access points are planned for 2024.

2.4.4 Comparison of the properties of the 2.4 GHz and the 5/6 GHz band

Connection reliability and interference caused by other devices:

The immense popularity of the 2.4 GHz band also means that a large number of devices that actually have nothing to do with WLANs also transmit in this range. These devices include microwave ovens, Bluetooth devices and cordless DECT telephones.
This may cause interferences and problems when setting up a WLAN. Depending on the type of interference source, it may be advisable to switch to the 5/6 GHz band.

In any case, the optimal configuration for the illumination, frequency band and antennas must be evaluated with a radio field analysis prior to setting up the system.

Size

Due to the shorter wave lengths used, it is possible to produce 5/6 GHz components that are smaller in size than the 2.4 GHz modules (This does not apply for devices designed for operation in both bands ("dual-use")).

Licensing

2.4 GHz as well as 5/6 GHz networks can be operated without a license in most countries. In chapter 7, the topic of country approvals is described in more detail.

3 Alternative radio technologies with IWLAN

Apart from the IEEE 802.11 standard for WLANs, there are also several different technologies that communicate via radio networks and that are used in industrial environments.

3.1 Bluetooth

"Bluetooth" is the name for the IEEE 802.15.1 standard that describes the networking of small devices over short distances. Its main area of application is for cable connections between office devices such as PDAs, cellular phones, computers, printers and other peripheral equipment.

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

The maximum transmission power is 100 mW with a range of at most approx. 100 m. However, most portable devices transmit at a lower power in order to conserve battery life. This is why the ranges typically fall below 10 m.

The standard is monitored and further developed by the "Bluetooth Special Interest Group".

Note

Additional information on this subject is available online at the following URL:
https://www.bluetooth.org

3.2 Wireless HART

HART ("Highway Addressable Remote Transducer") is a fieldbus communication standard that also defines wireless communication as "WirelessHART" (based on IEEE standard 802.15.4).

WirelessHART also uses the ISM frequency band (2.4 GHz with a maximum of 250 kbit/s) and independently establishes mesh networks whose range can be far greater than the nominal wireless range of an individual station (approx. 200 m). The network is self-organizing. It analyzes all connection information from the WirelessHART Gateway (IE/WSN-PA Link) and uses this information to automatically provide redundant paths. This can be used to achieve very high availability for the communication connection, as it is able to cover bad connections or the failure of individual nodes. Furthermore, the availability of the entire network can be significantly increased with the use of two redundant gateways.

The focus during the development process for WirelessHART was also on the simple commissioning and maintenance of the self-organizing network, requiring only a minimal workload for the configuration. This comes at the price of real-time capabilities, i.e. there are no guaranteed response times with WirelessHART.

The main application area for WirelessHART here is the regular transmission of lower, non-time-critical data volumes at large intervals (typically between approx. 15 seconds and several hours) over relatively large distances (such as is used in the process industry). Due to the lower energy consumption levels for WirelessHART devices, a long battery life of up to five to ten years can be achieved, e.g. WirelessHART field devices prove to be extremely low-maintenance during the operating phase.

The protocol is very robust and when the mesh network has sufficient illumination, it is able to "heal" failures in the intermediate stations.

WirelessHART is managed by the "HART Communication Foundation" (HCF).

Note

Additional information on this subject is available at the following URLs:

https://new.siemens.com/global/en/products/automation/process-instrumentation/communication-and-software.html

http://www.hartcomm.org/

3.3 Zigbee

As with WirelessHART, Zigbee is also based on IEEE standard 802.15.4 and also uses the ISM band at 2.4 GHz. However, in contrast to HART, the focus here is not on industrial environments, but on building automation and building services. The aim is to install devices in areas that are difficult to access and that are capable of staying in operation for years without requiring any maintenance (electricity or heating meters, light switches, etc.).

The Zigbee protocol is less "robust" than the WirelessHART protocol, and failure of a central controller could compromise communication for the entire network. In exchange, Zigbee offers reduced response times, which makes it suitable for real-time applications as well.

The Zigbee standard is overseen by the Zigbee Alliance, which also provides further information on this topic.

Note

Additional information on this subject is available online at the following URL: http://www.zigbee.org/

3.4 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) was defined in the IEEE standard for the 802.16 family and developed in parallel to the IEEE 802.11. This technology makes it possible to use wireless broad band technology for a Metropolitan Area Network (MAN) without the need for extensive cable-based infrastructure. Due to its application in a very broad frequency spectrum in the gigahertz range, WiMAX can be used worldwide.

In contrast to WLAN standards, WiMAX can also cover larger distances, allowing remote and rural regions to also be supplied with broadband. Due to this property, WiMAX is viewed as an alternative to landline DSL.

The theoretical range is 50 km with a transmission rate of up to 75 Mbit/s. However, in practice, these values falls well below the given levels.

Note

Additional information on this subject is available online at the following URL: http://www.wimax.com/

4 Topology, configuration and organization of IWLANs

4.1 The structure of a WLAN

4.1.1 Structuring by cell distribution

Unstructured radio networks and their disadvantages

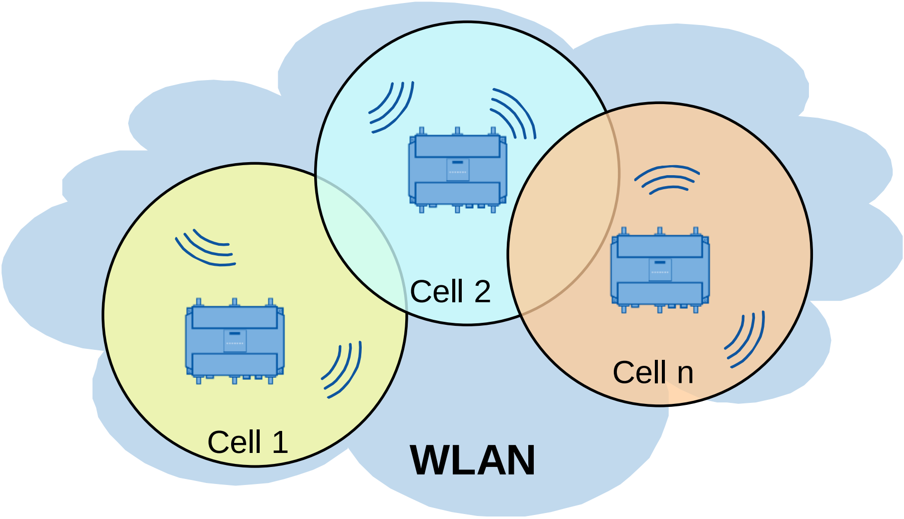
In practice, the range of radio transmitters is limited. The area that is to be covered by a LAN will generally be too large to have reliable "illumination" from one single transmitter.

Even if it would be technically possible to set the transmission power high enough for all of the nodes, in many cases this would not be recommended or permitted. If, for example, the LAN nodes were arranged along a straight line, then an unnecessarily large area on the left and right of the line would be illuminated. This would make it easy for third parties to install additional receivers and listen in on radio communications without being detected.

Structuring radio networks with wireless cells

Furthermore, it is more economical to divide the WLAN into individual cells since only one station can send on each channel at any given time. If several cells are available, an active transmitter can be located in *each* cell, allowing the actual data throughput to increase. Additionally, as a result of the short distances, it only requires comparatively low transmission power. The following figure shows the division of the WLAN into several cells.

Figure 4-1



Note

Additional information on this subject is available online at the following URL:
https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-wireless-lan.html

4.1.2 Connecting individual wireless cells: Access points and clients

The use of access points is required to control the communication in a cell or to connect several wireless cells to each other. 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 wireless cell or if communication only occurs within one cell, then the access point can be used to coordinate communication within this cell.

When using encryption methods, clients can either be granted or denied access to the network (see chapter 5). The access point can meet real-time requirements for 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 interference (compare chapter 4.4).

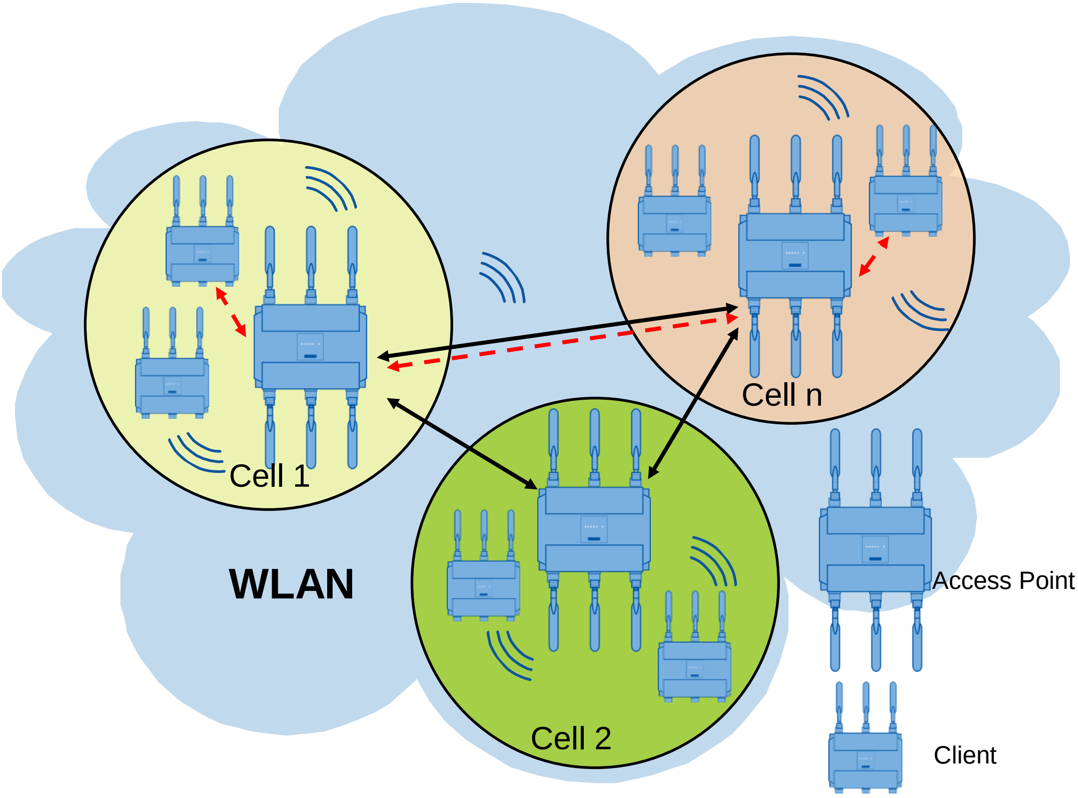
Access points as the "backbone" of communications

For a WLAN consisting of several wireless cells, each of the access points communicates with all the regular nodes in its cell, the so-called "clients" – irrespective of whether they are stationary or mobile. At the same time, the access points of a WLAN also maintain the connection to each other. This is achieved either via cable or a second, independent radio network.[14] This makes communication beyond the limits of the wireless cells possible.

In this case, the term "backbone" indicates the merging of the different wireless cells or networks.

[14] An access point with two or more radio interfaces is required for this purpose.

Figure 4-2



The figure shows the division of a WLAN into three wireless cells (yellow, red, green) with a number of clients and one access point for each. The red arrows follow the communication path between a client of the yellow cell and a client of the red cell.

4.2 The "roaming" method

Movement of clients between the wireless cells: Roaming

If a WLAN spans over a larger area, the radio field of one access point (wireless cell) is usually not sufficient. Several wireless cells are required to illuminate the area using radio technology. If the radio areas of the access points overlap only slightly, the clients should be permitted to move freely, without causing an interruption to the network connection. This includes movement, not only within their own wireless cells but also by crossing over into other wireless cells.

The transfer of nodes from one access point to the next is called roaming. The term hand-over is also commonly used in the same context as roaming.

In the roaming process, it is necessary for the individual wireless cells to overlap each other and for the bordering wireless cells to communicate with each other on different channels. If all wireless cells were to use the same channel, a client located in the overlapping area would have permanently impaired reception (see chapter 1.4.4).

Challenges of the roaming process

Due to roaming in accordance with the standard from IEEE 802.11, a delay time of several hundred milliseconds occurs. This time is necessary in order to

- detect that a client is exiting the old wireless cell
- establish a connection to a new wireless cell.

If this time is tolerated by all communication nodes, communication will continue uninterrupted.

If very fast update times are necessary, e.g. for PROFINET I/O communication, then access points and client modules should be used that support the proprietary iPCF protocol (see chapter 4.6.1) for fast roaming and deterministic data traffic.

4.3 Infrastructure networks

Operating WLANs with the aid of coordinating access points is called "Infrastructure mode".

The following sections show several examples of infrastructure network topologies.

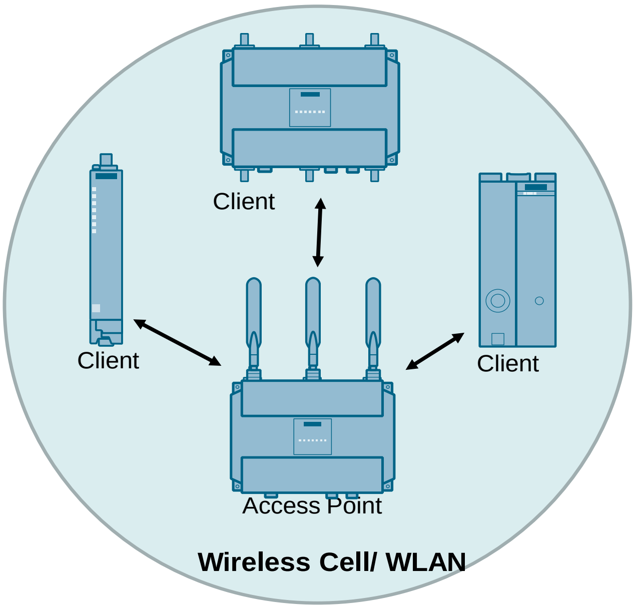
4.3.1 Standalone networks

Description

Stand alone networks consist of a number of clients that are all located in the wireless cell of one single access point. The access point’s function is limited to coordinating clients' communication with each other.

Illustration

Figure 4-3



The figure above shows this kind of stand alone network. It include an access point, which coordinates the data traffic of the different bus nodes and through which all of the traffic is directed. The access point determines the "SSID" ("Service Set Identifier") of the network, in other words, its "name".

It is not necessary for all network nodes of a stand alone network to have direct contact with each other.

The maximum extension of such a network is limited by the fact that all of the clients must be located within range of the access point (red circle).

4.3.2 Mixed networks

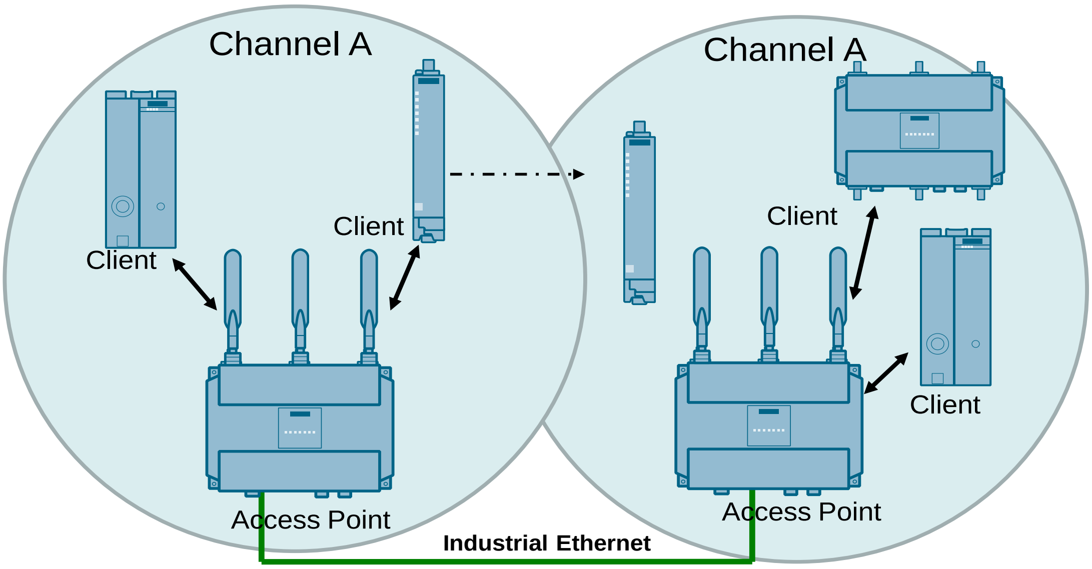
Description

In mixed networks, the access points are not only used to allow clients to communicate with each other. They also provide the connection to a cable-based network. (This cable-based network is typically an Industrial Ethernet.)

Several access points can be connected to the cable-based network. This, in turn, means that the access points create several wireless cells. If these cover a specific area without any gaps, the clients can move from wireless cell to wireless cell within it (called "roaming", see chapter 4.2).

Illustration

Figure 4-4



A number of access points are connected to each other via a wired Ethernet cable. (Any number of other stationary nodes could also be connected to the Ethernet segment.) Within the radio field covered by the access points (red circles above), there are several nodes connected via WLAN (clients).

Mixed networks allow roaming, i.e. the switching of a mobile node from one wireless cell to an adjacent one (see the dotted arrow above).

WLANs that are set up in this manner can theoretically be of any size. Interferences with reception may occur within the overlapping range of the radio cells since the access points operate on the same frequency.

4.3.3 Multichannel configuration

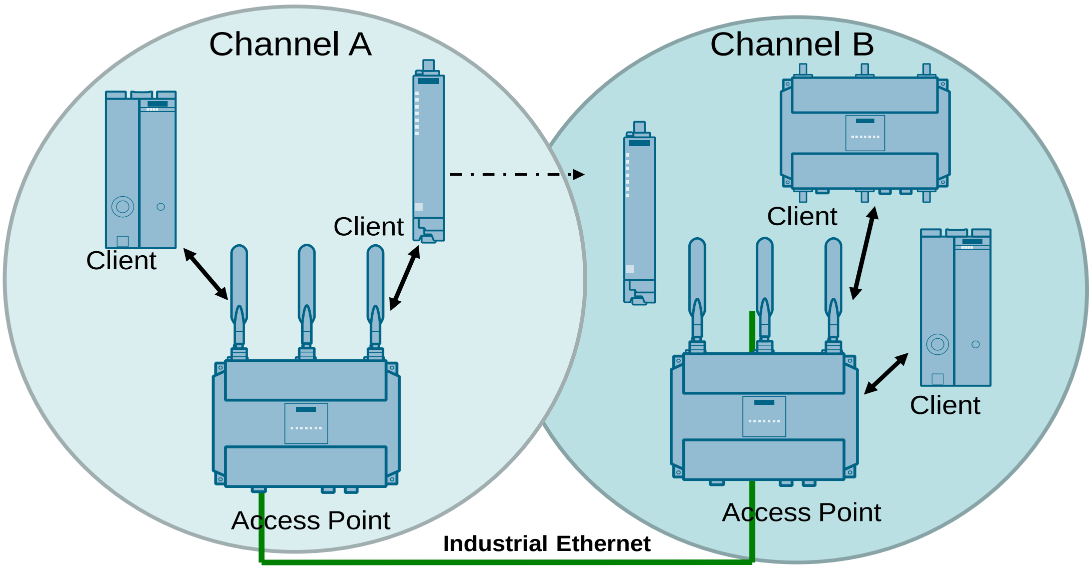
Description

The multi-channel configuration corresponds to the mixed network (see chapter 4.3.2). However, the individual access points operate on different, non-overlapping radio channels (see chapter 2.4). This ensures that interferences no longer occur where wireless cells overlap.

At the same time, roaming, or the process of changing a client from one cell to another, is facilitated, resulting in a considerable increase in performance.

Illustration

Figure 4-5



In this configuration, the individual access points form a backbone, and are connected to one another via a wired Ethernet cable. (Other stationary nodes do not have to be connected to the Ethernet segment.) Several nodes connected via WLAN (clients) are located within the radio field covered by the access points. The different frequencies used by the access points for transmissions are indicated by circles in different colors.

This configuration is the most prevalent WLAN configuration in practice and is normally chosen.

4.3.4 Wireless Distribution System (WDS)

Description

In normal operations, the access point is used as an interface to a cable-based network and communicates with clients. There are, however, situations in which several access points need to communicate with each other, for example to extend wireless coverage or to set up a wireless backbone (see following chapter). This mode of operation is possible with WDS (Wireless Distributed System).

WDS corresponds to the multi-channel configuration (see chapter 4.3.3) except for one important difference: The access points do not maintain the connection *to each other* via a second medium (as is the case with a multichannel configuration, i.e. an Industrial Ethernet cable). Instead, the connection is via the wireless network.

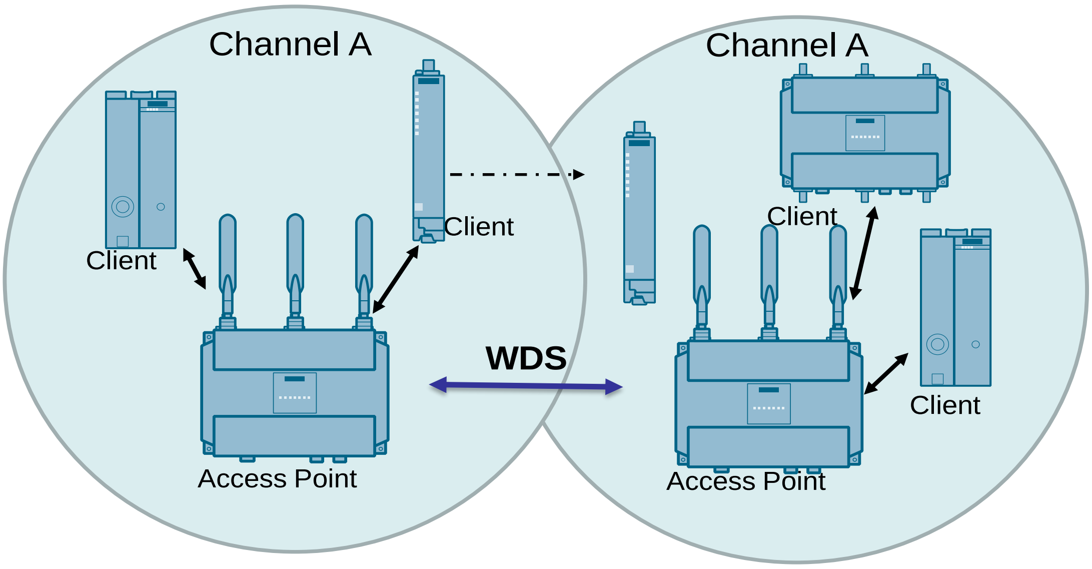
If communication between the access points is now permitted and client access is blocked, it is referred to as a pure WDS.

WDS is distinguished by three properties:

- The distance between the access points must be short enough to allow each access point to be located within the range of its communication partner.
- If several WDS connections are used on the same frequency or if the client-access-point communication is also permitted, the effective data rate for the access point is reduced, due to the fact that the bandwidth has to be shared.
- All access points that are to communicate with each other are required to use the same channel.

Illustration

Figure 4-6



The Figure above illustrates the principle of operation, compare also Figure 4-4. Within the radio field covered by the access points (red circles above), there are several nodes connected via WLAN (clients). In addition, the access points maintain another wireless connection between each other.

4.3.5 Redundant wireless link

Description

To establish a redundant backbone, it is necessary to use access points that feature two wireless interfaces and that are then able to transmit simultaneously on several frequencies.

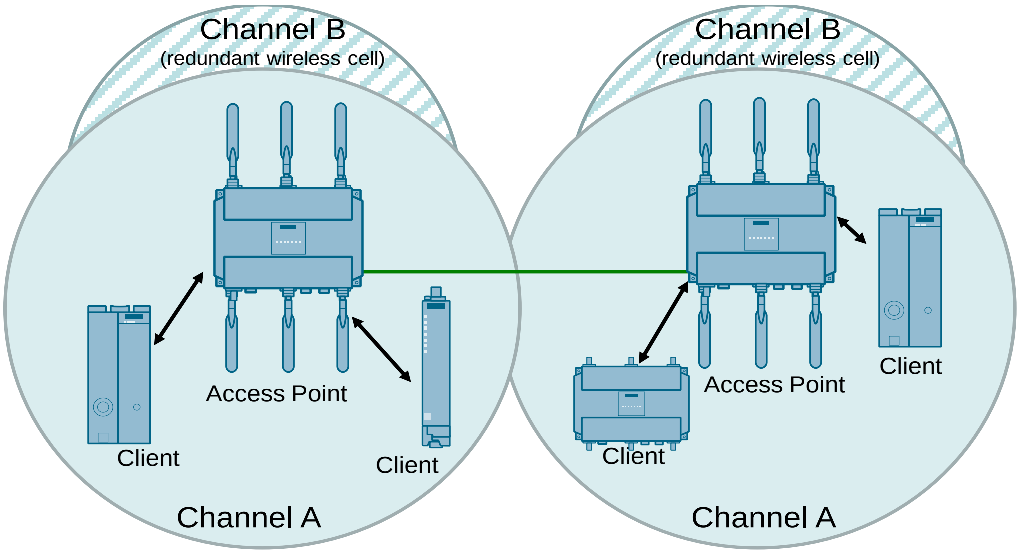
This condition makes it possible to establish:

- a redundant mixed network or
- a redundant wireless distribution system (see chapter 4.3.4), which cannot be established as a wired network due to its location.

This ensures the achievement of high connection reliability in combination with high data rates: Even if a frequency range is interrupted temporarily by interfering nodes, shadowing or interferences, there is a high probability that a connection will still be possible using the other channel.

Redundant mixed network

Figure 4-7

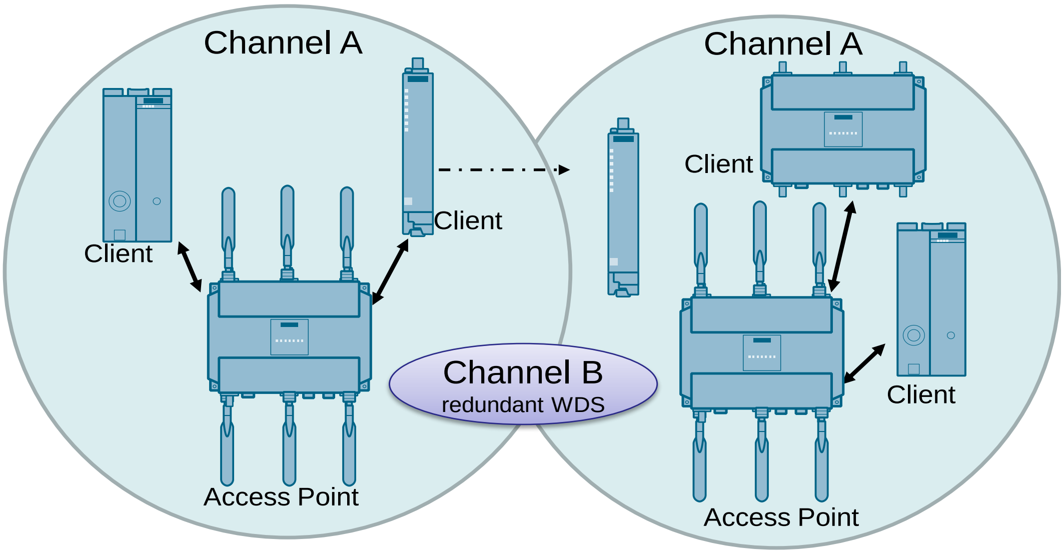


The access points establish an independent wireless cell for each wireless interface, where only one wireless cell is primarily used.

If data transfer with the access point is no longer possible via the wireless cell of the first wireless interface, the clients can automatically switch to the wireless cell of the second wireless interface. Communication between the access points is cable-based via Industrial Ethernet.

Redundant WDS

Figure 4-8



The access points do not communicate with each other on the primary frequency, but on the second frequency with a second set of antennas.

4.4 Coordination of data transfer

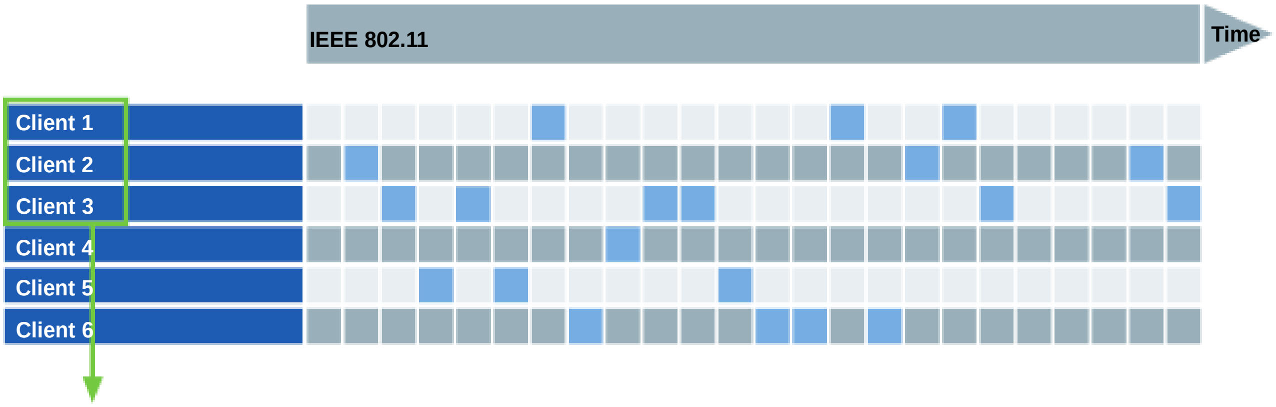
For a WLAN compliant with the IEEE 802.11 standard, there are two approaches identified to coordinate communication in a shared medium:

- the basic access method with a decentralized approach (Distributed Coordination Function, DCF)
- the centralized method (Point Coordination Function, PCF)

4.4.1 Distributed Coordination Function (DCF)

For a WLAN in accordance with the IEEE 802.11 standard, all nodes are essentially "responsible for themselves" and exercise uncoordinated access to the wireless channel. The access of nodes carrying critical data cannot be predicted.

Figure 4-9



The access of nodes carrying critical data cannot be predicted.

All nodes exercise uncoordinated access to the wireless channel.

Data transmission in accordance with the CSMA/CA method is binding for all participants.

In order to reduce the probability of collisions, a station that is ready to send listens to the medium for a waiting time that consists of a constant waiting time (DIFS; Distributed Coordination Function InterFrame Space) and a random waiting time. If the medium is occupied, the station waits until the end of the data transmission. Afterwards, the fixed waiting time starts again and is extended with the reduced random waiting time. If the medium is still free, the data transmission will start.

The addressee that has received a message intended for it, will in turn send back an acknowledgment message. In this case as well, a constant waiting time (SIFS; Short Coordination Function InterFrame Space) must first be observed in order to avoid a collision.

DCF does not guarantee that a specific data volume will be transmitted within a maximum time interval. For this reason, it is primarily suitable for *asynchronous* data transmission (such as email or web browsers).

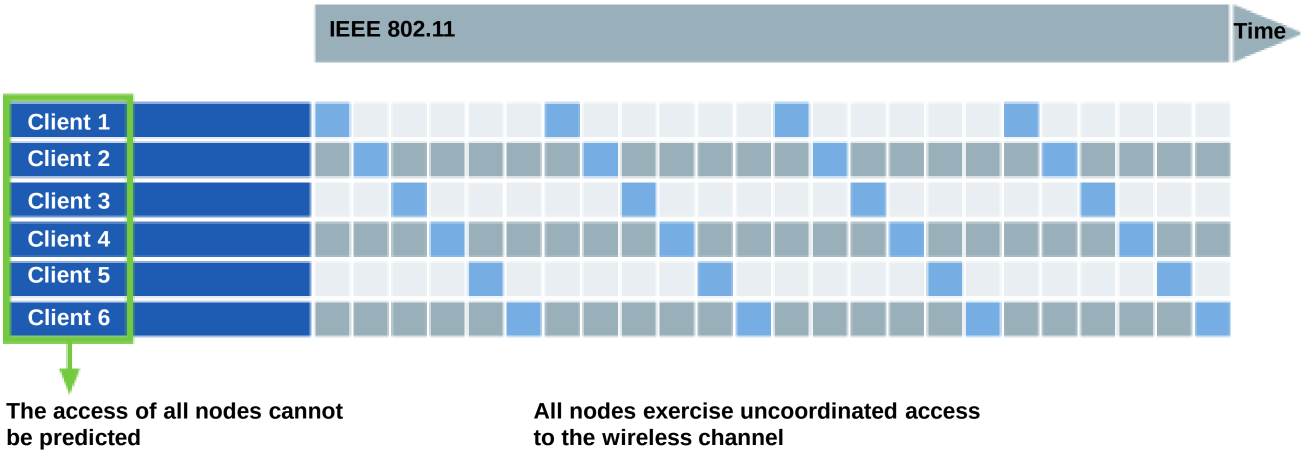
The data throughput of some DCF network configurations can be increased by using the RTS/CTS method.

4.4.2 OFDM

The standard modulation method in PCF (up to IEEE 802.11ac) is OFDM (Orthogonal Frequency Division Multiplexing), in which only one client is allowed to transmit at any given time.

In PCF, not all network nodes have equal rights. Instead, one or more access points act as central administrators in the network. One 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.

Figure 4-10


IEEE 802.11
Time
Client 1
Client 2
Client 3
Client 4
Client 5
Client 6
The access of all nodes cannot be predicted
All nodes exercise uncoordinated access to the wireless channel

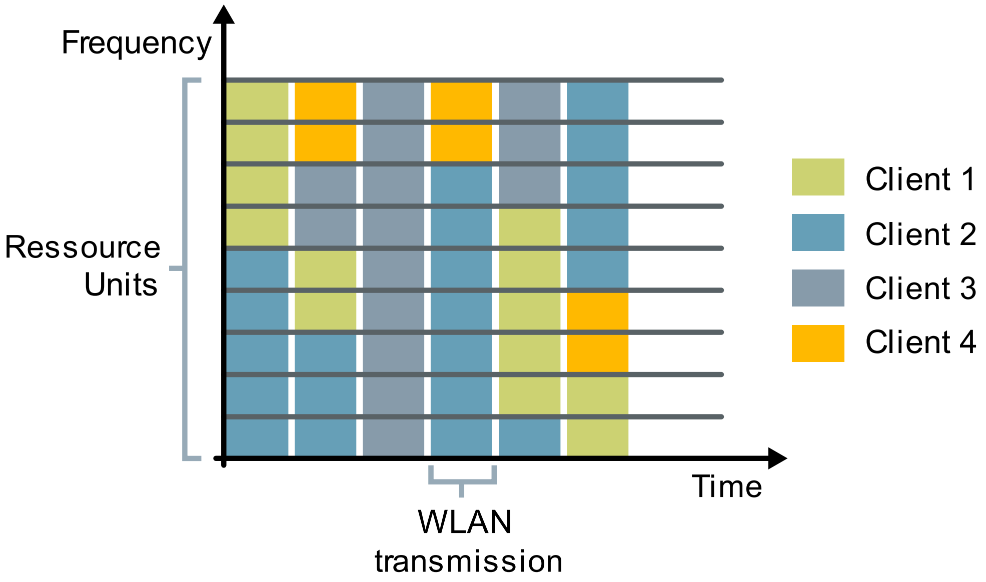
Using PCF, it is possible to assign regular network access to the individual clients and to ensure the transmission of data within a specific period. For this reason, PCF is preferable solution for applications requiring continuous data flows. (*Synchronous* data transmission, e.g. video or audio streams,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

But it is possible to allow networks to change between DCF and PCF at intervals if the communication requirements call for it.

4.4.3 OFDMA

OFDMA (Orthogonal Frequency Division Multiple Access) was introduced with the IEEE 802.11ax standard. Here, one communication channel is divided into 9 sub-channels (resource units). These sub-channels can then be split up between various clients. This means that these clients can communicate simultaneously.

Figure 4-11



One access point communicates with one client per resource unit. Conversely, multiple clients can communicate with one access point, allowing for more efficient communication.

4.4.4 Hidden Station and RTS / CTS methods for collision avoidance

A station is not always able to detect whether the medium is free. This is especially the case if two nodes from a wireless cell cannot "see" each other (i.e., they are not located within reach of each other). This WLAN issue is expressed by the term, "hidden station".

If, however, both nodes attempt to communicate with a third node that is located between them (and that has simultaneous contact with both transmitters), conflicts could occur.

The solution to the "hidden station" issue lies in the RTS / CTS method.
In order to avoid disturbances, the station that is ready to send and the receiving station block the medium from other stations for a period of time using a request to send (RTS) and clear to send (CTS) dialog. Here, it is sufficient if all the stations in the catchment area of the transmitting station listen to one of the two RTS / CTS signals in order to be put into waiting mode.

This method considerably reduces the number of necessary transmission repetitions since the collision is already detected before sending longer data packets. However, the overhead caused by the RTS/CTS telegrams can lower the achievable data throughput.

4.4.5 Point Coordination Function (PCF)

The abbreviation PCF describes a method of access defined in the 802.11 standard. However, implementation of this method is not mandatory. The method can be used to avoid some of the disadvantages of the DCF method.

In practice, PCF is rarely supported by manufacturers. With iPCF ("Industrial Point Coordination Function"), SIEMENS provides a proprietary alternative to PCF (see chapter 4.6.1).

4.5 Functions for network management

4.5.1 Virtual LANs (VLANs)

Segmentation of a physical network into multiple logical "virtual" networks can be performed for both cable-based and wireless networks. Nowadays, VLANs normally follow the IEEE 802.1Q standard.[15]

Segmentation of data traffic

For this type of network usage, the individual ports of a switch (or access point) are assigned a so-called VLAN ID during configuration. Communication is then only possible within a VLAN (ports with the same VLAN ID).
For this purpose, the Ethernet data packets ("frames") are extended by a data block (a "tag"), which contains a VLAN ID. The switches (or access points) only forward the message to those members of the VLAN to which the message is addressed.

Benefits

Using VLANs helps achieve a number of advantages:

- Configuration errors remain restricted to the VLAN in which they were made, and can no longer cripple the entire LAN.
- Broadcasts, i.e. transmissions to a general group of recipients, are no longer performed via the entire LAN but only via the VLAN involved, helping to reduce the network load.
- Individual VLANs can have various priorities assigned to them, allowing groups of high-priority nodes to have preferential status for message relaying.
- In contrast to using IP subnets, nodes from different VLANs can share the same IP addresses. This makes better use of limited IP address space, and allows production cells of identical structure to be configured with identical IP addresses, helping to reduce expenses for configuration and administration.
- The VLAN configuration is transparent for the end node, i.e. the end nodes do not know to which VLANs they belong and cannot listen in on their data traffic. This achieves a certain level of security for the network.

Note Further information and articles concerning this topic can be found in the Siemens Industry Online Support (see chapter 12).

4.5.2 Spanning Tree Protocol (STP)

Description

Redundant networks are networks in which messages are forwarded between the end nodes via switches, where each pair of end nodes is connected to each other by more than one path. This kind of a network can be cable-based or wireless. In the latter case, the access points act as switches.

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

[15] Older protocols such as ISL ("Inter Switch Link") and VLT ("Virtual LAN Trunk") are no longer relevant today.

For this purpose, the "Spanning Tree Protocol" STP was developed as IEEE standard 802.1d.

This measure reduces the active connection paths of any intermeshed network structure and passes it into a tree topology (spanning tree).

Functional sequence

In addition to regular data traffic, the switches interchange special BPDUs ("Bridge Protocol Data Units"). The MAC addresses of the sender and the forwarding switches are listed in these BPDUs. By evaluating this information, the self-learning switches can develop a "map" of the network and learn which data paths are available.

The best path is determined using two criteria:

- In principal, the path that contains the lowest "path costs" is preferred. Here, the path costs are inversely proportional to the data rate of a connection.
- If the path costs of two connections are equal, the route with a higher priority is selected. The prioritization of individual ports is configured at the switches themselves.

During regular operations, all messages run along the best path.

4.5.3 Rapid Spanning Tree Protocol (RSTP)

One disadvantage of an STP is that the network has to reconfigure itself in the event of a disruption or device failure: the switches only start negotiating new paths at the moment the disruption occurs. This process can take up to 30 seconds, a period that is not acceptable for many automation processes.

For this reason, STP has been expanded as the "Rapid Spanning Tree Protocol" (RSTP,
IEEE 802.1w). The main difference to the STP is the switches, which already collect information on alternative routes during the period of undisturbed operations.

This allows the reconfiguration time to be reduced to a few seconds for an RSTP-controlled network.

Note Further information and articles concerning this topic can be found in the Siemens Industry Online Support (see chapter 12).

4.5.4 Multiple Spanning Tree Protocol (MSTP)

Both STP and RSTP work with a global tree topology (spanning tree) for the entire network. Here, certain paths remain unused in order to guarantee loop freedom. That means that existing path resources are not used efficiently. The disadvantage of using just one individual spanning tree is that reconfiguration takes a relatively long time for large networks.

The Multiple Spanning Tree Protocol (MSTP) is a further development of RSTP and can often be found together with VLANs.

MSTP not only works with a tree topology, but also operates an individual spanning tree in each VLAN. Long reconfiguration times can be avoided due to the shorter STP instances and the paths blocked by RSTP within individual VLANs can be made available.

4.6 Proprietary extensions of the IEEE 802.11 standard: iFeatures

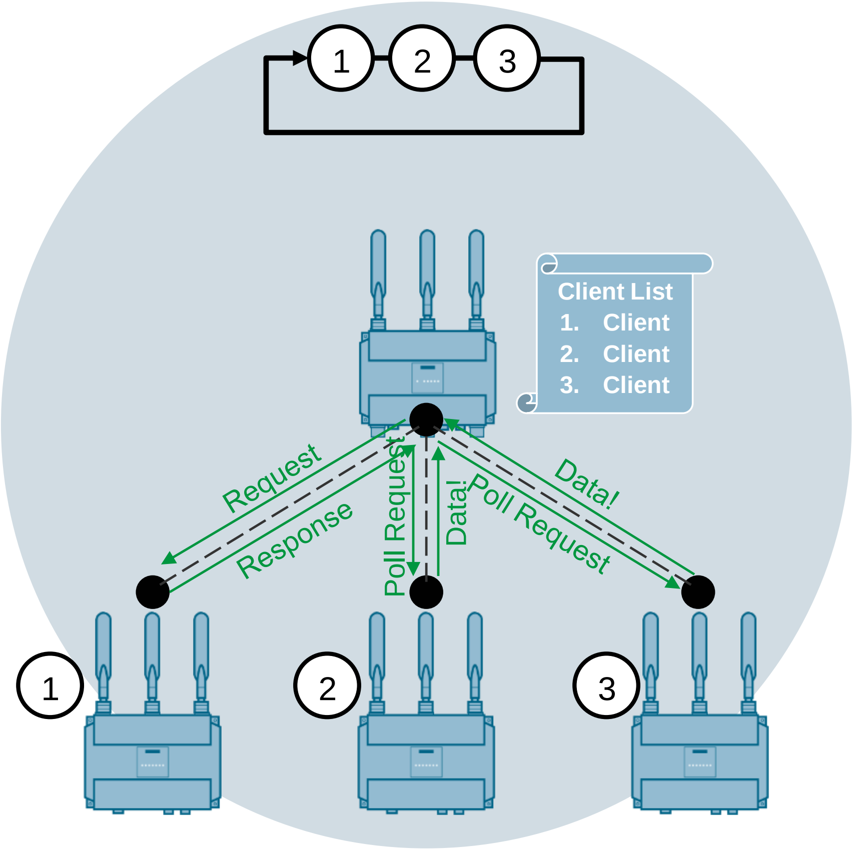
4.6.1 Industrial Point Coordination Function (iPCF)

The Industrial Point Coordination Function (iPCF) represents a proprietary alternative to PCF developed by SIEMENS, and is used to solve several of the existing issues with PCF (see chapter 4.4.5). Furthermore, iPCF enables the clients to change wireless cell extremely fast, where the log-off and new log-in of the client ("handover") happens so quickly that the real-time requirements for communication are still met.

Operating principle

In iPCF, the access points poll the clients in their wireless cell in regular, very short intervals. The clients respond with the relevant data frames and can register their need to send further data telegrams. However, they only initiate another broadcast when they are polled again by the access point according to their need.

Figure 4-12



These properties result in the following effects:

- The access point can be parameterized to poll at a very rapid rate. This results in very low response times for each client (deterministic transmission) and very short roaming times.
  You can find recommended reaction times in Table 2-2 of the following article: "IWLAN: Setup of a Wireless LAN in the Industrial Environment" - https://support.industry.siemens.com/cs/ww/en/view/22681042
- The transmission of larger, non-time-critical telegrams is delayed until free cycle time becomes available.
- The scanning of a node is seen by all other nodes in the cell. This allows a client to detect the quality of the wireless link to the access point even when it is not communicating with the access point itself.
- Due to the shorter polling cycle times, a client will find out very quickly whether the connection to its access point still exists or not. If the contact has been lost, the client can react within a very short time, establishing a connection to an alternative access point.
- In iPCF mode, both the search for a new access point and the registration with this new access point have been optimized in terms of time. Handover times well below 50 ms are achieved.

That means that with iPCF, industrial applications with medium level real-time requirements are WLAN-capable in the 2-digit millisecond range. The wireless connection for PROFINET IO devices falls in this range. However, iPCF can also be used with EtherNet/IP.

Optimal performance with iPCF can be achieved if the clients follow fixed paths (e.g. when using RCoax cables). Application of iPCF-MC is recommended for free-moving nodes in communication with stationary access points (see chapter 4.6.2).

iPCF-2:

All current and future iPCF-2 features are available only in IEEE 802.11ax devices, where they replace iPCF.

Note

The iPCF versions are not cross-compatible.

Restrictions concerning iPCF

iPCF can only be operated alone. Combining it with other industrial functionalities (iFeatures such as iPCF-MC or Dual Client) is not possible.

The iPCF method is a Siemens AG in-house development and only works with nodes where iPCF has been implemented. However, for one access point with two WLAN interfaces, it is possible to configure iPCF as well as standard WLAN at the same time.

When the iPCF mode is enabled, only the "open system" security settings with the AES encryption method with 128 bit key length are supported.

When iPCF is used in conjunction with PROFINET IO, then "Layer 2 Tunnel" should be selected as the MAC mode in the client.

The number of clients per access point influences the iPCF cycle time. Each client adds about 2 ms to the cycle time.

If you are using multiple antennas, then they must be set up correctly. More information on this topic can be found in the following article: https://support.industry.siemens.com/cs/ww/en/view/109793293

Compatibility with other WLAN standards

"Mixed networks" in which the devices are partly connected via DCF / iPCF, are not possible with iPCF.

Also make sure that the area where iPCF is being used is completely free of interference. This applies not only to WLAN transmissions, but also to any other type of radiation.

4.6.2 iPCF – Management Channel (iPCF-MC)

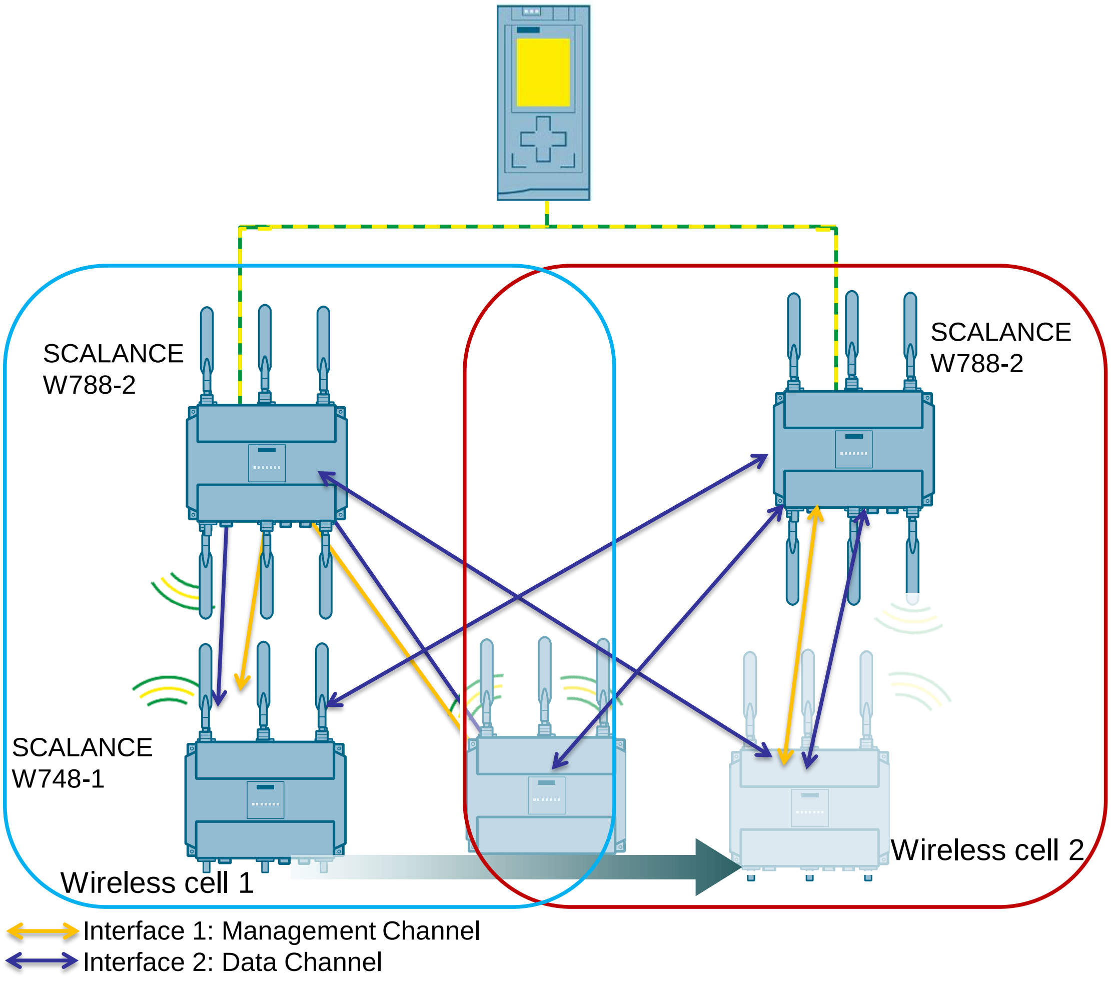
iPCF and iPCF-MC

iPCF-MC was developed in order to also make the advantages achieved by iPCF possible for free-moving nodes, (see chapter 4.6.1) which communicate regardless of whether an RCoax cable or directional antenna is used. For iPCF-MC, the client still searches for potentially suitable access points if it receives iPCF requests from the access point and if the existing connection to an access point is interference free. If required, this can allow for a very fast changeover to a different access point. In contrast to iPCF, the handover times for the iPCF-MC do not depend on the number of radio channels used.

Operating principle

If iPCF-MC is used, it is necessary to use an access point with two radio interfaces, known as a dual access point. One interface works as a management channel, transmitting short messages ("beacons") containing administrative information (e.g. channel settings for the data channel and SSID). The other interface (data channel) only transmits the user data.

Figure 4-13



Restrictions concerning iPCF-MC

Access points with a WLAN interface cannot participate in the iPCF-MC procedure. However, iPCF is possible.

iPCF and iPCF-MC are not compatible with each other and cannot be used simultaneously on one device.

The iPCF-MC method is a Siemens AG in-house development and only works with nodes where iPCF-MC has been implemented.

Requirements

The following requirements are necessary in order to use this function:

- iPCF-MC uses the two wireless interfaces of the access point differently: One interface works as a management interface. The other interface transmits the user data. That means that only SCALANCE W700 devices with two WLAN interfaces can be used as access points.
- The management and data channels must be operated in the same frequency band and have matching radio coverage. iPCF-MC will not work if both radio interfaces are equipped with directional antennas covering different areas.
- The management channel for all access points between which a client is to be changed must use the same channel. A client only scans this one channel to find an accessible access point.

- For the management channel, the transmission method according to IEEE 802.11h cannot be used. However, 802.11h is possible for the data channel.
- A client has to support this feature on its WLAN interface.

4.6.3 iREF

The industry-specific extension "Industrial Range Extension Function" (iREF) is used to improve transmission conditions.

By minimizing the number of access points used along a route and by avoiding overlapping radio channels, this results in less interference with adjacent access points, resulting in higher data throughput for the entire system.

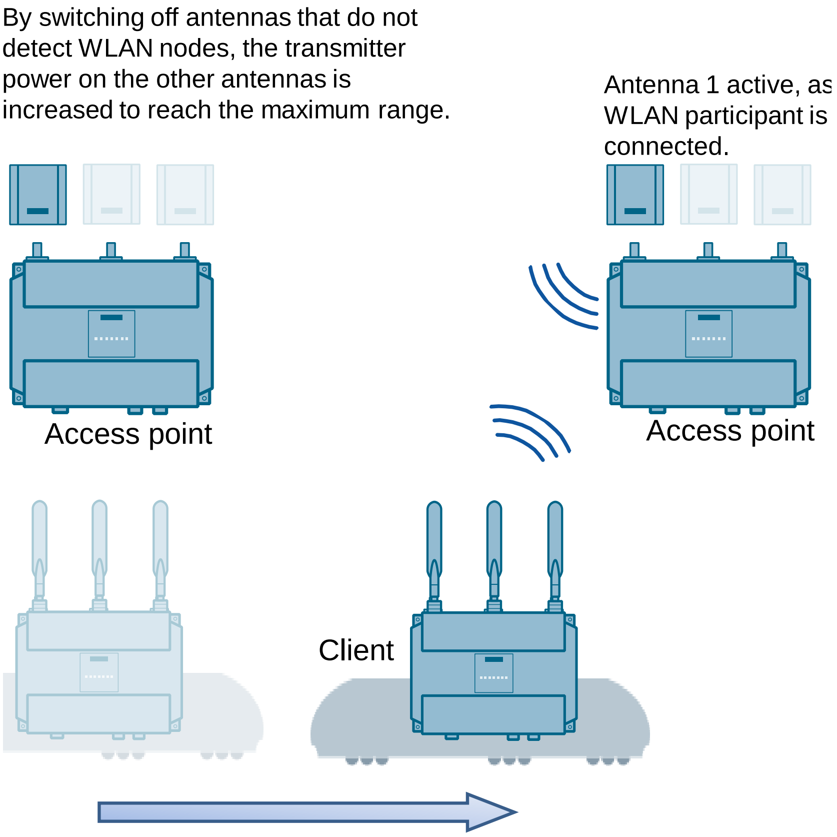
Operating principle

iREF (industrial Range Extension Function) ensures data traffic from the access point to each client runs via the most appropriate antenna.

The most suitable antenna is determined by the access point on the basis of the RSSI value of the received packets. Taking into account antenna gain and possible cable loss, packets are only sent on antennas for which the maximum signal strength is to be expected on the client side.

During this time, the other antennas are inactive and the transmission power permitted by law is available for the selected antenna.

Figure 4-14


By switching off antennas that do not detect WLAN nodes, the transmitter power on the other antennas is increased to reach the maximum range.
Antenna 1 active, as WLAN participant is connected.
Access point
Access point
Client

Restrictions concerning iREF

iREF can only be operated alone. Combining it with other industrial functionalities (iFeatures such as iPCF or iPCF-MC) is not possible.

Only a maximum data rate of up to 150 Mbps is possible.

Requirements

In order to use the iREF technology, the device must have at least two activated antennas.

4.6.4 Inter AP blocking

Clients that are connected to an access point can normally communicate with all devices of the layer 2 network.

And with inter AP blocking, communication of clients linked with the access point can be restricted. Only devices whose IP addresses are known to the access point are accessible to the clients. Communication with other nodes in the network is thus prevented.

Note

Additional documents on the topic of "Current IWLAN technologies" can be found on the SIEMENS Automation Portal at the URL:

www.siemens.com/wlan

4.6.5 iPRP

PRP

The parallel redundancy protocol (PRP) is a redundancy protocol designed for cable-based networks on layer 2. It is defined in Part 3 of the IEC 62439 standard.

A PRP network is composed of two completely independent networks. If there is a disturbance in one of the networks, the frames are sent uninterrupted (bumpless) via the parallel redundant network.

PRP-enabled devices each have at least two separate Ethernet interfaces connected to independent networks. Devices that are not PRP-enabled are connected to a Redundancy Box (RedBox).

PRP requires specific transmission rates that are designed for standard Ethernet networks only.

Note The standard is defined for transmission over routes that have an equal level of performance. The two independent networks must be designed for the same level of performance.

iPRP

Industrial Parallel Redundancy Protocol (iPRP) allows PRP redundancy technology to be used in parallel for parallel utilization of dual radio links in wireless networks. This supplementary function facilitates redundant communication over two WLAN routes, even with moving applications.

Whenever the roaming process is delayed or interference occurs, communication continues to run smoothly via this second path.

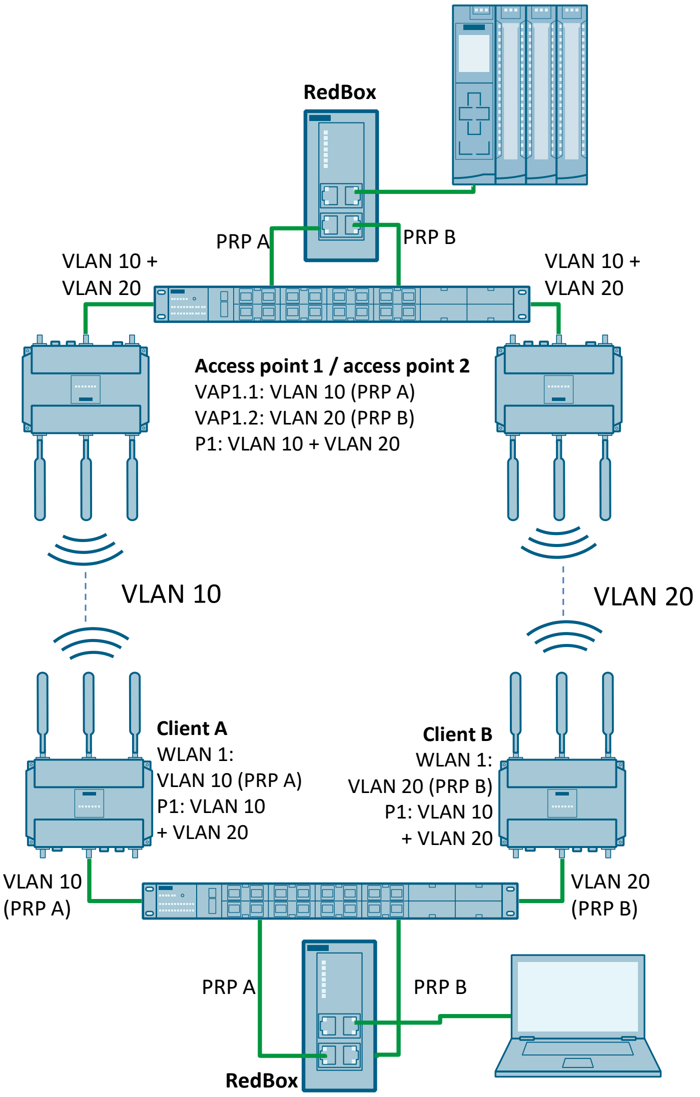
Operating principle

PRP technology ensures that if one transmission path is lost, data communication can continue without interruption. Bumpless transmission is made possible due to the fact that PRP works with two independent networks.

Each PRP-enabled device has at least one interface per network. When the device transmits data, the device duplicates the frames and sends the frame to each network in parallel. Thus, the device transmits the frames along two different transmission paths.

If PRP technology is used in a WLAN, the access points and any Red Boxes are connected via a switch. PRP network A and PRP network B are separated from each other by VLANs.

Figure 4-15



Restrictions with iPRP

iPRP can only be operated alone. Combining it with other industrial functionalities (iFeatures such as iPCF or iPCF-MC) is not possible.

In order to use oversize frames, all devices in the network must be configured for oversize frames (jumbo frames).

The corresponding iPRP VLAN can be used as an agent VLAN. This depends on where the device is located.

- If the device is in PRP network A or PRP network B, use the VLAN associated with the respective PRP network A or PRP network B as the agent VLAN.
- If the access points are in both PRP networks, you can use either one of the VLANs as the agent VLAN. Alternatively, you can also use other VLANs as agent VLANs. The partitioning of the networks into PRP A and B has to remain the same. Single management VLAN for all the devices in network A and B is not necessarily possible.

Requirements

The following requirements are necessary in order to use this function:

- The base-bridge mode "802.1Q VLAN Bridge" is configured.
- The PRP networks are separated via VLANs and those VLANs are applied.
- In access point mode, the VAP interface has to be activated.
- In client mode, it must be configured to MAC mode "Layer 2 Tunnel".

Note Further information and articles concerning this topic can be found in the Siemens Industry Online Support (see chapter 12).

4.6.6 Sleep Mode

This function enables a WLAN client to be put in an energy-saving "sleep mode" (including the CPU), but then to automatically switch back to production mode after a configurable time.

This function is present in all 11n/ac/ax SCALANCE devices.

An application example with these functions can be found in Siemens Industry Online Support: https://support.industry.siemens.com/cs/ww/en/view/57249109

4.6.7 TCP event roaming

Using "TCP event roaming", a WLAN client can initiate a roaming procedure to another access point in a rapid and targeted fashion via TCP telegram.

For an application example that demonstrates the various possibilities with "TCP event roaming", see the Siemens Industry Online Support: https://support.industry.siemens.com/cs/ww/en/view/109815243

4.6.8 Usable IWLAN devices

The following Table shows an overview of which iFeatures are compatible with which IWLAN devices:[16]

Table 4-1

SCALANCE IWLAN device	Type	iPCF	iPCF-2:	iPCF-MC	iREF	iPRP	Inter AP blocking
W788-1 RJ45 / M12	AP	KEY-PLUG	-	- (only as client)	KEY-PLUG	KEY-PLUG	KEY-PLUG
W788-2 RJ45 / M12 (EEC)			-	KEY-PLUG			
W786-1 RJ45			-	- (only as client)			
W786-2 RJ45 / SFP			-	KEY-PLUG			
W786-2IA RJ45			-				
W774-1 RJ45/ M12 (EEC)			-	- (only as client)			
W1788-1 M12		CLP	-	CLP	CLP	CLP	CLP
W1788-2 M12 EEC			-				
W1788-2IA M12			-				
W761-1 RJ45		-	-	-	-	-	-
WAM766-1		-	CLP	-		CLP	-
WAM766-1 EEC		-	CLP	-	-	CLP	-
WAM763-1			CLP			CLP	
W748-1 RJ45 / M12	Client			KEY-PLUG	-	KEY-PLUG	-
W734-1 RJ45					-		-
W722-1 RJ45		x		x	-	-	-
W721-1 RJ45		-		-	-	-	-
WUM763-1		-	CLP	-	-	CLP	-
WUM766-1		-	CLP	-	-	CLP	-

[16] x: The function is available
-: The function is not available
KEY-PLUG / CLP: The function requires activation via the corresponding KEY-PLUG / CLP (see chapter 9.1.1).

4.6.9 iFeatures and PROFINET I/O

PROFINET is an open, cross-vendor product standard based on Industrial Ethernet, which facilitates vertical integration for automation, i.e. networking of all levels of the production process. PROFINET I/O is designed for the data exchange in real-time.

WLAN has its roots as a shared medium. All nodes are essentially "responsible for themselves" and exercise uncoordinated access to the wireless channel. The access of nodes carrying critical data cannot be predicted. With these requirements, PROFINET I/O can only be used under very limited or particular conditions in a standard WLAN.

The proprietary SIEMENS iFeatures

- iPCF / iPCF-2 and
- iPCF-MC

also facilitate real-time communication for a radio network.

5 Data Security and Encryption

5.1 Attack scenarios and security mechanisms

5.1.1 Basics of WLAN security

When using WLANs, users can easily get the feeling that the connection is not secure, as it is not necessary for an intruder, for example, to access a factory site or to physically connect with the network in order to listen in on data: in principle, anyone located within range of the radio signal can listen in on a network's data traffic. However, this assumption is misleading as hardly any cable-based, isolated LANs remain today: in reality, most LANs are connected with the internet and so they, too, are potentially vulnerable to external attack. Security must be deliberately configured for radio networks as well as for cable-based networks.

Thanks to advances in security standards and in component performance, radio networks today can be considered as secure as cable-based networks.

One of the simplest measures for securing a radio network consists of configuring the access points and their transmission performance, for example, so that they only actually cover the required space without any overshoot. This restricts the radio network to the company site and prevents external eavesdropping.

A reduction in the radio power can certainly only provide limited protection and cannot be realized for every scale. More advanced, effective and secure methods include the selection of a suitable infrastructure as well as the use of powerful encryption and authentication protocols, as described in the following chapter.

5.1.2 Attack scenarios

Compromising the security concept

A WLAN's security concept can be unintentionally compromised in several ways:

- *Erroneously configured access points*: 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 put in place, then the access point in question will provide free network access for anyone.
- *Ad hoc wireless network*: Operating systems such as Windows make it possible to configure networks consisting of several wireless clients without requiring an access point in between. If one of the computers is configured in such a way as to form part of an ad hoc network while also establishing connections to the company WLAN, it may provide unintentional access for hackers.
- *Faulty client connections:* If companies are located in close physical proximity to each other, 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 this access point belongs to a neighboring WLAN, this may cause a security risk.

Attack methods

Malicious users can often take advantage of the security gaps described above. However, the following examples also describe scenarios in which you can create your own WLAN access:

- *Rogue access points:* An illegal access point connects to the cable-based network, creating free LAN access for malicious or unauthorized users.
- *Honeypot access points*: Some hackers are capable of determining a WLAN's configuration settings and setting up an access point using the same settings within the network reach. Through this intentional faulty connection, the clients create a connection with these "honeypots" assuming that they are contacting an official access point. Experienced hackers can take advantage of this by connecting network resources with the AP. These network resources bait the users to log on as usual, giving the hacker the opportunity to take unauthorized possession of their passwords or confidential documents.
- *Access point MAC spoofing*: Wireless client computers can be configured as access points. This can allow a hacker to 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 available for manipulating the company network:

- *Unauthorized client accesses:* Hackers are continuously searching for access options in wireless networks. If a network has a weak or non-existent user authentication process, access to the company network is made very easy, allowing hackers to retrieve information or attack resources, which can lead 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 it can handle. Distributed DoS attacks intensify the problem by using a hidden code to prepare a number of "unsuspecting" computers, which then simultaneously perform DoS attacks of possibly enormous proportions.
- *"Man in the Middle"*: If data is unprotected, hackers can intercept messages and manipulate contents by disguising themselves as nodes on the route of a communication connection.
- *IP spoofing*: By manipulating the source IP address in the package header, a hacker can access the traffic from a correctly authenticated user, making it appear as though the user is using the hacker's computer. Subsequently, all data and messages from the server go back to the hacker.
- *Hijacking*: Using software secretly installed on the PC of a company user, a hacker can take control of the affected computer, gaining access to the resources that are accessible to the user, or damaging servers or other computers.

5.1.3 IEEE 802.11 security mechanisms

To protect from unauthorized accesses and attacks to the company network it is essential to enable suitable security mechanisms in the WLAN components.

WEP

WEP ("Wired Equivalent Privacy") 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 802.11 standard.

With this method, a user password is used as a key to generate a series of pseudo random numbers. Each character of the telegram to be transmitted is then encoded with next number of this series and decoded at the receiver.

The method is relatively simple and can be compromised relatively easily for two reasons. On one hand, the key must be exchanged between transmitter and receiver when establishing the connection. This exchange is, of course, unencrypted.

On the other hand, statistical methods can be used to identify properties from the transmitted message traffic, which in turn allow conclusions to be drawn about the key used as long as there is an adequate number of messages for analysis.[17]

With the right 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 provide adequate security.

ACL access control

In network management, filter tables ("Access Control Lists") with IP addresses can be created that allow or deny access to specific addresses. This simple, albeit comparatively unreliable method of access protection can be implemented for the network.

It does not exclude the possibility of IP addresses being manipulated (called "spoofing"), meaning that ACL only offers adequate protection for a network in combination with other measures.

SSID

The SSID (Service Set Identifier) is a name for the WLAN that can be selected freely and that is used to identify it.
A WLAN access point sends this SSID when a client searches for wireless networks.

For this reason and from a security point of view, SSID should not give away the network company, the purpose of the network or the location. Otherwise, this information could spark the curiosity of hackers or other unauthorized individuals. The transmission of the network name can also be suppressed. Since the clients can no longer "see" the wireless network, the SSID has to be entered correctly in the client configuration so that it can connect with the desired WLAN.

[17] If the user were to frequently change the keys manually, this would increase security. However, this is rarely performed consistently in practice.

Note Since no encryption is used for the SSID transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA2 (RADIUS) or WPA2-PSK if this is not possible) provides higher security. It is also to be expected that certain end devices may have issues accessing a hidden SSID.

5.2 Measures for increasing the WLAN security

5.2.1 The IEEE 802.11i extension - encryption methods

The WEP method is associated with a number of weaknesses, meaning that this type of encryption can no longer be considered reliable.

IEEE has detected these security risks and responded accordingly. A new task group for the extension of the 802.11i standards was founded that deals with the security of data transmissions via WLANs, especially concerning the definition of encryption algorithms and integrity checks[18] for wireless transmissions.
The aim of the IEEE 802.11i extension is the development of standardized security measures for wireless data transmissions that meet today's security requirements.

It resulted in three methods:

- TKIP (Temporary Key Integrity Protocol) as a temporary solution for older WLAN devices.
- AES-CCMP (Advanced Encryption Standard, CTR / CBC-MAC Protocol) as a final encryption method that is recommended by the NIST (National Institute of Standards and Technology) today.
- AKM (Authentication and Key Management) to secure a unique authentication process in a WLAN.

TKIP

TKIP is an optional encryption method developed by the task group that, although it is based on the WEP method, it largely fills its security gaps. This interim solution was necessary to ensure the operation of older WLAN devices in a network.

The "Temporal Key Integrity Protocol" uses a key as well as an additional initialization vector in order to encode a message. Using various combinations of the initial key and initialization vector makes encoding work as if the key is being changed continuously, making it more difficult to crack the code.

The integrity check (Message Integrity Check, MIC) is performed via a special HASH algorithm, called "Michael".

[18] An integrity check can be used to prevent data manipulation during data transmissions.

AES-CCMP

AES-CCMP is the final method for encrypting data in a WLAN.

This method requires new WLAN chip sets and cannot be used on older WLAN products.

AES-CCMP, like WEP, pursues a process of "adding together" a key and the message. On the one hand one block of raw data at a time is processed with the same key respectively, on the other hand several processing passes are carried with respectively varying block limits.

Calculating the integrity check (Message Integrity Check, MIC) is performed via temporary keys. The transmitter's MAC address (i.e. the unique hardware ID) is incorporated into the keys, making it even more difficult to falsify the address of the sender of a message.

Note Due to the rising security requirements with iPCF and iPCF-MC, only the AES encryption method is supported.

AKM

Apart from the definitions for secure data transmissions and checking the frame integrity, the IEEE 802.11i extension also makes provisions for further authentication measures and algorithms for automatic key management. The standards of IEEE 802.11X or PSK (Pre-Shared Key) are used as an authentication method (see chapter 5.3).

5.2.2 Wi-Fi Protected Access security standard (WPA)

The IEEE 802.11i working group's development of an encryption algorithm that was supposed to replace WEP was delayed, leading the Wi-Fi Alliance to recommend the application of WPA ("Wi-Fi Protected Access") with TKIP as a subset of the 802.11i standard as an interim solution.

However, following the adoption of the 802.11i standard, this became irrelevant and the Wi-Fi Alliance established WPA2 ("Wi-Fi Protected Access 2") as the new security standard. Encryption with WPA2 focuses on the full implementation of the IEEE 802.11i extension and uses AES-CCMP. In keeping with WPA, authentication can be performed via an authentication server or PSK.

WPA provides the following options for authentication:

- WPA (RADIUS): Authentication by a server (RADIUS server) is mandatory for WPA (RADIUS) (see chapter 5.3.1). The dynamic exchange of the keys in each data frame introduces further security.
- WPA-PSK: With this method, authentication is achieved using a password rather than a server (see chapter 5.3.2). This password is configured manually on the client and server.
- WPA2 (RADIUS) (Wi-Fi Protected Access 2) is an evolution on WPA and implements the functions of the IEEE 802.11i security standard. Authentication works in tandem with the RADIUS server.
- WPA2-PSK is based on the 802.11i standard. WPA authentication works without a RADIUS server, however. Instead, a key (passphrase) is stored on every client and access point. The passphrase is used for authentication and subsequent encryption.

- WPA3-SAE replaces WPA2 and uses Simultaneous Authentication of Equals (SAE) to authenticate access points and clients. With SAE, keys are stored and exchanged mutually, but the passphrase is not revealed. Consequently, attackers cannot find the keys with brute-force dictionary attacks. WPA3-SAE is only possible in 802.11ax WLAN mode!

Note The transmission standard IEEE 802.11n with the "802.11n" or "802.11n only" setting, only supports WPA2/ WPA2-PSK with AES in the security settings.

5.3 Authentication and key management

5.3.1 IEEE 802.1X authentication

Standard IEEE 802.1X does not define the encryption of the data traffic between access point and client, but rather the login procedure as well as the assignment of access rights for clients. For this purpose, the RADIUS protocol is used based on "EAP" (Extensible Authentication Protocol) for larger networks, and PSK in office networks.

RADIUS protocol

The RADIUS protocol (Remote Authentication Dial In User Service) for authentication on the network was originally developed for cable-based systems. However, it has also proven to be successful in other areas, particularly the wireless sector.

With RADIUS, there is a central server referred to as RADIUS, which contains a list including the access authorizations for all nodes. If a client wishes to connect to the network, the access point forwards the request to the RADIUS server. It reacts by generating a "challenge", i.e. a request for the client to send an appropriate "response" if it has the password saved on the RADIUS server.

This method has two advantages:

- The password is never sent via the network in plain text, meaning it cannot be intercepted by an unauthorized individual.
- 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 from the clients, but they can request them any time from the RADIUS computer.

EAP

The acronym EAP covers a wide framework of different authentication mechanisms for network access. In other words, EAP is not an authentication method itself, but rather describes the mechanism according to which the 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 network communication. In other words, 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 different, partially manufacturer-specific protocols exist that can be used with EAP.

5.3.2 Pre-Shared Key (PSK)

The pre-shared key is an alternative to the RADIUS authentication and, amongst others, is made up of a clearly defined key that has to be known to the nodes before communicating.

Additional parameters for generating the PSK include the SSID and the SSID length.

5.4 Safety functions and data rate

Information

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

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

Further information regarding SCALANCE W devices is available in chapter 8.1.2.

Recommendations

To ensure safe operation of networks, some safety-relevant settings should be configured on SCALANCE devices in order to prevent unauthorized access to the network.

Note

In the Siemens Industry Online Support, you will find a checklist that can help with the implementation of the recommendations.
https://support.industry.siemens.com/cs/ww/en/view/109745536

6 Coexistence of IWLANs with other wireless networks

Possible sources of interference in operations

In the industrial environment, there are basically three sources of interference that can affect the function of an IWLAN:

- An environment containing obstacles and objects that exert an influence over the propagation of radio waves (e.g. metal etc.),
- other radio transmitters using the same frequency band (other WLAN nodes, as well as Bluetooth, etc.),
- devices sending unspecific interference pulses (e.g., welding devices, switching devices).

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

Coexistence management

"Radio", as such, is a limited resource. Due to its nature as a "shared medium" it is not possible to increase capacity by simply installing more cables, for example. With proactive coexistence management, it is possible to optimize the use of this resource, which in most cases meets the requirements of industrial applications.

An expert should always be consulted concerning coexistence management.

Radio analysis

The first step should always involve the precise radio analysis of the environment. This 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 volume of data to be transferred?
- Does transmission occur cyclically, sporadically or continuously?
- Where are the nodes stationed?

The principle of the decoupling

The individual radio fields can work independently of one another if they are "decoupled" in at least one of the four domains, i.e. separated:

- Space
- Frequency
- Time
- Code

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 minimum required (no overshoot), by selecting suitable antennas (directional antennas or omnidirectional, compare chapter 9.3), as well as optimizing the setup location for access points and clients, insofar as is possible within the framework of the function of the system.

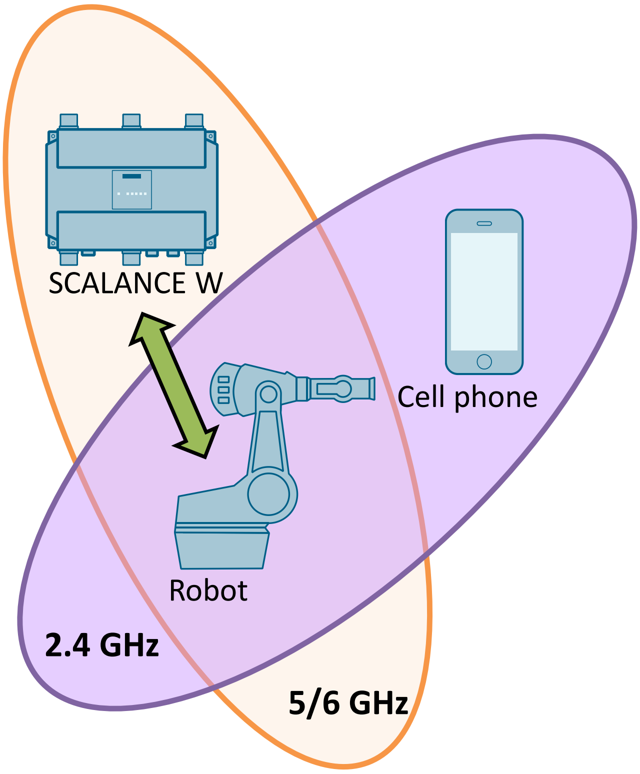
For **frequency decoupling**, it is critical that the frequency ranges of the individual radio systems overlap as little as possible. In the simplest case, this is achieved by selecting the respective radio channels. In a more advanced case, this is achieved by modulation and multiplex methods such as MIMO (see chapter 1.6).

For **temporal decoupling**, the configuration of the individual nodes is decisive. These must be selected in such a way that the probability of a time-critical transmission such as PROFINET I/O overlapping with another transmission is as low as possible. (It is possible, for example, to reserve a channel exclusively for time-critical transmissions, as long as this is feasible in practice.)

For **code decoupling**, it is mainly the separation and distinction of different data streams transmitted in parallel via a shared frequency band that has priority. To make each distinct, the data streams of the nodes are coded with independent and individual spreading codes (orthogonal codes). This is how determining which signal belongs to which user can be clearly detected on the receiver.

The following graphic shows an example of decoupling in the frequency range: The access point can communicate with the robot, even though the robot is in the transmission area of the smartphone at the same time, since both are communicating on different frequencies (orange: 5/6 GHz, purple: 2.4 GHz). Even though the fields overlap in space and time, they are decoupled in the frequency domain.

Figure 6-1



Note

More information on this topic can be found on the web and in various brochures published by the ZVEI (German Electrical and Electronic Manufacturers' Association)[19].

[19] https://www.zvei.org/en/

7 Country approvals

7.1 General remarks

Not all radio modes are approved in all countries. Different restrictions for approved configurations in each country can include:

- permitted frequency bands and channels,
- maximum transmission power,
- indoor/outdoor modes,
- 802.11 standards ("a", "b", "g", "h", "n", "Turbo"),
- specific methods for improving transmission quality such as DFS and TCP (compare chapter 2.3.1)

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

Affected components

A radio network is considered an "entity" in which the corresponding approvals must exist for all participating systems. These are primarily all active components that have direct influence on the network, such as:

- Access points,
- Clients (including interface modules)
- Antennas

Note

Passive components (e.g. network sniffer software, power supplies) do not have their own approvals but are approved in the system together with the access points and clients. More information can be found in the list of countries at http://www.siemens.de/funkzulassungen.

Responsibility

In principle, the responsibility for proper operation of a radio system lies with the operator, and not with the manufacturer. Technically, it is always possible to configure a device that has approval in a country in such a way that it violates the standards of this same country in actual operation.

7.2 Country approvals in the SCALANCE W devices

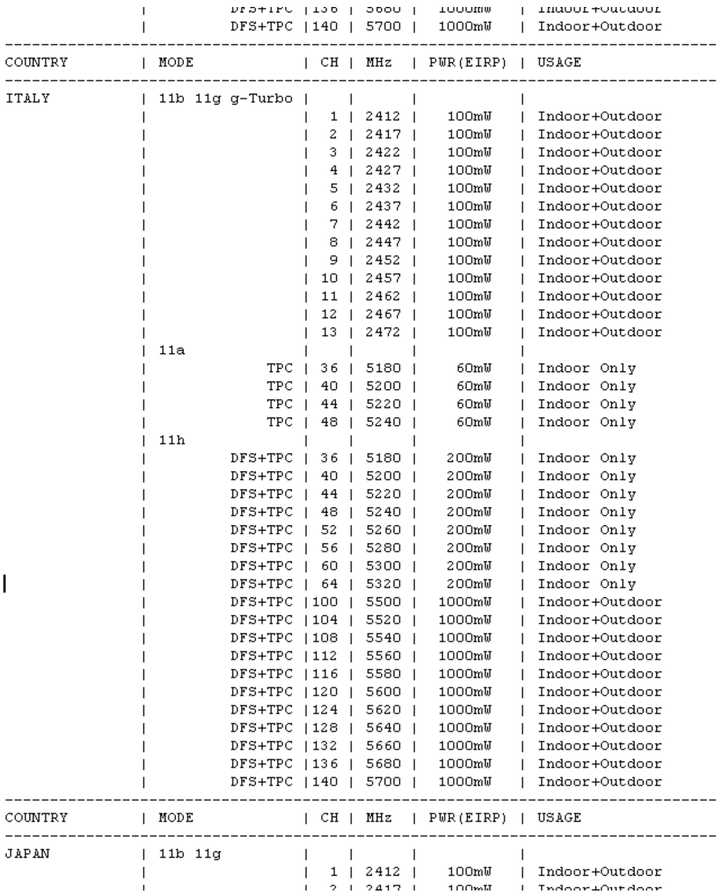
The national standards that were current at the time the firmware was published are stored in the firmware of each SCALANCE W device (compare chapter 8.1.2). These standards can be read via the web interface for the access point or the client in the menu under "System" > "Load&Save".

Note Current descriptions can be found in the manual for the respective device. These can be found in the Siemens Industry Online Support: https://support.industry.siemens.com/cs/products?dtp=Manual&mfn=ps&pnid=15853&lc=en-WW

Please note that this list is for informational purposes only. It is not related to any functional restrictions for 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 generally not permitted in countries that are not listed in the country list.

The following screenshot shows a possible country approval list from an access point. The excerpt below shows the entries of the radio modes permitted in Italy.

Figure 7-1



```
                 |         DFS+TPC |136 | 5680 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |140 | 5700 |  1000mW   | Indoor+Outdoor
--------------------------------------------------------------------------------
COUNTRY          | MODE            | CH | MHz  | PWR(EIRP) | USAGE
--------------------------------------------------------------------------------
ITALY            | 11b 11g g-Turbo |    |      |           |
                 |                 |  1 | 2412 |   100mW   | Indoor+Outdoor
                 |                 |  2 | 2417 |   100mW   | Indoor+Outdoor
                 |                 |  3 | 2422 |   100mW   | Indoor+Outdoor
                 |                 |  4 | 2427 |   100mW   | Indoor+Outdoor
                 |                 |  5 | 2432 |   100mW   | Indoor+Outdoor
                 |                 |  6 | 2437 |   100mW   | Indoor+Outdoor
                 |                 |  7 | 2442 |   100mW   | Indoor+Outdoor
                 |                 |  8 | 2447 |   100mW   | Indoor+Outdoor
                 |                 |  9 | 2452 |   100mW   | Indoor+Outdoor
                 |                 | 10 | 2457 |   100mW   | Indoor+Outdoor
                 |                 | 11 | 2462 |   100mW   | Indoor+Outdoor
                 |                 | 12 | 2467 |   100mW   | Indoor+Outdoor
                 |                 | 13 | 2472 |   100mW   | Indoor+Outdoor
                 | 11a             |    |      |           |
                 |             TPC | 36 | 5180 |    60mW   | Indoor Only
                 |             TPC | 40 | 5200 |    60mW   | Indoor Only
                 |             TPC | 44 | 5220 |    60mW   | Indoor Only
                 |             TPC | 48 | 5240 |    60mW   | Indoor Only
                 | 11h             |    |      |           |
                 |         DFS+TPC | 36 | 5180 |   200mW   | Indoor Only
                 |         DFS+TPC | 40 | 5200 |   200mW   | Indoor Only
                 |         DFS+TPC | 44 | 5220 |   200mW   | Indoor Only
                 |         DFS+TPC | 48 | 5240 |   200mW   | Indoor Only
                 |         DFS+TPC | 52 | 5260 |   200mW   | Indoor Only
                 |         DFS+TPC | 56 | 5280 |   200mW   | Indoor Only
                 |         DFS+TPC | 60 | 5300 |   200mW   | Indoor Only
                 |         DFS+TPC | 64 | 5320 |   200mW   | Indoor Only
                 |         DFS+TPC |100 | 5500 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |104 | 5520 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |108 | 5540 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |112 | 5560 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |116 | 5580 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |120 | 5600 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |124 | 5620 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |128 | 5640 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |132 | 5660 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |136 | 5680 |  1000mW   | Indoor+Outdoor
                 |         DFS+TPC |140 | 5700 |  1000mW   | Indoor+Outdoor
--------------------------------------------------------------------------------
COUNTRY          | MODE            | CH | MHz  | PWR(EIRP) | USAGE
--------------------------------------------------------------------------------
JAPAN            | 11b 11g         |    |      |           |
                 |                 |  1 | 2412 |   100mW   | Indoor+Outdoor
                 |                 |  2 | 2417 |   100mW   | Indoor+Outdoor
```

Note

Updated lists of country approvals for individual SCALANCE W products can be found for each product at its corresponding link:

- SCALANCE W700 802.11n at https://support.industry.siemens.com/cs/ww/en/view/109476834.
- SCALANCE W1700 802.11ac at https://support.industry.siemens.com/cs/ww/en/view/109759610
- SCALANCE W700 802.11ax at https://support.industry.siemens.com/cs/ww/en/view/109802595
- For a general overview of all current approvals for the IWLAN devices, see: https://www.siemens.com/wireless-approvals

8 SIMATIC NET products for setting up an IWLAN

8.1 General information

8.1.1 Overview of product range

SIEMENS offers a wide product range for setting up secure and reliable WLANs. The following chapters offer an introduction to the product properties and demonstrate their application and practical use.

The following Figure shows an selection of SIMATIC wireless products.

Figure 8-1

Note Additional, continuously updated information on SCALANCE W products is available at: https://www.siemens.com/iwlan

8.1.2 Division of SCALANCE W products

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

The product family of SCALANCE W devices includes the products:

- Access points and
- Client module.

The access points

The W1788, W78x-, W77x-, W76x and WxB modules are access points that serve as network switches for each cell and as transitions between Industrial Ethernet and WLAN segments.

Note Manuals for the SCALANCE access points can be found in the Siemens Industry Online Support: https://support.industry.siemens.com/cs/ww/en/ps/15860/man

The client modules

The client modules have the designations "W74x", "W78x", "W76x", "W73x", "W72x", "W1748" and "WUx76x". They are connected via Ethernet to mobile end nodes and communicate with each other via the access points.

Note

Manuals on SCALANCE clients can be found in the Siemens Industry Online Support:
https://support.industry.siemens.com/cs/ww/en/ps/15882/man

8.2 SCALANCE W access points

SCALANCE access points are available in three different versions:

- Access Points according to IEEE 802.11 ax
- Access Points according to IEEE 802.11 ac
- Access Points according to IEEE 802.11 n

NOTE

In this document, we will only discuss the newer APs according to the IEEE 802.11 ax/ac standard in detail. Descriptions of the 802.11 n components can be found in Siemens Industry Online Support.

8.2.1 IEEE 802.11 ax access points

The SCALANCE Wxx76x / WAx76x product family builds on the IEEE 802.11ax WLAN standard. The access points support the 2.4 GHz band and 5 GHz band (see chapter 2.2.4).

A maximum data rate of 1201 Mbit/s is possible for each wireless interface. The device family features 2 radio modules, which can be connected to 2 remote antennas. This makes it possible to split the data stream between two transmission antennas via MIMO (spatial multiplexing).

The SCALANCE W-76x devices are available in the following configurations:

- Standard model WAM766-1 for outdoor use, with external antenna connections.
- Standard model WAM763-1 for switchgear enclosures, with external antenna connections.
- The EEC model WAM766-1 EEC (Enhanced Environment Conditions), with external antenna connections.

The access points for indoor/outdoor use have an IP65 rating, while the ones for switchgear enclosures have an IP30 rating.

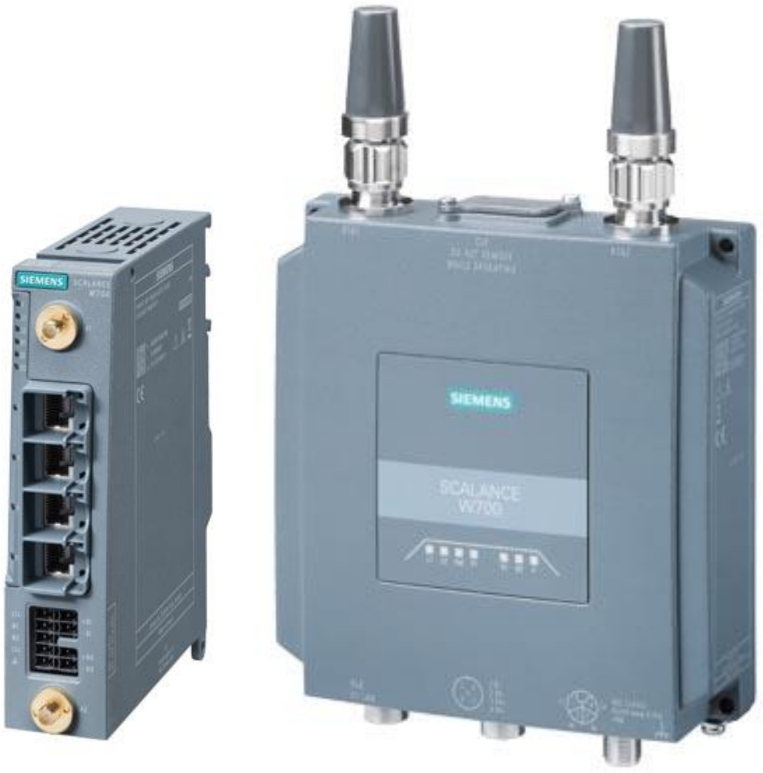
In addition, the EEC version can be used in high-performance plant networks and applications with high temperatures or EMC requirements.

The Ethernet interface with the EEC and indoor/outdoor model has an electrified (M12 Pro) design, while the switchgear variant has an RJ45 design.

For connection to external antennas, R-SMA jacks are provided on the switchgear variant while robust N-Connect jacks are provided on the other variants.

All variants have a slot for inserting a CLP storage medium.

Figure 8-2



The access points of the WAM76x product family are available to order in the following variants:

- WAM763-1 (switchgear variant)
  - Part number: 6GK5763-1AL00-7DA0
- WAM766-1 (for indoor use)
  - Part number: 6GK5766-1GE00-7DA0 or
  - Part number: 6GK5788-2GY01-0AB0 (US variant)
- WAM766-1 EEC
  - Part number: 6GK5766-1GE00-7TA0 or
  - Part number: 6GK5766-1GE00-7TB0 (US variant)

8.2.2 IEEE 802.11 ac access points

The SCALANCE W-1700 product family builds on the technology as defined by the IEEE 802.11ac Wave 2 WLAN standard. The access points support the 2.4 GHz band and 5 GHz band (see chapter 2.2.4).

And thanks to MU-MIMO (multi-user MIMO) technology, data streams can be structured to achieve even more efficient data transmission rates. This achieves data rates of up to 1733 Mbit/s.

Up to four antennas can be connected to each radio module. This distributes the data stream to up to four transmitting antennas (spatial multiplexing).

The SCALANCE W1788-x M12 is available in two models:

- The standard version W1788-x M12 with external antenna connections

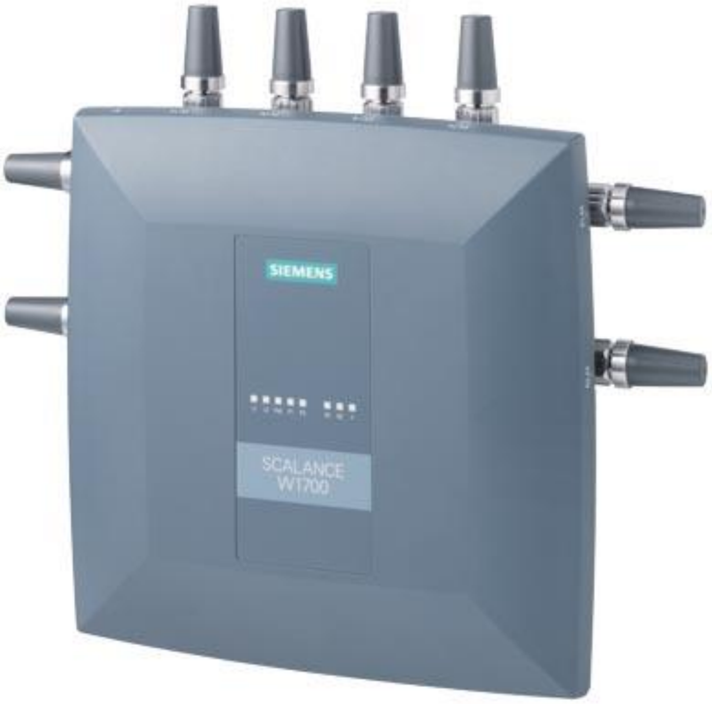
- The standard version W1788-2IA M12 with internal antennas
- The EEC version W1788-2 M12 EEC (Enhanced Environment Conditions) with external antenna connections.

All access points have degree of protection IP65 and are suitable for indoor installation in industrial environments with especially challenging environmental conditions.

In addition, the EEC version can be used in high-performance plant networks and applications with high temperatures or EMC requirements.

The Ethernet interface is implemented electrically (M12). Robust N-Connect sockets are provided for connecting external antennas for the access points W1788-x M12.
The modules have a slot for inserting a CLP storage medium.

Figure 8-3



The access points of the W1788 product family are available in the following variants:

- W1788-1 M12 with one wireless interface
  - Part number: 6GK5788-1GY01-0AA0 or
  - Part number: 6GK5788-1GY01-0AB0 (US variant)
- W1788-2 M12 with two independent wireless interfaces
  - Part number: 6GK5788-2GY01-0AA0 or
  - Part number: 6GK5788-2GY01-0AB0 (US variant)
- W1788-2 M12 EEC with two independent wireless interfaces
  - Part number: 6GK5788-2GY01-0TA0 or
  - Part number: 6GK5788-2GY01-0TB0 (US variant)
- W1788-2IA M12 with two independent wireless interfaces
  - Part number: 6GK5788-2HY01-0AA0

8.3 SCALANCE W clients

The SCALANCE W clients can be operated both at standalone access points and on controller-based access points.

The construction of the modules is identical to that of the corresponding access points (see chapter 8.2). However, their software differs in functionality. In contrast to the access points, these devices are not intended for network management, but for communicating with each other and with other network devices.

The clients also constitute the interface between Ethernet-connected devices and the WLAN. However, they do not transmit all network traffic, but rather only transmit messages for a limited number of Ethernet devices.

The SCALANCE client modules are available in three different versions:

- Client modules compliant with IEEE 802.11 ax
- Client modules compliant with IEEE 802.11 ac
- Client modules compliant with IEEE 802.11 n

NOTE

In this document, we will only discuss the newer IWLAN clients according to the IEEE 802.11 ax/ac standard in detail. Descriptions of the 802.11 n components can be found in Siemens Industry Online Support.

The client modules can work in both the 2.4 GHz band and the 5 GHz band.

The clients are equipped with one or two radio modules. Up to four antennas can be connected to each radio module. This makes it possible to distribute the data stream between up to four transmitting antennas (spatial multiplexing).

Note

As a part of the implementation of the new WLAN standard 802.11n in the SCALANCE W products, the modules were completely modernized and all of the old devices discontinued. The new devices cannot be used as spare parts for the old devices.

The following FAQ list shows which SCALANCE W products with the 802.11n standard replace the old devices without the 802.11n standard.
https://support.industry.siemens.com/cs/ww/en/view/109479635

Note

The discontinuation of the Mobile Panel 277 (F) IWLAN and the corresponding transponders has been declared.
Discontinued products are not recommended for new applications. For new machines and systems, successor products Mobile Panel 2nd Generation or SIMATIC Industrial Tablet PC are recommended. Further information on the successor devices and recommendations for migration are available in the following product note:
https://support.industry.siemens.com/cs/de/de/view/109747989

8.3.1 IEEE 802.11 ax client modules

SCALANCE WUM763-1 clients

The SCALANCE WUM763-1 modules are built with an IP30 rating and are suitable for use in switchgear enclosures within industrial environments.

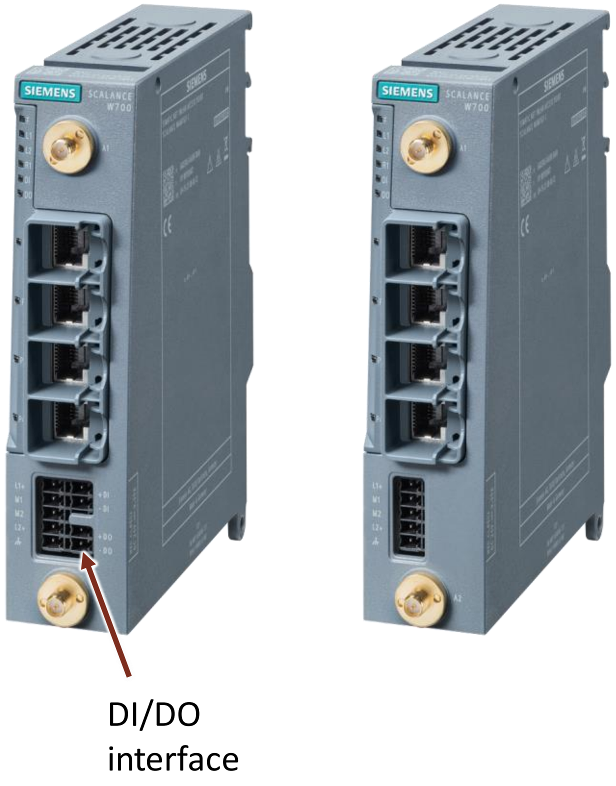
The integrated managed 4-port Ethernet switch is electrified (RJ45) and gigabit-capable.

R-SMA sockets are provided for connecting the two external antennas.

The module has a PLUG slot for inserting a CLP (Configuration and License PLUG).

The module allows for energy-optimized operation of mobile, battery-powered end devices in the industrial environment thanks to a digital input/output interface and the Sleep Mode function.

Figure 8-4



The SCALANCE WUM763-1 is available to order in the following variants:

- Part number: 6GK5763-1AL00-3DA0 (with DI/DO) or
- Part number: 6GK5763-1AL00-3AA0 (without DI/DO)

SCALANCE WUM766-1 clients

These clients have degree of protection IP65 and are suitable for indoor installation in industrial environments.

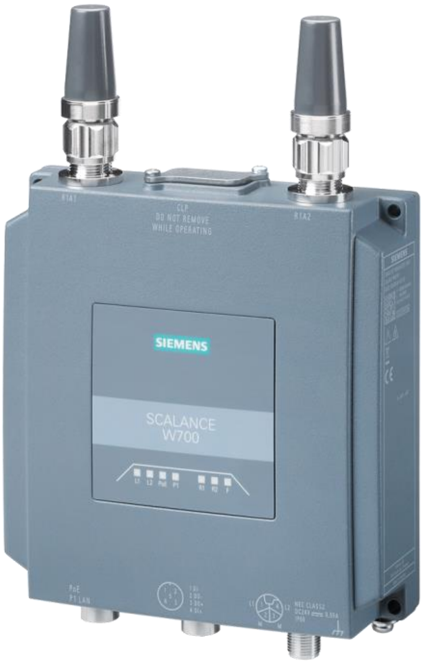
The Ethernet interface has an electrified (M12 PRO) design, is gigabit-capable and enables Power over Ethernet.

Robust N-Connect sockets are provided for connecting the two external antennas.

The module has a PLUG slot for inserting a CLP (Configuration and License PLUG).

The module allows for energy-optimized operation of mobile, battery-powered end devices in the industrial environment thanks to a digital input/output interface and the Sleep Mode function.

Figure 8-5



The SCALANCE WUM766-1 is available to order in the following variants:

- Part number: 6GK5766-1GE00-3DA0 or
- Part number: 6GK5766-1GE00-3DB0 (US variant)

8.3.2 IEEE 802.11ac client modules

SCALANCE W1748 M12 client

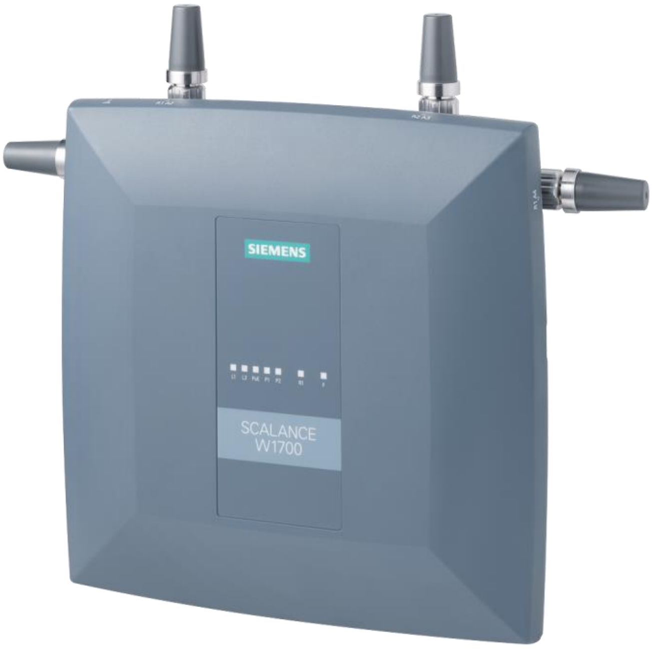
This client has an IP65 rating and is suitable for installation in interior areas in industrial environments.

The 2 Ethernet interfaces are electrified (M12 design), are gigabit-capable and enable Power-over-Ethernet.

Robust N-Connect sockets are provided for connecting the four external antennas (MIMO-capable).

The module has a PLUG slot for inserting a CLP (Configuration and License PLUG).

Figure 8-6



The SCALANCE W 1748 M12 is available to order in the following variant:

- Part number: 6GK5748-1GY01-0AA0

8.4 Configuring the SCALANCE W devices

The SCALANCE W700 access points and client modules can be configured and managed in the following ways:

- Web Based Management (WBM)
- Command Line Interface (CLI) via Telnet
- TIA Portal (integrated as PROFINET device via GSDML file)
- SINEC NMS (Network Management System)

Web Based Management

WBM accesses the configuration data from the SCALANCE W via the Ethernet interface or an existing WLAN connection. A web browser on the configurator PC communicates with an HTTP server that runs on the SCALANCE W. Using the HTTP server, configuration data can be viewed and edited using conventional forms such as those used on websites.

A number of software wizards are available in Web Based Management for the user-friendly installation and configuration of both the access points and the client modules. These modules can be adapted perfectly to the communication task at hand. Both the network operating mode and the required security level for the WLAN can be configured here with minimal effort.

Note

There are a number of configuration manuals available in the Siemens Industry Online Support. You can find a selection at the following links:

- Configuring the SCALANCE W780/W740 via WBM: http://support.automation.siemens.com/WW/view/en/62516763
- Configuring the SCALANCE W770/W730 via WBM: https://support.industry.siemens.com/cs/document/109480849
- Configuring the SCALANCE W760/W720 via WBM: https://support.industry.siemens.com/cs/document/109480845
- Configuring the IEEE 802.11ax SCALANCE W700 via WBM: https://support.industry.siemens.com/cs/ww/en/view/109797832

SINEC NMS

SINEC NMS is ideal for managing larger SCALANCE W systems (diagnostics, firmware management, security management).

Note

The following links in the Siemens Industry Online Support provide additional information on SINEC NMS:

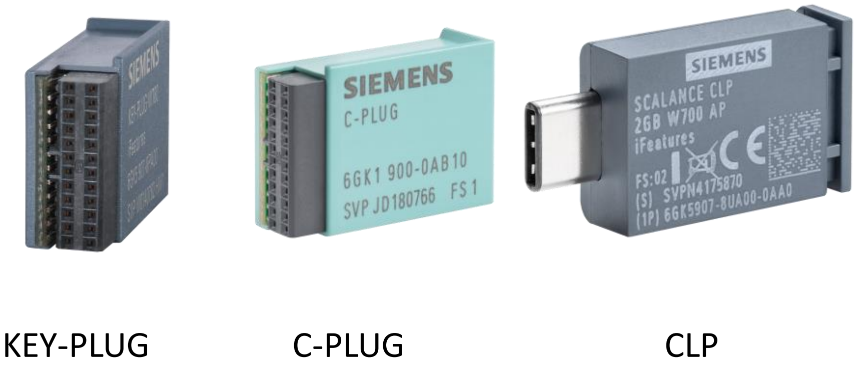
- SIMATIC NET: Network management with SINEC NMS
  https://support.industry.siemens.com/cs/ww/en/view/109762749
- Using and Understanding SINEC NMS
  https://support.industry.siemens.com/cs/ww/en/view/109762792
- WLAN configuration with SINEC NMS, parts 1 through 3
  https://www.youtube.com/watch?v=g57tYeBX-RU (in German)
  (English: https://www.youtube.com/watch?v=Q17ieFzegqk)
  https://www.youtube.com/watch?v=9B6I11ooKk4 (in German)
  (English: https://www.youtube.com/watch?v=bCxdRSbmyso)
  https://www.youtube.com/watch?v=oFRfRqEGkHs (in German)
- (English: https://www.youtube.com/watch?v=EhC_Ug2B5nI)

9 Accessories for wireless networks (WLANs)

9.1 Optional storage media

A KEY-PLUG / C-PLUG / CLP (Configuration Plug / Configuration License Plug) is a removable storage device that can be inserted into a corresponding slot in the hardware.
C-PLUGs and KEY-PLUGs share a similar design, but their differ with regard to their function and color.

Figure 9-1



9.1.1 SCALANCE CLP

The SCALANCE CLP is used in cases where the replacement of network components or communication modules needs to be quick and easy when a fault occurs, without having to configure the replacement part and without the need for specialist personnel. The CLPs can also be used as a memory expansion for software applications. They can be used in any SCALANCE device that has a CLP slot (SCALANCE access points and client modules built to comply with IEEE 802.11ac/ax). The following versions are available:

- SCALANCE CLP 2GB
  used to back up and restore configurations for hot-swapping devices in the event of a fault.
- SCALANCE CLP W700 AP 2GB W700 AP iFeatures
  for upgrading the iFeatures in the SCALANCE access points.
- SACLANCE CLP W700 2GB W700 Client iFeatures
  for upgrading the iFeatures in the SCALANCE client modules.

9.1.2 KEY-PLUG

Different KEY-PLUGs unlock additional functions for various industrial network components from Siemens AG.

When combined with the SCALANCE W7xx for IEEE 802.11a/g/n, the KEY-PLUG W780 or W740 activates the iFeatures (see chapter 4.6):

- the KEY-PLUG W780 iFeatures enables the iFeatures in access point mode and in client mode,
- the KEY-PLUG W740 iFeatures enables the iFeatures only in client mode.

- the KEY-PLUG W700 Security enables additional security functions in the access point.

This means that each SCALANCE W 11n standard device can be expanded/upgraded with additional functions without having to replace the hardware.

In addition, the KEY-PLUG includes the same functions as the C-PLUG.

9.1.3 C-PLUG

The SCALANCE W700 devices in accordance with the IEEE 802.11a/b/g/n standard are equipped with internal flash storage as well a C-PLUG slot for storing the configuration data.

If a C-PLUG is inserted, the configuration data and other changes are always automatically stored on it. This helps facilitate the replacement of devices. By simply replacing the C-PLUG, all data can be adopted in the replacement device without the need for a programming device.

Note

Further information on the use of C-PLUGs with SCALANCE W devices can be found in the Siemens Industry Online Support (Article ID 29823212):

https://support.industry.siemens.com/cs/document/29823212

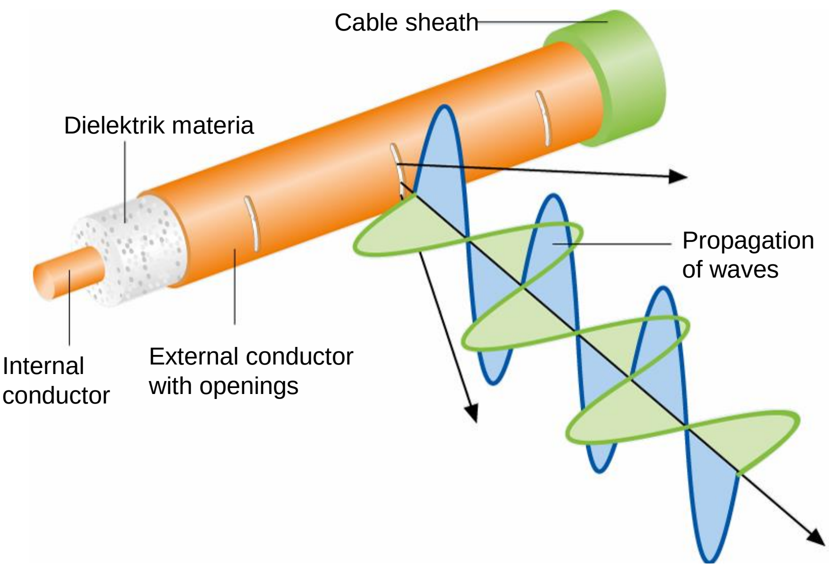
9.2 RCoax radiating cables

Description

The RCoax cables are radiating cables that act as special antennas for the SCALANCE W access points in environments with complex radio coverage.

Radiating cables are coaxial cables whose external sheaths defines interruptions in the radio signal. This design results in a defined, cone-shaped radio field generated along the RCoax cable.

Figure 9-2



The RCoax cable

RCoax cables replace standard radio antennas at selected access points with an antenna segment at a customable length. They transmit and receive in the 2.4 GHz or 5 GHz band. They are preferably used for environments in which nodes move within limited areas or exclusively on predefined paths (monorail conveyors, high-bay racking systems) and where a lot of shadowing or reflection is to be expected.

The RCoax cable can be bent during installation of the system and is therefore able to adjust to the local conditions. For example, it can directly follow the course of a monorail overhead conveyor. In challenging environments, this offers the option of providing reliable illumination for the sections of the wireless cell that are difficult to access. This avoids having to use high maintenance sliding contacts or trailing cables.

iPCF and PROFINET I/O

The IEEE 802.11 protocol for the access point is not influenced by the use of RCoax cables. In particular, the data rates and the protocols for data backup remain unchanged. iPCF and communication via PROFINET I/O are possible as before – provided that the respective access points and clients are available.

Data rate and segment length

Any SCALANCE W access point can be upgraded with an RCoax cable. In order to create longer, uninterrupted wireless ranges, several radiating cable segments (each with an assigned access point) can be arranged one after another.

Attenuation of the RCoax cable increases along the radiating cable, reducing the signal strength. With the increasing cable length and increasing distance from the cable, the achievable data rate is also reduced.

Note

Further information on this topic as well as performance data can be found in the "RCoax system manual" in the Siemens Industry Online Support.
https://support.industry.siemens.com/cs/ww/en/view/109480869

Connecting mobile nodes

In an RCoax network, an access point feeds in the RCoax cable. The RCoax cable acts as an antenna for mobile partner stations (e.g. SCALANCE W clients) that travel along the RCoax cable and that receive information from this cable either via their antenna or by coupling to the cable.

The connection to the wireless RCoax network is achieved via antennas that are to be installed in the immediate proximity of the RCoax cable using the flexible connection cable.

Note

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

https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-wireless-lan/iwlan-rcoax-cable.html

9.3 Antennas

9.3.1 Overview of WLAN antennas

Next to device selection, antennas are the top priority in achieving the ideal radio field architecture. The following points are particularly crucial:

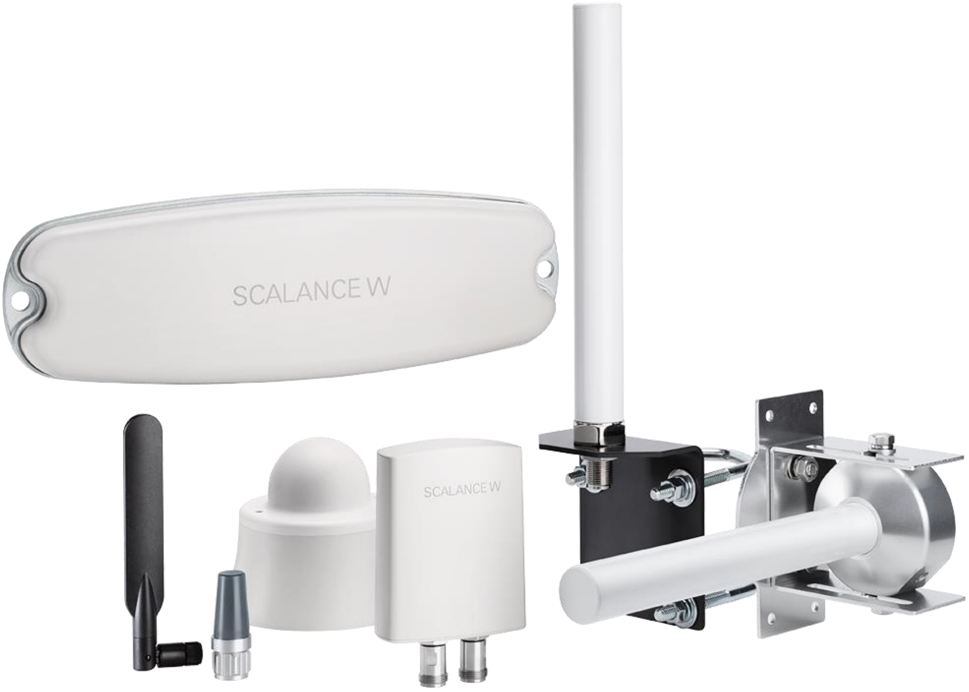
- Antenna properties (radio coverage)
- Location of application (indoors or outdoors)
- Required data rates

The SIMATIC portfolio includes a number of omnidirectional and directional antennas (for basic information on antennas, see also chapter 1.5). They can either be installed directly or separately from the device, e.g. on a mast or wall, in order to achieve optimized illumination of the space to be covered.

Antennas with two (dual slant) or three connections (MIMO) increase the data throughput and reliability through targeted use of multipath propagation.

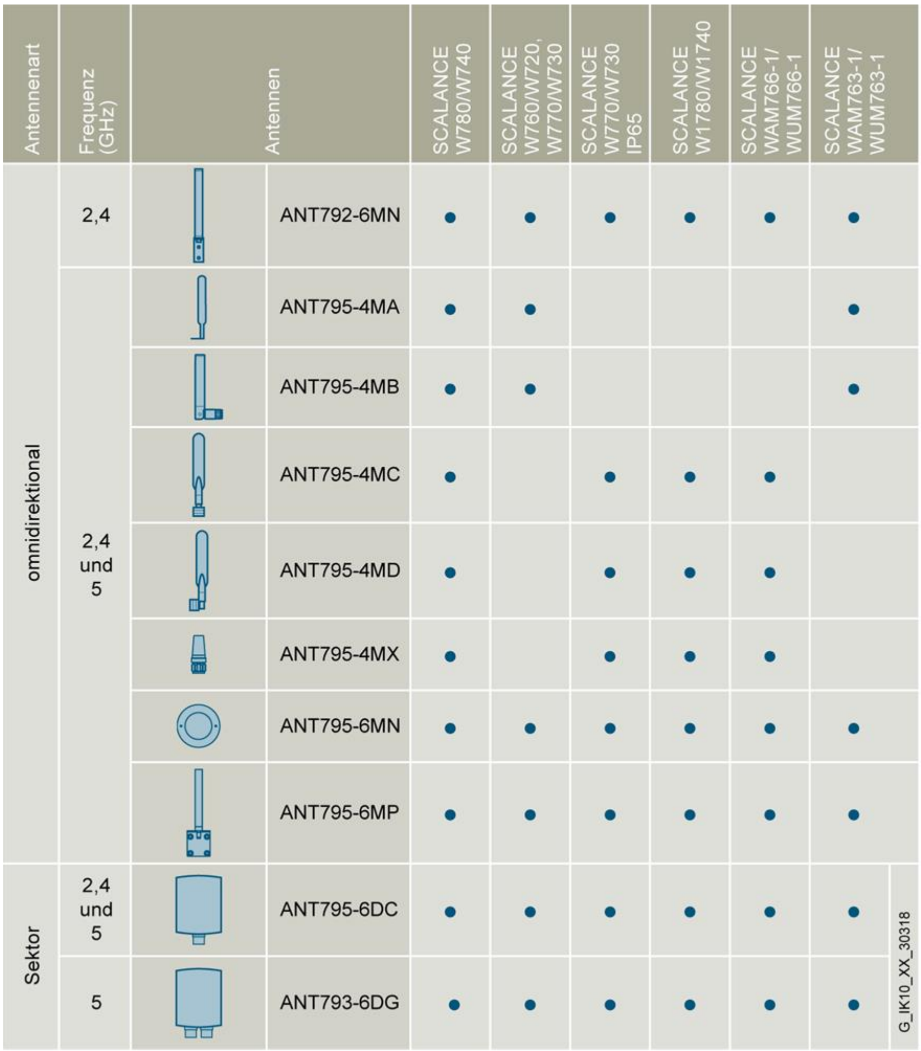
The following Figure shows an overview of WLAN antennas:

Figure 9-3



The properties for the most important antenna types are listed in the following Table:

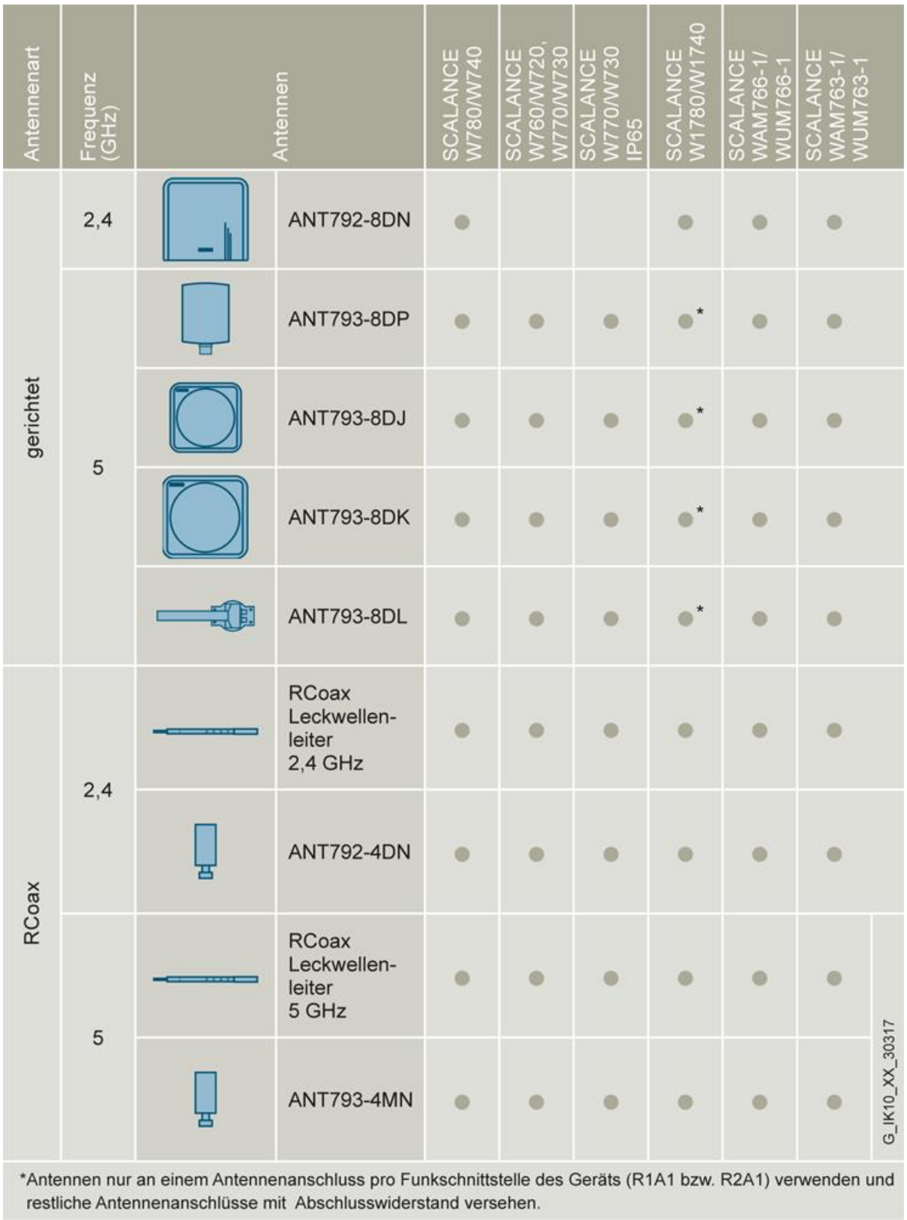
Figure 9-4



Antennenart	Frequenz (GHz)	Antennen	SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65	SCALANCE W1780/W1740	SCALANCE WAM766-1/ WUM766-1	SCALANCE WAM763-1/ WUM763-1
omnidirektional	2,4	ANT792-6MN	●	●	●	●	●	●
	2,4 und 5	ANT795-4MA	●	●				●
		ANT795-4MB	●	●				●
		ANT795-4MC	●		●	●	●	
		ANT795-4MD	●		●	●	●	
		ANT795-4MX	●		●	●	●	
		ANT795-6MN	●	●	●	●	●	●
		ANT795-6MP	●	●	●	●	●	●
Sektor	2,4 und 5	ANT795-6DC	●	●	●	●	●	●
	5	ANT793-6DG	●	●	●	●	●	●

G_IK10_XX_30318

Figure 9-5



Antennenart	Frequenz (GHz)	Antennen	SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65	SCALANCE W1780/W1740	SCALANCE WAM766-1/ WUM766-1	SCALANCE WAM763-1/ WUM763-1
gerichtet	2,4	ANT792-8DN	●			●	●	●
	5	ANT793-8DP	●	●	●	●*	●	●
		ANT793-8DJ	●	●	●	●*	●	●
		ANT793-8DK	●	●	●	●*	●	●
		ANT793-8DL	●	●	●	●*	●	●
RCoax	2,4	RCoax Leckwellenleiter 2,4 GHz	●	●	●	●	●	●
		ANT792-4DN	●	●	●	●	●	●
	5	RCoax Leckwellenleiter 5 GHz	●	●	●	●	●	●
		ANT793-4MN	●	●	●	●	●	●

*Antennen nur an einem Antennenanschluss pro Funkschnittstelle des Geräts (R1A1 bzw. R2A1) verwenden und restliche Antennenanschlüsse mit Abschlusswiderstand versehen.

G_IK10_XX_30317

Note on IWLAN antenna naming conventions

The most important functional properties are reflected in code in the name of the antenna types:

ANT79w-xyz

w = 2 / 3 / 5: Frequency range 2.4 GHz / 5 GHz / dual band (2.4 and 5 GHz)

x = 4 / 6 / 8: Measure for passive amplification

y = M / D: Omnidirectional / directional

Example: ANT792-8DN (2 GHz, high gain, directional, N-connect)

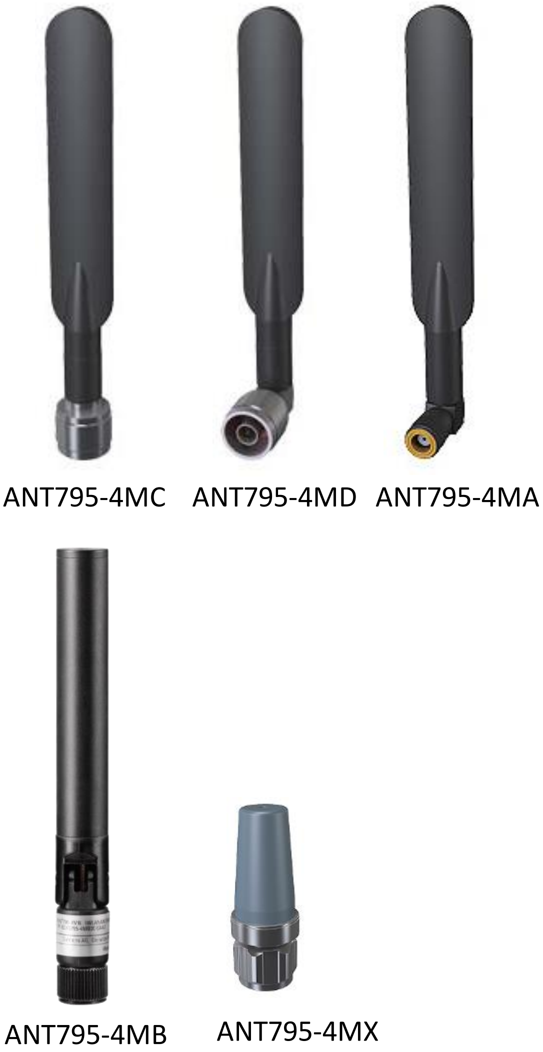
9.3.2 Antennas with an omnidirectional property

SIMATIC NET offers a coordinated range of antennas with omnidirectional properties for various applications, both indoors and outdoors. The antennas differ with regard to their location of installation, connections, protection class and frequency range.

ANT795-4Mx antenna

The antenna type ANT795-4Mx is suitable for installation directly on the access point or client.

Figure 9-6



The following Table shows the variants:

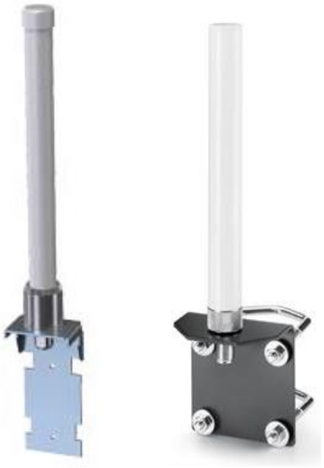
Table 9-1

Antenna	Connection	Protection class	Comment
ANT795-4MC	1 x N-connect male	IP65	Straight
ANT795-4MD	1 x N-connect male	IP65	Fixed 90° angle
ANT795-4MA	1 x R-SMA male	IP30	With additional joint; can be pivoted at an angle between 0° and 90°.
ANT795-4MX	1 x N-connect male	IP68	Straight
ANT795-4MB	1 x R-SMA male	IP65	With additional joint; can be pivoted at an angle between 0° and 90°.

ANT792-6MN / ANT795-6MP antennas

Antenna type ANT79x-6Mx can either be installed on wall or a mast.

Figure 9-7



ANT792-6MN   ANT795-6MP

The following Table shows the variants:

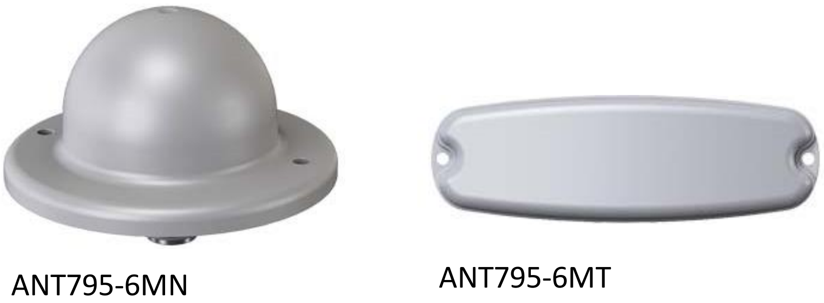
Table 9-2

Antenna	Connection	Protection class	Comment
ANT792-6MN	1 x N-connect female	IP65	
ANT795-6MP	1 x N-connect female	IP67	

ANT795-6Mx antenna

Antenna type ANT795-6Mx can be installed directly on a wall, ceiling or roof.

Figure 9-8



The following Table shows the variants:

Table 9-3

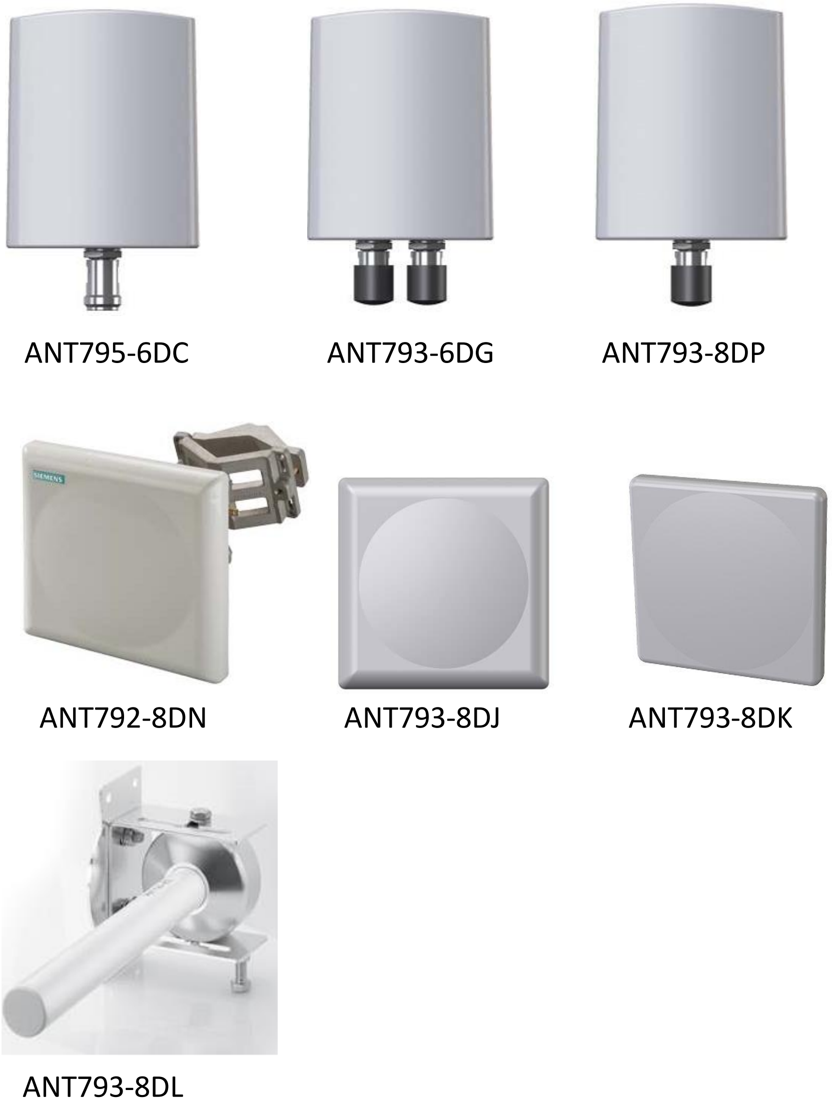
Antenna	Connection	Protection class	Comment
ANT795-6MN	1 x N-connect female	IP65	
ANT795-6MT	3 x QMA female	IP65	MIMO antenna

9.3.3 Antennas with directional effect

The SIMATIC NET product range also offers a large selection of directional antennas. The antennas differ with regard to location of installation, protection class and frequency range.

Antenna type ANT79x-xDx is designed for installation on walls or masts.

Figure 9-9


ANT795-6DC
ANT793-6DG
ANT793-8DP
ANT792-8DN
ANT793-8DJ
ANT793-8DK
ANT793-8DL

The following Table shows the variants:

Table 9-4

Antenna	Connection	Protection class	Comment
ANT795-6DC	1 x N-connect female	IP67	
ANT793-6DG	2 x N-connect female	IP67	Dual slant
ANT793-8DN	1 x N-connect female	IP65	
ANT793-8DP	1 x N-connect female	IP67	
ANT793-8DJ	2 x N-connect female	IP67	Dual slant
ANT793-8DK	2 x N-connect female	IP67	Dual slant
ANT793-8DL	2 x N-connect female	IP67	Dual slant

9.3.4 Antennas for RCoax

When using an RCoax system, the product portfolio offers two antennas that only differ with regard to their frequency range.

Figure 9-10

ANT792-4DN ANT793-4MN

The following Table shows the variants:

Table 9-5

Antenna	Connection	Protection class	Comment
ANT793-4MN	1 x N-connect female	IP66	
ANT792-4DN	1 x N-connect female	IP65	

Note

Further product information on antennas can be found at:

https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-wireless-lan/antenna-accessories.html

Information on RCoax antennas can be found in the "RCoax system manual" in the Siemens Industry Online Support https://support.industry.siemens.com/cs/ww/en/view/109480869

9.4 Connections and cabling

In industrial scenarios, different antenna plugs are used depending on the application. They vary in size, mechanical properties and area of use.

SCALANCE W access points and clients have N-connect or R-SMA connections, depending on the model. The antennas are also equipped with QMA connections. These connections are characterized by their high-class transmissions, reliable connections and use of union nuts and low form factor.

N-connect

The N plug is designed for use with all coaxial cable types. Due to a mechanical fixture it boasts a high level of durability and is very well suited for outdoor use thanks to its additional sealing ring.

SMA connection

The SMA connection is a miniature coaxial plug or socket and is made up of a thread and inner contact. It is offered in two designs:

- SMA variant
- Reverse (R)SMA variant

The differences are shown in the Table below:

Table 9-6

Plug/socket variants	Feature
SMA plug	Internal threads and inner pin contact
SMA socket	External threads and inner barrel contact
R-SMA plug	Internal threads and inner barrel contact
R-SMA socket	External threads and inner pin contact

For SCALANCE W devices with connections of these sizes, the R-SMA variant is used.

QMA connection

QMA connections have the same high electric power as the SMA series, but with a simpler and faster installation. QMA connections are mainly used for the new generation of SCALANCE W antennas (IEEE 802.11n), where several connections are placed within a very small space.

9.5 Additional accessories

A comprehensive, coordinated range of coaxial accessories is offered to provide a flexible combination and installation of the individual IWLAN components for both indoors and outdoors. This range encompasses antenna connecting cables as well as diverse connectors, lightning protection elements, a power splitter and an attenuator.

Note

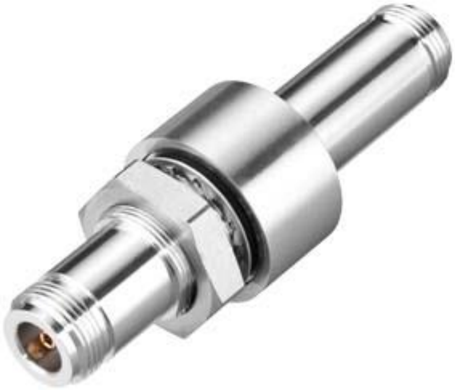
The FAQs in the Siemens Industry Online Support show which connection cables and additional devices can be used to connect external antennas to the SCALANCE W

https://support.industry.siemens.com/cs/document/62544764

Lightning protectors

The LP798-2N lightning protector expands the applications of SCALANCE W700 products using remote antennas, particularly for the outdoors.

Figure 9-11



A lightening protector secures the active device against destructive overvoltage (e.g. lighting) via antenna connections. If an overvoltage event occurs, these currents are conducted away through the ground.

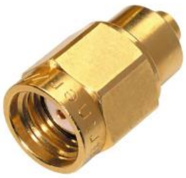
The lighting protector should be installed and grounded as closely as possible to the active device (e.g. the wall of the control cabinet). It is connected to the antenna and the active device via antenna connection cables.

A collection of lightening protection element variants are available.

Terminating resistors

With SCALANCE W700 products, the TI795-1R terminating resistor (see Figure) or TI795-1N has to be used for each antenna connection that is not being used, in order to provide high-frequency termination.

Figure 9-12

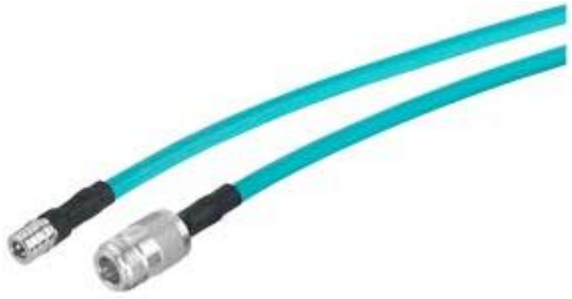


Flexible connecting cables

The flexible IWLAN RCoax/antenna connecting cables are required for connecting RCoax segments or antennas to active devices. They can also be used as adapter cables if the antenna and the WLAN modules have different connections. They are available in different lengths (0.3 m to 10 m) and connection combinations (N-connect, R-SMA, SMA, QMA).

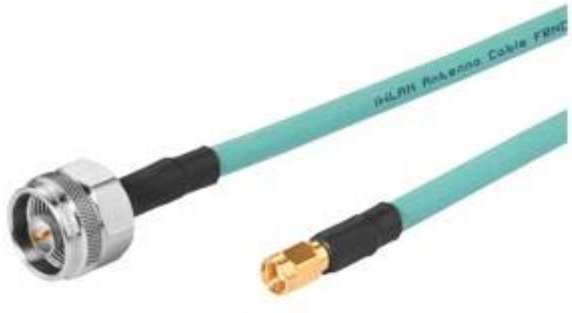
The following Figure shows a QMA/N-connect male/female connection cable:

Figure 9-13



The next Figure shows a connection cable that is used to link a SCALANCE W78x RJ45 and, for example, a remote antenna or a different component with an N-connect connection:

Figure 9-14



Note

Further information and additional application examples can be found in the FAQ "What connection cables and IWLAN devices can you use to connect an external antenna to the SCALANCE W?"

https://support.automation.siemens.com/WW/view/en/43895062

The cables offer low attenuation so that the quality of the radio signal is only minimally affected. All antenna cables are flame-resistant, chemical-resistant and silicone-free.

Power splitter

Figure 9-15

With the help of the power splitter, the transmission power of an access point is divided between two RCoax or antenna segments. This enables wireless coverage in two different areas using just one access point.

SITOP PS307 power supply

The SITOP PowerSupply is a high-quality DC voltage supply for use in industrial environments with protection type IP20. Special supplementary modules protect the power supply from disturbances on the network and the DC sides, as well as providing the necessary supply security.

Figure 9-16

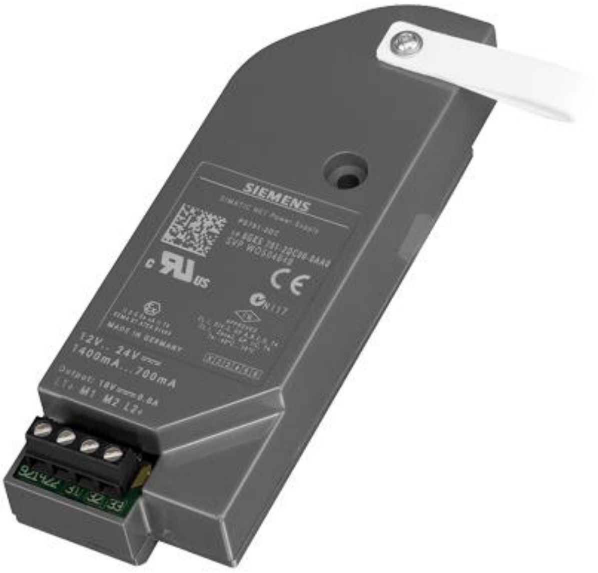
Note When using the SITOP PS307 for the SCALANCE W788 M12 devices the power supply has to be installed in a control box.

Power supply adapter

The power supply adapters PS791-2DC and PS791-2AC were designed for the SCALANCE W786 product line. The power supply adapters are constructed specially for the SCALANCE W786 access points and are directly integrated into them.

Both power supply adapters are provided with an optional energy supply with additional nominal voltages.

Figure 9-17



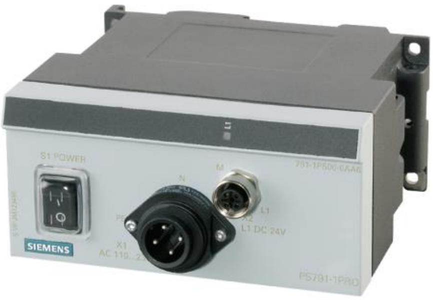
The PS791-2DC power supply adapter is a DC/DC power supply for input voltages of DC 12-24 V and an output voltage of DC 18 V for all SCALANCE W786 products.

The PS791-2AC power supply adapter is an AC/DC power supply for input voltages of AC 100-240 V and an output voltage of DC 18 V for all SCALANCE W786 products.

Alternating voltage power supply with IP65

The SCALANCE W700 modules in protection type IP65 can be directly supplied with power from the socket via the PS791-1PRO power supply. Due to the broad input voltage range (input voltages of AC 90 to 265 V), it can be used worldwide.

Figure 9-18

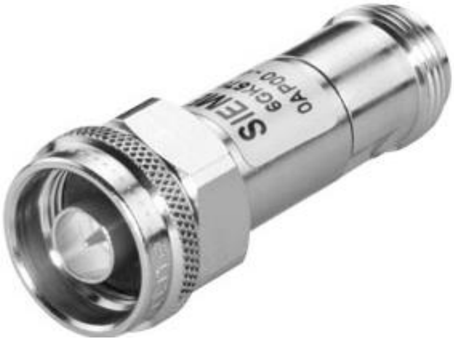


The power supply unit itself has a robust metal housing with protection from water and dust in protection class IP65. The fact that it is short-circuit proof, no-load proof and bridges short power network disturbances guarantee high operational reliability.

Attenuator

The attenuator is always used when the transmitted power has to be reduced in both the sending and receiving directions. Typical application areas include short RCoax segments or directional wireless links whose expansion is to be limited. The insertion loss of the attenuator is 10 dB.

Figure 9-19

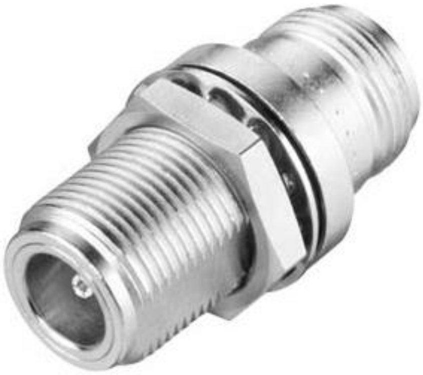


Switch cabinet bushings

Together with the antenna connecting cables, the cabinet feedthroughs allow for the remote antennas to be easily connected to the active components located in the control cabinet/box. The cabinet feedthrough is available with the connection combinations:

- SMA female / N female for wall thicknesses of up to 4.5 mm
- N-connect female / N-connect female for wall thicknesses of up to 4.5 mm

Figure 9-20



Note

Additional product information on passive network components can be found in the "System manual for Industrial Wireless LAN Passive Network Components" in the Siemens Industry Online Support
https://support.industry.siemens.com/cs/document/109480868

9.6 Useful tools

9.6.1 Industrial Wireless LAN – Distance Estimation Tool

General remarks

The IWLAN Distance Estimation Tool helps the IWLAN installation planner estimate the hardware and configurable parameters needed to provide a certain minimum transmission distance.

Description

The web tool can help you make estimates in the following two scenarios:

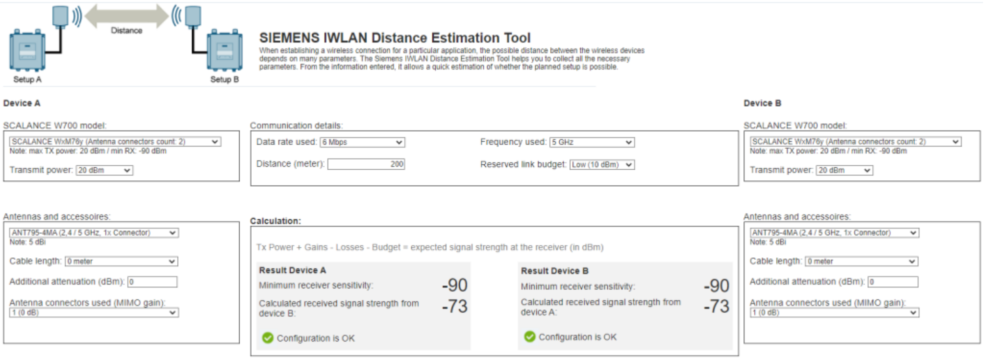
- You have a specified distance and are looking for the right hardware that meets this requirement.
- You can use a variable combination of devices and antennas to find the maximum distance attainable in this case.

User interface

The user interface of the IWLAN Distance Estimation Tool is divided intuitively into the following panes:

- Hardware specification of Device A
- Hardware specification of Device B
- Transmission distance parameters
- Calculated results

Figure 9-21



SIEMENS IWLAN Distance Estimation Tool

When establishing a wireless connection for a particular application, the possible distance between the wireless devices depends on many parameters. The Siemens IWLAN Distance Estimation Tool helps you to collect all the necessary parameters. From the information entered, it allows a quick estimation of whether the planned setup is possible.

Device A

SCALANCE W700 model: SCALANCE WxM76y (Antenna connectors count: 2)
Note: max TX power: 20 dBm / min RX: -90 dBm
Transmit power: 20 dBm

Antennas and accessoires: ANT795-4MA (2,4 / 5 GHz, 1x Connector)
Note: 5 dBi
Cable length: 0 meter
Additional attenuation (dBm): 0
Antenna connectors used (MIMO gain): 1 (0 dB)

Communication details:
Data rate used: 6 Mbps
Frequency used: 5 GHz
Distance (meter): 200
Reserved link budget: Low (10 dBm)

Calculation:

Tx Power + Gains - Losses - Budget = expected signal strength at the receiver (in dBm)

Result Device A
Minimum receiver sensitivity: -90
Calculated received signal strength from device B: -73
✓ Configuration is OK

Result Device B
Minimum receiver sensitivity: -90
Calculated received signal strength from device A: -73
✓ Configuration is OK

Device B

SCALANCE W700 model: SCALANCE WxM78y (Antenna connectors count: 2)
Note: max TX power: 20 dBm / min RX: -90 dBm
Transmit power: 20 dBm

Antennas and accessoires: ANT795-4MA (2,4 / 5 GHz, 1x Connector)
Note: 5 dBi
Cable length: 0 meter
Additional attenuation (dBm): 0
Antenna connectors used (MIMO gain): 1 (0 dB)

Installation

You can launch the web tool directly in SIOS through the following page:

https://support.industry.siemens.com/cs/ww/en/view/109809305

Note

The tool provides calculated values. The real setup can deviate from the calculated distances or signal strengths due to environmental conditions.

9.6.2 TIA Selection Tool

General remarks

The selection and ordering tool TIA Selection Tool facilitates the selection of Industrial Ethernet switches and components for Industrial Wireless Communication.

The tool is mainly intended to simplify the ordering process and assist customers in product selection.

Description

The TIA selection tool is the successor of the SIMATIC selection tool. It unites familiar automation technology configurators into one tool and includes significantly more products than its predecessor.

It provides several software wizards to help select the desired devices and networks. There are also configurators for selecting modules and accessories, as well as for checking for correct functionality.

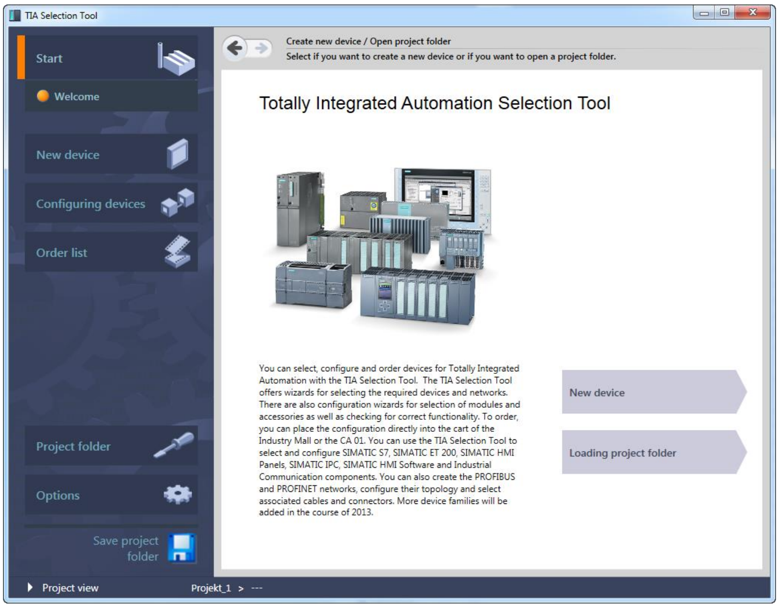
A complete order list can be generated using the product selection or product configuration. You can export it directly into the shopping cart of the Industry Mall or to the CA 01.

User interface

The user interface for the TIA selection tool is similar to the engineering software for TIA portal.

The tool has a java-based, graphical interface. The individual options and products are shown as tabs. It is possible to select the tab directly or to be guided step by step using the tool.

Figure 9-22



Create new device / Open project folder

Select if you want to create a new device or if you want to open a project folder.

Totally Integrated Automation Selection Tool

You can select, configure and order devices for Totally Integrated Automation with the TIA Selection Tool. The TIA Selection Tool offers wizards for selecting the required devices and networks. There are also configuration wizards for selection of modules and accessories as well as checking for correct functionality. To order, you can place the configuration directly into the cart of the Industry Mall or the CA 01. You can use the TIA Selection Tool to select and configure SIMATIC S7, SIMATIC ET 200, SIMATIC HMI Panels, SIMATIC IPC, SIMATIC HMI Software and Industrial Communication components. You can also create the PROFIBUS and PROFINET networks, configure their topology and select associated cables and connectors. More device families will be added in the course of 2013.

Supported components

The following products can be selected and configured with the TIA Selection Tool:

- SIMATIC S7,
- SIMATIC ET 200,
- SIMATIC HMI Panels,
- SIMATIC IPC, SIMATIC
- HMI software
- Industrial communication components

In addition, PROFIBUS and PROFINET networks can be created, their topology can be configured, and associated cables and connectors can be selected.

Installation

The TIA Selection Tool can be started directly in the Siemens Industry Mall or downloaded as a file.

Note Additional information can be found at: https://www.siemens.com/tst

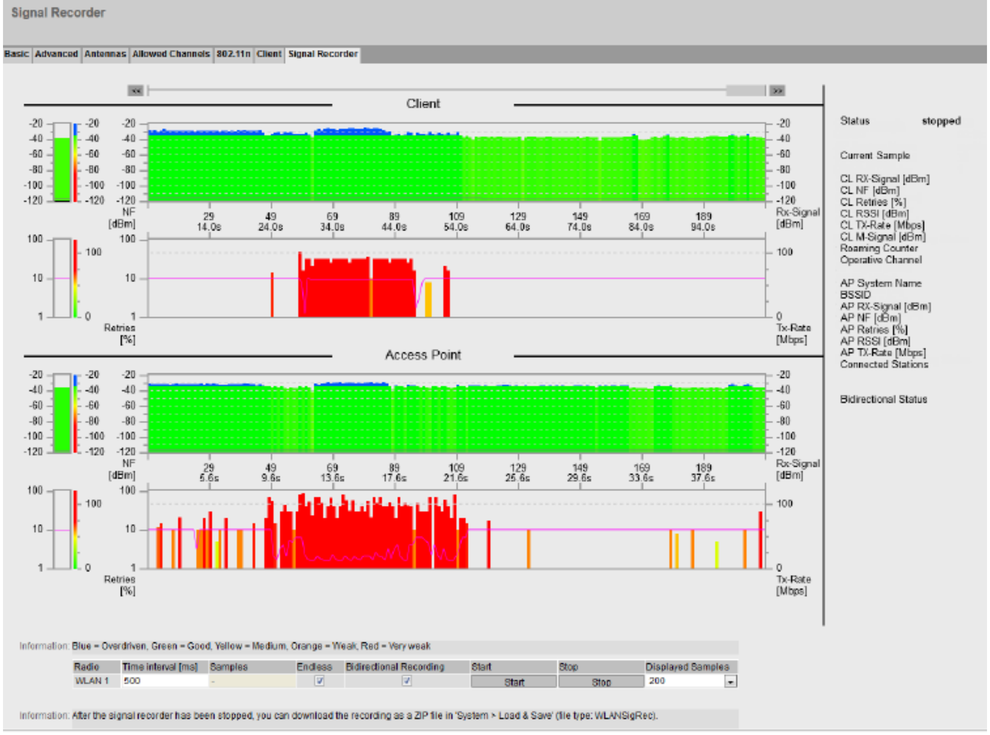
9.6.3 Signal recorder

General remarks

The signal recorder records the effective useful signal between the access point and the client. Using this data, areas with insufficient signal strength can be detected. The signal recorder can be particularly useful in scenarios where clients move along a fixed path.

You can find the signal recorder in the Web Based Management in the menu "Interfaces > WLAN".

Figure 9-23



Status stopped

Current Sample

CL RX-Signal [dBm]
CL NF [dBm]
CL Retries [%]
CL RSSI [dBm]
CL TX-Rate [Mbps]
CL M-Signal [dBm]
Roaming Counter
Operative Channel

AP System Name
BSSID
AP RX-Signal [dBm]
AP NF [dBm]
AP Retries [%]
AP RSSI [dBm]
AP TX-Rate [Mbps]
Connected Stations

Bidirectional Status

Information: Blue = Overdriven, Green = Good, Yellow = Medium, Orange = Weak, Red = Very weak

Radio	Time interval [ms]	Samples	Endless	Bidirectional Recording	Start	Stop	Displayed Samples
WLAN 1	500	-	☑	☑	Start	Stop	200

Information: After the signal recorder has been stopped, you can download the recording as a ZIP file in 'System > Load & Save' (file type: WLANSigRec).

Description

The SCALANCE W components have an integrated signal recorder. The signal recorder records the signal strength of the access point and other connection data on the IWLAN client side. It is a useful tool for obtaining initial reports on connection quality and illumination of a system, as well as for finding possible options for optimization.

Since FW version 6.1, an extended version of the signal recorder has been released, which also records the data of the access point at the same time. This makes it possible to gain even more insight from the signal recorder.

Result of the recording

After the recording of the signal recorder is complete, the edited data can be downloaded as a .zip file.

The .zip file contains the following:

- csv file with the measured values of the signal recorder
- pdf file with the measured values and an additional graphical presentation of the measured values.

Requirements

This signal recorder is only available in client mode.

The WLAN interface of the SCALANCE W700 device must be activated, otherwise no recording can be made.

Note

An FAQ with instructions for operating the signal recorder can be found in the Siemens Online Support https://support.industry.siemens.com/cs/ww/en/view/109470655

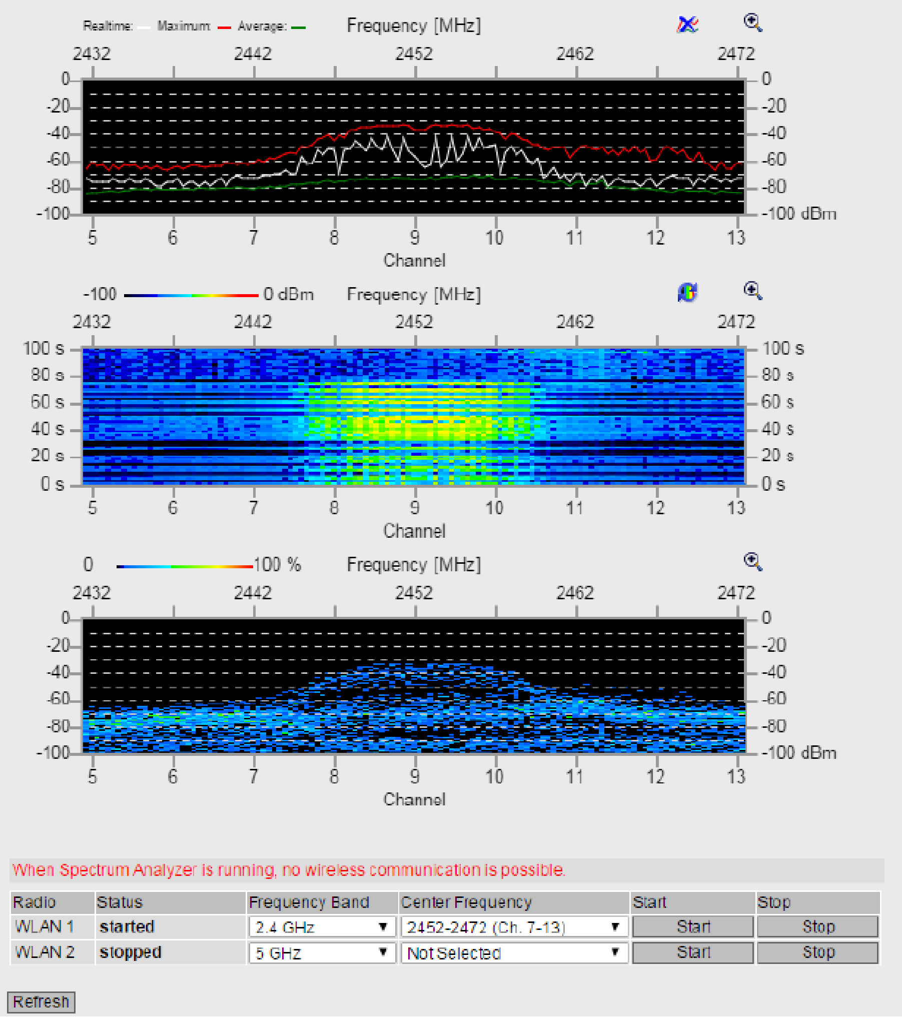
9.6.4 Spectrum analyzer

General remarks

The spectrum analyzer can be used to detect and display the electromagnetic signals of a frequency range. The strength of all the signals that are in the proximity of the access point can be measured.

You can find the spectrum analyzer in the Web Based Management in the menu "Interfaces > WLAN"

Figure 9-24



When Spectrum Analyzer is running, no wireless communication is possible.

Radio	Status	Frequency Band	Center Frequency	Start	Stop
WLAN 1	**started**	2.4 GHz ▼	2452-2472 (Ch. 7-13) ▼	Start	Stop
WLAN 2	**stopped**	5 GHz ▼	Not Selected ▼	Start	Stop

Refresh

Result of the recording

After the recording of the spectrum analyzer is complete, the prepared data can be downloaded as a .zip file.

The zip file contains a csv file with the measured values of the spectrum analyzer.

Requirements

The spectrum analyzer is only available in access point mode.

The device’s WLAN interface of must be activated, otherwise the frequency ranges cannot be scanned.

Note

> Using the spectrum analyzer in "Apply manually" editing mode is not recommended.
>
> When the spectrum analyzer is started, all WLAN connections are disconnected on both WLAN interfaces. The access point will not send any beacons.
>
> Do not activate the spectrum analyzer when the device is in productive operations. The device’s performance can be affected.
>
> The spectrum analyzer does not replace measurements taken using professional spectrum measurement devices.

9.6.5 Remote capture

General remarks

The remote capture feature allows network traffic to be recorded from remote interfaces on the access point using Wireshark.

You can find the function in the Web Based Management in the "Interfaces" menu.

Description

Wireshark records the traffic flowing through the interface over a certain period of time. Afterwards, you can view the contents of the frames or filter for specific content in the recording. Wireshark uses the "Remote Packet Capture Protocol Service" to make these recordings.

In order for Wireshark to be able to record the network data from the remote SCALANCE W, you must first activate the "Remote Capture" function in SCALANCE W via the Command Line Interface or Web-Based Management and then configure a "Remote Capture" interface in Wireshark.

Note

> The configuration manual for the SCALANCE W contains detailed instructions on how to activate the "Remote Capture" function and how to configure the interface in Wireshark (see chapter 12).

Requirements

If you are looking to record and analyze remote network traffic with Wireshark, please note the following:

- If you use the "iPCF" protocol in the WLAN, the "iPCF" frames in Wireshark are marked as defective. "iPCF" is a SIEMENS proprietary protocol.
- Only enable the "Remote Capture" feature for analysis purposes. Increased data traffic can affect the performance of the device and the network.
- Ensure that you are able to reach the SCALANCE W via Port 2002 and that no firewall is preventing access to it. The "Remote Packet Capture Protocol Service" in SCALANCE W is contacted via this port number.

9.6.6 Network management with SINEC NMS

General remarks

The SINEC NMS software program is a network management system for monitoring and managing industrial networks. It enables you to fully visualize and monitor networks. Additionally, SINEC NMS offers the ability to configure the network infrastructure. Using the rule-based approach, cross-device configurations can be made independent of device types on the network, and regular backups of device configurations can be made to keep track of configuration changes. Another important point is the central function for a firmware update in the network infrastructure.

Description

Using SINEC NMS, you can:

- Fully configure SCALANCE W access points and clients,
- check the status of your SCALANCE W access points and clients, and
- manage firmware for all devices in the network.

Note

Refer to Siemens Online Support for a "Getting Started" with instructions on using SINEC NMS:
https://support.industry.siemens.com/cs/ww/en/view/109762792

10 IWLAN in use

The use of wireless data networks can help make the design of processes significantly more efficient. The primary advantage of wireless solutions is simple and flexible accessibility for mobile or difficult to reach nodes.

Using wireless communication for automation devices and industrial terminal devices can help in attaining higher flexibility, simplified maintenance work, reduced service and downtime, and more effective use of staff.

Even challenging applications with real-time and redundancy requirements in industrial applications can be realized with Industrial Wireless LAN (IWLAN).

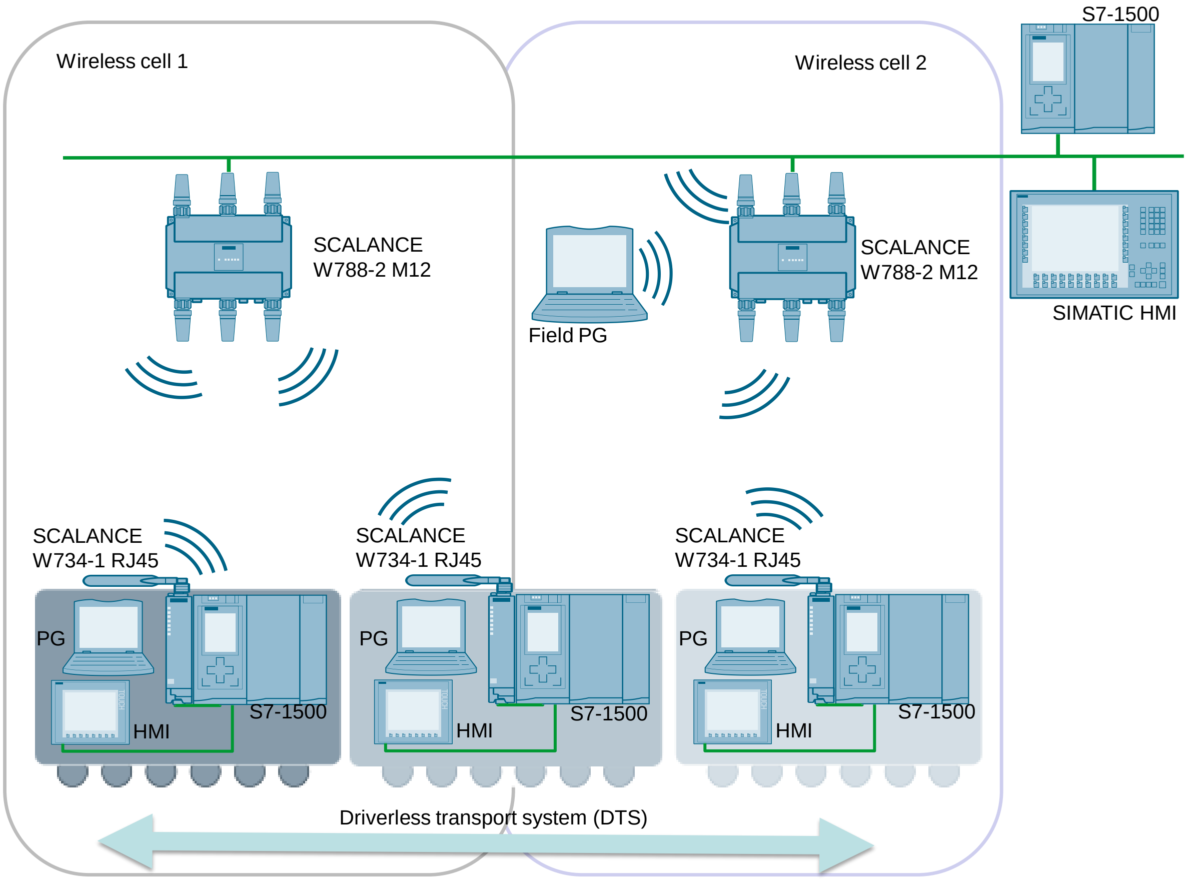
The use of IWLAN is briefly demonstrated below, using selected application locations and examples.

Driverless transport system Mobile device roaming

The figure below shows an example of intralogistics, where individual W788-2 access points span across several adjacent wireless cells. They are interconnected via a cable-based Ethernet string, and facilitate communication between the driverless transport system containing a W734-1 client module and a mobile S7-1500 CPU, and a stationary S7-1500 CPU on one hand, and an HMI panel on the other.

This configuration makes it possible for the automated guided vehicle system to change from one wireless cell to another ("roaming") without losing contact.

Figure 10-1

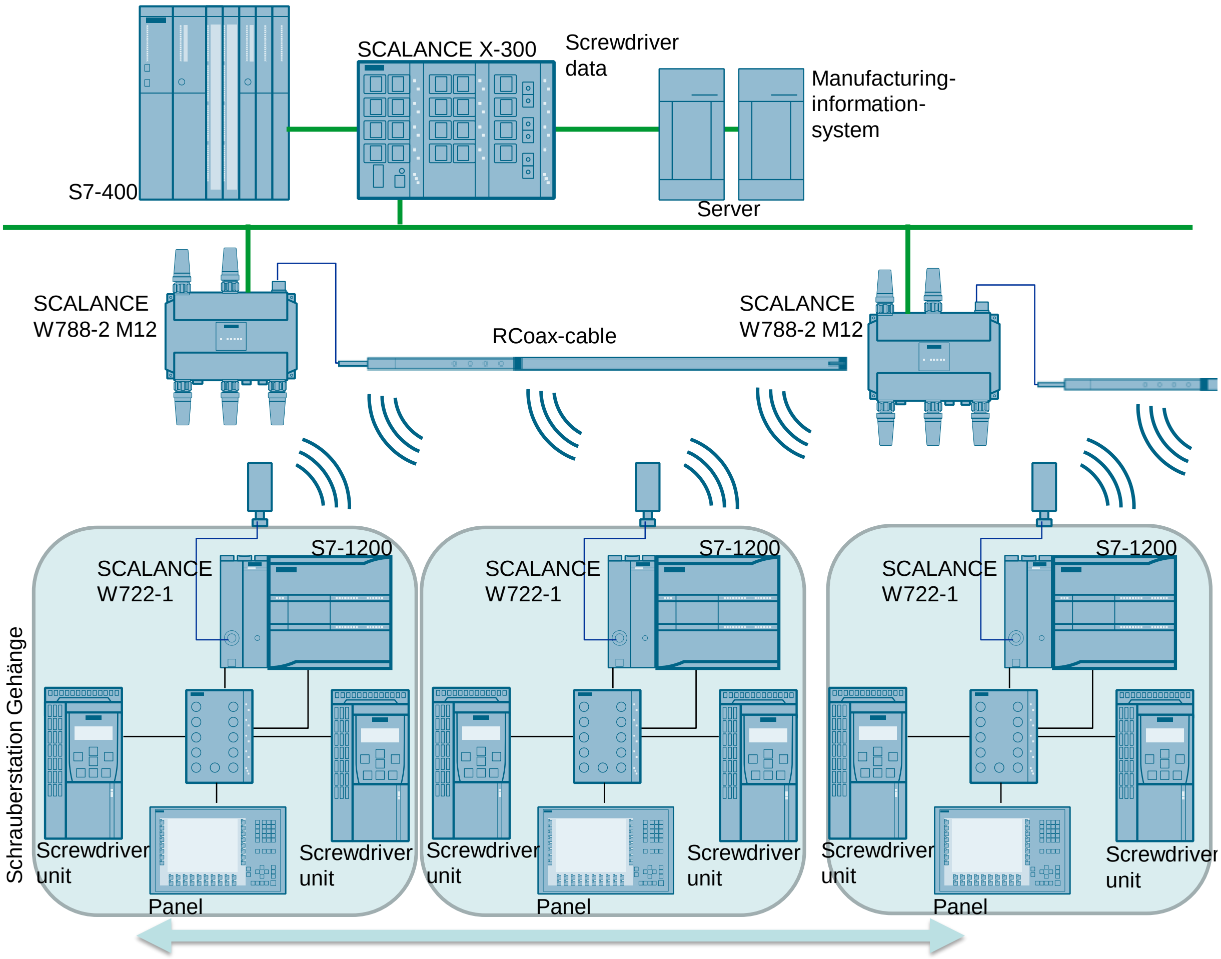


Overhead conveyor system: Using RCoax

In the example below taken from the automotive industry, an IWLAN RCoax radiating cable is used to set up a wireless data transmission along the coding rail. It creates a defined and reliable radio field. The W788-2 access points are used as a supplying station for the RCoax cable.

The mobile screwdriver stations – each equipped with a W722-1 client module, a SIMATIC S7-1200, two screwdriver units and a Panel – move along the path of the overhead conveyor system and are able to communicate with the cable-based network via their client module and the access point.

Figure 10-2



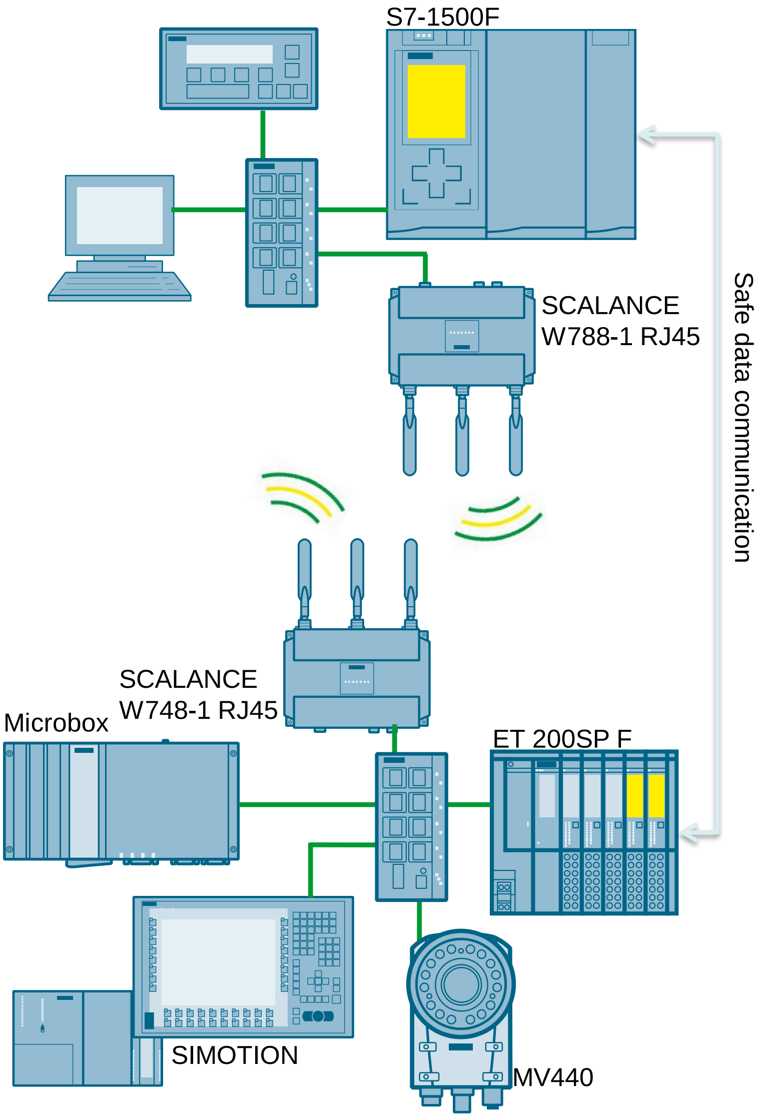
Safety over wireless: PROFIsafe with SCALANCE W

PROFIsafe is a protocol extension of PROFIBUS / PROFINET for safety-related communication.

The following example demonstrates the safety-related operation of a robot.

Since PROFIsafe is a protocol extension, mixed traffic for both "secure" and standard messages can take place on the same network.

Figure 10-3



Note

An application example including safety topics can be found in the Siemens Industry Online Support at

https://support.industry.siemens.com/cs/document/25702331

11 Glossary

802.11

A series of standards for wireless network protocols developed by → IEEE.

Access point

"AP", a node from a → WLAN that simultaneously performs administrative functions in the network and, for example, provides → clients with a connection to wired networks or other clients in the same wireless cell or in other wireless cells. See chapter 4.1.2

***Ad hoc* network**

An unstructured → WLAN without → access points. The → clients communicate "at their own risk" without higher-level coordination. The opposite of this is a network in → infrastructure mode.

AES

"Advanced Encryption Standard", an encryption method, see chapter 5.2.2.

Antenna pattern

A graphic display of the antenna's radiation pattern, used to evaluate its performance. The values for the antenna pattern are measured and recorded or generated via simulation programs.

Antenna diversity

The simultaneous availability of two radio interfaces on one device. In areas that pose difficulties for wireless communication, it is possible to switch over to the interface with the frequency currently providing the best reception.

Antenna gain

The use of appropriate design to concentrate the radio field of an antenna in a limited spatial direction. This achieves a (passive!) amplification in this direction in space in comparison to an isotropic radiator. In turn, other spatial directions are weakened. The form of the radio field is specified in more detail in the → antenna pattern.

Bandwidth

Practically synonymous with "maximum usable data rate". The term is derived from the fact that by transmitting at a certain data rate, a segment of the wireless spectrum of proportional width will be occupied. See also chapter 1.4.4.

Bluetooth

A short-range wireless standard for communication between office devices and mobile phones, see chapter 3.

CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, an encryption algorithm used in → WPA2 contexts, see chapter 5.2.2.

Client

Here: a node in a → WLAN that has no internal infrastructure capabilities but that accesses a wireless network via an → access point.

CSMA/CA

"Carrier Sense Multiple Access with Collision Avoidance", a method for detecting "collisions", or simultaneous attempts by more than one sender to start transmission on a frequency. When this happens, both senders stop their transmissions and wait for a more or less random period of time. They only start to repeat their transmission if the other sender has not started its transmit during this period. It is only possible for a second collision to occur if both randomly selected delays are identical.

DCF

"Distributed Coordination Function", an organizational model for wireless networks (see chapter 4.4.1).

DFS

Dynamic Frequency Selection is an extension of the → 802.11h standard. If another (non-network) user is detected on a channel during operations, the → access point changes the channel being used. This avoids influence from other systems using the 5 GHz band (radar, satellite radio and satellite navigation).

DoS

"Denial of Service", a method of attack against a network.

DSSS

"Direct Sequence Spread Spectrum", a spread spectrum transmission method in IEEE 802.11b.

EAP

"Extensible Authentication Protocol", a method in the context of the → RADIUS protocol, that is used to help the server and client agree on a *procedure* for the authentication before the actual authentication.

GFSK

"Gaussian Phase Shift Keying", a modulation method with IEEE 802.11.

GPRS

"General Packet Radio Service", a data transmission service used for mobile phone communication.

Handover

The transfer of a mobile client from one access point and its wireless cell to the next (→ roaming); in particular, the reintegration in the network.

Hidden node problem

same as → Hidden station problem

Hidden station problem

A connection issue that occurs if one receiver is addressed simultaneously by two senders that are not able to hear each other, resulting in a collision at the receiver.

HMI

"Human Machine Interface", display and operator devices for plant control, such as SIMATIC mobile Panels

IEEE

"Institute of Electrics and Electronics Engineers", a US institute that develops guidelines and technical recommendations; to some extent comparable with DIN.

.

Infrastructure mode

A wireless network organized in such a way that one or more → access points form cells, giving the network a "structure". The opposite is an → *ad hoc* network.

IP 30

A degree of protection that indicates that a component in this category is protected from the intrusion of coarse solid foreign bodies (from 2.5 mm in diameter), but is not protected from the ingress of water. This corresponds to a normal electrical household appliance.

IP 65

A degree of protection that indicates that the component in this category is fully protected from dust and water jets. This corresponds to a virtually airtight encapsulation.

iPCF

"Industrial Point Coordination Function", a proprietary network protocol supported by SIEMENS that enables short → handover times (in the range of 30 ms) while → the mobile nodes are roaming. iPCF is not compatible with → iQoS.

iQoS

"Industrial Quality of Service", a process that reserves certain → bandwidths for individual → clients. The result is a highly probable, but not certain response time. This means that iQoS meets less strict real-time requirements than → iPCF. It is not compatible with → iPCF.

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.

LAN

"Local Area Network", a locally defined network, in contrast to the internet, for example.

Radiating cables

A coaxial cable whose outer sheath is interrupted at defined points. This results in the cable generating a spatially limited radio field that can be "shaped" to follows the bends in the cable.

Link check

An access point function to monitor the connection to the clients. Various events (client login, logout, etc.) can trigger automated responses from the AP (sending mails / traps, turning on the *fault* LED, etc.). All SCALANCE W access points support link check.

MAC

"Media Access Control", a protocol for controlling access to a transmission medium (cable, wireless) that cannot be accessed by all nodes at the same time.

MAC address

A worldwide unique identification number for every hardware component of importance in a network. → MAC

Middleware

Software that performs a intermediary function between operating systems and drivers on the one hand, and user applications on the other.

MIMO

"Multiple Inputs, Multiple Outputs", a method in which each wireless participant simultaneously transmits or receives using multiple antennas. MIMO is part of the → IEEE → 802.11n standard.

MPI

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

N-connect

A connector system for IWLAN antennas.

OFDM

"Orthogonal Frequency Division Multiplex", a modulation method with IEEE 802.11a and g.

PCF

"Point Coordination Function", an organizational model for wireless networks.

PoE

"Power over Ethernet", power supply of bus devices via an Industrial Ethernet cable.

Polling

Regular queries for status data or variables from a data source ("server") by a client. (This client is not necessarily the client of a WLAN.) The alternative to this is event controlled transmission. In this case, the server independently transmits data to the client as soon as any changes in the data appear.

PROFIBUS

A field bus system for serial data transmission in automation technology based on → MPI hardware specifications.

PROFINET

An extension of the Ethernet communication standards created to meet "Industrial Ethernet" requirements, i.e. for use in an industrial environment. New properties include measures to increase transmission security and fault tolerance and the use of durable components, etc. The SCALANCE product generation is designed for use with PROFINET.

PROFIsafe

A protocol extension for → PROFIBUS and → PROFINET, whose use increases transmission security considerably.

PSK

"Pre-Shared Key", an authentication procedure in the context of subrack systems of the → WPA/WPA2 protocols.

Quality of Service

Guaranteed transmission quality in the context of a network.

RADIUS

"Remote Authentification Dial In User Service", an access control procedure in which authentication between the client and access point is handled by a third, separate server that stores the access data.

Rapid Spanning Tree

A method for optimizing data paths in networks, similar to → Spanning Tree. Rapid Spanning Tree, however, was designed to keep reconfiguration time as short as possible in the event of an access point failure.

RC4

An encryption algorithm used within the context of the → WEP and → WPA standards.

RCoax

A → radiating cable used for setting up real-time-capable wireless networks with a limited range, particularly suitable for → clients with fixed motion paths (e.g. driverless systems) or in heavily shielded environments (e.g. tunnels).

RFID

"Radio Frequency IDentification", a method where objects (e.g. books in a library) are fitted with passive radio transponders. The transponder responds to a transmitter request (e.g. reader at the check-out section of the library) with an ID to track them. The transponders are small, cheap and fed by the energy of the reader. The range and data capacity, however, are low.

Roaming

The movement of a → WLAN node from one wireless cell to the next.

R/SMA

"Reverse (Polarity) SubMiniature (version) A (Connector)", a connection system for WLAN antennas.

RSTP

"Rapid Spannung Tree Protocol", an algorithm used by switches in a network to both automatically determine the best paths for data transmission between two end nodes, and to determine alternatives in the event of a failed transmission point. See chapter 4.5.3.

RTS / CTS

"Read-to-Send / Clear-to-Send", a method for avoiding network collisions and for avoiding the → Hidden station problem.

Spanning tree

A technique used to optimize data paths in (wireless) networks. The spanning tree method determines physically redundant network structures and prevents the generation of loops by disabling redundant paths. 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 among the remaining network nodes. See also → Rapid Spanning Tree

Spoofing

Same as "Parody, swindle", a general term for attacks on networks where the attacker disguises its own IP or MAC address ("IP spoofing", "MAC spoofing"), in order to fake the "identity" of a (authorized) network node.

SSID

"Service Set Identifier", within the context of a → "Wi-Fi" WLAN, the name of a network that needs to be known to all network nodes at the same time and that constitutes part of each transferred message. SSIDs alone provide only extremely weak access protection against third parties and should always be supplemented by other encryption methods.

SSL

"Secure Sockets Layer", a protocol for encrypted data transfer in the Internet that obtains its security by using "public key" algorithms.

TKIP

"Temporary Key Integrity Protocol", a protocol for dynamically changing the key in a → WLAN.

TPC

"Transmit Power Control", an expansion of the → 802.11h standard, in which only the transmission power that is required for interference-free reception of known clients is emitted. This prevents overshoot generation.

UMTS

"Universal Mobile Telecommunications System", a high-capacity wireless mobile standard for data transmission.

VLAN

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

VNS

"Virtual Network Services", the organization of logical networks within one or more physical networks.

VoIP

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

VPN

"Virtual Private Network", a protocol expansion that is closely related to → VLANs, where the data traffic of a (virtual) subnet is "tunneled" through a larger network, e.g. concealed from the other nodes. This property means that VPNs are suitable for increasing a network’s security.

WAN

"Wide Area Network", a limited extensive network, but larger than a → LAN.

WBM

"Web Based Management", configuration of an access point or client via a web interface.

WDS

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

WEP

"Wire Equivalent Protocol", an encryption method in wireless data communication.

Wi-Fi

A designation introduced by the "WiFi Alliance" group of manufacturers for → WLAN products that are compatible with a specific subset of the → 802.11 standard. It is occasionally (and incorrectly) used as a synonym for WLAN in general.

Wireless HART

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

WLAN

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

WMM

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

WPA, WPA2

"Wi-Fi Protected Access", two encryption methods used in wireless data communication.

Zigbee

A wireless standard similar to → WirelessHART, however, it is used for domestic operations or for building automation.

Acknowledgment button

When working in hazardous environments, personnel can use hand-held acknowledgment buttons with three button positions. It is only possible to operate the device controlled by the acknowledgment buttons in the middle position using a moderately firm grip. If the acknowledgment button is released completely or held very firmly ("panic circuit"), the emergency stop of the device is triggered.

12 Appendix

12.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:

siemens.com/SupportRequest

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

12.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

12.3 Links and literature

Table 12-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/22681042
\3\	Segmenting a Network Using VLANs https://support.industry.siemens.com/cs/document/109749844
\4\	Setting up a meshed network based on "RSTP" https://support.industry.siemens.com/cs/document/109742120
\5\	Configuration of a Ring Topology Based on "MRP" https://support.industry.siemens.com/cs/document/109739614
\6\	With PROFINET IO via WLAN how do you set the update time and F-monitoring time in the TIA Portal? https://support.industry.siemens.com/cs/document/109475919
\7\	With PROFINET IO via WLAN how do you set the update time and F-monitoring time in STEP 7 V5.x? https://support.industry.siemens.com/cs/document/109474533
\8\	How do you link a PNIO device to a PNIO controller via WLAN and iPCF? https://support.industry.siemens.com/cs/document/92649989
\9\	Application Example: Setup of redundant, wireless networks with iPRP https://support.industry.siemens.com/cs/ww/en/view/109751341
\10\	Wi-Fi 6E information https://www.litepoint.com/wi-fi-6e/
\11\	Industrial WLAN – An Overview of the Most Important Documents and Links https://support.industry.siemens.com/cs/ww/en/view/109784526

12.4 Change documentation

Table 12-2

Version	Date	Change
V1.0	2006-04-01	First edition
V2.0	2010-01-01	Various updates
V2.1	2011-08-02	Various updates
V3.0	04/2013	Complete revision of the structure and extension with new features / devices for IEEE 802.11n
V4.0	01/2016	Inclusion of the latest devices / antennas. Removal of old devices according to IEEE 802.11a/b/g standard; Image update
V5.0	04/2018	Added latest iFeatures/devices/antennas; updates images and links.
V5.1	03/2020	Edited text in chapter 4.6.1
V6.0	03/2021	Added brief text passages / added SINEC NMS
V6.1	03/2023	Additions for new products (IEEE 802.11 ax). General overhaul of all chapters.